IRONKEY™S1000B
ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

About This Guide (11062023)

IronKey™ S1000B is a non-managed drive.

Quick Start

Windows 11, 10 & macOS 11.x – 14.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 S1000B USB 3.2 Gen 1 is a portable flash drive with built-in password security and data encryption. It is designed with advanced AES 256-bit encryption and other features that enhance mobile data security. Now you can safely carry your files and data with you wherever you go.

How Is This Different Than a Regular USB Drive?

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

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

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

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

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

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

What Systems Can I Use It On?

- Windows® 11
- Windows® 10
- macOS® 11.x – 14.x
- Linux (4.4.x or higher) Note: The Linux CLI Unlocker does not support any features that require network access, for example, setting up your device or changing your password.

Some features are only available on specific systems:

Windows Only

- Device Updates

Product Specifications

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

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

OS Compatibility	- Windows 11, Windows 10 (Requires Two Free Drive Letters) - macOS 11.x – 14.x - Linux 4.4.x***
Warranty	5-year warranty. Free technical support

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

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

Recommended Best Practices

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

Setting Up My Device

To ensure there is ample power provided to the S1000B encrypted USB drive, insert it directly into a USB 2.0/3.2 Gen 1 port on a notebook or desktop. Avoid connecting it to any peripheral devices that may feature a USB port, such as a keyboard or USB-powered hub. Initial setup of the device must be done on a supported Windows or macOS based operating system.

Device Access (Windows Environment)

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

   • Windows 11 and 10 users will receive a device driver notification.

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

2. Select the option **IronKey.exe** inside of the IRONKEY partition that can be found in File Explorer. Please note that the partition letter will vary based on the next free drive letter. The drive letter may change depending on what devices are connected. In the image below, the drive letter is (E:).

Device Access (macOS Environment)

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

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

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

Device Initialization

Initialization on supported Windows or macOS operating system.

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

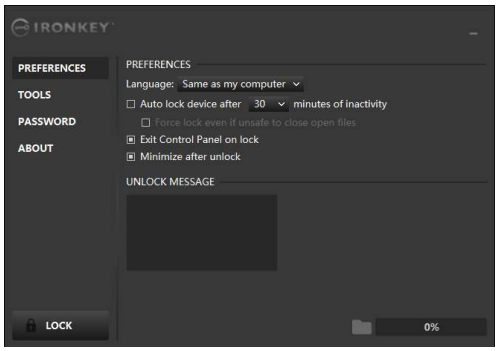
2. Review the license agreement, check the checkbox to accept it, and click Continue.

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

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

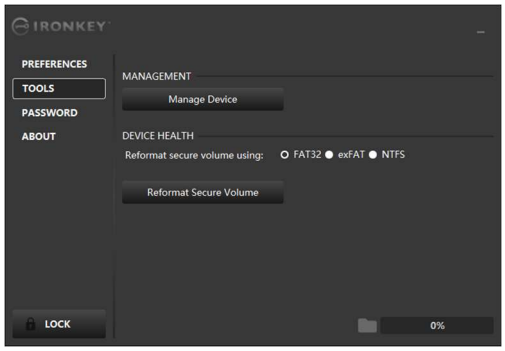
5. By default, the option to 'Reset the device instead of self-destructing' is Enabled. Click Continue. The device will finish initializing. Once complete, the IronKey Control Panel will open. Your device is now ready to store and protect your data.

IronKey Control Panel



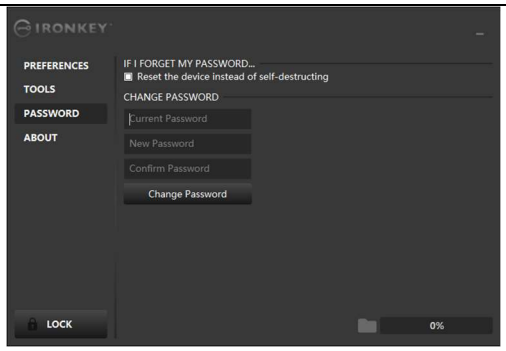
PREFERENCES

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



TOOLS

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



PASSWORD

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

ABOUT

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

Using My Device

Verifying Device Security

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

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

Accessing My Secure Files

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

To access your secure files:

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

   - Windows: Opens Windows Explorer to the IRONKEY SECURE FILES USB drive.

   - macOS: Opens Finder to the KINGSTON USB drive.

2. Do one of the following:

   - To open a file, double-click the file on the S1000B USB drive.

   - To save a file, drag the file from your computer to the S1000B USB drive.

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

Unlocking In Read-Only Mode

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

When working in this mode, the IronKey Control Panel will display the text *Read-Only Mode*. In this mode, you cannot perform any operations that involve modifying files on the device. For example, you cannot reformat the device or edit files on the drive.

To unlock the device in Read-Only Mode:

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

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

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

Changing The Unlock Message

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

To change the Unlock Message:

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

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

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

Minimize Control Panel When Unlocked

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

To disable Minimize after unlock:

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

Locking The Device

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

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

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

To manually lock the device:

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

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

To set a device to automatically lock:

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

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

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

To run CHKDSK (Windows only):

1. Unlock the device.

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

3. Type CMD and press ENTER.

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