User Manual

IronKey 1000E

Find the language and latest documentation here.

 ..... For instructions in English

 ..... Para instrucciones en Español

 ..... Für Anleitungen in Deutsch

 ..... Pour des instructions en Français

 ..... Per le istruzioni in Italiano

 ..... Por as instruções em Português

 ..... Instrukcje w jezyku Polskim

 .....日本語マニュアル用

Simplified Chinese .....简体中文说明书

Traditional Chinese ....繁體中文說明

IRONKEY™S1000E
ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

About This Guide (04152025)

IronKey™ S1000E is a Managed drive that requires a device license and can be managed by SafeConsole. SafeConsole is a secure cloud or on-premises management platforms that allow your organization to centrally manage compatible USB (Universal Serial Bus) storage devices easily and efficiently.

This guide will explain how to setup and initialize a S1000E drive on a SafeConsole to be a 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 > IronKey Unlocker > 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 S1000E 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 S1000E 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.*
NOTE: *Admins can reset password using SafeConsole.*

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
Interface/Connector Type/Speed**	USB 3.2 Gen 1 / Type-A - 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.; MILSTD-810F

Temperature	Operating: 0°C to 50°C; Storage: -20°C to 85°C
Hardware Encryption	256-bit AES (XTS Mode)
Key Certifications	FIPS 140-2 Level 3 TAA/CMMC Compliant, Assembled on USA
OS Compatibility	- Windows 11, Windows 10 (Requires Two Free Drive Letters) - macOS 12.x – 15.x - Linux 4.4.x***
Warranty	5 Years Limited

Designed and assembled in the U.S.A., S1000E 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. No online management features.

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 S1000E 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 S1000E 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 S1000E 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.

Setting Up a S1000E Device with SafeConsole

The initialization process will begin by allowing the device to be ready to communicate with the SafeConsole server. The steps needed to register a S1000E to SafeConsole will depend on the policies that your administrator is enforcing. Not all dialogs will be shown.

A SafeConsole Connection Token will be needed. The SafeConsole Connection Token is obtained by the System Administrator through the Quick Connect Guide, located inside of the SafeConsole user interface.

1. Enter the SafeConsole Connection Token that is obtained in the steps above. Review the license agreement, check the checkbox to accept it, and click **Activate** in the bottom left-hand corner.

   • **Optionally Enabled Policies** - These policies may or may not be enabled by your System Administrator. They will appear during device registration if they have been enabled.

   - Confirm Ownership of the device: Enter the Windows username and password that is associated with the login credentials of the computer the device is plugged into.

   - Custom Device Information: Required information about you or your device. The required fields will vary.

   - Unique User Token: This token is directly associated with the end user's account and will be provided by the System Administrator.

   - Administrator Registration Approval: The System Administrator may require their approval to proceed with device registration.

2. Enter a secure Password and Confirm it. Once the password created meets the requirements listed to the right side of the input fields, click Continue. The requirements of this password will depend on the policy selected by your administrator. Passwords are case-sensitive and must have at least 8 characters along with more requirements if Strong Password is enabled.

3. Choose a Secure Volume File System (see Formatting My Device) and click Continue.

4. The device will now finalize the setup process and be ready for use. Access the Encrypted Storage by clicking the **Folder Icon** in the top menu. The settings of the device can be accessed and altered by clicking the **Gear Icon**. See the IronKey Control Panel for more information.

Strong Password

While creating or changing the password for the device there is an option to enable Enforce Strong Password. For Managed devices this option may be configured or enforced by your System Administrator. When enabled the following rules are checked against all potential passwords.

- Must be at least eight (8) characters in length.

- Must include characters from at least three (3) of the following character classes:

  - ASCII digits (0123456789) Note: If the last character of the password is an ASCII digit, then it does not count as an ASCII digit for this restriction.

  - lowercase ASCII (abc…xyz)

  - uppercase ASCII (ABC…XYZ) Note: If the first character of the password is an uppercase ASCII letter, then it is not counted as an uppercase ASCII letter for this restriction.

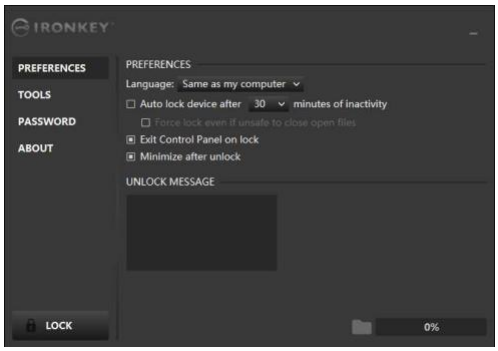
  - non-alphanumeric ASCII (!@#$, etc)

  - non-ASCII characters

Strong Password Examples

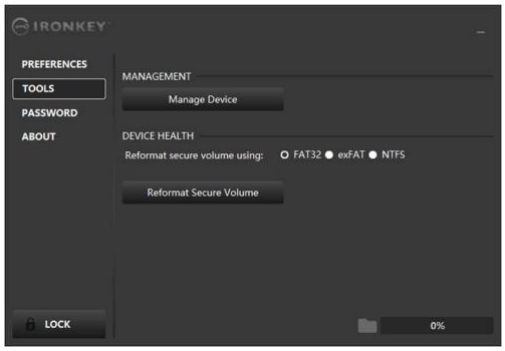
Example Passwords	Results
password	Failed: 8 characters long, however, only contains 1 unique character class (lowercase ASCII).
Password1	Failed: 9 characters long, however the Capital 'P' and '1' do not count toward the unique character classes, leaving only lowercase ASCII.
pa$$Word	Pass: 8 characters long. Contains lowercase ASCII, uppercase ASCII, and non-alphanumeric ASCII.

IronKey Control Panel



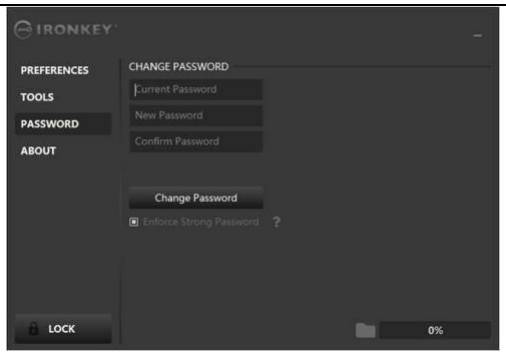
PREFERENCES

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. UPDATE: Check for Updates
2. DEVICE HEALTH: Reformat secure volume using FAT32 or exFAT. (macOS only allows formatting FAT32)



PASSWORD

1. CHANGE PASSWORD: Change drive log-in password.
2. Enforce Strong Password: Enable/Disable Strong password requirement

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 **Files** on menu bar of the IronKey Control Panel.
   - Windows: Opens Windows Explorer to the IRONKEY SECUREFILESUSB drive.
   - macOS: Opens Finder to the KINGSTONUSB drive.
2. Do one of the following:
   - To open a file, double-click the file on the S1000EUSB drive.
   - To save a file, drag the file from your computer to the S1000EUSB 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. Managed devices can be forced to unlock in a read-only state by an administrator.

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. For Managed devices, this feature may or may not be enabled by your System Administrator.

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 7 lines and 200 characters).

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. For Managed devices, this feature may or may not be enabled by your System Administrator.

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**.

Note: Managed devices will automatically lock during use if an administrator remotely disables the device. You will not be able to unlock the device until the System Administrator re-enables the 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.

Password policy settings are determined by your System Administrator. 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. Passwords are case-sensitive and must have at least 8 characters along with more requirements if Strong Password is enabled.
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 or exFAT.

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 erase all

your files 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.

Your System Administrator may have this option disabled. Contact your administrator if you need to reset your device.

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.

Note: If the device was originally standard and connected to a management server, the management requirements will still be enforced even after a reset.

Accessing My Device If I Forget My Password

If you forget your password and an administrator has granted you password reset privileges, you can reset it. If your administrator has not granted password reset privileges, you must contact your administrator for help resetting your password.

To reset your password:

1. Plug in your device and start the IronKey.
2. Click Password Help.
3. You may receive an email with instructions on how to obtain your recovery code. Otherwise, you will need to contact your administrator to obtain this code. In the latter case, you may be required to provide the request code and serial number to your System Administrator. Your System Administrator's email and phone number should be provided for your convenience. Clicking the email address will open your default email client and pre-populate this information to be sent.
4. Once received the recovery code will need to be copied and pasted exactly as it is given to you. Incorrect codes count against the ten unlock attempts before the device is reset.
5. Type your new password and confirm it in the fields provided, then click **Change Password**. Note: Passwords are case-sensitive and must have at least 8 characters along with more requirements id Strong Password is enabled.

Restricted Files Notifications

If enabled by your SafeConsole administrator, your device may restrict certain files from being saved to the secure storage. When an affected files is restricted, you receive a notification containing the file's name. If desired, you can disable these notifications.

NOTE: Affected files will still be restricted when notifications are disabled.

To disable restricted files notifications:

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 Show restricted files notifications.

Scanning My Device for Malware

If enabled by your System Administrator, the Malware Scanner is a self-cleaning technology that detects and removes malware on your device from an infected file or computer. Powered by the McAfee® AntiVirus and Anti-Malware signature database, and\ constantly updated to combat the latest malware threats, the scanner first checks for the latest updates, scans your device, then reports and cleans any malware that is found.

Your system administrator may require the anti-malware definition to be updated before the device can be unlocked. In this event, the full anti-malware definition will need to be downloaded to a temporary folder on the local computer before the password can be entered. This can increase the time it takes to unlock the device based on the host computer's networking connection and the size of malware updates needed.

Some things to know about scanning your device:

- The scanner runs automatically when you unlock your device.
- It scans all onboard files (compressed and uncompressed).
- It will report and delete any detected malware.
- (Optional) If your SafeConsole administrator has enabled Quarantine, it may quarantine any malware it finds. See Restoring or Deleting a Quarantine File for more information.
- The scanner will automatically update itself before each scan to protect you from the latest malware threats.
- An update requires an internet connection. Ensure a minimum of 135 MB of free space on the device to accommodate the downloaded malware signature files.
- Your first update may take a long time to download, depending on your internet connection.
- The date of the last update is displayed onscreen.
- If the scanner becomes too far out of date, it will need to download a large file to bring it back up to date.

Restoring or Deleting a Quarantined File

If your SafeConsole administrator has enabled Quarantine, you will have the option of restoring or deleting detected malware. This process helps when McAfee detects a valid document as malware.

NOTE: Depending on the size of the infected files, Quarantine may not be available. If the file cannot be quarantined, it will be deleted. Deleted files cannot be restored using the following process.

To view quarantined files:

1. Unlock your device and click Settings in the IronKey Control Panel.
2. Click Quarantine on the left sidebar.

Select a file from the list will display additional details including, Threat Name, Threat Type, anti-malware definition version, and the date of quarantine. After the file is selected files can either be Restored or Deleted.

Restored files will be exempt from automatic scanning while the device is currently unlocked. The file will be scanned during the next unlock or if a manual scan is selected from the Anti-Malware tab. If the anti-malware definitions still determine that the file is infected, it will quarantine the file once again.

Deleted files will be permanently deleted.

Sanitize

Sanitize allows for the content of the encrypted drive to be securely erased. This is accomplished by erasing the encrypted key that the drive uses to access files on the Secure Volume while still retaining the connection to SafeConsole.

Warning: Performing this action will completely erase all data on the Secure Volume. This action is permanent.

The ability to sanitize a drive depends on the setting configured by your SafeConsole administrator. If allowed your drive can be sanitized by the following steps:

1. Unlock your device and open the device Control Panel by launching IronKey.exe.
2. Right-click the system tray icon for the Control Panel and select Sanitize Device.
3. Enter the numbers prompted in the dialog box to confirm that all data can be wiped from the drive.
4. The device will reset. Unplug and plug your device back into your workstation.
5. Launch IronKey.exe and input the device password.

Using ZoneBuilder in SafeConsole

If enabled by your System Administrator, ZoneBuilder is a SafeConsole tool used to create a Trusted Zone of computers. It can be used to restrict device access to computers within the Trusted Zone and, if enabled, can automatically unlock your device, which eliminates the need to enter your password.

If your administrator chooses to enable this policy, you may be required to trust the account. Trusting the account:

1. Unlock your device and click **Settings** in the IronKey Control Panel.
2. Click **ZoneBuilder** on the left sidebar.
3. Click Trust This Account.
4. Enter the password for the device and click OK. Your account will now show up in the Trusted Accounts box.

Your account is now in the Trusted Zone of computers. Depending on the policy set by your System Administrator, you may have restricted device access outside of the Trusted Zone or when offline. Your device may also be set to automatically unlock on trusted computers.

To remove a trusted account, simply highlight the account you wish to remove and click Remove.

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. Some Managed device policies, set by the System Administrator, may restrict usage of the device to systems only running Windows or macOS operating systems.

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.
6. Policies that will block the device.
   - If the device is disabled within the policy settings in SafeConsole you will not be able to unlock the device.

Where Can I Get Help?

The following resources provide more information about IronKey products. Please contact your Help Desk or System Administrator if 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.

IRONKEY™ S1000E
UNIDAD ENCRIPTADA FLASH USB 3.2 Gen 1

Guía del usuario

Contenidos

Acerca de esta guía (04152025)

IronKey™ S1000E es una unidad administrada que requiere una licencia de dispositivo y puede ser administrada por SafeConsole. SafeConsole es una plataforma de gestión segura en la nube o local que permite a su organización gestionar de forma centralizada dispositivos de almacenamiento USB (Universal Serial Bus) compatibles de forma fácil y eficiente.

Esta guía explicará cómo configurar e inicializar un dispositivo S1000E en un SafeConsole para que sea un disco administrado.

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 IRONKEY SECURE FILES 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 S1000E 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 S1000E 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.
NOTA: Los administradores pueden restablecer la contraseña usando SafeConsole.

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
Interfaz/Tipo de conector/Velocidad**	USB 3.2 Gen 1 / Type-A - 4GB a 32GB: 180MB/seg de lectura; 80MB/seg de escritura. - 64GB: 230MB/seg de lectura; 160MB/seg de escritura. - 128GB: 230MB/seg de lectura; 240MB/seg de escritura. USB 2.0: - 4GB a128GB: 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); MILSTD-810F

Temperatura	Funcionamiento: 0°C hasta 50°C; Almacenamiento: -20° a 85°C
Encriptado por Hardware	AES de 256 bits (Modo XTS)
Certificaciones clave	FIPS 140-2 Nivel 3 Conformidad con TAA/CMMC, ensamblado en EE.UU.
Compatibilidad con SO	- Windows 11, Windows 10 (requiere dos letras de unidad libres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantía	Garantía de 5 años limitada

Diseñados y ensamblados en los EE. UU., los dispositivos S1000E 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. No hay funciones de gestión en línea.

Mejores prácticas recomendadas

1. Bloquee el 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 S1000E 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 S1000E 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 S1000E 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.

Configurar un dispositivo S1000E con SafeConsole

El proceso de inicialización comenzará permitiendo que el dispositivo esté listo para comunicarse con el servidor SafeConsole. Los pasos necesarios para registrar un S1000E en SafeConsole dependerán de las políticas que su administrador esté aplicando. No se mostrarán todos los cuadros de diálogo.

Se necesitará un token de conexión SafeConsole. El Token de Conexión SafeConsole es obtenido por el Administrador del sistema a través de la Guía de conexión rápida, ubicada dentro de la interfaz de usuario de SafeConsole.

1. Ingrese el token de conexión SafeConsole que se obtiene en los pasos anteriores. Revise el acuerdo de licencia, marque la casilla de verificación para aceptarlo y haga clic en **Activar** en la esquina inferior izquierda.

   - **Políticas opcionales:** estas políticas pueden o no ser habilitadas por su Administrador de Sistema. Aparecerán durante el registro del dispositivo si se han habilitado.

     - Confirmar la propiedad del dispositivo: Ingrese el nombre de usuario y la contraseña de Windows asociados a las credenciales de inicio de sesión del equipo al que está conectado el dispositivo.

     - Información personalizada del dispositivo: Información requerida sobre usted o su dispositivo. Los campos obligatorios variarán.

     - Token de usuario único: Este token está directamente asociado con la cuenta del usuario final y será proporcionado por el Administrador del sistema.

     - Aprobación de registro de Administrador: El administrador del sistema puede requerir su aprobación para proceder con el registro del dispositivo.

2. Introduzca una contraseña segura y confírmela. Una vez que la contraseña creada cumpla con los requisitos enumerados en el lado derecho de los campos de entrada, haga clic en Continuar. Los requisitos de esta contraseña dependerán de la política seleccionada por su administrador. Las contraseñas distinguen entre mayúsculas y minúsculas y deben tener al menos 8 caracteres junto con más requisitos si la contraseña segura está habilitada.

3. Elija un sistema de archivos de volumen seguro (consulte Formatear mi dispositivo) y haga clic en **Continuar**.

4. El dispositivo finalizará ahora el proceso de configuración y estará listo para su uso. Acceda al almacenamiento encriptado haciendo clic en el icono de carpeta en el menú superior. Se puede acceder a la configuración del dispositivo y modificarla haciendo clic en el icono de engranaje. Consulte el Panel de control de IronKey para obtener más información.

Contraseña segura

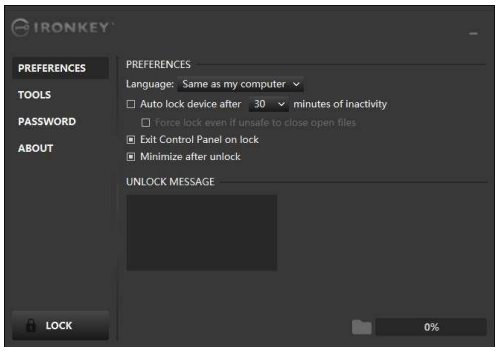
Al crear o cambiar la contraseña para el dispositivo, hay una opción para habilitar Forzar contraseña segura. Para dispositivos administrados, esta opción puede ser configurada o impuesta por su Administrador de Sistema. Cuando se activa, las siguientes reglas se controlan con todas las contraseñas potenciales.

- Debe tener al menos ocho (8) caracteres de longitud.
- Debe incluir caracteres de al menos tres (3) de las siguientes clases de caracteres:
  - Dígitos ASCII (0123456789) Nota: Si el último carácter de la contraseña es un dígito ASCII, entonces no cuenta como un dígito ASCII para esta restricción.
  - ASCII en minúsculas (abc…xyz)
  - ASCII en mayúsculas (ABC…XYZ) Nota: Si el primer carácter de la contraseña es una letra ASCII mayúscula, entonces no se cuenta como una letra ASCII mayúscula para esta restricción.
  - ASCII no alfanumérico (!@#$, etc)
  - caracteres no ASCII

Ejemplos de contraseñas seguras

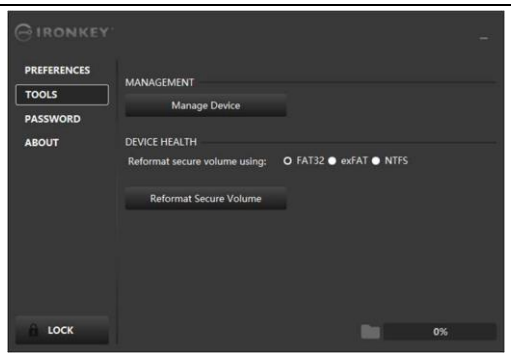
Ejemplos de contraseñas seguras	Resultados
Contraseña	fallida: 8 caracteres de longitud, sin embargo, sólo contiene 1 única clase de caracteres (ASCII minúsculas).
Contraseña1	fallida: 9 caracteres, sin embargo, las mayúsculas ‘P’ y ‘1’ no cuentan para las clases de caracteres únicas, dejando solo ASCII minúsculas.
pa$$Word	Aprobada: 8 caracteres de longitud. Contiene ASCII en minúsculas, ASCII en mayúsculas y ASCII no alfanumérico.

Panel de control IronKey



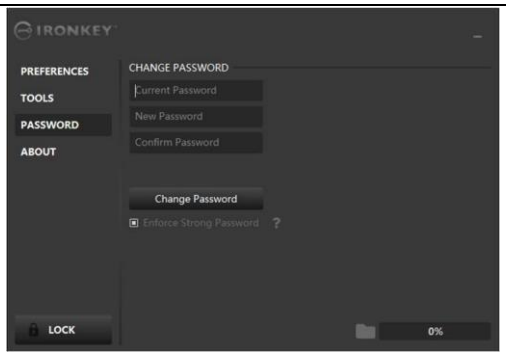
PREFERENCIAS

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 permitir que se mantenga maximizado.
5. MENSAJE DE DESBLOQUEO Agregue un mensaje que se mostrará en la ventana de inicio de sesión.



HERRAMIENTAS

1. ACTUALIZAR: Buscar actualizaciones
2. ESTADO DEL DISPOSITIVO: Vuelva a formatear el volumen seguro utilizando FAT32 o exFAT. (macOS solo permite formatear FAT32)



CONTRASEÑA

1. CAMBIAR CONTRASEÑA: Cambie la contraseña de inicio de sesión de la unidad.
2. Imponga una contraseña segura: Habilitar/deshabilitar el requisito de contraseña segura

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 **Archivos** en la barra de menú 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 S1000E.
   - Para guardar un archivo, arrástrelo desde su computadora a la unidad USB S1000E.

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. Los dispositivos administrados pueden ser forzados a desbloquearse en un estado de solo lectura por un administrador.

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. En el caso de los dispositivos administrados, esta función puede estar activada o no por el administrador del sistema.

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 7 líneas y 200 caracteres).

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. En el caso de los dispositivos administrados, esta función puede estar activada o no por el administrador del sistema.

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**.

Nota: Los dispositivos administrados se bloquearán automáticamente durante el uso si un administrador deshabilita el dispositivo de forma remota. No podrá desbloquear el dispositivo hasta que el Administrador del sistema lo vuelva a habilitar.

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.

La configuración de la política de contraseñas la determina su Administrador de Sistema. 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. Las contraseñas distinguen entre mayúsculas y minúsculas y deben tener al menos 8 caracteres junto con más requisitos si la contraseña segura está habilitada.
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 o exFAT.

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 borrará todos sus archivos, 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. Para reformatear un dispositivo:

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.

Es posible que su administrador de sistema tenga esta opción deshabilitada. Póngase en contacto con su administrador si necesita restablecer su dispositivo.

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.

Nota: Si el dispositivo era originalmente estándar y estaba conectado a un servidor de administración, los requisitos de administración se aplicarán incluso después de un restablecimiento.

Acceder a mi dispositivo si olvidé mi contraseña

Si olvida su contraseña y un administrador le ha otorgado privilegios de restablecimiento de contraseña, puede restablecerla. Si su administrador no ha otorgado privilegios de restablecimiento de contraseña, debe comunicarse con su administrador para obtener ayuda para restablecer su contraseña.

Para restablecer su contraseña:

1. Enchufe su dispositivo e inicie IronKey.
2. Haga clic en Ayuda para contraseña.
3. Es posible que reciba un correo electrónico con instrucciones sobre cómo obtener su código de recuperación. De lo contrario, deberá comunicarse con su administrador para obtener este código. En este último caso, es posible que deba proporcionar el código de solicitud y el número de serie a su Administrador de Sistema. El correo electrónico y el número de teléfono de su Administrador del Sistema deben proporcionarse para su conveniencia. Al hacer clic en la dirección de correo electrónico, se abrirá su cliente de correo electrónico predeterminado y se rellenará previamente esta información para enviarla.
4. Una vez recibido, el código de recuperación tendrá que ser copiado y pegado exactamente como se le da a usted. Los códigos incorrectos cuentan para los diez intentos de desbloqueo antes de restablecer el dispositivo.
5. Escriba su nueva contraseña, confirme la contraseña en los campos correspondientes y haga clic en **Cambiar contraseña**. Nota: Las contraseñas distinguen entre mayúsculas y minúsculas y deben tener al menos 8 caracteres junto con más requisitos si la contraseña segura está habilitada.

Notificaciones de archivos restringidos

Si lo habilita su administrador de SafeConsole, su dispositivo puede restringir que ciertos archivos se guarden en el almacenamiento seguro. Cuando se restringe un archivo afectado, recibe una notificación que contiene el nombre del archivo. Si lo desea, puede desactivar estas notificaciones.

NOTA: Los archivos afectados seguirán estando restringidos cuando las notificaciones estén deshabilitadas.

Deshabilitar las notificaciones de archivos restringidos:

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 Mostrar notificaciones de archivos restringidos.

Escanear mi dispositivo en busca de malware

Si está habilitado por su Administrador de Sistema, el Malware Scanner es una tecnología de autolimpieza que detecta y elimina el malware en su dispositivo proveniente de un archivo o computadora infectados. Impulsado por la base de datos de firmas McAfee® AntiVirus y Anti-Malware, y\ constantemente actualizado para combatir las últimas amenazas de malware, el escáner primero busca las últimas actualizaciones, analiza su dispositivo, luego informa y limpia cualquier malware que se encuentre.

Es posible que el administrador de su sistema requiera que se actualice la definición del antimalware antes de que se pueda desbloquear el dispositivo. En este caso, la definición anti-malware completa tendrá que ser descargada a una carpeta temporal en el equipo local antes de que la contraseña pueda ser introducida. Esto puede aumentar el tiempo que lleva desbloquear el dispositivo en función de la conexión de red del equipo huésped y el tamaño de las actualizaciones de malware necesarias.

Algunas cosas que debe saber sobre el escaneo de su dispositivo:

- El escáner se ejecuta automáticamente al desbloquear el dispositivo.

- Analiza todos los archivos integrados (comprimidos y sin comprimir).

- Informará y eliminará cualquier malware detectado.

- (Opcional) Si su administrador de SafeConsole ha habilitado la cuarentena, puede poner en cuarentena cualquier malware que encuentre. Consulte Restauración o eliminación de un archivo de cuarentena para obtener más información.

- El escáner se actualizará automáticamente antes de cada análisis para protegerle de las últimas amenazas de malware.

- Una actualización requiere conexión a Internet. Asegure un mínimo de 135 MB de espacio libre en el dispositivo para acomodar los archivos de firmas de malware descargados.

- Su primera actualización puede tardar mucho tiempo en descargarse, dependiendo de su conexión a Internet.

- La fecha de la última actualización se muestra en pantalla.

- Si el escáner está demasiado desactualizado, tendrá que descargar un archivo grande para volver a actualizarlo.

Restauración o eliminación de un archivo en cuarentena

Si su administrador de SafeConsole ha habilitado la cuarentena, tendrá la opción de restaurar o eliminar el malware detectado. Este proceso ayuda cuando McAfee detecta un documento válido como malware.

NOTA: Dependiendo del tamaño de los archivos infectados, la cuarentena puede no estar disponible. Si el archivo no se puede poner en cuarentena, se eliminará. Los archivos eliminados no se pueden restaurar mediante el mismo procedimiento.

Para ver los archivos en cuarentena:

1. Desbloquee el dispositivo y haga clic en **Configuración** en el panel de control de IronKey.
2. Haga clic en **cuarentena** en la barra lateral izquierda.

Al seleccionar un archivo de la lista se mostrarán detalles adicionales, como el nombre de la amenaza, el tipo de amenaza, la versión de la definición antimalware y la fecha de cuarentena. Después de seleccionar el archivo, los archivos se pueden Restaurar o Eliminar.

Los archivos restaurados estarán exentos del escáner automático mientras el dispositivo esté desbloqueado. El archivo se analizará durante el próximo desbloqueo o si se selecciona un escáner manual en la pestaña Anti-Malware. Si las definiciones antimalware siguen determinando que el archivo está infectado, lo pondrá en cuarentena una vez más.

Los archivos eliminados se borrarán permanentemente.

Desinfectar

Desinfectar permite que el contenido de la unidad encriptada se borre de forma segura. Esto se logra borrando la clave encriptada que utiliza la unidad para acceder a los archivos en el Volumen seguro mientras conserva la conexión a SafeConsole.

Advertencia: Al realizar esta acción, se borrarán por completo todos los datos del Volumen seguro. Esta acción es permanente.

La capacidad de desinfectar una unidad depende de los ajustes configurados por su administrador de SafeConsole. Si se permite, la unidad se puede desinfectar siguiendo estos pasos:

1. Desbloquee su dispositivo y abra el Panel de control del dispositivo iniciando IronKey.exe.
2. Haga clic con el botón derecho en el icono de la bandeja del sistema para el Panel de control y seleccione Desinfectar dispositivo.
3. Introduzca los números que se indican en el cuadro de diálogo para confirmar que todos los datos se pueden borrar de la unidad.
4. El dispositivo se restablecerá. Desenchufe y vuelva a conectar el dispositivo a su estación de trabajo.
5. Inicie IronKey.exe e ingrese la contraseña del dispositivo.

Uso de ZoneBuilder en SafeConsole

Si está habilitado por su Administrador de Sistema, ZoneBuilder es una herramienta SafeConsole utilizada para crear una Zona de Confianza de computadoras. Se puede usar para restringir el acceso del dispositivo a las computadoras dentro de la Zona de confianza y, si está habilitado, puede desbloquear automáticamente su dispositivo, lo que elimina la necesidad de ingresar su contraseña.

Si su administrador elige habilitar esta política, es posible que deba confiar en la cuenta. Confiar en la cuenta:

1. Desbloquee el dispositivo y haga clic en **Configuración** en el panel de control de IronKey.
2. Haga clic en **ZoneBuilder** en la barra lateral izquierda.
3. Haga clic en **Confiar en esta cuenta**.
4. Introduzca la contraseña para el dispositivo y haga clic en **Aceptar**. Su cuenta ahora aparecerá en el cuadro Cuentas de confianza.

Su cuenta se encuentra ahora en la Zona de confianza de las computadoras. Dependiendo de la política establecida por su Administrador de Sistema, es posible que tenga acceso restringido al dispositivo fuera de la Zona de Confianza o sin conexión. Su dispositivo también puede estar configurado para desbloquearse automáticamente en equipos de confianza.

Para eliminar una cuenta de confianza, simplemente resalte la cuenta que desea eliminar y haga clic en **Eliminar**.

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. Algunas políticas de dispositivos administrados, establecidas por el Administrador del sistema, pueden restringir el uso del dispositivo a sistemas que solo ejecutan sistemas operativos Windows o macOS.

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.
6. Políticas que bloquearán el dispositivo.
   - Si el dispositivo está deshabilitado dentro de la configuración de políticas en SafeConsole, usted no podrá desbloquearlo.

¿Dónde puedo obtener ayuda?

Los siguientes recursos proporcionan más información sobre los productos IronKey. Por favor, póngase en contacto con su Mesa de Ayuda o Administrador del Sistema 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™ S1000E
VERSCHLÜSSELTER USB 3.2 Gen 1-STICK

Anleitung

Inhalt

Über diese Bedienungsanleitung (04152025)

Der IronKey™ S1000E ist ein verwalteter Stick, der eine Gerätelizenz erfordert und über SafeConsole verwaltet werden kann. SafeConsole ist eine sichere Cloud- oder Vor-Ort-Managementplattform, mit der Ihr Unternehmen kompatible USB-Speichergeräte (Universal Serial Bus) einfach und effizient zentral verwalten kann.

In dieser Anleitung wird erklärt, wie ein S1000E-Laufwerk als ein über SafeConsole verwaltetes Laufwerk eingerichtet und initialisiert werden kann.

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 S1000E 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 S1000E 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. ***HINWEIS:*** Administratoren können das Passwort mit SafeConsole zurücksetzen.

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
Schnittstelle/Anschlusstyp/Geschwindigkeit**	USB 3.2 Gen 1 / Type-A - 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; MILSTD-810F

Temperatur	Betrieb: 0 bis 50°C; Lagerung: -20°C bis 85°C
Hardware-Datenverschlüsselung	256-Bit AES(XTS-Modus)
Zertifizierung	FIPS 140-2 Level 3 TAA/CMMC-konform, montiert in den USA
OS-Kompatibilität	- Windows 11, Windows 10 (erfordert zwei freie Laufwerksbuchstaben) - macOS 12.x – 15.x - Linux 4.4.x***
Garantie	5 Jahre, eingeschränkt

Die in den USA entwickelten und montierten S1000E-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. Keine Online-Verwaltungsfunktionen.

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 S1000E 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 S1000E 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 S1000E 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.

Einrichten eines S1000E-Sticks mit SafeConsole

Der Initialisierungsprozess beginnt, sobald Sie die Berechtigung gewähren, dass der Stick mit dem SafeConsole-Server kommunizieren kann. Die erforderlichen Schritte zum Registrieren eines S1000E in SafeConsole hängen von den Richtlinien ab, die Ihr Administrator festgelegt hat. Es werden nicht alle Dialoge angezeigt.

Es wird ein SafeConsole „Connection Token“ benötigt. Das SafeConsole „Connection Token“ erhält der Systemadministrator über die Schnellverbindungsanleitung, die in der SafeConsole-Benutzeroberfläche zu finden ist.

1. Geben Sie das SafeConsole „Connection Token“ ein, das Sie mithilfe der obigen Schritten erhalten haben. Lesen Sie die Lizenzvereinbarung durch, markieren Sie das Kontrollkästchen, um sie zu akzeptieren, und klicken Sie unten links auf „**Aktivieren**“.

   • **Optional aktivierte Richtlinien** – Diese Richtlinien sind evtl. von Ihrem Systemadministrator aktiviert. Sie werden bei der Geräteregistrierung angezeigt, falls sie aktiviert sind.

   - Bestätigen der Eigentümerschaft des Geräts: Geben Sie den Windows-Benutzernamen und das Passwort ein, die mit den Anmeldedaten des Computers verknüpft sind, an den das Gerät angeschlossen ist.

   - Benutzerdefinierte Geräteinformationen: Erforderliche Informationen über Sie oder Ihr Gerät. Die erforderlichen Felder sind unterschiedlich.

   - Eindeutiges Benutzer-Token: Dieses Token ist direkt mit dem Konto des Endbenutzers verbunden und wird vom Systemadministrator bereitgestellt.

   - Administrator-Registrierungsgenehmigung: Der Systemadministrator benötigt möglicherweise ihre Zustimmung, um mit der Geräteregistrierung fortzufahren.

2. Geben Sie ein sicheres Passwort ein und bestätigen Sie es. Wenn das erstellte Passwort die rechts neben den Eingabefeldern aufgeführten Anforderungen erfüllt, klicken Sie auf „Weiter“. Die Anforderungen an dieses Passwort hängen von der Richtlinie ab, die von Ihrem Administrator ausgewählt wurde. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen mindestens 8 Zeichen lang sein, wenn das sichere Passwort aktiviert ist.

3. Wählen Sie ein „Secure Volume File System“ (siehe Formatieren des Geräts) und klicken Sie auf „**Weiter**“.

4. Das Gerät schließt nun den Einrichtungsvorgang ab und ist betriebsbereit. Greifen Sie auf den verschlüsselten Speicher zu, indem Sie auf das **Ordnersymbol** im oberen Menü klicken. Die Einstellungen des Geräts können durch Klicken auf das **Zahnradsymbol** aufgerufen und geändert werden. Weitere Informationen erhalten Sie unter dem IronKey-Bedienfeld.

Starkes Passwort

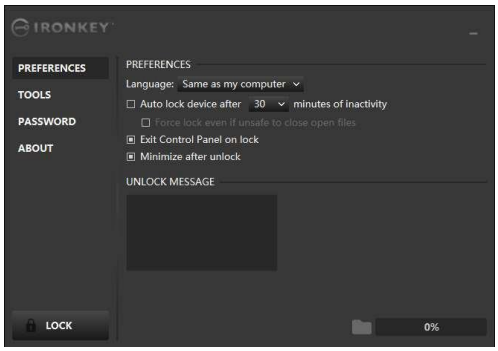
Beim Erstellen oder Ändern des Passworts für das Gerät gibt es eine Option zum Aktivieren von „Enforce Strong Password“. Bei verwalteten Geräten kann diese Option von Ihrem Systemadministrator konfiguriert oder erzwungen werden. Wenn diese Option aktiviert ist, werden die folgenden Regeln für alle potenziellen Passwörter überprüft.

- Die Länge muss mindestens acht (8) Zeichen betragen.
- Das Passwort muss Zeichen aus mindestens drei (3) der folgenden Zeichenklassen enthalten:
  - ASCII-Ziffern (0123456789) Hinweis: Wenn das letzte Zeichen des Passworts eine ASCII-Ziffer ist, zählt es für diese Einschränkung nicht als ASCII-Ziffer.
  - Kleinbuchstaben ASCII (abc...xyz)
  - Großbuchstaben ASCII (ABC...XYZ) Hinweis: Wenn das erste Zeichen des Passworts ein ASCII-Großbuchstabe ist, wird es für diese Einschränkung nicht als ASCII-Großbuchstabe gezählt.
  - Nicht-alphanumerische ASCII-Zeichen (!@#$, usw.)
  - Nicht-ASCII-Zeichen

Beispiele für sichere Passwörter

Beispielpasswörter	Ergebnisse
Passwort	Fehlgeschlagen: 8 Zeichen lang, enthält aber nur 1 eindeutige Zeichenklasse (Kleinbuchstaben-ASCII).
Passwort1	Fehlgeschlagen: 9 Zeichen lang, allerdings zählen der Großbuchstabe „P“ und „1“ nicht zu den eindeutigen Zeichenklassen, wodurch nur Kleinbuchstaben im ASCII-Format übrig bleiben.
pa$$Word	Bestanden: 8 Zeichen lang. Enthält ASCII-Kleinbuchstaben, ASCII-Großbuchstaben und nicht-alphanumerische ASCII-Zeichen.

IronKey-Bedienfeld

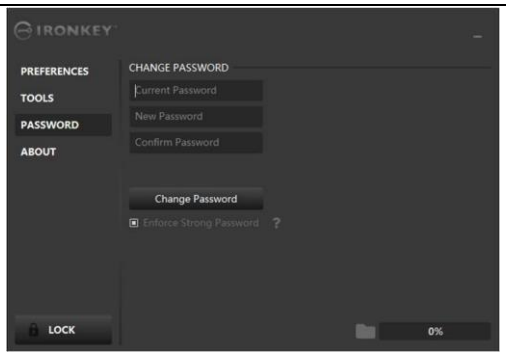


VOREINSTELLUNGEN

1. Language: Ändern der Gerätesprache
2. Auto lock device: Ändern des Timers für die Sperre
3. Exit on Control Panel on lock: Verhalten zum Beenden oder Offenlassen des Bedienfelds ändern, wenn das Gerät gesperrt ist.
4. Minimize after unlock: Ändern, um das Bedienfeld zu minimieren, wenn das Gerät entsperrt ist oder erlauben, dass es maximiert bleibt.
5. UNLOCK MESSAGE: Hinzufügen einer Meldung, die im Anmeldefenster angezeigt werden soll.

TOOLS

1. UPDATE: Suche nach Updates
2. DEVICE HEALTH: Formatiert das sichere Laufwerk mit FAT32 oder exFAT neu. (macOS erlaubt nur die Formatierung mit FAT32)



PASSWORT

1. CHANGE PASSWORD: Ändern des Passworts für die Anmeldung beim Laufwerk.
2. Enforce Strong Password: Aktivieren bzw. Deaktivieren der Anforderung eines sicheren Passworts

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 in der Menüleiste des IronKey-Bedienfelds auf „**Files**“.
   - 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 S1000E USB-Stick.
   - Zum Speichern einer Datei ziehen Sie die Datei von Ihrem Computer auf den S1000E 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. Für verwaltete Geräte kann von einem Administrator festgelegt werden, dass sie nur in einem schreibgeschützten Zustand entsperrt werden.

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. Bei verwalteten Geräten ist diese Funktion evtl. von Ihrem Systemadministrator aktiviert.

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. 7 Zeilen mit 200 Zeichen).

Sperren des Geräts

Sperren Sie Ihr Gerät, wenn es nicht benutzt wird, um unerwünschten Zugriff auf Ihre sicheren Dateien auf dem USB-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. Bei verwalteten Geräten ist diese Funktion evtl. von Ihrem Systemadministrator aktiviert.

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**“.

Hinweis: Verwaltete Geräte werden während der Verwendung automatisch gesperrt, wenn ein Administrator das Gerät per Fernzugriff deaktiviert. Dieser Stick kann erst wieder entsperrt werden, bis der Systemadministrator das Gerät wieder freigibt.

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.

Die Einstellungen der Passwortrichtlinie werden von Ihrem Systemadministrator festgelegt. 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.

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. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen mindestens 8 Zeichen lang sein, wenn das sichere Passwort „Strong Password“ aktiviert ist.
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, das IRONKEY SECURE FILES USB-Laufwerk entweder als FAT32 oder exFAT 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-Laufwerks alle Ihre Dateien gelöscht, nicht aber Ihr Gerätepasswort und Ihre Einstellungen.

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.

Ihr Systemadministrator hat diese Option möglicherweise deaktiviert. Wenden Sie sich an Ihren Administrator, wenn Ihr Gerät zurückgesetzt werden muss.

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.

Hinweis: Wenn das Gerät ursprünglich standardmäßig mit einem Verwaltungsserver verbunden war, werden die Verwaltungsanforderungen auch nach einem Reset weiterhin erfüllt.

Zugriff auf das Gerät, wenn das Passwort vergessen wurde

Wenn Sie Ihr Passwort vergessen haben und ein Administrator Ihnen die Berechtigung zum Zurücksetzen des Passworts erteilt hat, können Sie es zurücksetzen. Wenn Ihr Administrator keine Berechtigung zum Zurücksetzen des Passworts erteilt hat, müssen Sie sich an Ihren Administrator wenden, um Hilfe beim Zurücksetzen Ihres Passworts zu erhalten.

Zurücksetzen Ihres Passwort:

1. Schließen Sie Ihr Gerät an und starten Sie den IronKey.
2. Klicken Sie auf „Password Help“.
3. Möglicherweise erhalten Sie eine E-Mail mit Anweisungen, wie Sie Ihren Wiederherstellungscode erhalten können. Andernfalls müssen Sie sich an Ihren Administrator wenden, um diesen Code zu erhalten. In letzterem Fall müssen Sie Ihrem Systemadministrator möglicherweise den Anforderungscode und die Seriennummer mitteilen. Die E-Mail-Adresse und die Telefonnummer Ihres Systemadministrators sollten zu Ihrer Information angegeben werden. Wenn Sie auf die E-Mail-Adresse klicken, wird Ihr Standard-E-Mail-Programm geöffnet und die zu versendenden Informationen werden vorausgefüllt.
4. Der Wiederherstellungscode muss nach dem Empfang genau so kopiert und eingefügt werden, wie er Ihnen übermittelt wird. Falsche Codes werden auf die zehn Entsperrversuche angerechnet, bevor das Gerät zurückgesetzt wird.
5. Geben Sie Ihr neues Passwort ein und bestätigen Sie es in den anderen Feldern, und klicken Sie dann auf „**Change Password**“. Hinweis: Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen mindestens 8 Zeichen lang sein, wenn das sichere Passwort „Strong Password“ aktiviert ist.

Benachrichtigungen zu eingeschränkten Dateien

Wenn Ihr SafeConsole-Administrator dies aktiviert hat, kann Ihr Gerät das Speichern bestimmter Dateien im sicheren Speicher einschränken. Wenn eine betroffene Datei eingeschränkt wird, erhalten Sie eine Benachrichtigung mit dem Namen der Datei. Falls gewünscht, können diese Benachrichtigungen deaktiviert werden.

HINWEIS: Die betroffenen Dateien werden auch dann eingeschränkt, wenn die Benachrichtigungen deaktiviert sind.

Deaktivieren von „Restricted Files Notifications“:

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 „Show Restricted Files Notifications“.

Scannen des Geräts auf Malware

Wenn er von Ihrem Systemadministrator aktiviert wurde, ist der Malware-Scanner eine selbstreinigende Technologie, die Malware auf Ihrem Gerät anhand einer infizierten Datei oder eines infizierten Computers erkennt und entfernt. Unter Verwendung von McAfee® AntiVirus und der Anti-Malware-Signaturdatenbank, die ständig aktualisiert wird, um die neuesten Malware-Bedrohungen zu bekämpfen, sucht der Scanner zunächst nach den neuesten Updates, scannt Ihr Gerät und meldet und bereinigt dann jede gefundene Malware.

Ihr Systemadministrator kann verlangen, dass die Anti-Malware-Definition aktualisiert wird, bevor das Gerät entsperrt werden kann. In diesem Fall muss die vollständige Anti-Malware-Version in einen temporären Ordner auf dem lokalen Computer heruntergeladen werden, bevor das Passwort eingegeben werden kann. Dies kann die Zeit, die zum Entsperren des Geräts benötigt wird, je nach Netzwerkverbindung des Host-Computers und dem Umfang der erforderlichen Malware-Updates verlängern.

Einige Dinge, die Sie über das Scannen Ihres Geräts wissen sollten:

- Der Scanner läuft automatisch, sobald Sie Ihr Gerät entsperren.
- Er scannt alle Onboard-Dateien (komprimiert und unkomprimiert).
- Er meldet und löscht jede gefundene Malware.
- (Optional) Wenn Ihr SafeConsole-Administrator die Quarantäne aktiviert hat, kann er jede gefundene Malware unter Quarantäne stellen. Weitere Informationen finden Sie unter „Deleting a Quarantine File“.
- Er aktualisiert sich automatisch vor jedem Scan, um Sie vor den neuesten Malware-Bedrohungen zu schützen.
- Das Update erfordert eine Internetverbindung. Stellen Sie sicher, dass mindestens 135MB freier Speicherplatz auf dem Gerät vorhanden ist, um die heruntergeladenen Malware-Signaturdateien zu speichern.
- Der Download des ersten Updates kann je nach Internetverbindung einige Zeit in Anspruch nehmen.
- Das Datum der letzten Aktualisierung wird auf dem Bildschirm angezeigt.
- Wenn der Scanner stark veraltet ist, muss eine große Datei herunterladen werden, um ihn wieder auf den neuesten Stand zu bringen.

Wiederherstellen oder Löschen einer in Quarantäne gestellten Datei

Wenn Ihr SafeConsole-Administrator die Quarantäne aktiviert hat, haben Sie die Möglichkeit, erkannte Malware wiederherzustellen oder zu löschen. Dieser Vorgang ist eine Hilfe, wenn McAfee ein gültiges Dokument als Malware erkennt.

HINWEIS: Je nach Größe der infizierten Dateien ist die Quarantäne möglicherweise nicht verfügbar. Wenn die Datei nicht unter Quarantäne gestellt werden kann, wird sie gelöscht. Gelöschte Dateien können mit dem folgenden Vorgang nicht wiederhergestellt werden.

Anzeigen von unter Quarantäne gestellten Dateien:

1. Entsperren Sie Ihr Gerät und klicken Sie im IronKey-Bedienfeld auf „**Settings**“.
2. Klicken Sie in der linken Seitenleiste auf „**Quarantine**“.

Wenn Sie eine Datei aus der Liste auswählen, werden zusätzliche Details angezeigt, darunter der Name der Bedrohung, der Bedrohungstyp, die Version der Anti-Malware-Definition und das Datum der Quarantäne. Nach dem Auswählen der Datei können die Dateien entweder wiederhergestellt oder gelöscht werden.

Wiederhergestellte Dateien sind von der automatischen Überprüfung ausgenommen, solange das Gerät nicht gesperrt ist. Die Datei wird beim nächsten Entsperren gescannt oder wenn auf der Registerkarte „Anti-Malware“ ein manueller Scan ausgewählt wird. Wenn die Anti-Malware-Definitionen immer noch feststellen, dass die Datei infiziert ist, wird die Datei erneut unter Quarantäne gestellt.

Gelöschte Dateien werden dauerhaft gelöscht.

Bereinigen

Mit „Sanitize“ kann der Inhalt des verschlüsselten Laufwerks sicher gelöscht werden. Dies geschieht durch Löschen des verschlüsselten Schlüssels, den das Laufwerk für den Zugriff auf die Dateien auf dem „Secure Volume“ verwendet, während die Verbindung zu SafeConsole erhalten bleibt.

Warnhinweis: Durch diese Aktion werden alle Daten auf dem „Secure Volume“ vollständig gelöscht. Diese Maßnahme ist dauerhaft.

Die Möglichkeit, ein Laufwerk zu säubern, hängt von den Einstellungen ab, die Ihr SafeConsole-Administrator vorgenommen hat. Wenn zulässig, kann Ihr Laufwerk durch die folgenden Schritte bereinigt werden:

1. Entsperren Sie Ihr Gerät und öffnen Sie das IronKey-Bedienfeld des Geräts, indem Sie IronKey.exe starten.
2. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol für das Bedienfeld und wählen Sie „Sanitize Device“.
3. Geben Sie die im Dialogfeld abgefragten Zahlen ein, um zu bestätigen, dass alle Daten vom Laufwerk gelöscht werden können.
4. Das Gerät wird zurückgesetzt. Trennen Sie das Gerät vom Netz und schließen Sie es wieder an Ihren Computer an.
5. Starten Sie IronKey.exe und geben Sie das Gerätepasswort ein.

Verwenden des ZoneBuilder in SafeConsole

Wenn es von Ihrem Systemadministrator aktiviert wurde, ist ZoneBuilder ein SafeConsole-Instrument, mit dem Sie eine vertrauenswürdige Zone von Computern erstellen können. ZoneBuilder kann verwendet werden, um den Gerätezugriff auf Computer innerhalb der vertrauenswürdigen Zone zu beschränken. Wenn er aktiviert ist, kann ZoneBuilder Ihr Gerät automatisch entsperren, wodurch die Eingabe des Passworts überflüssig wird.

Wenn Ihr Administrator diese Richtlinie aktiviert hat, müssen Sie dem Konto möglicherweise vertrauen. Vertrauen für das Konto:

1. Entsperren Sie Ihr Gerät und klicken Sie im IronKey-Bedienfeld auf „**Settings**“.
2. Klicken Sie in der linken Seitenleiste auf „**ZoneBuilder**“.
3. Klicken Sie auf „**Trust This Account**“.
4. Geben Sie das Passwort für das Gerät ein und klicken Sie auf „**OK**“. Ihr Konto wird nun im Feld „Trusted Accounts“ angezeigt.

Ihr Konto befindet sich jetzt in der vertrauenswürdigen Zone von Computern. Je nach der von Ihrem Systemadministrator festgelegten Richtlinie kann der Gerätezugriff außerhalb der vertrauenswürdigen Zone oder im Offline-Modus eingeschränkt sein. Ihr Gerät kann auch so eingestellt sein, dass es auf vertrauenswürdigen Computern automatisch entsperrt wird.

Zum Entfernen eines vertrauenswürdigen Kontos markieren Sie einfach das Konto, das entfernt werden soll, und klicken Sie auf „**Remove**“.

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“. Einige Richtlinien für verwaltete Geräte, die vom Systemadministrator festgelegt werden, können die Verwendung des Geräts auf Systeme beschränken, auf denen nur Windows- oder macOS-Betriebssysteme laufen.

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.
6. Richtlinien, die das Gerät blockieren.
   - Wenn das Gerät innerhalb der Richtlinieneinstellungen in SafeConsole deaktiviert ist, können Sie das Gerät nicht entsperren.

Wo kann man Hilfe erhalten?

Die folgenden Ressourcen bieten weitere Informationen über IronKey-Produkte. Wenden Sie sich an Ihren Helpdesk oder Systemadministrator, wenn Sie weitere Fragen haben.

- kingston.com/usb/encrypted_security: Informationen, Marketingmaterial und Video-Anleitungen.
- kingston.com/support: Produkt-Support, Häufig gestellte Fragen (FAQs) 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.

IRONKEY™ S1000E
CLÉ USB CHIFFRÉE 3.2 Gen 1

Manuel d'utilisation

Sommaire

À propos de ce Manuel (04152025)

L'IronKey™ S1000E (l'« appareil ») est un lecteur géré qui nécessite une licence d'appareil et peut être géré par SafeConsole. SafeConsole est une plateforme de gestion sécurisée dans le cloud ou sur site qui permet à votre organisation de gérer de manière centralisée les appareils de stockage USB (Universal Serial Bus) compatibles, facilement et efficacement.

Ce manuel explique comment configurer et initialiser une clé USB S1000E sur une plateforme SafeConsole afin d'en faire un lecteur 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 S1000E USB 3.2 Gen 1 est une clé USB qui intègre la sécurité des mots de passe et le chiffrement des données. 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 S1000E 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*.
REMARQUE : Les administrateurs peuvent réinitialiser le mot de passe à l'aide de SafeConsole.

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
Interface/Type de connecteur/Vitesse**	USB 3.2 Gen 1 / Type-A - 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 ; MILSTD-810F

Température	En fonctionnement : 0°C à 50°C ; Stockage : -20°C à 85°C
Chiffrement matériel	AES 256 bits (mode XTS)
Certifications	FIPS 140-2 niveau 33 Conformité TAA/CMMC, assemblé aux États-Unis
Compatibilité SE	- Windows 11, Windows 10 (nécessite deux lettres de lecteur libres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantie	Limitée de 5 ans

Conçues et assemblées aux États-Unis, les clés USB S1000E 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. Aucune fonction de gestion en ligne.

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 S1000E 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, tel qu'un clavier ou un Hub 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 S1000E 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 appareils connectés. Dans l'image ci-dessous, la lettre du lecteur est (E:).

Accès à l'appareil (environnement macOS)

1. Branchez la clé USB chiffrée S1000E 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.

Configuration de la S1000E avec SafeConsole

Le processus d'initialisation commencera par permettre à l'appareil de communiquer avec le serveur SafeConsole. Les étapes nécessaires pour enregistrer une S1000E dans SafeConsole dépendront des politiques que votre administrateur applique. Toutes les boîtes de dialogue ne seront pas affichées.

Un jeton de connexion SafeConsole sera nécessaire. Le jeton de connexion SafeConsole est obtenu par l'administrateur système via le guide de connexion rapide, situé à l'intérieur de l'interface utilisateur SafeConsole.

1. Saisissez le jeton de connexion SafeConsole obtenu dans les étapes ci-dessus. Lisez l'accord de licence, cochez la case pour l'accepter et cliquez sur **Activate** (Activer) dans le coin inférieur gauche.

   • **Optionally Enabled Policies (Politiques activées en option) :** Ces politiques peuvent être activées ou non par votre administrateur système. Si elles ont été activées, elles apparaîtront lors de l'enregistrement de l'appareil.

   - Confirm Ownership of the device (Confirmez la propriété de l'appareil) : Saisissez le nom d'utilisateur et le mot de passe Windows associés aux informations d'identification de l'ordinateur sur lequel l'appareil est branché.

   - Custom Device Information (Informations personnalisées sur l'appareil) : Informations requises à propos de vous ou de votre appareil. Les champs obligatoires varient.

   - Unique User Token (Jeton utilisateur unique) : Ce jeton est directement associé au compte de l'utilisateur final, et sera fourni par l'administrateur système.

   - Administrator Registration Approval (Approbation de l'enregistrement par l'administrateur) : L'administrateur système peut exiger son approbation pour procéder à l'enregistrement de l'appareil.

2. Saisissez un mot de passe sécurisé et confirmez-le. Une fois que le mot de passe créé répond aux exigences énumérées à droite des champs de saisie, cliquez sur Continue (Continuer). Les exigences relatives à ce mot de passe dépendent de la politique sélectionnée par votre administrateur. Les mots de passe sont sensibles à la casse et doivent comporter au moins 8 caractères, avec des exigences supplémentaires si l'option de mot de passe fort est activée.

3. Choisissez un système de fichiers à volume sécurisé (voir Formater mon appareil) et cliquez sur **Continue** (Continuer).

4. L'appareil va maintenant finaliser le processus de configuration. Vous pourrez ensuite l'utiliser. Accédez au stockage chiffré en cliquant sur **l'icône de dossier** dans le menu supérieur. Vous pouvez accéder aux paramètres de l'appareil et les modifier en cliquant sur **l'icône engrenage**. Consultez le panneau de contrôle IronKey pour plus d'informations.

Strong Password (Mot de passe fort)

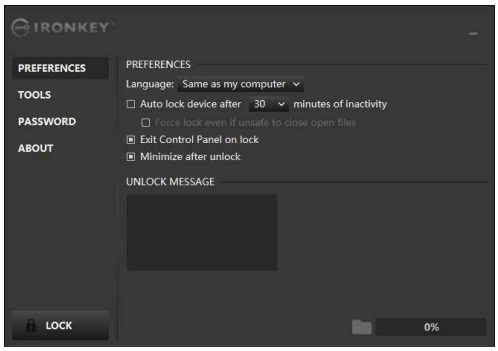
Lors de la création ou de la modification du mot de passe de l'appareil, une option permet d'activer l'application d'un mot de passe fort. Pour les appareils managed, cette option peut être configurée ou activée par votre administrateur système. Lorsque cette option est activée, tous les mots de passe potentiels doivent respecter les règles suivantes.

- Doit comporter au moins huit (8) caractères.
- Doit contenir trois (3) des types de caractères suivants :
  - Chiffres ASCII (0123456789) Remarque : Si le dernier caractère du mot de passe est un chiffre ASCII, il n'est pas considéré comme un chiffre ASCII dans le cadre de cette restriction.
  - Minuscule ASCII (abc...xyz)
  - Majuscule ASCII (ABC…XYZ) Remarque : Si le premier caractère du mot de passe est une lettre ASCII majuscule, il n'est pas considéré comme une lettre ASCII majuscule dans le cadre de cette restriction.
  - Caractères ASCII non alphanumériques (!@#$, etc.)
  - Caractères non ASCII

Exemples de mots de passe forts

Exemples de mots de passe	Résultats
Password	Échec : 8 caractères, mais ne contient qu'un seul type de caractères (minuscule ASCII).
Password1	Échec : 9 caractères, mais la majuscule '« P » et le chiffre '« 1 » ne sont pas pris en compte pour les types de caractères exigés. Il ne reste donc que les minuscules ASCII.
pa$$Word	Correct : Comporte 8 caractères. Contient des minuscules ASCII, une majuscule ASCII et des caractères ASCII non alphanumériques.

Panneau de contrôle IronKey

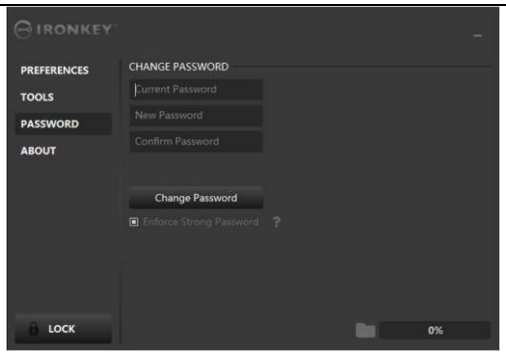


PRÉFÉRENCES

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) : Quitter 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. UPDATE (MISE À JOUR) : Vérifier les mises à jour
2. DEVICE HEALTH (SANTÉ DE L'APPAREIL) : Reformater le volume sécurisé en utilisant FAT32 ou exFAT (macOS ne permet que le formatage FAT32).



PASSWORD (MOT DE PASSE)

1. CHANGE PASSWORD (MODIFIER LE MOT DE PASSE) : Modifier le mot de passe de connexion à l'appareil.
2. Enforce Strong Password (Appliquer un mot de passe fort) : Activer/désactiver l'exigence d'un mot de passe fort

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 **Files** (Fichiers) dans la barre de menu du panneau de contrôle IronKey.
   - Windows : Ouvrez l’Explorateur Windows et affichez le lecteur IRONKEY SECUREFILESUSB.
   - macOS : Ouvrez le Finder et affichez le lecteur USB KINGSTON.
2. Effectuez l’une des opérations suivantes :
   - Pour ouvrir un fichier, double-cliquez sur le fichier souhaité sur le lecteur S1000EUSB.
   - Pour enregistrer un fichier, faites glisser le fichier de votre ordinateur vers le lecteur S1000EUSB.

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 **Secure Files** (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. Les appareils managed peuvent être forcés à se déverrouiller en mode lecture seule par un administrateur.

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-Only** (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 les appareils gérés, cette fonction peut être activée ou non par votre administrateur système.

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 7 lignes et 200 caractères).

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. Pour les appareils managed, cette fonction peut être activée ou non par votre administrateur système.

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 **Lock Device** (Verrouiller l'appareil).

Remarque : Les appareils managed se verrouilleront automatiquement en cours d'utilisation si un administrateur désactive l'appareil à distance. Vous ne pourrez pas déverrouiller l'appareil tant que l'administrateur système ne l'aura pas réactivé.

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 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.

Les paramètres de la politique de mot de passe sont déterminés par votre administrateur système. 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.

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. Les mots de passe sont sensibles à la casse et doivent comporter au moins 8 caractères, voire plus si l'option de mot de passe fort est activée.
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 en FAT32 ou exFAT.

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 effacera tous vos fichiers, mais pas votre mot de passe ni vos paramètres.

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 Informations 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 gestion

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 Info (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.

Il se peut que votre administrateur système ait désactivé cette option. Si vous devez réinitialiser votre appareil, contactez votre administrateur.

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.

Remarque : Si l'appareil était à l'origine standard et connecté à un serveur de gestion, les exigences de gestion seront toujours appliquées même après une réinitialisation.

Accéder à mon appareil en cas d'oubli du mot de passe

Si vous avez oublié votre mot de passe et qu'un administrateur vous a accordé des privilèges de réinitialisation de mot de passe, vous pouvez le réinitialiser. Si votre administrateur ne vous a pas accordé de privilèges de réinitialisation de mot de passe, vous devez le contacter pour qu'il vous aide à réinitialiser votre mot de passe.

Pour réinitialiser votre mot de passe :

1. Branchez votre appareil et démarrez IronKey.
2. Cliquez sur Password Help (Aide pour le mot de passe).
3. Il se peut que vous receviez un e-mail contenant des instructions sur la façon d'obtenir votre code de récupération. Sinon, vous devrez contacter votre administrateur pour obtenir ce code. Dans ce dernier cas, il vous sera peut-être demandé de communiquer le code de demande et le numéro de série à votre administrateur système. L'adresse e-mail et le numéro de téléphone de votre administrateur système doivent être fournis pour votre commodité. Le fait de cliquer sur l'adresse e-mail ouvrira votre système de messagerie par défaut et pré-remplira les informations à envoyer.
4. Une fois reçu, le code de récupération doit être copié et collé exactement comme il vous a été fourni. Les codes incorrects sont décomptés des dix tentatives de déverrouillage avant que l'appareil ne soit réinitialisé.
5. Saisissez votre nouveau mot de passe et confirmez-le dans les champs prévus à cet effet, puis cliquez sur **Change Password** (Modifier le mot de passe). Remarque : Si l'option de mot de passe fort est activée les mots de passe sont sensibles à la casse et doivent comporter au moins 8 caractères, entre autres exigences.

Notifications de fichiers restreints

Si cette option est activée par votre administrateur SafeConsole, votre appareil peut restreindre l'enregistrement de certains fichiers dans le stockage sécurisé. Lorsqu'un fichier concerné est restreint, vous recevez une notification contenant le nom du fichier. Si vous le souhaitez, vous pouvez désactiver ces notifications.

REMARQUE : Même lorsque les notifications sont désactivées, les fichiers concernés restent restreints.

Pour désactiver les notifications relatives aux fichiers restreints :

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. Cochez la **case** Show restricted files notifications (Afficher les notifications relatives aux fichiers restreints).

Détecter des logiciels malveillants sur mon appareil

S'il est activé par votre administrateur système, le scanner de logiciels malveillants est une technologie d'auto-nettoyage qui détecte et supprime les logiciels malveillants sur votre appareil provenant d'un fichier ou d'un ordinateur infecté. Alimenté par la base de signatures de McAfee® AntiVirus et Anti-Malware, et constamment mis à jour pour lutter contre les dernières menaces de logiciels malveillants, ce scanner vérifie d'abord les dernières mises à jour, analyse votre appareil, puis signale et nettoie tout programme malveillant détecté.

Votre administrateur système peut exiger la mise à jour de la définition du programme malveillant avant de pouvoir déverrouiller l'appareil. Dans ce cas, la définition complète du programme malveillant devra être téléchargée dans un dossier temporaire sur l'ordinateur local avant que le mot de passe puisse être saisi. Cela peut augmenter le temps nécessaire au déverrouillage de l'appareil en fonction de la connexion réseau de l'ordinateur hôte et de la taille des mises à jour de programmes malveillants nécessaires.

Informations pratiques concernant l'analyse de votre appareil :

- Le scanner s'exécute automatiquement lorsque vous déverrouillez votre appareil.

- Il analyse tous les fichiers contenus (compressés et non compressés).

- Il signale et supprime tout programme malveillant détecté.

- (Facultatif) Si votre administrateur SafeConsole a activé la fonction de quarantaine, il peut mettre en quarantaine les programmes malveillants qu'il détecte. Pour plus d'informations, consultez la section Restauration ou suppression d'un fichier en quarantaine.

- Le scanner se met automatiquement à jour avant chaque analyse pour vous protéger contre les dernières menaces de programmes malveillants.

- Une mise à jour nécessite une connexion Internet. Veillez à disposer d'au moins 135 Mo d'espace libre sur l'appareil pour les fichiers de signatures de programmes malveillants à télécharger.

- Le téléchargement de la première mise à jour peut prendre un certain temps, en fonction de votre connexion Internet.

- La date de la dernière mise à jour est affichée à l'écran.

- Si le scanner n'est plus à jour, il devra télécharger un fichier volumineux pour se remettre à jour.

Restauration ou suppression d'un fichier mis en quarantaine

Si votre administrateur SafeConsole a activé la quarantaine, vous aurez la possibilité de restaurer ou de supprimer les programmes malveillants détectés. Ce processus est utile lorsque McAfee signale un document valide comme étant un programme malveillant.

REMARQUE : Selon la taille des fichiers infectés, il se peut que la quarantaine ne soit pas disponible. Si le fichier ne peut pas être mis en quarantaine, il sera supprimé. Les fichiers supprimés ne peuvent pas être restaurés à l'aide de la procédure suivante.

Pour afficher les fichiers en quarantaine :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans le panneau de contrôle IronKey.

2. Cliquez sur **Quarantine** (Quarantaine) dans la barre latérale gauche.

Sélectionnez un fichier dans la liste pour afficher des détails supplémentaires, notamment le nom et le type de la menace, la version de la définition du programme malveillant et la date de mise en quarantaine. Une fois le fichier sélectionné, vous pouvez le restaurer ou le supprimer.

Les fichiers restaurés sont exemptés de l'analyse automatique tant que l'appareil est déverrouillé. Le fichier sera analysé lors du prochain déverrouillage ou si une analyse manuelle est sélectionnée dans l'onglet Anti-Malware (Anti-logiciels malveillants). Si les définitions de programmes malveillants indiquent toujours que le fichier est infecté, il sera à nouveau mis en quarantaine.

Les fichiers supprimés seront définitivement éliminés.

Assainissement

L'option d'assainissement permet d'effacer en toute sécurité le contenu du lecteur chiffré. Pour ce faire, la clé chiffrée utilisée par le lecteur pour accéder aux fichiers du volume sécurisé est effacée, tout en conservant la connexion à SafeConsole.

Avertissement : L'exécution de cette action effacera complètement toutes les données sur le volume sécurisé. Cette action est permanente.

La possibilité d'assainir un lecteur dépend du paramètre configuré par votre administrateur SafeConsole. Si cela est autorisé, votre lecteur peut être assaini en suivant les étapes suivantes :

1. Déverrouillez votre appareil et ouvrez le panneau de contrôle de l'appareil en lançant IronKey.exe.

2. Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état système du panneau de contrôle et sélectionnez Sanitize Device (Assainir l'appareil).

3. Saisissez les chiffres demandés dans la boîte de dialogue pour confirmer que toutes les données peuvent être effacées du lecteur.

4. L'appareil se réinitialise. Débranchez et rebranchez votre appareil sur votre station de travail.

5. Lancez IronKey.exe et saisissez le mot de passe de l'appareil.

Utilisation de ZoneBuilder dans SafeConsole

S'il est activé par votre administrateur système, ZoneBuilder est un outil SafeConsole utilisé pour créer une zone de confiance d'ordinateurs. Il peut être utilisé pour limiter l'accès de l'appareil aux ordinateurs de la zone de confiance et, s'il est activé, peut déverrouiller automatiquement votre appareil, ce qui élimine la nécessité de saisir votre mot de passe.

Si votre administrateur décide d'activer cette stratégie, il se peut que vous deviez définir le compte comme étant de confiance. Définir le compte comme étant de confiance :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans le panneau de contrôle IronKey.
2. Cliquez sur **ZoneBuilder** dans la barre latérale gauche.
3. Cliquez sur **Trust This Account** (Faire confiance à ce compte).
4. Saisissez le mot de passe de l'appareil et cliquez sur OK. Votre compte apparaîtra maintenant dans la section Comptes de confiance.

Votre compte se trouve maintenant dans la zone de confiance d'ordinateurs. En fonction de la stratégie définie par votre administrateur système, il se peut que l'accès à l'appareil soit limité lorsqu'il est en dehors de la zone de confiance ou lorsqu'il est hors ligne. Votre appareil peut également être configuré pour se déverrouiller automatiquement sur les ordinateurs de confiance.

Pour supprimer un compte de confiance, il vous suffit de mettre en surbrillance le compte que vous souhaitez supprimer et de cliquer sur **Remove** (Supprimer).

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. Certaines politiques relatives aux appareils managed, définies par l'administrateur système, peuvent restreindre l'utilisation de votre appareil aux seuls systèmes Windows ou macOS.

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 d'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.
6. Politiques qui bloqueront l'appareil.
   - Si l'appareil est désactivé dans les paramètres de politique de SafeConsole, vous ne pourrez pas déverrouiller l'appareil.

Où puis-je obtenir de l'aide ?

Les ressources suivantes fournissent plus d'informations sur les produits IronKey. Veuillez contacter votre service d'assistance ou votre administrateur système si vous avez d'autres questions.

- 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™ S1000E
DRIVE FLASH USB 3.2 Gen 1 CRITTOGRAFATO

Guida per l’utente

Sommario

Informazioni sulla presente guida (04152025)

IronKey™ S1000E è un drive gestito che richiede una licenza e può essere gestito mediante SafeConsole. SafeConsole è una piattaforme di gestione sicura disponibile in cloud o in locale, che consentono alle aziende di gestire in modo centralizzato dispositivi di storage USB (Universal Serial Bus) compatibili con la massima semplicità ed efficienza.

Questa guida illustra le procedure per inizializzare e configurare un drive S1000E su SafeConsole, in modo che diventi un drive 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:
    - Windows: Start > Questo PC > IronKey Unlocker > IronKey.exe
    - 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, in modo che 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 S1000E 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 S1000E 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 reimpostazione. **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.
NOTA: gli amministratori possono reimpostare la password tramite SafeConsole.

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 dispositivo

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
Interfaccia / Tipo di connettore / Velocità**	USB 3.2 Gen 1 / Type-A - 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; MILSTD-810F

Temperatura	Funzionamento: da 0°C a 50°C; Conservazione: da -20 °C a 85°C
Crittografia hardware	256-bit AES (modalità XTS)
Certificazioni chiave	FIPS 140-2 di livello 3 Certificazione di conformità TAA/CMMC. Assemblato negli Stati Uniti
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 limitata

Progettati e assemblati negli Stati Uniti, i dispositivi S1000E 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. Nessuna funzionalità di gestione online.

Best practice raccomandate

1. Bloccare il dispositivo:
   - quando non in uso
   - prima di disconnetterlo
   - 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 S1000E, 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 S1000E 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 S1000E 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.

Configurazione di un dispositivo S1000E con SafeConsole

La procedura di inizializzazione inizia preparando il dispositivo a comunicare con il server SafeConsole. I passi necessari per registrare un dispositivo S1000E su SafeConsole dipendono dai criteri adottati dall'amministratore. Non tutte le finestre di dialogo vengono visualizzate.

È necessario utilizzare un Token di connessione SafeConsole. Il token di connessione SafeConsole può essere ottenuto dall'amministratore di sistema attraverso la guida di connessione rapida situata all'interno dell'interfaccia utente di SafeConsole.

1. Immettere il token di connessione SafeConsole precedentemente ottenuto mediante la procedura di cui sopra. Leggere l'accordo di licenza; spuntare la casella di selezione per accettare i termini e le condizioni e fare clic su **Activate** (Attiva) nell'angolo inferiore sinistro.

   • **Criteri opzionali** - Questi possono essere attive o meno a seconda di quanto stabilito dall'amministratore di sistema. Le regole vengono visualizzate durante la registrazione del dispositivo se sono state abilitate.

   - Conferma della proprietà del dispositivo: immettere il nome utente e la password di Windows dell'utente che eseguito l'accesso al computer cui è collegato il dispositivo.

   - Informazioni del dispositivo personalizzate: informazioni obbligatorie relative all'utente o al dispositivo dell'utente. I campi obbligatori potrebbero risultare diversi.

   - Token utente univoco: questo token è direttamente associato all'account dell'utente e sarà fornito dall'amministratore di sistema.

   - Approvazione di registrazione dell'amministratore: l'amministratore di sistema potrebbe richiedere la sua approvazione per procedere alla registrazione del dispositivo.

2. Inserire una password sicura e confermarla. Una volta creata una password conforme ai requisiti previsti e indicati alla destra dei campi di inserimento, fare clic su **Continue** (Continua). I requisiti della password dipendono dalle regole impostate dall'amministratore. È obbligatorio inserire una password composta da almeno 8 caratteri; viene rilevata la differenza tra lettere maiuscole e minuscole e, se è abilitata la funzione Strong Password, potrebbero essere previsti ulteriori requisiti.

3. Selezionare un file system con un volume sicuro (vedere sezione Formattazione del dispositivo) e fare clic su **Continue** (Continua).

4. Il dispositivo procederà ora a finalizzare il processo di configurazione e successivamente sarà pronto per l'uso. Effettuare l'accesso alla partizione di storage crittografato facendo clic sull'icona della cartella visualizzata nel menu in alto. L'accesso alle impostazioni del dispositivo può essere effettuato e le impostazioni modificate facendo clic sull'icona raffigurante un ingranaggio. Per ulteriori informazioni, vedere Pannello di controllo IronKey.

Strong Password

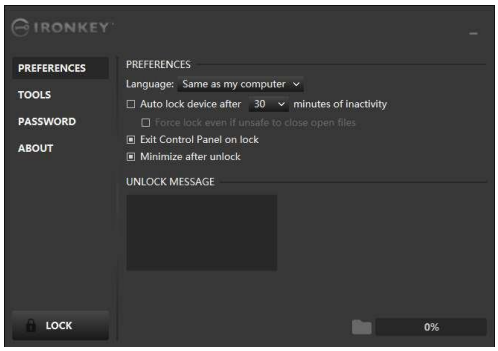
Durante la creazione o la modifica della password del dispositivo, è possibile attivare l'opzione "Enforce Strong Password" (Imponi password più sicure). Nel caso dei dispositivi gestiti, questa opzione può essere configurata o resa obbligatoria dall'amministratore di sistema. Quando è attiva, viene controllato il rispetto delle seguenti regole ad ogni operazione di creazione password.

- Lunghezza minima di otto (8) caratteri.
- Presenza di caratteri provenienti da almeno tre (3) delle seguenti classi di carattere:
  - Numeri ASCII (0123456789) Nota: se l'ultimo carattere della password è un numero ASCII, non viene considerato come numero ASCII richiesto da questa regola.
  - Lettera minuscola ASCII (abc…xyz)
  - Lettera maiuscola ASCII (ABC…XYZ) Nota: Se il primo carattere della password è una lettera maiuscola ASCII, non viene considerato come lettera maiuscola ASCII richiesta da questa regola.
  - Carattere ASCII non alfanumerico (!@#$, ecc.)
  - Caratteri non-ASCII

Esempi di password più sicure

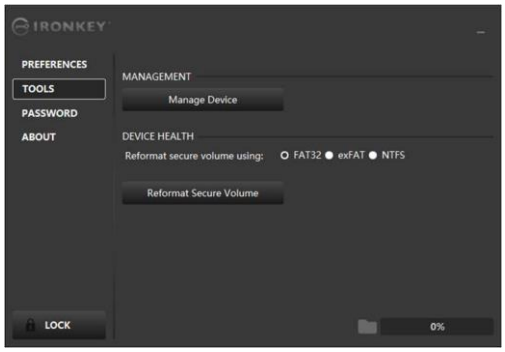
Password di esempio	Risultato
Password	Non valida: è composta da 8 caratteri, ma usa una sola classe di caratteri (lettere ASCII minuscole).
Password1	Non valida: è composta da 9 caratteri, ma la "P" maiuscola e il numero "1" non contano come classi diverse di caratteri, così che la password risulta composta da sole lettere minuscole ASCII.
pa$$Word	Valida: è composta da 8 caratteri. Contiene lettere minuscole ASCII, lettere maiuscole ASCII e caratteri non alfanumerici ASCII.

Pannello di controllo IronKey



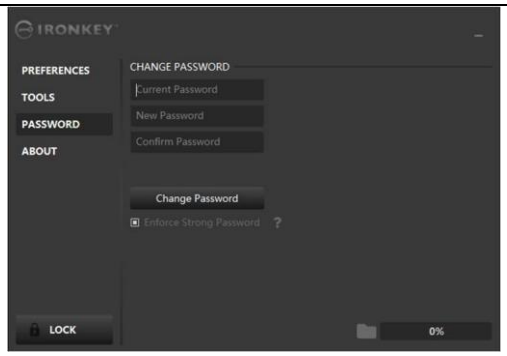
PREFERENCES (preferenze)

1. Language (lingua): modifica la lingua.
2. Auto lock device (blocco automatico del dispositivo): modifica timer di blocco.
3. Exit on Control Panel on lock (Esci 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. UPDATE (aggiornamento): verifica la disponibilità di aggiornamenti.
2. DEVICE HEALTH (stato di salute del dispositivo): riformatta il volume sicuro utilizzando FAT32 o exFAT. (il sistema macOS supporta esclusivamente FAT32).



PASSWORD

1. CHANGE PASSWORD (modifica password): modifica la password di accesso al drive.
2. Enforce Strong Password (imponi password più sicure): attiva/disattiva i requisiti previsti dall'opzione "Strong 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 su **Files** (File) sulla barra dei menu del Pannello di controllo IronKey.
   - Windows: Si aprirà una schermata di Esplora risorse in cui viene visualizzato il drive USB IRONKEY SECURE FILES.
   - macOS: Si aprirà una schermata di 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 S1000EUSB.
   - Per salvare un file, trascinarlo dalla cartella del computer in cui risiede e rilasciarlo nella relativa cartella del drive S1000EUSB.

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. Lo sblocco dei dispositivi gestiti in modalità di sola lettura può essere forzato da un amministratore.

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, se si aggiungono i dati di contatto, sarà possibile visualizzare in che modo un drive smarrito e ritrovato da terzi può essere restituito al padrone. Nel caso dei dispositivi gestiti, queste funzionalità possono essere attive o meno, a seconda di quanto stabilito dall'amministratore di sistema.

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 7 righe e 200 caratteri).

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. Nel caso dei dispositivi gestiti, queste funzionalità possono essere attive o meno, a seconda di quanto stabilito dall'amministratore di sistema.

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).

Nota: i dispositivi gestiti saranno bloccati automaticamente durante l'utilizzo se un amministratore decide di disabilitare l'unità da remoto. In tal caso, non sarà possibile sbloccare il dispositivo fino a quando l'amministratore di sistema non decide di riabilitarlo.

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 USB IRONKEY SECURE FILES; 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.

Le regole di impostazione password sono determinate dall'amministratore di sistema. 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. È obbligatorio inserire una password composta da almeno 8 caratteri; viene rilevata la differenza tra lettere maiuscole e minuscole e, se è abilitata la funzione Strong Password, potrebbero essere previsti ulteriori requisiti.
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 in formato FAT32 o exFAT.

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 eliminerà tutti i file e l'elenco delle applicazioni, ma non eliminerà 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.

L’amministratore di sistema può disabilitare tale opzione. Contattare l’amministratore se è necessario effettuare la reimpostazione del dispositivo.

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 a caso. Una volta inserita la conferma, il dispositivo verrà riportato alla configurazione iniziale di fabbrica.

Nota: se un dispositivo originariamente di tipo standard è stato collegato a un server di gestione, i requisiti di gestione saranno applicati anche dopo la reimpostazione.

Accesso al dispositivo in caso di smarrimento della password

In caso di smarrimento della password, se l’amministratore ha concesso i privilegi di reimpostazione della password all’utente, questi potrà procedere autonomamente alla modifica della password. Se l’amministratore non ha concesso all’utente privilegi di reimpostazione della password, sarà necessario contattare l’amministratore per chiedere il suo intervento qualora si voglia modificare la password.

Per effettuare la reimpostazione della password:

1. Connettere il dispositivo e avviare l’unità IronKey.
2. Fare clic su Password Help (Aiuto password).
3. L’utente potrebbe ricevere una email con le istruzioni su come ottenere il codice di reimpostazione. In caso contrario, sarà necessario contattare l’amministratore per ottenere questo codice. Nell’ultimo caso, l’amministratore di sistema potrebbe richiedere all’utente di fornire il codice di richiesta e il numero di serie. Sarebbe opportuno fare in modo che l’utente sia a conoscenza dell’e-mail e del numero di telefono dell’amministratore di sistema. Facendo clic sull’indirizzo e-mail, si aprirà il client di posta elettronica predefinito e verranno precompilate le informazioni da inviare.
4. Una volta ottenuto, il codice di reimpostazione deve essere copiato e incollato esattamente nel formato originario in cui è stato ricevuto. I codici non corretti fanno parte del conteggio dei dieci tentativi di sblocco, dopo i quali il dispositivo procederà a effettuare il ripristino allo stato iniziale.
5. Immettere la nuova password e confermarla reinserendola nei campi richiesti; quindi fare clic su **Change Password** (Cambia password). Nota: è obbligatorio inserire una password composta da almeno 8 caratteri; viene rilevata la differenza tra lettere maiuscole e minuscole e, se è abilitata la funzione Strong Password, potrebbero essere previsti ulteriori requisiti.

Notifiche relative ai file oggetto di limitazioni

L’amministratore di SafeConsole può configurare il dispositivo in modo che limiti il salvataggio di alcuni file nell’archivio sicuro. In questo caso, si riceve una notifica contenente il nome del file interessato dalla limitazione. È possibile disattivare l’invio di queste notifiche.

NOTA: la disattivazione delle notifiche non ha effetto sulla limitazione dei file che resterà attiva.

Per disattivare le notifiche relative ai file oggetto di limitazioni:

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 “Show restricted files notifications” (Mostra notifiche relative ai file oggetto di limitazioni).

Scansione antimalware del dispositivo

Quando abilitata dall’amministratore di sistema, la scansione antimalware funziona come una tecnologia di disinfezione automatica che rileva e rimuove i malware presenti sul dispositivo e provenienti da file o computer infetti. La funzione antimalware utilizza le tecnologie antimalware e i database delle firme di McAfee® AntiVirus. Tali funzionalità sono costantemente aggiornate per sconfiggere le più recenti minacce malware. Lo scanner verifica prima la presenza di aggiornamenti recenti per poi procedere alla scansione del dispositivo e generare un rapporto, eliminando qualunque traccia di malware rilevata.

L’amministratore di sistema potrebbe imporre che venga eseguito l’aggiornamento della definizione anti-malware per poter sbloccare il dispositivo. In questo caso, è necessario scaricare la versione completa dell’antimalware in una cartella temporanea del computer locale prima di poter inserire la password. La qualità della connessione di rete del computer host e la dimensione degli aggiornamenti del malware potrebbero determinare un allungamento dei tempi necessari allo sblocco del dispositivo.

Alcune cose da sapere sulla funzione di scansione del dispositivo:

- La scansione avviene in maniera automatica quando il dispositivo viene sbloccato.

- La funzione di scansione verifica tutti i file (compressi e non compressi).

- Segnalerà ed eliminerà qualsiasi malware eventualmente rilevato.

- (Facoltativo) Se l’amministratore di SafeConsole ha attivato la funzione di Quarantena, potrà mettere in quarantena i malware eventualmente rilevati. Per ulteriori informazioni, consultare la sezione “Ripristino o cancellazione dei file in quarantena”.

- Lo scanner effettua autonomamente l’aggiornamento prima di ogni scansione, per proteggere il dispositivo e i dati in esso contenuti dalle più recenti minacce malware.

- L’aggiornamento necessita di una connessione a internet. Il dispositivo necessita di almeno 135 MB di spazio libero al fine di poter installare i file con le firme dei malware.

- Il primo aggiornamento può richiedere più tempo per lo scaricamento, in base alla velocità della connessione internet.

- La data dell’ultimo aggiornamento viene visualizzata sullo schermo.

- Se le firme dello scanner non vengono aggiornate per un lungo periodo di tempo, il successivo aggiornamento consisterà in un file di grandi dimensioni il cui download richiederà più tempo.

Ripristino o cancellazione dei file in quarantena

Se l'amministratore di SafeConsole ha attivato la funzione di Quarantena, sarà possibile ripristinare o eliminare i malware eventualmente rilevati. Grazie a questa procedura è possibile ripristinare i documenti validi che McAfee ha invece considerato malware.

NOTA: la Quarantena potrebbe risultare non disponibile per file di grandi dimensioni. I file che non possono essere messi in quarantena vengono direttamente eliminati. Questi file non potranno essere ripristinati tramite il procedimento di seguito indicato.

Per visualizzare i file in quarantena:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni) nel Pannello di controllo IronKey.
2. Fare clic su **Quarantine** (Quarantena) nella barra laterale sinistra.

Selezionare un file dall'elenco per visualizzare i relativi dettagli, quali il nome della minaccia, il tipo di minaccia, la versione della definizione anti-malware e la data in cui è stato messo in quarantena. Dopo aver selezionato il file, è possibile ripristinarlo o eliminarlo.

I file ripristinati mentre il dispositivo è sbloccato non verranno sottoposti alla scansione automatica. La scansione del file avverrà durante lo sblocco successivo o, prima, nel caso si selezioni una scansione manuale dalla scheda Anti-Malware. Se le definizioni anti-malware continuano a considerarlo infetto, il file verrà nuovamente messo in quarantena.

I file eliminati vengono invece eliminati in modo definitivo.

Sanitize (Sanificazione)

Questa funzione consente di cancellare in modo sicuro il contenuto dell'unità crittografata. In questo caso viene cancellata la chiave crittografata utilizzata dall'unità per accedere ai file del volume sicuro, mantenendo comunque la connessione a SafeConsole.

Attenzione: l'esecuzione di questa azione cancella completamente tutti i dati presenti nel volume sicuro. Si tratta di un'azione definitiva.

La possibilità di sanificare un'unità dipende dalla configurazione eseguita dall'amministratore di SafeConsole. Se previsto, l'unità può essere sanificata con i seguenti passaggi:

1. Sbloccare il dispositivo e aprire il Pannello di controllo eseguendo IronKey.exe.
2. Fare clic con il tasto destro del mouse sull'icona della barra delle applicazioni del Pannello di controllo e selezionare Sanitize Device (Sanifica dispositivo).
3. Digitare i numeri visualizzati nella finestra di dialogo per dare conferma che si desidera procedere alla cancellazione definitiva di tutti i dati presenti nell'unità.
4. Il dispositivo verrà ripristinato. Scollegare per poi ricollegare nuovamente il dispositivo alla workstation.
5. Eseguire IronKey.exe e inserire la password del dispositivo.

Utilizzo di ZoneBuilder su SafeConsole

Se viene abilitato dall'amministratore di sistema, è possibile utilizzare lo strumento ZoneBuilder in SafeConsole per creare una zona sicura all'interno dei computer. La funzione può essere utilizzata per limitare l'accesso del dispositivo ai soli computer inclusi nella zona sicura. Inoltre, se abilitata, tale funzione può anche consentire lo sblocco automatico del dispositivo eliminando la necessità di inserire la password.

Se l'amministratore decide di abilitare questa regola, all'utente potrebbe essere chiesto di abilitare l'account. Convalida dell'account:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni) nel Pannello di controllo IronKey.
2. Fare clic su **ZoneBuilder** nella barra laterale sinistra.
3. Fare clic su **Trust This Account** (Convalida questo account).
4. Immettere la password del dispositivo e fare clic su **OK**. L'account sarà ora visualizzato nella casella degli account convalidati, denominata Trusted Accounts.

L'account utente è ora compreso tra quelli facenti parte dei computer della zona sicura (Trusted Zone). In base al tipo di regole impostate dall'amministratore di sistema, l'accesso al dispositivo fuori dalla zona sicura o quando si trova in modalità locale non connessa, può essere soggetto a limitazioni. Il dispositivo può anche essere impostato per lo sblocco automatico sui computer convalidati.

Per rimuovere un account convalidato è sufficiente evidenziarne il nome nell'elenco e fare clic su **Remove** (Rimuovi).

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. Alcune regole relative ai dispositivi gestiti, impostate dall'amministratore di sistema, possono limitare l'uso del dispositivo ai soli sistemi che utilizzano sistemi operativi Windows o macOS.

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.
6. Regole che bloccano il dispositivo
   - Se il dispositivo è disabilitato mediante le impostazioni delle regole su SafeConsole, l'utente non sarà in grado di sbloccare il dispositivo.

Come ottenere assistenza?

Le seguenti risorse offrono maggiori informazioni sui prodotti IronKey. Contattare l'Help Desk o l'amministratore di sistema qualora fossero necessarie ulteriori informazioni.

- 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™ S1000E
PENDRIVE CRIPTOGRAFADO USB 3.2 Gen 1

Manual do Usuário

Índice

Sobre este Manual (04152025)

O IronKey™ S1000E é um drive gerenciado que precisa de uma licença de dispositivo e pode ser gerenciado pelo SafeConsole. O SafeConsole é uma plataforma segura de gestão local ou com base em nuvem que permite que sua organização gerencie de forma centralizada dispositivos de armazenamento USB (Universal Serial Bus) compatíveis de forma fácil e eficiente.

Este manual explicará como configurar e iniciar um drive S1000E em um SafeConsole para ser um drive 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 S1000E 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 S1000E 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 em 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*.
OBSERVAÇÃO: *Os administradores podem redefinir a senha usando o SafeConsole.*

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 de 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
Interface/Tipo de Conector/Velocidade **	USB 3.2 Gen 1 / Tipo-A - 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 3 metros.; MILSTD-810F

Temperatura	Operacional: 0°C a 50°C ; Armazenamento: -20°C a 85°C
Criptografia de Hardware	256 bits AES (Modo XTS)
Principais Certificações	FIPS 140-2 Nível 3 Em conformidade com TAA/CMMC, montado nos EUA
Compatibilidade de SistOp	- Windows 11, Windows 10 (Precisa de duas letras de drive livres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantia	Limitada de 5 anos

Projetados e montados nos EUA, o dispositivo S1000E 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. Sem funcionalidades de gerenciamento on-line.

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 S1000E, 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 S1000E 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 S1000E 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.

Configurar um dispositivo S1000E com SafeConsole

O processo de inicialização começará permitindo que o dispositivo esteja pronto para se comunicar com o servidor SafeConsole. As etapas necessárias para registrar um S1000E para SafeConsole dependerá das políticas que seu administrador estiver aplicando. Nenhum diálogo será exibido.

Um token de conexão SafeConsole será necessário. O token de conexão SafeConsole é obtido pelo administrador do sistema através do Manual rápido de conexão, localizado dentro da interface do usuário do SafeConsole.

1. Insira o token de conexão do SafeConsole obtido nas etapas abaixo. Revise o acordo de licença, marque a caixa de seleção para aceitá-lo e clique em "**Ativar**" no canto inferior esquerdo.

   • **Políticas habilitadas de forma opcional** - Estas políticas podem ou não ser habilitadas pelo administrador do seu sistema. Elas aparecerão durante o registro do dispositivo se tiverem sido habilitadas.

   - Confirme a propriedade do dispositivo: Insira o nome de usuário e senha do Windows que sejam associados com as credenciais de login do computador no qual o dispositivo é conectado.

   - Personalizar as informações dos dispositivos: Informações necessárias sobre você ou sobre o seu dispositivo. Os campos obrigatórios variam.

   - Token de usuário único: Este token é associado diretamente com a conta do usuário final e será fornecido pelo administrador do sistema.

   - Aprovação de registro do administrador: O administrador do sistema pode precisar dessa aprovação para dar continuidade ao registro do dispositivo.

2. Insira uma senha segura e confirme-a. Uma vez que a senha criada atender aos requisitos listados no lado direito dos campos de entrada, clique em "Continuar". Os requisitos desta senha dependerão da política selecionada por seu administrador. As senhas são sensíveis a maiúsculas e minúsculas e precisam ter pelo menos 8 caracteres juntamente com mais requisitos se a Senha Forte estiver ativada.

3. Escolha um sistema de arquivo de volume seguro (veja Formatar meu dispositivo) e clique em "**Continuar**".

4. O dispositivo encerrará o processo de instalação e estará pronto para uso. Acesse o Armazenamento criptografado clicando no **ícone de pasta** no menu superior. As configurações do dispositivo podem ser acessadas e alteradas clicando no **ícone de engrenagem**. Veja o Painel de controle IronKey para obter mais informações.

Senha forte

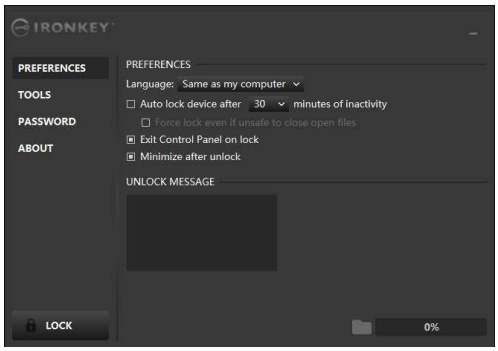
Ao criar ou alterar a senha para o dispositivo, há uma opção para ativar Enforce Strong Password (Aplicar Senha Forte). Para dispositivos gerenciados esta opção pode ser configurada ou aplicada pelo administrador do seu sistema. Quando ativada, as seguintes regras são verificadas em relação a todas as possíveis senhas.

- Deve ter pelo menos oito (8) caracteres.
- Deve incluir caracteres de, pelo menos, três (3) das seguintes classes de caracteres:
  - Dígitos ASCII (0123456789) Observação: Se o último caractere da senha for um dígito ASCII, ele não conta como um dígito ASCII para esta restrição.
  - ASCII minúscula (abc... xyz)
  - ASCII maiúscula (ABC... XYZ) Observação: Se o primeiro caractere da senha for um letra letra maiúscula ASCII, ele não conta como um letra letra maiúscula ASCII para esta restrição.
  - ASCII não-alfanumérico (!@#$, etc)
  - Caracteres não-ASCII

Exemplos de senha fortes

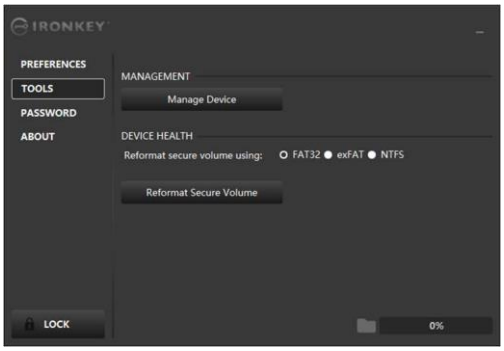
Exemplo de senha	Resultados
Senha	Reprovada: 8 caracteres, no entanto, contém apenas 1 classe de caracteres únicos (ASCII minúsculas).
Senha1	Reprovada: 9 caracteres, no entanto, o ‘S maiúsculo e o ‘1 não contam para as classes de caracteres únicas, sendo apenas ASCII minúsculas.
pa$$Word	Aprovada: 8 caracteres. Contém ASCII minúscula, ASCII maiúscula e ASCII não-alfanumérico.

Idioma: Alterar o idioma do dispositivo



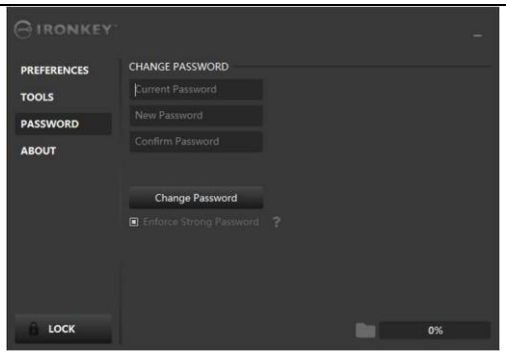
PREFERÊNCIAS

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 Controle quando o dispositivo for desbloqueado ou permitir que fique maximizado.
5. DESBLOQUEAR MENSAGEM: Adicione uma mensagem que será apresentada na janela de login.



FERRAMENTAS

1. ATUALIZAÇÃO: Verifique se há atualizações
2. SAÚDE DO DISPOSITIVO: Reformatar o volume seguro usando FAT32 ou exFAT. (O macOS só permite formatar o FAT32)



SENHA

1. MUDAR SENHA Alterar a senha de login do drive.
2. Aplicar Senha Forte: Ativar/desativar o requisito de senha forte

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 facilita que você trabalhe normalmente como em um drive comum, enquanto tem segurança forte e ininterrupta garantida.

Para acessar seus arquivos seguros:

1. Clique em **Arquivos** na barra do menu do Painel de controle 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 S1000E.
   - Para salvar um arquivo, arraste o arquivo de seu computador para o drive USB S1000E.

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. Os dispositivos gerenciados podem ser forçados a desbloquear para um estado de somente leitura por um administrador.

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 dispositivos gerenciados, esta funcionalidade pode ou não ser habilitada pelo administrador do seu sistema.

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 7 linhas e 200 caracteres).

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. Para dispositivos gerenciados, esta funcionalidade pode ou não ser habilitada pelo administrador do seu sistema.

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**.

Observação: Os dispositivos gerenciados bloquearão automaticamente durante o uso se um administrador desabilitar o dispositivo remotamente. Você não poderá desbloquear o dispositivo até que o administrador do sistema reabilite o 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.

As configurações da política de senha são determinadas pelo administrador do seu sistema. 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. As senhas são sensíveis a maiúsculas e minúsculas e precisam ter pelo menos 8 caracteres juntamente com mais requisitos se a senha forte estiver ativada.
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 inicializar no Windows, você receberá a opção de formatar o drive USB IRONKEY SECURE FILES, assim como FAT32 ou exFAT.

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

Após a inicialização, a reformatação do drive USB IRONKEY SECURE FILES apagará todos os seus arquivos, mas não apaga a senha e as definições do seu 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.

O administrador do seu sistema pode ter esta opção desabilitada. Entre em contato com seu administrador se precisar restaurar seu dispositivo.

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.

Observação: Se o dispositivo era originalmente padrão e conectado a um servidor de gestão, os requisitos de gestão ainda serão aplicados mesmo após uma reconfiguração.

Acessar o meu dispositivo se eu esquecer a minha senha

Se você esquecer sua senha e um administrador der a você privilégios de restauração de senha, você pode restaurá-la. Se seu administrador não deu privilégios de restauração de senha, você precisa entrar em contato com seu administrador para ajudar a restaurar sua senha.

Para restaurar sua senha:

1. Conecte seu dispositivo e inicie o IronKey.
2. Clique em Ajuda com a senha.
3. Você deve receber um e-mail com instruções de como obter seu código de recuperação. Caso contrário, você precisará contatar seu administrador para obter este código. Neste último caso, você pode precisar fornecer o código da solicitação e o número de série ao seu administrador do sistema. O e-mail e o número de telefone do administrador do sistema devem ser fornecidos para sua conveniência. Clicar no endereço de e-mail irá abrir o seu cliente de e-mail padrão e preencher previamente esta informação a ser enviada.
4. Quando recebido, o código de recuperação precisará ser copiado e colado exatamente como foi dado a você. Códigos incorretos contam dentro das dez tentativas de desbloqueio antes do dispositivo ser restaurado.
5. Digite sua nova senha e confirme-a nos campos fornecidos, depois clique em “**Mudar senha**”. Observação: As senhas são sensíveis a maiúsculas e minúsculas e precisam ter pelo menos 8 caracteres juntamente com mais requisitos se a senha forte estiver ativada.

Notificações de arquivos restritos

Se ativado pelo administrador do SafeConsole, o dispositivo pode impedir que certos arquivos sejam salvos no armazenamento seguro. Quando um arquivo afetado é restrito, você recebe uma notificação contendo o nome do arquivo. Se desejar, pode desativar estas notificações.

OBSERVAÇÃO: Os arquivos afetados continuarão sendo restritos quando as notificações estiverem desativadas.

Para desativar as notificações de arquivos restritos:

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** Mostrar notificações de arquivos restritos.

Escanear o meu dispositivo à procura de malware

Se habilitado pelo administrador do seu sistema, o scanner de malwares é uma tecnologia autolimpante que detecta e remove malwares de seu dispositivo em um computador ou arquivo infectado. Desenvolvido pela base de dados anti-malware e antivírus da McAfee®, e\ constantemente atualizado para combater as últimas ameaças de malware, o scanner primeiro verifica as últimas atualizações, escaneia seu dispositivo e depois reporta e limpa qualquer malware encontrado.

O administrador do sistema pode exigir que a definição anti-malware seja atualizada antes que o dispositivo possa ser desbloqueado. Neste caso, a definição completa do anti-malware terá de ser transferida para uma pasta temporária no computador local antes que a senha possa ser introduzida. Isso pode aumentar o tempo necessário para desbloquear o dispositivo com base na conexão de rede do computador host e no tamanho das atualizações de malware necessárias.

Algumas coisas para estar ciente ao escanear seu dispositivo:

- O scanner roda automaticamente quando você desbloqueia seu dispositivo.
- Ele verifica todos os arquivos integrados (compactados e não compactados).
- Ele irá relatar e excluir qualquer malware detectado.
- (Opcional) Se o administrador do SafeConsole tiver ativado a Quarentena, ele pode colocar em quarentena qualquer malware que encontrar. Para obter mais informações, consulte Restaurar ou excluir um arquivo de quarentena.
- O scanner se atualizará automaticamente antes de cada verificação para proteger você das últimas ameaças de malware.
- Uma atualização precisa de uma conexão à Internet. Garanta um mínimo de 135 MB de espaço livre no dispositivo para acomodar os arquivos de assinatura de malware baixados.
- Sua primeira atualização pode demorar mais tempo para baixar, dependendo da conexão de sua Internet.
- A data da última atualização é exibida na tela.
- Se a verificação estiver muito desatualizada, será preciso baixar um grande arquivo para atualizá-la novamente.

Restaurar ou excluir um arquivo em quarentena

Se o administrador do SafeConsole tiver ativado a Quarentena, você terá a opção de restaurar ou excluir o malware detectado. Este processo ajuda quando a McAfee detecta um documento válido como malware.

OBSERVAÇÃO: Dependendo do tamanho dos arquivos infectados, a quarentena pode não estar disponível. Se o arquivo não puder ser colocado em quarentena, será excluído. Os arquivos excluídos não podem ser restaurados utilizando o seguinte processo.

Para ver arquivos em quarentena:

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

2. Clique em "**Quarentena**" na barra lateral esquerda.

Selecionar um arquivo da lista irá apresentar detalhes adicionais, incluindo Nome da ameaça, Tipo de ameaça, versão da definição anti-malware e a data de quarentena. Depois que o arquivo for selecionado, os arquivos podem ser restaurados ou excluídos.

Os arquivos restaurados estarão isentos da verificação automática enquanto o dispositivo estiver desbloqueado. O arquivo será analisado durante o próximo desbloqueio ou se for selecionada uma verificação manual na guia Anti-Malware. Se as definições anti-malware ainda determinarem que o arquivo está infectado, ele irá colocar o arquivo em quarentena mais uma vez.

Arquivos excluídos serão permanentemente excluídos.

Limpeza

A Limpeza permite que o conteúdo do drive criptografado seja apagado de forma segura. Isso é feito ao apagar a chave criptografada que o drive usa para acessar arquivos no Secure Volume enquanto mantém a conexão ao SafeConsole.

Aviso: Executar esta ação irá apagar completamente todos os dados no Secure Volume. Esta ação é permanente.

A capacidade de limpar um drive depende da configuração definida pelo administrador do SafeConsole. Se permitido, seu drive pode ser limpo através dos seguintes passos:

1. Desbloqueie o seu dispositivo e abra o Painel de Controle do dispositivo, iniciando o IronKey.exe.

2. Clique com o botão direito do mouse no ícone da barra de tarefas do Painel de Controle e selecione Limpar Dispositivo.

3. Digite os números solicitados na caixa de diálogo para confirmar que todos os dados podem ser apagados do drive.

4. O dispositivo será restaurado. Desconecte e conecte o dispositivo novamente na estação de trabalho.

5. Inicie o IronKey.exe e introduza a senha do dispositivo.

Usar ZoneBuilder em SafeConsole

Se habilitado pelo administrador do seu sistema, o ZoneBuilder é uma ferramenta do SafeConsole usada para criar uma zona de confiança de computadores. Ele pode ser usado para restringir o acesso de dispositivos a computadores dentro da Zona de confiança e, se habilitado, pode desbloquear automaticamente seu dispositivo, eliminando a necessidade de inserir sua senha.

Se seu administrador escolher habilitar esta política, você pode precisar verificar a conta. Aprovar a conta:

1. Desbloqueie seu dispositivo e clique em "**Configurações**" no Painel de controle IronKey.
2. Clique em "**ZoneBuilder**" na barra lateral esquerda.
3. Clique em **Trust This Account** (Aprovar esta conta).
4. Introduza a senha do dispositivo e clique em **OK**. Sua conta agora aparecerá na caixa de "Contas de confiança".

Sua conta está agora na Zona de confiança dos computadores. Dependendo da política configurada pelo administrador do seu sistema, você pode ter acesso restrito ao dispositivo fora da Zona de confiança ou quando estiver off-line. Seu dispositivo também pode ser configurado para desbloquear automaticamente em computadores de confiança.

Para remover uma conta de confiança, basta destacar a conta que deseja remover e clicar em "**Remover**".

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. Algumas políticas de dispositivo gerenciado, configuradas pelo administrador do sistema, podem restringir o uso do dispositivo para sistemas rodando apenas sistemas operacionais Windows ou maOS.

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.
6. Políticas que bloquearão o dispositivo.
   - Se o dispositivo for desabilitado dentro das configurações da política em SafeConsole você não poderá desbloquear o dispositivo.

Onde posso obter ajuda?

Os seguintes recursos fornecem mais informações sobre os produtos IronKey. Entre em contato com a Assistência técnica ou Administração do sistema se tiver mais perguntas.

- kingston.com/usb/encrypted_security: Informações, materiais de marketing e tutoriais em vídeo.
- kingston.com/support: Suporte de produto, Perguntas frequentes e downloads

OBSERVAÇÃO: Kingston 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™ S1000E
SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

Instrukcja obsługi

Spis treści

Informacje o instrukcji obsługi (04152025)

IronKey™ S1000E to pamięć zarządzana, który wymaga licencji na korzystanie z urządzenia i może być zarządzana w systemie SafeConsole. SafeConsole to bezpieczna platforma do zarządzania w chmurze lub w siedzibie firmy, która umożliwia organizacji łatwe i efektywne centralne zarządzanie zgodnymi urządzeniami pamięci masowej USB (Universal Serial Bus).

W tej instrukcji wyjaśniono, w jaki sposób należy skonfigurować i zainicjować pamięć S1000E w systemie SafeConsole, aby mogła pełnić funkcję pamięci zarządzanej.

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 S1000E USB 3.2 Gen 1 to przenośna pamięć flash z wbudowanymi funkcjami ochrony hasłem i szyfrowania danych. Wyposażono ją w zaawansowaną funkcję szyfrowania 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 S1000E 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.
UWAGA: administrator może zresetować hasło, korzystając z systemu SafeConsole.

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
Interfejs/typ złącza/szybkość**	USB 3.2 Gen 1 / Type-A - 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; MILSTD-810F

Temperatura	Temperatura pracy: 0°C do 50°C; przechowywanie: -20°C do 85°C
Szyfrowanie sprzętowe	256-bitowe AES (tryb XTS)
Certyfikaty klucza	FIPS 140-2 Level 3 Zgodność z wymogami TAA/CMMC, produkt montowany w USA
Zgodność z systemami operacyjnymi	- Windows 11, Windows 10 (wymaga dwóch wolnych liter dysku) - macOS 12.x – 15.x - Linux 4.4.x***
Gwarancja	5-letnia, ograniczona

Zaprojektowane i zmontowane w USA urządzenia S1000E 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. Brak funkcji zarządzania przez Internet.

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 S1000E, 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 S1000E 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 różnić się 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 S1000E 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.

Konfigurowanie urządzenia S1000E w systemie SafeConsole

Proces inicjalizacji rozpocznie się od ustawienia urządzenia w stan gotowości do komunikacji z serwerem SafeConsole. Czynności niezbędne do zarejestrowania pamięci S1000E w systemie SafeConsole będą zależały od zasad określonych przez administratora. Nie wszystkie okna dialogowe zostaną wyświetlone.

Wymagany będzie token łączności SafeConsole. Token łączności SafeConsole uzyskuje administrator systemu w sposób opisany w skróconej instrukcji nawiązywania połączenia (Quick Connect Guide) w interfejsie użytkownika systemu SafeConsole.

1. Wprowadź token łączności SafeConsole uzyskany w sposób opisany powyżej. Zapoznaj się z umową licencyjną, zaznacz pole wyboru, aby ją zaakceptować, i kliknij przycisk Activate (Aktywuj) w lewym dolnym rogu.

   • **Optionally Enabled Policies** (Zasady włączane opcjonalnie) – zasady te mogą, ale nie muszą zostać włączone przez administratora systemu. Będą one wyświetlane podczas rejestracji urządzenia, jeśli zostały włączone.

   - Confirm Ownership of the device (Potwierdź własność urządzenia): wprowadź nazwę użytkownika i hasło do systemu Windows, które są powiązane z poświadczeniami logowania komputera, do którego podłączone jest urządzenie.

   - Custom Device Information (Niestandardowe informacje o urządzeniu): wymagane informacje o użytkowniku lub urządzeniu. Wymagane pola mogą się różnić.

   - Unique User Token (Unikalny token użytkownika): token ten jest bezpośrednio związany z kontem użytkownika końcowego i zostanie dostarczony przez administratora systemu.

   - Administrator Registration Approval (Zatwierdzenie rejestracji przez administratora): administrator systemu może wymagać zgody na rejestrację urządzenia.

2. Wprowadź bezpieczne hasło i potwierdź je. Jeśli utworzone hasło spełnia wymagania wymienione po prawej stronie pól wprowadzania danych, kliknij przycisk Continue (Kontynuuj). Wymagania dotyczące hasła będą zależały od zasad określonych przez administratora. W hasłach rozróżniana jest wielkość liter i muszą one składać się z co najmniej 8 znaków, a jeśli włączona jest opcja Strong Password (Silne hasło) – muszą spełniać więcej wymagań.

3. Wybierz system plików dla bezpiecznego woluminu (patrz Formatowanie urządzenia) i kliknij **Continue** (Kontynuuj).

4. Urządzenie zakończy proces konfiguracji i będzie gotowe do użycia. Aby uzyskać dostęp do szyfrowanej pamięci, kliknij **ikonę folderu** w górnym menu. Aby przejść do ustawień urządzenia i zmienić je, kliknij **ikonę koła zębatego**. Więcej informacji zawarto w części Panel sterowania IronKey.

Silne hasło

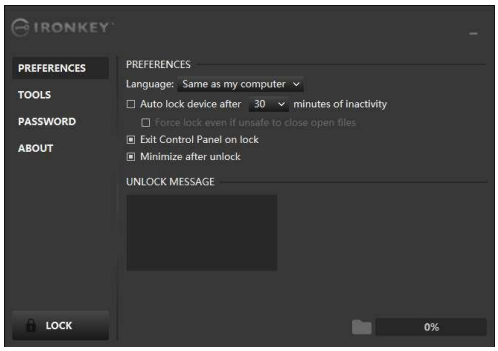
Podczas tworzenia lub zmiany hasła do urządzenia istnieje możliwość włączenia opcji Enforce Strong Password (Wymuszenie silnego hasła). W przypadku urządzeń zarządzanych opcję tę może włączyć administrator systemu. Po włączeniu tej opcji poniższe reguły będą odnosić się do wszystkich potencjalnych haseł.

- Hasło musi mieć długość co najmniej ośmiu (8) znaków.
- Hasło musi zawierać znaki z co najmniej trzech (3) następujących klas znaków:
  - cyfry ASCII (0123456789) Uwaga: jeśli ostatni znak hasła jest cyfrą ASCII, w przypadku tego ograniczenia nie jest on liczony jako cyfra ASCII.
  - małe litery ASCII (abc…xyz)
  - wielkie litery ASCII (ABC…XYZ) Uwaga: jeśli pierwszy znak hasła jest wielką literą ASCII, w przypadku tego ograniczenia nie jest on liczony jako wielka litera ASCII.
  - niealfanumeryczny znak ASCII (!@#$ itp.)
  - inne znaki niż ASCII

Przykłady silnych haseł

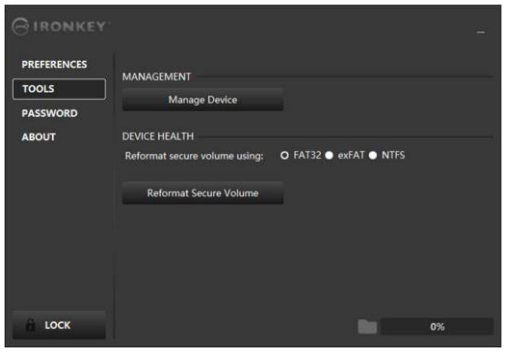
Przykładowe hasło	Rezultat
Password	Nieprawidłowe: długość 8 znaków, jednak zawiera tylko jedną unikalną klasę znaków (małe litery ASCII).
Password1	Nieprawidłowe: długość 9 znaków, jednak duża litera „P” i cyfra „1” nie wliczają się do unikalnych klas znaków, więc pozostają tylko małe litery ASCII.
pa$$Word	Prawidłowe: długość 8 znaków. Zawiera małe litery ASCII, wielkie litery ASCII i niealfanumeryczne znaki ASCII.

Panel sterowania IronKey



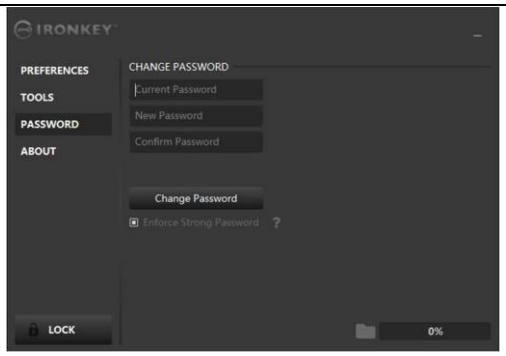
PREFERENCES (PREFERENCJE)

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. UPDATE (AKTUALIZACJA): sprawdzenie dostępności aktualizacji
2. DEVICE HEALTH (KONDYCJA URZĄDZENIA): ponowne formatowanie bezpiecznego woluminu przy użyciu systemu plików FAT32 lub exFAT (w systemie macOS możliwe jest tylko formatowanie FAT32).



PASSWORD (HASŁO)

1. CHANGE PASSWORD (ZMIANA HASŁA): zmiana hasła logowania do pamięci.
2. Enforce Strong Password (Wymuszenie silnego hasła): włączenie/wyłączenie wymogu wprowadzenia silnego hasła

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 przycisk **Files** (Pliki) na pasku menu w 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 S1000E.
   - Aby zapisać plik, przeciągnij go z komputera do okna pamięci USB S1000E.

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. Administrator może wymusić uruchomienie zarządzanego urządzenia w trybie tylko do odczytu.

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. W przypadku urządzeń zarządzanych funkcję tę może włączyć administrator systemu.

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. 7 wierszy i 200 znaków).

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. W przypadku urządzeń zarządzanych funkcję tę może włączyć administrator systemu.

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).

Uwaga: urządzenie zarządzane zostanie automatycznie zablokowane podczas użytkowania, jeśli administrator wyłączy je zdalnie. Urządzenie będzie można odblokować dopiero po ponownym włączeniu go przez administratora systemu.

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.

Ustawienia zasad dotyczących haseł są określane przez administratora systemu. Czasem zmiana hasła jest wymagana w celu zapewnienia zgodności z nowymi zasadami dotyczącymi haseł, które wprowadzono w 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.

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. W hasłach rozróżniana jest wielkość liter i muszą one składać się z co najmniej 8 znaków, a jeśli włączona jest opcja Strong Password (Silne hasło) – muszą spełniać więcej wymagań.
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 lub exFAT.

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 usunięcie wszystkich plików, jednak bez wpływu na hasło i ustawienia 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.

Administrator systemu może wyłączyć tę opcję. W przypadku konieczności zresetowania urządzenia skontaktuj się z administratorem.

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.

Uwaga: jeśli urządzenie było pierwotnie urządzeniem standardowym i zostało podłączone do serwera zarządzania, wymagania związane z zarządzaniem będą egzekwowane nawet po zresetowaniu urządzenia.

Dostęp do urządzenia w przypadku utraty hasła

Jeśli zapomnisz hasło, a administrator przydzieli Ci uprawnienia resetowania hasła, możesz je zresetować. Jeśli administrator nie nadał uprawnień do resetowania hasła, skontaktuj się z administratorem w celu uzyskania pomocy.

Aby zresetować hasło:

1. Podłącz urządzenie i uruchom pamięć IronKey.
2. Kliknij przycisk Password Help (Pomoc dotycząca hasła).
3. Możesz otrzymać wiadomość e-mail ze wskazówkami dotyczącymi sposobu uzyskania kodu odzyskiwania. W przeciwnym razie skontaktuj się z administratorem w celu otrzymania kodu. W tym przypadku może być konieczne podanie administratorowi kodu zgłoszenia i numeru seryjnego. Dla wygody użytkownika zaleca się podanie adresu e-mail i numeru telefonu administratora systemu. Kliknięcie adresu e-mail spowoduje otwarcie domyślnego klienta poczty e-mail i automatyczne wprowadzenie informacji do wysłania.
4. Po otrzymaniu kodu odzyskiwania należy skopiować go i wkleić dokładnie w takiej postaci, w jakiej go podano. Można podjąć dziesięć nieudanych prób odblokowania, po czym urządzenie zostanie zresetowane.
5. Wpisz nowe hasło i potwierdź je w odpowiednich polach, a następnie kliknij przycisk **Change Password** (Zmień hasło). Uwaga: w hasłach rozróżniana jest wielkość liter i muszą one składać się z co najmniej 8 znaków, a jeśli włączona jest opcja Strong Password (Silne hasło) – muszą spełniać więcej wymagań.

Powiadomienia o plikach objętych ograniczeniem

Jeśli administrator systemu SafeConsole włączył tę opcję, urządzenie może ograniczać zapisywanie niektórych plików w bezpiecznej pamięci. Jeśli dany plik podlega ograniczeniu, wyświetla się powiadomienie z nazwą pliku. W razie potrzeby można wyłączyć wyświetlanie tych powiadomień.

UWAGA: niezależnie od wyłączenia powiadomień określone pliki będą nadal podlegać ograniczeniu.

Aby wyłączyć powiadomienia o plikach objętych ograniczeniem:

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** dla opcji Show restricted files notifications (Wyświetlaj powiadomienia o plikach objętych ograniczeniem).

Skanowanie urządzenia w poszukiwaniu złośliwego oprogramowania

Skaner malware to technologia samooczyszczania, która wykrywa i usuwa z urządzenia złośliwe oprogramowanie z zainfekowanego pliku lub komputera. Funkcję włącza administrator systemu. Skaner, korzystający z bazy sygnatur McAfee® AntiVirus i Anti-Malware i stale aktualizowany w celu zwalczania najnowszych zagrożeń złośliwym oprogramowaniem, najpierw sprawdza dostępność najnowszych aktualizacji i skanuje urządzenie, a następnie raportuje i usuwa wykryte złośliwe oprogramowanie.

Administrator systemu może wymagać aktualizacji definicji ochrony przed złośliwym oprogramowaniem przed odblokowaniem urządzenia. W takim przypadku przed wprowadzeniem hasła konieczne będzie pobranie pełnej definicji ochrony przed złośliwym oprogramowaniem do tymczasowego folderu na lokalnym komputerze. W zależności od połączenia sieciowego komputera pełniącego funkcję hosta i rozmiaru pobieranych aktualizacji może to wydłużyć czas potrzebny do odblokowania urządzenia.

Kilka rzeczy, które warto wiedzieć o skanowaniu urządzenia:

- Skaner uruchamia się automatycznie po odblokowaniu urządzenia.

- Skanuje on wszystkie zapisane pliki (skompresowane i nieskompresowane).

- Informuje on o każdym przypadku wykrycia złośliwego oprogramowania i usuwa je.

- (Opcjonalnie) Jeśli administrator systemu SafeConsole włączy tę funkcję, skaner może poddawać wykryte złośliwe oprogramowanie kwarantannie. Aby uzyskać więcej informacji, patrz Przywracanie lub usuwanie pliku poddanego kwarantannie.

- Skaner będzie się automatycznie aktualizował przed każdym skanowaniem, aby zapewniać ochronę przed najnowszymi zagrożeniami ze strony złośliwego oprogramowania.

- Aktualizacja wymaga połączenia z Internetem. Należy zapewnić co najmniej 135 MB miejsca w pamięci, aby umożliwić pobieranie plików sygnatur złośliwego oprogramowania.

- Pierwsze pobieranie aktualizacji może zająć więcej czasu (zależnie od szybkości dostępnego łącza internetowego).

- Data ostatniej aktualizacji jest wyświetlana na ekranie.

- Jeśli skaner nie był długo aktualizowany, będzie musiał pobrać duży plik aktualizacji.

Przywracanie lub usuwanie pliku poddanego kwarantannie

Jeśli administrator SafeConsole włączył funkcję kwarantanny, użytkownik ma możliwość przywrócenia lub usunięcia objętego nią pliku. Jest to pomocne, gdy oprogramowanie McAfee uzna prawidłowy dokument za złośliwe oprogramowanie.

UWAGA: w zależności od rozmiaru zainfekowanych plików funkcja kwarantanny może być niedostępna. Jeśli pliku nie można poddać kwarantannie, zostanie on usunięty. Opisany niżej proces nie pozwala na przywrócenie usuniętych plików.

Aby wyświetlić pliki poddane kwarantannie:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) w panelu sterowania IronKey.
2. Kliknij przycisk **Quarantine** (Kwarantanna) na lewym pasku bocznym.

Wybierz plik z listy, aby wyświetlić dodatkowe szczegóły, w tym nazwę zagrożenia, typ zagrożenia, wersję definicji ochrony przed złośliwym oprogramowaniem oraz datę objęcia kwarantanną. Po wybraniu pliku można go przywrócić lub usunąć.

Przywrócone pliki zostaną wyłączone z automatycznego skanowania, jeśli urządzenie jest aktualnie odblokowane. Plik zostanie przeskanowany przy następnym odblokowaniu lub po wybraniu funkcji skanowania ręcznego na karcie Anti-Malware (Ochrona przed złośliwym oprogramowaniem). Jeśli definicje ochrony przed złośliwym oprogramowaniem znów wykażą, że plik jest zainfekowany, zostanie on ponownie poddany kwarantannie.

Usunięte pliki zostaną wymazane w trwały sposób.

Funkcja czyszczenia

Funkcja czyszczenia umożliwia bezpieczne usunięcie zawartości szyfrowanej pamięci. Odbywa się to poprzez usunięcie klucza szyfrowania, którego używa pamięć, aby uzyskać dostęp do plików zapisanych w bezpiecznym woluminie, przy jednoczesnym zachowaniu połączenia z systemem SafeConsole.

Ostrzeżenie: wykonanie tej czynności spowoduje całkowite usunięcie wszystkich danych z bezpiecznego woluminu. Czynność ta ma nieodwracalne skutki.

Możliwość wyczyszczenia pamięci zależy od ustawień skonfigurowanych przez administratora systemu SafeConsole. Jeśli jest dozwolona, można wyczyścić pamięć, wykonując następujące czynności:

1. Odblokuj urządzenie i otwórz panel sterowania urządzenia, uruchamiając plik IronKey.exe.
2. Kliknij prawym przyciskiem myszy ikonę panelu sterowania w zasobniku systemowym i wybierz opcję Sanitize device (Wyczyść urządzenie).
3. Wprowadź cyfry wyświetlone w oknie dialogowym, aby potwierdzić, że można usunąć wszystkie dane z pamięci.
4. Urządzenie zostanie zresetowane. Odłącz i ponownie podłącz urządzenie do stacji roboczej.
5. Uruchom plik IronKey.exe i wprowadź hasło do urządzenia.

Korzystanie z funkcji ZoneBulider w systemie SafeConsole

Jeśli administrator systemu włączył tę funkcję, ZoneBuilder jest narzędziem systemu SafeConsole służącym do tworzenia zaufanej strefy komputerów. Można jej używać do ograniczenia dostępu urządzenia do komputerów znajdujących się w strefie zaufanej, a jeśli jest włączona, może automatycznie odblokować urządzenie, co eliminuje konieczność wprowadzania hasła.

Jeśli administrator włączy tę zasadę, może być wymagane potwierdzenie zaufania konta. Ustawianie zaufanego konta:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) w panelu sterowania IronKey.
2. Kliknij przycisk **ZoneBuilder** na lewym pasku bocznym.
3. Kliknij przycisk **Trust This Account** (Ustaw konto jako zaufane).
4. Wprowadź hasło do urządzenia i kliknij OK. Twoje konto będzie się teraz wyświetlało w polu Trusted Accounts (Zaufane konta).

Twoje konto znajduje się teraz w strefie zaufanych komputerów. W zależności od zasad ustawionych przez administratora systemu dostęp do urządzenia poza strefą zaufaną lub w trybie offline może być ograniczony. Urządzenie może być również ustawione na automatyczne odblokowywanie na zaufanych komputerach.

Aby usunąć zaufane konto, wystarczy zaznaczyć konto, które ma zostać usunięte, i kliknąć przycisk **Remove** (Usuń).

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. Niektóre zasady dotyczące urządzeń zarządzanych, określone przez administratora systemu, mogą ograniczać korzystanie z urządzenia tylko do platform z systemem operacyjnym Windows lub macOS.

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:To lock the device, you must either unmount and physically remove (unplug) it, or run:

- Unlocker_xx.exe -l

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

1. Należy zwrócić uwagę na następujące ważne szczegóły dotyczące korzystania z urządzenia w systemie Linux:
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.
6. Zasady, które powodują zablokowanie urządzenia.
   - Jeśli urządzenie zostanie wyłączone w ramach ustawień zasad w systemie SafeConsole, nie będzie można odblokować urządzenia.

Jak uzyskać pomoc?

Więcej informacji na temat produktów IronKey jest dostępnych na poniższych stronach. W przypadku dalszych pytań należy skontaktować się ze swoim działem pomocy technicznej lub administratorem systemu.

- 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™ S1000E
ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

ユーザーガイド

目次

このガイドについて (04152025)

IronKey™ S1000E は、デバイスライセンスが必要なマネージドドライブであり、SafeConsole で管理できます。SafeConsole は、クラウドまたはオンプレミスの安全な管理プラットフォームです。企業組織は互換性のある USB ストレージデバイスを簡単かつ効率的に、一括管理できます。

このガイドでは、SafeConsole 上で S1000E ドライブをマネージドドライブに設定し、初期化する方法を説明します。

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ーの USB ポートに差し込みます。
2. デバイスの設定ウィンドウが表示されたら、画面の指示に従います。このウィンドウが表示されない場合は、手動で開きます。
    - 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ら、それ以降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 システムの中には、デバイスを最初に接続した後に再起動を促すものがあります。新しいドライバーやソフトウェアはインストールされないので、再起動せずに安心してプロンプトを閉じてください。

デバイスについて

IronKey S1000E USB 3.2 Gen 1 は、パスワードセキュリティとデータ暗号化の機能を内蔵した、ポータブルフラッシュドライブです。高度な AES 256 ビット暗号化およびモバイルデータのセキュリティを強化する、数々の機能を備えています。これで、ファイルやデータをどこにでも安全に持ち運ぶことができます。

通常の USB ドライブとの違いは何ですか？

FIPS 140-2 Level 3 認証 – IronKey S1000E は FIPS 認証を受けたデバイスであるため、規制要件に準拠しているという安心感があります。

ハードウェア暗号化 – デバイスに搭載された高度暗号化コントローラーは、政府の高度な機密情報と同レベルでデータを保護します。このセキュリティ技術機能は常にオンになっており、無効にすることはできません。

パスワード保護 – デバイスへのアクセスはパスワード保護で守られています。デバイスが紛失または盗難に遭った場合でも、他人がデータにアクセスできないように、パスワードは誰にも教えないでください。

デバイスのリセット – 高度暗号化コントローラーが物理的な改ざんを検出した場合、またはパスワードの連続不正試行回数が 10 回を超えた場合、デバイスはリセットを開始します。重要 - デバイスがリセットされると、オンボード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。
注意： 管理者は SafeConsole を使用してパスワードをリセットできます。

マルウェア防止のオートラン保護 – 未承認プログラムのオートラン実行を検出・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デバイスを保護することができます。また、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でロックを解除することもできます。

シンプルなデバイス管理 – デバイスには、ファイルへのアクセス、デバイスの管理、環境設定の編集、デバイスパスワードの変更、デバイスの安全なロック用のプログラム、IronKey コントロールパネルが付属します。

どのようなシステムで使用できますか？

- Windows®11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x 以降) 注意：Linux CLI Unlocker は、ネットワークアクセスが必要な機能 (デバ · スの設定やパスワードの変更など) には対応していません。

一部の機能は、特定のシステムでのみ使用できます：

Windows のみ

- デバイスのアップデート

製品仕様

デバイスの詳細については、IronKey コントロールパネルの**デバイス情報**ページをご覧ください。

仕様	詳細
容量*	4GB、8GB、16GB、32GB、64GB、128GB
インターフェイス/コネクタータイプ/速度**	USB 3.2 Gen 1 / Type-A - 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
防水性	最大 90 cm（3 フィート、MILSTD-810F)

温度	動作温度：0°C～50°C、保管温度：-20°C～85°C
ハードウェア暗号化	256-bit AES (XTSモード)
キー認証	FIPS 140-2 Level 3 TAA/CMMC 準拠、米国にて製造
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 年限定

米国で設計および組み立てられた S1000E デバイスは、ソフトウェアやドライバのインストールを必要としません。

* 表記容量は概算です。オンボードソフトウェア用に若干のスペースが必要です。
** 速度は、ホストハードウェア、ソフトウェア、および使用状況によって異なります。
*** 機能が制限されます。オンライン管理機能はありません。

推奨ベストプラクティス

1. 以下の場合、デバイスをロックしてください。
   - 使用しないとき
   - プラグを抜く前
   - システムがスリープモードに入る前
2. LED が点灯しているときは、絶対に電源をオフにしないでください。
3. デバイスのパスワードは絶対に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、コンピューター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

S1000E 暗号化 USB ドライブに十分な電力を供給するため、ノートブックやデスクトップの USB 2.0/3.2 Gen 1 ポートに直接挿入してください。キーボードや USB 電源供給ハブなど、USB ポートを備えた周辺機器への接続は避けてください。デバイスの初期設定は、サポートされている Windows または macOS ベースの OS で行う必要があります。

デバイスアクセス (Windows 環境)

1. S1000E 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の利用可能な USB ポートに差し込み、Windows が検出するのを待ちます。

   • Windows 11 および 10 を使用する場合、デバイスドライバーの通知が表示されます。

   • 新しいハードウェアの検出が完了すると、Windows は初期化プロセスの開始を促します。

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。次の空きドライブ文字に応じて、パーティション文字は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わることがあります。下の画像では、ドライブレターは (E:) です。

デバイスアクセス (macOS 環境)

1. S1000E 暗号化 USB ドライブを macOS ノートブックまたはデスクトップの利用可能な USB ポートに接続し、OS が検出するのを待ちます。

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」に表示されます)。ボリュームを強調表示し、Finder ウィンドウで 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。これで初期化プロセスが開始されます。

SafeConsole を使用した S1000E デバイスのセットアップ

初期化プロセスは、デバイスが SafeConsole サーバーと通信できる状態にすることから始まります。S1000E を SafeConsole に登録するために必要な手順は、管理者が実施するポリシーによって異なります。すべてのダイアログが表示されるわけではありません。

SafeConsole 接続トークンが必要です。SafeConsole 接続トークンは、システム管理者が SafeConsole ユーザーインターフェイスのクイック接続ガイドから取得します。

1. 上記の手順で取得した SafeConsole 接続トークンを入力します。ライセンス契約を確認し、同意するチェックボックスをオンにして、左下の「有効化」をクリックします。

   • **オプションで有効にできるポリシー** - これらのポリシーは、システム管理者によって有効にされる場合も、そうでない場合もあります。これらのポリシーが有効になっている場合は、デバイスの登録時に表示されます。

   - デバイスの所有権を確認します：デバイスが接続されているコンピューターのログイン情報に関連付けられている Windows ユーザー名とパスワードを入力します。

   - カスタムデバイス情報：ユーザーまたは使用するデバイスに関する必要な情報。必須フィールドは様々に異なります。

   - ユーザー別のトークン：このトークンは、エンドユーザーのアカウントに直接関連付けられ、システム管理者から提供されます。

   - ユーザー別のトークン：このトークンは、エンドユーザーのアカウントに直接関連付けられ、システム管理者から提供されます。

2. 安全なパスワードを入力し、確認します。作成されたパスワードが入力フィールドの右側に記載されている要件を満たしたら、「続行」をクリックします。このパスワードの要件は、管理者が選択したポリシーによって異なります。パスワードは、強力なパスワードを有効にする場合、大文字と小文字を区別し、8 文字以上でなければなりません。

3. 安全なボリュームファイルシステムを選択し (「デバイスのフォーマット」を参照)、「**続行**」をクリックします。

4. これでデバイスはセットアッププロセスを完了し、使用できるようになります。トップメニューの**フォルダーアイコン**をクリックして、暗号化ストレージにアクセスします。**歯車のアイコン**をクリックすると、デバイスの設定にアクセスし、変更することができます。詳細は IronKey コントロールパネルを参照してください。

強力なパスワード

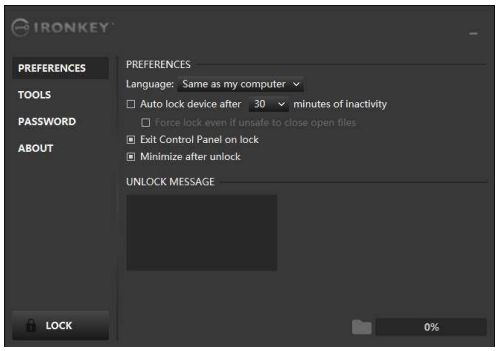
デバイスのパスワードを作成または変更する際に、強力なパスワードの強制を有効にするオプションがあります。マネージドデバイスの場合、このオプションはシステム管理者によって設定または実施されます。このオプションを有効にすると、以下のルールがすべてのパスワード候補に対してチェックされます。

- 長さは8文字以上であること。
- 以下の文字のうち、少なくとも 3 種類を含むこと：
  - ASCII 数字 (0123456789) 注意：パスワードの最後の文字が ASCII 数字の場合、このルールでは ASCII 数字としてカウントされません。
  - 小文字の ASCII (abc...xyz)
  - 大文字の ASCII (ABC...XYZ) 注意：パスワードの最初の文字が大文字の ASCII である場合、このルールでは大文字の ASCII 文字としてカウントされません。
  - 英数字以外の ASCII 文字 (!@#$ など)
  - 非 ASCII 文字

強力なパスワードの例

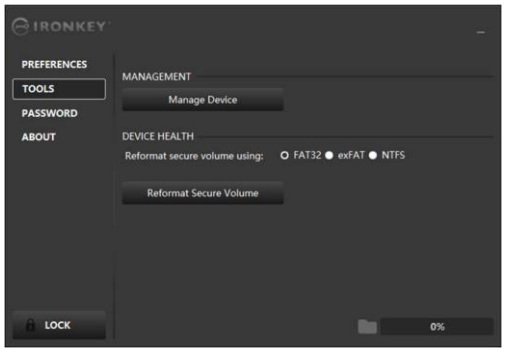
パスワードの例	結果
Password	不合格：8 文字長ですが、文字の種類が 1 つ (小文字の ASCII) しか含まれていません。
Password1	不合格：9 文字長ですが、大文字の‘ P」と‘ 1」は固有の文字とみなされず、小文字の ASCII だけが残ります。
pa$$Word	合格：8 文字。小文字の ASCII、大文字の ASCII、および英数字以外の ASCII を含んでいます。

IronKey コントロールパネル



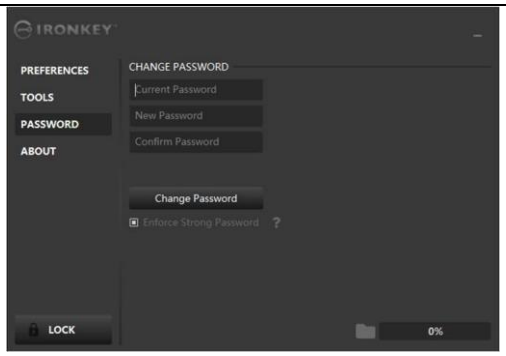
環境設定

1. 言語：デバイスの言語を変更します
2. デバイスを自動ロックする：ロックアウトタイマーを変更します
3. ロック時にコントロールパネルを終了する：デバイスがロックされた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設定します。
4. ロック解除後を最小化する：デバイスのロック解除時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. ロック解除メッセージ：ログイン画面に表示するメッセージを追加します。



ツール

1. 更新：更新を確認します
2. デバイスの正常動作：FAT32 または exFAT 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. パスワードを変更する：ドライブのログインパスワードを変更します。
2. 強力なパスワードを強制する：強力なパスワードを有効化/無効化します

デバイス情報

1. このデバイスについて：デバイスの情報を一覧表示します。
2. ウェブサイトを表示する：Kingston のウェブサイトを起動します
3. 法的通知：Kingston および DataLocker の法的通知ウェブサイトを起動します。
4. 証明書：暗号化された USB デバイス用の Kingston の証明書ページを起動します。

デバイスの使用

デバイスのセキュリティの確認

安全な USB ストレージデバイスが紛失したり、放置された場合は、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。攻撃者によるデバイスの改ざんが疑われる場合、またはセルフテストに失敗した場合は、安全な USB ストレージデバイスを廃棄すること。

- 安全な USB ストレージデバイスに改ざんを示すようなマークや新しい傷がないことを目視で確認します。
- 安全な USB ストレージデバイスを少しひねって、物理的に無傷であることを確認します。
- 安全な 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。
- コンピューターに接続したときに、安全な USB ストレージデバイスの青いインジケーターライトが点滅することを確認する (正しい点滅頻度は、初期接続時および読み取り/書き込み操作時に 1 秒間に 3 回)。
- 安全な 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。
- 仮想 DVD-RW ドライブのデバイスソフトウェアを実行する前に、DataLocker Inc. が発行したものであることを確認します。

安全なファイルへのアクセス

デバイスのロックを解除すると、安全なファイルにアクセスできます。ファイルをドライブに保存したり開いたりすると、ファイルは自動的に暗号化・復号化されます。この技術により、通常のドライブと同じように作業できる利便性と、強力な「常時オン」のセキュリティが実現します。

安全な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メニューバーにある「**ファイル**」をクリックします。
   - Windows：Windows エクスプローラーを開き、IRONKEY SECURE FILES USB ドライブにアクセスします。
   - macOS：KINGSTON USB ドライブの Finder を開きます。
2. 以下のいずれかの操作を行います。
   - ファイルを開くには、S1000E USB ドライブ上のファイルをダブルクリックします。
   - ファイルを保存するには、コンピューターから S1000E USB ドライブにファイルをドラッグします。

ヒント：Windows タスクバーの **IronKey アイコン**を右クリックし、「**安全なファイル**」をクリックしてもファイルにアクセスできます。

読み取り専用モードでのロック解除

読み取り専用モードでデバイスのロックを解除すれば、安全なドライブ上のファイルを変更不能にできます。たとえば、信頼されていないコンピューターや未知のコンピューターを使用する場合、読み取り専用モードでデバイスのロックを解除すると、そのコンピューター上のマルウェアがデバイスに感染したり、ファイルが変更されたりするのを防ぐことができます。マネージドデバイスは、管理者によって読み取り専用状態で強制的にロックを解除することができます。

このモードで作業すると、IronKey コントロールパネルに*読み取り専用モード*という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を変更する操作を実行できません。たとえば、デバイスを再フォーマットしたり、ドライブ上のファイルを編集したりすることはできません。

読み取り専用モードでデバイスのロックを解除するには、以下の手順に従います。

1. デバイスをホストコンピューターの USB ポートに挿入し、**IronKey.exe** を実行します。
2. パスワード入力ボックスの下にある**読み取り専用チェックボックス**をオンにします。
3. デバイスのパスワードを入力し、「**ロック解除**」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」*（Read-Only Mode）と表示されます。

ロック解除メッセージの変更

ロック解除メッセージは、デバイスのロック解除時に IronKey ウィンドウに表示されるカスタムテキストです。この機能により、表示されるメッセージをカスタマイズできます。たとえば、連絡先情報を追加すると、紛失したドライブの返却方法に関する情報が表示されます。マネージドデバイスの場合、この機能はシステム管理者によって有効または無効にされています。

ロック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「**環境設定**」をクリックします。
3. 「アンロックメッセージ」フィールドにメッセージを入力します。テキストは指定されたスペース (約 7 行、200 文字) に収まる必要があります。

デバイスのロック

使用していないときにデバイスをロックして、ドライブ上の安全なファイルへの不要なアクセスを防止します。デバイスを手動でロックすることも、指定した時間操作しないと自動的にロックするように設定することもできます。マネージドデバイスの場合、この機能はシステム管理者によって有効または無効にされています。

注意：デフォルトでは、デバイスが自動ロックを試みたときにファイルやアプリケーショ ンが開いている場合、アプリケーションやファイルを強制的に閉じることはあり ません。デバイスを強制的にロックするように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され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。

強制ロックの手順や、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。

デバイスを手動でロックするには：

1. IronKey コントロールパネルの左下にある「**ロック**」をクリックし、デバイスを安全にロックします。
   - キーボードショートカットを使用することもできます。**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、「**デバイスをロック**」をクリックします。

注意：マネージドデバイスは、管理者がリモートでデバイスを無効にすると、使用中に自動的にロックされます。システム管理者がデバイスを再度有効にするまで、デバイスのロックを解除することはできません。

デバイスを自動的にロックするように設定するには：

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「**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**チェックボックス**をクリックし、タイムアウトを5、15、30、60、120、180 分のいずれかの間隔に設定します。

CHKDSK を実行するには (Windows のみ)：

1. デバイスのロックを解除します。
2. WINDOWS ロゴキー + R を押して、Run プロンプトを開きます。
3. 「CMD」と入力して ENTER を押します。
4. コマンドプロンプトで、「CHKDSK」、IRONKEY SECURE FILES USB のドライブ文字、「/F /R」を入力します。 たとえば、IRONKEY SECURE FILES USB ドライブ文字が「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ます。

ロック時にコントロールパネルを終了する

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。必要に応じて、ユーザーがデバイスをロックした後に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。

ロック時にコントロールパネルの終了を無効化するには：

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「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」のチェックボックスをクリックします。

パスワードの管理

デバイスのパスワードは、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変更できます。

パスワードポリシーの設定はシステム管理者によって決定されます。企業の新しいパスワードポリシーに準拠するために、パスワードの変更が必要になる場合があります。変更が必要な場合は、次回デバイスのロックを解除したときにパスワード変更画面が表示されます。デバイスが使用中の場合はロックされ、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. 表示されたフィールドに現在のパスワードを入力します。
4. 表示されたフィールドに新しいパスワードを入力し、確認します。パスワードは、**強力なパスワード**を有効にする場合、大文字と小文字を区別し、8 文字以上でなければなりません。
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

デバイスをファイル保存に使用する前に、初期化時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 または exFAT でフォーマットするオプションが表示されます。

このオプションは Windows OS のみです。macOS は自動的に FAT32 にフォーマットされます。

- FAT32
  - 長所：クロスプラットフォーム互換 (Windows と mac OS)
  - 短所：個々のファイルサイズは 4GB まで
- exFAT
  - 長所：ファイルサイズの制限なし
  - 短所：Microsoft はライセンス義務によって使用を制限
- NTFS
  - 長所：ファイルサイズの制限なし
  - 短所：サポートされている macOS では、読み取り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、すべてのファイルが消去されますが、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 ドライブをクラウドストレージやコンピューターなど別の場所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. 「**デバイスの正常動**作」でファイル形式を選択し、「安全なボリュームを再フォーマット」をクリックします。

デバイスに関する情報の検索

IronKey コントロールパネルの右下にある容量メーターを使って、デバイスのストレージ空き容量を確認できます。緑色の棒グラフは、デバイスの容量を表しています。たとえば、デバイスが満杯の場合、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、残りの空き容量を示します。

デバイスに関する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」セクションには、お使いのデバイスに関する以下の詳細が記載されています。

- 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
- リリース日
- 安全なファイルドライブ文字
- IronKey ドライブ文字
- OS とシステム管理者権限
- 管理コンソール

注意：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ます。

ヒント：「**コピー**」をクリックすると、デバイス情報がクリップボードにコピーされ、電子メールやサポートリクエストに貼り付けることができます。

デバイスのリセット

デバイスを工場出荷時の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が安全に消去され、次回の使用のために新しいセキュリティキーが作成されます。

システム管理者がこのオプションを無効にしている場合があります。デバイスをリセットする必要がある場合は、管理者に連絡してください。

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. 「**デバイスをリセット**」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、ランダムな 4 桁の数字を入力するようポップアップが表示されます。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。

注意：デバイスが元々標準であり、管理サーバーに接続されていた場合、リセット後も管理要件が適用されます。

パスワードを忘れた場合のデバイスへのアクセス

パスワードを忘れてしまい、管理者からパスワードリセット権限を付与されている場合は、パスワードをリセットすることができます。管理者がパスワードリセット権限を付与していない場合は、管理者に連絡してパスワードのリセットを依頼する必要があります。

パスワードをリセットするには：

1. デバイスを接続し、IronKey を起動します。
2. 「パスワードヘルプ」をクリックします。
3. リカバリーコードの取得方法が記載されたメールが届く場合があります。そうでない場合は、管理者に連絡してこのコードを取得する必要があります。後者の場合、リクエストコードとシリアル番号をシステム管理者に提供する必要があるかもしれません。システム管理者のメールと電話番号は、お客様の便宜のために提供する必要があります。メールアドレスをクリックすると、デフォルトのメールクライアントが開き、送信する情報が事前に入力されます。
4. リカバリーコードを受信したら、そのコードをコピーして、指定されたとおりに貼り付ける必要があります。誤ったコードは、デバイスがリセットされるまでの 10 回のロック解除試行回数にカウントされます。
5. 新しいパスワードを入力し、表示されるフィールドで確認してから、「**パスワードを変更**」をクリックします。注意：パスワードは、強力なパスワードを有効にする場合、大文字と小文字を区別し、8 文字以上でなければなりません。

制限付きファイルの通知

SafeConsole 管理者が有効にしている場合、デバイスによって、特定のファイルが安全な ストレージに保存されないように制限されることがあります。対象となるファイルが制限されると、そのファイル名を含む通知が表示されます。必要に応じて、この通知を無効にできます。

注意：通知を無効にしても、影響を受けるファイルは制限されます。

制限されたファイルの通知を無効にするには：

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「**環境設定**」をクリックします。
3. 「制限されたファイルの通知を表示」の**チェックボックス**をクリックします。

デバイスのマルウェア検査

システム管理者が有効にした場合、Malware Scanner は、感染したファイルやコンピューターからデバイス上のマルウェアを検出して削除するセルフクリーニング技術です。McAfee® AntiVirus と Anti-Malware シグネチャデータベースを搭載し、最新のマルウェアの脅威に対処するために常に更新されるこのスキャナーは、まず最新のアップデートをチェックし、デバイスをスキャンした後、検出されたマルウェアを報告し、駆除します。

システム管理者は、デバイスのロックを解除する前にマルウェア対策を更新するよう要求する場合があります。この場合、パスワードを入力する前に、完全なマルウェア対策をローカルコンピューターの一時フォルダーにダウンロードする必要があります。このため、ホストコンピューターのネットワーク接続や必要なマルウェア更新のサイズに応じて、デバイスのロック解除にかかる時間が長くなる可能性があります。

デバイスのスキャンについて知っておくべきこと：

- スキャナーは、デバイスのロックを解除すると自動的に実行されます。
- スキャナーは、すべてのオンボードファイル (圧縮および非圧縮) をスキャンします。
- 検出されたマルウェアはすべて報告され、削除されます。
- (オプション) SafeConsole 管理者が「隔離」を有効にしている場合、検出されたマルウェアを隔離することができます。詳細については、「隔離ファイルの復元または削除」を参照してください。
- 最新のマルウェアの脅威からお客様を保護するために、スキャナーはスキャンの前に自動的に更新を行います。
- 更新にはインターネット接続が必要です。ダウンロードしたマルウェアシグネチャファイルを保存できるように、デバイスに 135 MB 以上の空き容量を確保してください。
- インターネット接続状況によっては、最初の更新のダウンロードに時間がかかる場合があります。
- 最後の更新の日付が画面に表示されます。
- スキャナーがあまりにも古くなった場合、最新の状態に戻すために大きなファイルをダウンロードする必要があります。

隔離されたファイルの復元または削除

SafeConsole の管理者が「隔離」を有効にしている場合、検出されたマルウェアを復元または削除するオプションがあります。このプロセスは、McAfee が有効な文書をマルウェアとして検出した場合に役立ちます。

注意：感染したファイルのサイズによっては、「隔離」を使用できない場合があります。隔離できない場合、ファイルは削除されます。削除されたファイルは、以下のプロセスでは復元できません。

隔離されたファイルを表示するには：

1. デバイスのロックを解除し、IronKey コントロールパネルの「**設定**」をクリックします。
2. 左サイドバーの「**隔離**」をクリックします。

リストからファイルを選択すると、脅威名、脅威の種類、マルウェア対策定義のバージョン、隔離日などの詳細が表示されます。ファイルを選択すると、「復元」または「削除」のいずれかを実行できます。

復元されたファイルは、デバイスのロックが解除されている間、自動スキャン の対象外となります。ファイルは、次回のロック解除時にスキャンされるか、「マルウェア対策」タブで手動スキャンが選択された場合にスキャンされます。マルウェア対策定義がファイルが感染していると判断した場合、ファイルは再度隔離されます。

削除されたファイルは恒久的に削除されます。

サニタイズ

サニタイズにより、暗号化されたドライブのコンテンツが安全に消去されます。これは、SafeConsole への接続を保持したまま、ドライブが安全なボリューム上のファイルへのアクセスに使用する暗号化キーを消去することで実現されます。

警告：この操作を実行すると、安全なボリューム上のすべてのデータが完全に消去されます。この操作はやり直しできません。

ドライブをサニタイズできるかどうかは、SafeConsole 管理者が設定した内容によって異なります。許可されている場合は、次の手順でドライブをサニタイズできます。

1. デバイスのロックを解除し、IronKey.exe を起動してデバイスのコントロールパネルを開きます。
2. コントロールパネルのシステムトレイアイコンを右クリックし、「デバイスをサニタイズ」を選択します。
3. ダイアログボックスに表示される数字を入力し、ドライブからすべてのデータを消去できることを確認します。
4. デバイスがリセットされます。デバイスを取り外し、ワークステーションに接続します。
5. IronKey.exe を起動し、デバイスのパスワードを入力します。

SafeConsole での ZoneBuilder の使用

システム管理者が有効にした場合、ZoneBuilder は、コンピューターの Trusted Zone を作成するために使用される SafeConsole ツールです。このツールを使用して、デバイスへのアクセスを信頼済みゾーン内のコンピューターに制限することができます。また、有効にすると、デバイスのロックが自動的に解除されるため、パスワードを入力する必要がなくなります。

管理者がこのポリシーを有効にした場合、アカウントの信頼が必要になることがあります。アカウントの信頼：

1. デバイスのロックを解除し、IronKey コントロールパネルの「**設定**」をクリックします。
2. 左サイドバーの「**ZoneBuilder**」をクリックします。
3. 「**このアカウントを信頼する**」をクリックします。
4. デバイスのパスワードを入力し、「**OK**」をクリックします。これで、あなたのアカウントが「信頼済みアカウント」ボックスに表示されます。

これであなたのアカウントはコンピューターの信頼済みゾーンに入りました。システム管理者が設定したポリシーによっては、信頼済みゾーン外またはオフライン時のデバイスアクセスが制限される場合があります。また、デバイスが信頼済みコンピューターで自動的にロック解除されるように設定されている場合もあります。

信頼済みアカウントを削除するには、削除するアカウントをハイライトし、「**削除**」をクリックします。

Linux でのデバイスの使用

デバイスは、Linux のいくつかのディストリビューションで使用できます。linux フォルダーには、Unlocker_32.exe と Unlocker_64.exe の 2 つの実行ファイルがあります。このガイドでは、Unlocker_xx.exe をお使いのシステムと互換性のある実行ファイルに置き換えてください。

デバイスは、Windows または macOS OS を使用してセットアップされている必要があります。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。システム管理者によって設定されたマネージドデバイスポリシーの中には、デバイスの使用を Windows または macOS OS を実行しているシステムのみに制限するものがあります。

Unlocker の使用

ファイルにアクセスするには、Linux 用の Unlocker_xx.exe を使用します。お使いの 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 フォルダーにあるプログラム Unlocker_xx.exe を使用するには 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。そうでない場合は、以下のコマンドを使用して、実行前に実行ビットを手動で設定する必要があります。

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

システムに接続されているデバイスが 1 台だけの場合は、引数なしでコマンドシェルからプログラムを実行します (例えば、Unlocker_xx.exe)。すると、ドライブのロックを解除するためのデバイスパスワードの入力を求めるプロンプトが表示されます。複数のデバイスがある場合は、ロックを解除するデバイスを指定する必要があります。

以下は、デバイスソフトウェアで使用可能なパラメーターです。

オプション：

`-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解除

注意：Unlocker_xx.exe は IRONKEY SECURE FILES USB のロックを解除するだけです。マウントする必要があります。最近の Linux ディストリビューションの多くは、これを自動的に行います。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するだけでは、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、以下を実行する必要があります。

- Unlocker_xx.exe -l

Linux でデバイスを使用する場合、以下の重要な点に注意してください：

1. カーネルのバージョンは 4.4.x 以上でなければなりません。
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てください。
   - 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、以下のコマンドを実行する必要があります：mount /dev/[デバイス名] / media/ [マウントされたデバイス名]
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
   - 外付け/USB/デバイスをマウントする権限が必要です。
   - Unlocker を起動するために、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。
   - root ユーザー権限が必要な場合もあります。
5. IronKey for Linux は x86 および x86_64 システムをサポートしています。
6. デバイスをブロックするポリシー。
   - SafeConsole のポリシー設定でデバイスが無効になっている場合、デバイスのロックを解除することはできません。

ヘルプはどこで入手できますか？

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。ご不明な点がございましたら、ヘルプデスクまたはシステム管理者に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

注意：IronKey は、この資料に含まれる技術的または編集上の誤りおよび/または脱落、また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。ここに記載されている情報は、予告なく変更されることがあります。この資料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る情報の正確性を保証することはできません。この文書は情報提供のみを目的としています。IronKey はこの文書において、明示または黙示を問わず、いかなる保証も行うものではありません。IronKey、および IronKey のロゴは Kingston Digital, Inc. およびその子会社の商標です。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 の許可の下で使用されています。All rights reserved.

FCC 情報 このデバイスは FCC 規則パート 15 に準拠しています。操作は、以下の 2 つの条件に従うものとします。(1) このデバイスは有害な干渉を引き起こさないこと、(2) 望ましくない動作を引き起こす干渉を含め、このデバイスは受信した干渉を受け入 れなければならないこと。この装置は、FCC 規則パート 15 に従い、クラス B デジタルデバイスの制限に準拠していることがテストにより確認されています。これらの制限は、住宅での設置において有害な干渉から適切に保護するためのものです。この装置は、無線周波数エネルギーを発生、使用、放射する可能性があり、説明書に従って設置および使用されない場合、無線通信に有害な干渉を引き起こす可能性があります。ただし、特定の設置場所で干渉が発生しないことを保証するものではありません。ラジオやテレビの受信に有害な干渉 (電源を入れたり、切ったりすることで判断できます) を引き起こす場合は、以下の対策により干渉を修正することをお勧めします。

- 受信アンテナの向きを変えるか、場所を変える。
- 装置と受信機の距離を離す。
- 受信機が接続されている回路とは別の回路のコンセントに装置を接続する。
- 販売店または経験豊富なラジオ/テレビ技術者に相談する。

注意：コンプライアンスに責任を持つ当事者によって明示的に承認されていない変更または修正 は、この装置を操作するユーザーの権限を無効にする可能性があります。

IRONKEY™ S1000E
USB 3.2 Gen 1 加密闪存盘

用户指南

目录

关于本指南 (04152025)

IronKey™ S1000E 是一款管理型驱动器，需要设备许可证，并可通过 SafeConsole 进行管理。SafeConsole 是一个安全的云或本地管理平台，它允许您的组织轻松高效地集中管理兼容的 USB（通用串行总线）存储设备。

本指南将介绍如何在 SafeConsole 上设置和初始化 S1000E 闪存盘，使之成为受管理闪存盘。

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 S1000E 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 S1000E 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。
注意： 管理员可以使用 SafeConsole 重置密码。

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
接口/连接器类型/速度**	USB 3.2 Gen 1 / Type-A - 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	深达 3 英尺；MILSTD-810F

温度	操作：0°C 到 50°C；存放：-20°C 到 85°C
硬件加密	256 位 AES（XTS 模式）
按键认证	FIPS 140-2 Level 3 符合 TAA/CMMC 标准，在美国组装
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 年有限保固

S1000E 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。没有在线管理功能。

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. 永远不要在 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 S1000E 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 S1000E 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 S1000E 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。

使用 SafeConsole 设置 S1000E 设备

初始化流程的第一步是让此设备准备好与 SafeConsole 服务器进行通信。向 SafeConsole 注册 S1000E 所需步骤将取决于您的管理员实施的策略。并非所有对话都显示。

需要 SafeConsole 连接令牌。系统管理员通过位于 SafeConsole 用户界面内的快速连接指南来获取 SafeConsole 连接令牌。

1. 输入在上述步骤中获得的 SafeConsole 连接令牌。阅读许可协议，选中复选框以接受协议，然后点击左下角的“**激活**”。

   - **可选启用的策略** - 系统管理员不一定会启用这些策略。如果它们已被启用，则会在设备注册期间出现。

     - 确认设备的所有权：输入与设备所插入的计算机的登录凭据相关联的 Windows 用户名和密码。

     - 自定义设备信息：关于您或您的设备的必要信息。必填字段将有所不同。

     - 唯一用户令牌：此令牌直接与最终用户的帐户相关联，并将由系统管理员提供。

     - 管理员注册审批：系统管理员可能要求他们批准才能继续进行设备注册。

2. 输入安全密码并确认密码。一旦创建的密码满足输入字段右侧列出的要求，点击“继续”。此密码的要求将取决于您的管理员所选的策略。密码区分大小写，并且至少需要 8 个字符，如果启用了“强密码”，则还需要满足更多要求。

3. 选择一个安全卷文件系统（请参阅“格式化我的设备”），然后点击“**继续**”。

4. 此设备现在将完成设置流程，并可以使用。点击顶部菜单中的**文件夹图标**，即可访问加密存储。点击**齿轮图标**可以访问和修改设备的设置。参见 IronKey 控制面板，了解更多信息。

强密码

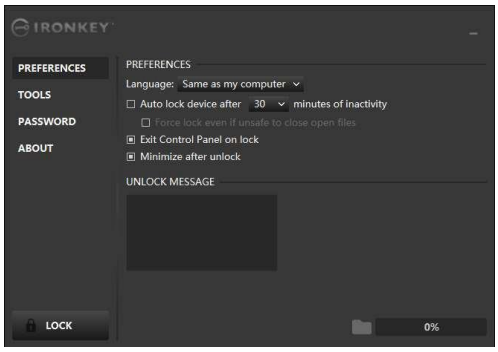
在创建或更改设备密码时，有一个选项可以启用“强制使用强密码”。对于受管理设备，系统管理员可能会配置或强制启用此选项。当启用时，将对所有潜在密码执行以下规则检查。

- 长度必须至少有八 (8) 个字符。
- 必须包含以下字符类别中至少三个 (3) 个字符：
  - ASCII 数字 (0123456789) 注意：如果密码的最后一个字符是 ASCII 数字，则不会计入此限制中的 ASCII 数字。
  - 小写 ASCII (abc…xyz)
  - 大写 ASCII (ABC…XYZ) 注意：如果密码的第一个字符是大写的 ASCII 字母，则不会计入此限制中的大写 ASCII 字母。
  - 非字母数字 ASCII（!@#$ 等）
  - 非 ASCII 字符

强密码示例

示例密码	结果
password	失败：长度为 8 个字符，但仅包含 1 个唯一的字符类别（小写 ASCII 字符）。
Password1	失败：长度为 9 个字符，但是大写字母 ‘P’ 和数字 ‘1’ 不计入独特的字符类别，所以只剩下小写 ASCII 字符。
pa$$Word	通过：8 个字符长。包含小写 ASCII 字母、大写 ASCII 字母和非字母数字 ASCII 字符。Pass: 8 characters long. Contains lowercase ASCII, uppercase ASCII, and non-alphanumeric ASCII.

IronKey 控制面板

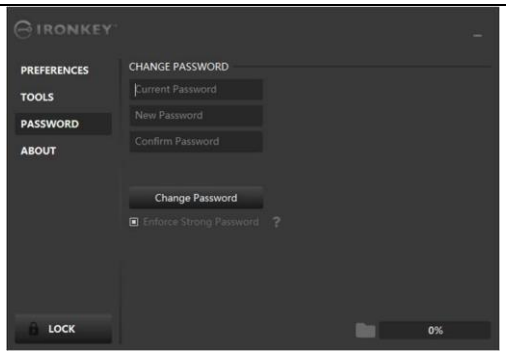


PREFERENCES（首选项）

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. UPDATE（更新）：检查更新
2. DEVICE HEALTH（设备运行状况）：使用 FAT32 或 exFAT 重新格式化安全卷。（macOS 只允许格式化 FAT32）



PASSWORD（密码）

1. CHANGE PASSWORD（更改密码）：更改驱动器登录密码。
2. Enforce Strong Password（强制使用强密码）：启用/禁用强密码要求

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 控制面板的菜单栏上的 **Files**（文件）。
   - 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 S1000EUSB 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 S1000EUSB 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。管理员可以强制要求受管理设备在只读模式下解锁。

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。对于受管理设备，系统管理员不一定会启用此功能。

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 7 行，200 个字符）。

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。对于受管理设备，系统管理员不一定会启用此功能。

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“**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）。

注意：如果管理员远程停用受管理的设备，此设备会在使用期间自动锁定。在系统管理员重新启用此设备前，您将无法解锁设备。

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。

密码策略设置由您的系统管理员确定。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。密码区分大小写，并且至少需要 8 个字符，如果启用了“强密码”，则还需要满足更多要求。
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 或 exFAT。

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）
  - 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 闪存盘将删除您的所有文件，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：

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。

您的系统管理员可能禁用了此选项。如需重置您的设备，请联系您的管理员。

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。

注意：如果该设备原本是标准设备并连接到了管理服务器，即使进行了重置，管理要求仍然会被强制执行。

在忘记密码的情况下访问我的设备

如果您忘记了密码，并且管理员已授予您密码重置权限，您可以重置密码。如果您的管理员没有授予密码重置权限，您必须联系管理员以获取重置密码的帮助。

要重置您的密码：

1. 插入设备并启动 IronKey。
2. 单击 Password Help（密码帮助）。
3. 您可能会收到一封包含如何获取恢复码说明的电子邮件。否则，您需要联系管理员以获取此代码。在后一种情况下，您可能需要向系统管理员提供请求码和序列号。为了方便您，应该已经提供了系统管理员的电子邮件和电话号码。点击电子邮件地址将打开您的默认电子邮件客户端，并预先填写这些信息以便发送。
4. 收到后，复制并粘贴的恢复代码必须与提供给您的恢复代码完全一样。在设备重置之前，不正确的代码将计入十次解锁尝试的次数限制内。
5. 在提供的字段中输入新密码并确认密码，然后单击 **Change Password**（更改密码）。
   注意：密码区分大小写，并且至少需要 8 个字符，如果启用了“强密码”，则还需要满足更多要求。

受限文件通知

如果您的 SafeConsole 管理员已启用此功能，您的设备可能会限制将某些文件保存到安全存储中。当受影响的文件受到限制时，您将收到一个包含文件名的通知。如果需要，您可以禁用这些通知。

注意：禁用通知后，受影响的文件仍然会受到限制。

要禁用受限文件通知：

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. 单击 Show restricted files notifications（显示受限文件通知）**复选框。**

对我的设备执行恶意软件扫描

如果您的系统管理员启用了恶意软件扫描程序，它是一种自我清理技术，可以检测并清除您设备中受感染文件或计算机上的恶意软件。该扫描程序由 McAfee® AntiVirus 和 Anti-Malware 签名数据库提供支持，并且会不断更新以应对最新的恶意软件威胁。扫描程序首先检查最新更新，然后扫描您的设备，接着报告并清除检测到的任何恶意软件。

您的系统管理员可能要求在解锁设备之前更新反恶意软件定义。在这种情况下，需要在输入密码之前将完整的反恶意软件定义下载到本地计算机的临时文件夹中。这可能会增加根据主机计算机的网络连接和所需恶意软件更新的大小来解锁设备所需的时间。

关于设备扫描，您需要了解的一些事情：

- 解锁设备时，扫描程序会自动运行。
- 它会扫描所有板载文件（包括已压缩和未压缩的文件）。
- 它将报告并删除任何检测到的恶意软件。
- （可选）如果您的 SafeConsole 管理员已启用隔离功能，它可能会将找到的任何恶意软件隔离。更多信息，请参阅“恢复或删除隔离文件”。
- 扫描程序将在每次扫描之前自动更新，让您免受最新恶意软件威胁的侵害。
- 更新需要连接互联网。请确保设备上至少有 135MB 的可用空间，以便下载恶意软件签名文件。
- 根据互联网连接速度，首次更新的下载时间可能会很长。
- 最后一次更新的日期会显示在屏幕上。
- 如果扫描程序过于陈旧，它将需要下载一个大文件来更新到最新版本。

恢复或删除隔离的文件

如果您的 SafeConsole 管理员已启用隔离功能，您将可以选择恢复或删除检测到的恶意软件。此过程有助于 McAfee 将有效文档误检测为恶意软件时进行处理。

注意：根据受感染文件的大小，隔离功能可能不可用。如果文件无法被隔离，它将被删除。使用以下过程无法恢复已删除的文件。

要查看隔离的文件：

1. 解锁您的设备，并在 IronKey 控制面板中点击 **Settings**（设置）。
2. 点击左边栏中的 **Quarantine**（隔离）。

从列表中选择一个文件将显示更多详细信息，包括威胁名称、威胁类型、反恶意软件定义版本和隔离日期。选择文件后，可以选择 Restored（恢复）或 Deleted（删除）。

恢复的文件在设备当前解锁时将免于自动扫描。该文件将在下次解锁时或如果从 Anti-Malware（反恶意软件）选项卡中选择手动扫描时进行扫描。如果反恶意软件定义仍然确定该文件已被感染，它将再次隔离该文件。

已删除的文件将被永久删除。

净化

“净化”功能允许安全地擦除加密驱动器的内容。这是通过擦除驱动器用于访问安全卷上文件的加密密钥来实现的，同时仍保持与 SafeConsole 的连接。

警告：执行此操作将完全擦除安全卷上的所有数据。此操作是永久性的。

对驱动器进行净化的能力取决于 SafeConsole 管理员配置的设置。如果允许，您可以通过以下步骤对驱动器进行净化：

1. 解锁您的设备，并通过启动 IronKey.exe 打开设备控制面板。
2. 右键单击系统托盘中的控制面板图标，并选择 Sanitize Device（净化设备）。
3. 在对话框中输入提示的数字，以确认可以擦除驱动器上的所有数据。
4. 设备将重置。拔出设备并重新插入到工作站中。
5. 启动 IronKey.exe 并输入设备密码。

使用 SafeConsole 中的 ZoneBuilder

如果您的系统管理员已启用，ZoneBuilder 是 SafeConsole 中的一个工具，用于创建计算机的受信任区域。它可用于限制设备对受信任区域内计算机的访问，并且如果已启用，可以自动解锁您的设备，从而无需输入密码。

如果您的管理员选择启用此策略，您可能需要信任该帐号。信任帐号：

1. 解锁您的设备，并在 IronKey 控制面板中点击 **Settings**（设置）。
2. 点击左边栏中的 **ZoneBuilder**。
3. 点击 **Trust This Account**（信任此帐号）。
4. 输入设备的密码，然后点击 **OK**（确定）。您的帐号即会显示在 Trusted Accounts（信任的帐号）框中。

您的帐号现已在计算机受信任区中。根据系统管理员设置的策略，您可能在受信任区域之外或离线时受到设备访问的限制。您的设备还可能被设为在受信任计算机上自动解锁。

要移除受信任帐号，只需高亮显示要移除的帐号，并单击 **Remove**（移除）。

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。一些由系统管理员设置的受管理设备策略可能仅允许在运行 Windows 或 macOS 操作系统的系统上运行。

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。
6. 将会阻止设备的策略。
   - 如果设备在 SafeConsole 的策略设置中被禁用，您将无法解锁该设备。

我在哪里可以获取帮助?

以下资源提供关于 IronKey 的更多信息。如有任何进一步的问题，请联系您的帮助台或系统管理员。

- 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™ S1000E
加密 USB 3.2 Gen 1 隨身碟

使用者指南

目錄

關於本指南 (04152025)

IronKey™ S1000E 是需要裝置驗證受管理裝置，可由 SafeConsole 管理。SafeConsole 是一個安全的雲端或本機管理平台，可讓您的組織輕鬆且有效率地集中管理相容的 USB (通用序列匯流排) 儲存裝置。

本指南將說明如何在 SafeConsole 上將 S1000E 隨身碟設定和初始化為受管理隨身碟。

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 S1000E 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 – T IronKey S1000E 是一款經 FIPS 認證、遵循法規要求的裝置，讓您放心使用。

硬體加密 – T 您裝置中的進階加密控制器，以等同高度機密政府資訊的保護等級守護您的資料。此安全技術功能隨時處於啟用狀態，無法停用。

密碼保護 – T 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 – T 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。
附註：*管理者可以使用 SafeConsole 重設密碼。*

防惡意軟體自動執行保護 – T 您的裝置能夠偵測並防範未經核准的程式自動執行，以保護您免受針對 USB 隨身碟的許多最新惡意軟體威脅。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 – T 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
介面/連接器類型/傳輸速度**	USB 3.2 Gen 1 / Type-A - 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；MILSTD-810F

溫度	運作溫度：0°C ~ 50°C；儲存溫度：-20°C 至 85℃
硬體加密	256 位元 AES (XTS 模式)
安全性認證	FIPS 140-2 Level 3 符合 TAA/CMMC 標準，並於美國當地組裝
作業系統	Windows 11、Windows 10 (需要兩個可用的相容磁碟機代號) - macOS 12.x – 15.x - Linux 4.4.x***
保固	5 年有限保固

S1000E 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。無線上管理功能。

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 S1000E 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 S1000E 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 S1000E 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。

使用 SafeConsole 設定 S1000E 裝置

初始化流程將從允許裝置準備好與 SafeConsole 伺服器通訊開始。將 S1000E 註冊到 SafeConsole 所需步驟依系統管理員所執行的政策而定。並非所有對話框都會顯示。

需要一個 SafeConsole 連接權杖。系統管理員可在 SafeConsole 使用者介面中的《快速連接指南》取得 SafeConsole 連接權杖。

1. 輸入在上述步驟中取得的 SafeConsole 連接權杖。查看授權協議，選取對應的核取方塊，接著按一下左下角的「**啟動**」。

   - **(選用) 啟用政策** - 系統管理員可以也可能不會啟用這些政策。如果已啟用，它們將在裝置註冊期間顯示。

     - 確認裝置的所有權：輸入裝置所插入之電腦的登入憑證相關聯的 Windows 使用者名稱和密碼。

     - 自訂裝置資訊：有關您或您裝置的必要資訊。所需欄位會有所不同。

     - 專屬使用者權杖：該權杖是系統管理員所提供，與最終使用者帳戶直接相關連。

     - 系統管理員註冊核准：系統管理員可能需要取得核准才能進行裝置註冊。

2. 輸入一個安全的密碼並確認。輸入的密碼滿足輸入欄位右側所列出的要求後，請按一下「繼續」。密碼的設定要求依系統管理員所選擇的政策而定。密碼區分大小寫，且必須至少包含 8 個字元，如果啟用強式密碼，則會有更多要求。

3. 選擇一個 Secure 磁碟區檔案系統 (請參閱格式化我的裝置)，然後按一下「**繼續**」。

4. 該裝置現在將完成設定流程，並且可以使用。按一下頂部選單中的**資料夾圖示**，可存取加密儲存內容。按一下**齒輪圖示**，可以存取和變更裝置的設定。關於更多資訊，請查看 IronKey 控制面板。

強式密碼

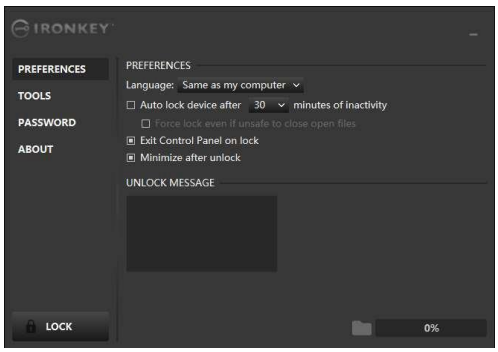
建立或變更裝置密碼時，可選擇啟用強式密碼。對於受管理裝置，此選項可由系統管理員配置或強制執行。啟用後，將根據所有潛在密碼檢查以下規則。

- 長度必須至少為八 (8) 個字元。
- 必須包含至少三 (3) 個以下類別的字元：
  - ASCII 數字 (0123456789) 附註：如果密碼的最後一個字元是 ASCII 數字，則此限制不會將其計為 ASCII 數字。
  - 小寫 ASCII (abc…xyz)
  - 大寫 ASCII (ABC…XYZ) 附註：如果密碼的第一個字元是大寫 ASCII 字母，則此限制不會將其計為大寫 ASCII 字母。
  - 非字母數字 ASCII (!@#$ 等)
  - 非 ASCII 字元

強式密碼範例

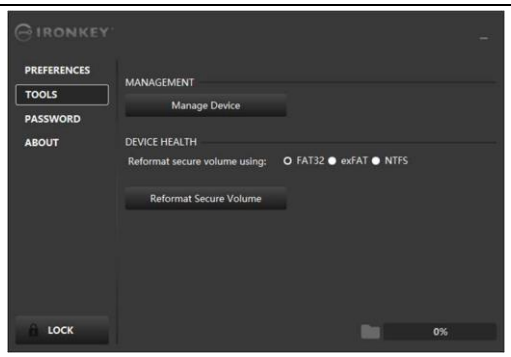
範例密碼	結果
密碼	失敗：8 個字元長度，但僅包含 1 個唯一字元類別 (小寫 ASCII)。
密碼1	失敗：9 個字元長度，但大寫 'P' 和 '1' 不計入唯一字元類別，僅計入小寫 ASCII。
pa$$Word	通過：8 個字元長度包含小寫 ASCII、大寫 ASCII 和非字母數字 ASCII。

IronKey 控制面板



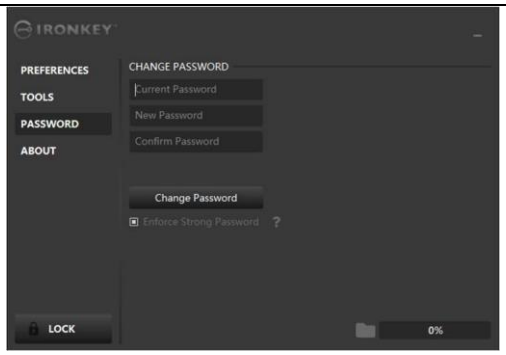
偏好

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. 更新：檢查更新
2. 裝置健康狀態：使用 FAT32 或 exFAT 重新格式化安全磁碟區。(macOS 僅允許格式化 FAT32)



密碼

1. 變更密碼：變更隨身碟登入密碼。
2. 強制使用強式密碼：啟用/停用強式密碼要求

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. 法務聲明：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，確保外觀無被竄改的痕跡或新的刮痕。
- 輕輕扭轉安全 USB 儲存裝置，確認外觀形狀完好。
- 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 控制面板選單欄上的**檔案**。
   - 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 S1000EUSB USB 隨身碟上的檔案。
   - 欲儲存檔案，請將檔案從電腦拖曳到 S1000EUSB USB 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。系統管理員可以強制受管理裝置僅使用唯讀狀態解鎖。

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，或者編輯隨身碟上的檔案。

以唯讀模式解鎖裝置：

1. 將裝置插入電腦的 USB 連接埠，然後執行 **IronKey.exe**。
2. 在輸入密碼欄位下方選取**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。針對受管理裝置，系統管理員可以也可能不會啟用這些功能。

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 7 行和 200 個字元)。

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。針對受管理裝置，系統管理員可以也可能不會啟用這些功能。

注意：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。您可以配置為自動鎖定設定以強制鎖定裝置，但這樣做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**。

附註：如果系統管理員遠端停用裝置，則受管理裝置將在使用過程中自動鎖定。在系統管理員重新啟用裝置之前，您將無法解鎖裝置。

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。

密碼政策設定是由系統管理員決定。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。密碼區分大小寫，且必須至少包含 8 個字元，如果啟用強式密碼，則會有更多要求。
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 或 exFAT。

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 FILESUSB 隨身碟，將執行快速格式化，並擦除所有檔案，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「**裝置資訊**」。

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。

您的系統管理員可能停用了此選項。如果您需要重置裝置，請聯絡系統管理員。

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。

附註：如果裝置最初是標準裝置並連接到管理伺服器，則即便在重置後，仍將強制執行管理要求。

如果忘記密碼，存取我的裝置

如果您忘記密碼，且系統管理員已授予您重置密碼權限，則您可以進行重置。如果您的系統管理員尚未授予重置密碼權限，則您必須聯絡系統管理員，取得重置密碼協助。

若要重設密碼：

1. 請插入裝置並啟動 IronKey。
2. 按一下「**密碼協助**」。
3. 您可能會收到一封電子郵件，其中包含如何取得復原代碼的相關說明。否則，您需要聯絡管理員以取得此代碼。在後者的情況下，您可能需要向系統管理員請求代碼和序號。為了方便起見，應提供您的系統管理員的電子郵件和電話號碼。按一下電子郵件地址，將開啟您的預設電子郵件用戶端，並預先填入要傳送的訊息。
4. 收到復原代碼後，需要完全複製和貼上提供給您的復原代碼。重置裝置之前，您有輸入 10 次不正確代碼解鎖的機會。
5. 輸入您的新密碼並確認所提供欄位中的密碼，然後按一下「**變更密碼**」。附註：密碼區分大小寫，且必須至少包含 8 個字元，如果啟用強式密碼，則會有更多要求。

受限檔案通知

如果您的 SafeConsole 管理員啟用了該功能，您的裝置可能會限制某些檔案儲存到安全儲存。當受影響的檔案受到限制時，您會收到包含文件名稱的通知。如果需要，可以停用這些通知。

附註：停用通知後，受影響的檔案仍將受到限制。

若要停用受限檔案通知：

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. 按一下顯示受限檔案通知的**核取方塊**。

掃瞄我的裝置中是否存在惡意軟體

如果由系統管理員啟用，則惡意軟體掃描程式是一種自我清除技術，可在受感染的檔案或電腦中偵測並刪除裝置上的惡意軟體。由 McAfee®AntiVirus 和 Anti-Malware 資料庫提供支援，並不斷進行更新以應對最新的惡意軟體威脅，該掃描程式首先會檢查最新更新、掃描您的裝置，再報告並清除找到的所有惡意軟體。

您的系統管理員可能會要求先更新防惡意軟體定義，然後才能解鎖裝置。在這種情況下，需要將完整的防惡意軟體定義下載到本機端上的臨時資料夾中，然後才能輸入密碼。根據主機的網路連線和所需的惡意軟體更新大小，可能會增加解鎖裝置所需的時間。

有關掃描裝置的一些注意事項：

- 有關掃描裝置的一些注意事項：
- 掃描所有搭載檔案 (壓縮和未壓縮)。
- 報告並刪除任何偵測到的惡意軟體。
- (可選) 如果您的 SafeConsole 管理員啟用隔離功能，這可能會隔離系統發現的任何惡意軟體。請參閱復原或刪除隔離檔案，以了解詳細資訊。
- 每次掃描前會自動更新掃描程式，保護您免受最新的惡意軟體威脅。
- 更新需要連接網路。請確保裝置上至少有 135 MB 的可用空間，以容納下載的惡意軟體簽署檔案。
- 第一次更新可能需要很長時間才能下載完畢，具體時間依您的網路連接速度而定。
- 最後更新的日期會顯示在畫面上。
- 如果掃描程式過時，則需要下載較大的檔案，使其恢復為最新狀態。

復原或刪除隔離的檔案

如果您的 SafeConsole 管理員已啟用隔離功能，您將可以選擇復原或刪除偵測到的惡意軟體。當 McAfee 將有效文件偵測為惡意軟體時，此流程會有所幫助。

附註：根據受感染檔案的大小而定，可能無法使用隔離功能。如果無法隔離該檔案，則會將其刪除。使用下列流程無法恢復已刪除的檔案。

如要查看隔離的檔案：

1. 解鎖裝置，然後在 IronKey 控制面板中按一下「**設定**」。
2. 按一下左側邊欄中的「**隔離**」。

從清單中選擇一個檔案，將顯示其他詳細資訊，包括威脅名稱、威脅類型、防惡意軟體定義版本和隔離日期。選擇檔案後，可復原或刪除檔案。

當裝置目前解鎖時，復原的檔案將免於自動掃描。在下次解鎖期間或如果從「防惡意軟體」標籤中選擇手動掃描，將掃描該檔案。如果防惡意軟體定義仍然確定該檔案被感染，系統將再次隔離該檔案。

已刪除的檔案將會永久刪除。

Sanitize

Sanitize 可安全擦除加密磁碟機中的內容。這是擦除磁碟機用於存取安全磁碟區上檔案的加密金鑰，藉此達成目的，同時仍保留與 SafeConsole 的連線。

警告：執行此操作將完全擦除安全磁碟區上的所有資料。此操作無法復原。

對隨身碟進行掃毒的能力是根據 SafeConsole 管理員配置的設定而定。如果允許，您的隨身碟以透過以下步驟進行掃毒：

1. 啟動 IronKey.exe，解鎖您的裝置，並開啟裝置控制面板。
2. 右鍵按一下控制台的系統匣圖示，並選擇裝置掃毒。
3. 輸入對話方塊中提示的數字，確認可以擦除磁碟機中的所有資料。
4. 裝置將重置。拔下裝置，並將其重新插入工作站。
5. 啟動 IronKey.exe，並輸入裝置密碼。

在 SafeConsole 中使用 ZoneBuilder

由系統管理員啟用，ZoneBuilder 是用於建立電腦受信任區域的 SafeConsole 工具。它可將裝置限制為存取「受信任區域」內的電腦，如果啟用，它可以自動解鎖裝置，而無需輸入密碼。

如果您的系統管理員選擇啟用此政策，則您可能需要信任該帳戶。信任帳戶：

1. 解鎖裝置，然後在 IronKey 控制面板中按一下「**設定**」。
2. 按一下左側邊欄中的「**ZoneBuilder**」。
3. 按一下「**信任此帳戶**」。
4. 輸入裝置的密碼，然後按一下「**確定**」。您的帳戶現在將顯示在「受信任的帳戶」中。

您的帳戶現在位於電腦的受信任區域中。根據系統管理員所設定的策略，您可能在受信任區域之外或離線時會被限制裝置存取權限。您的裝置也可以設定為在受信任的電腦上自動解鎖。

要刪除受信任的帳戶，只需選取要刪除的帳戶，然後按一下「**刪除**」。

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」。系統管理員設定的某些受管理裝置策略，可能會讓裝置限制為僅能在 Windows 或 macOS 作業系統下執行。

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：

選擇：

-h, -help	說明
-l, -lock	鎖定裝置
-r, -readonly	解鎖成唯讀狀態

附註：Unlocker_xx.exe 僅解鎖 IRONKEYSECURE FILESUSB；稍後必須將其安裝。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 隨身碟。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磁碟區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。
6. 將封鎖裝置的政策。
   - 如果 SafeConsole 的政策設定中停用裝置，則您將無法解鎖該裝置。

我可以在哪裡取得協助？

以下資源提供 IronKey 產品的更多資訊。如有其他疑問，請聯絡您的服務台系統或系統管理員。

- 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 對此處包含的技術或編輯錯誤和/或遺漏不承擔任何責任；也不提供因使用或使用此資料而造成的附帶或間接損失。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。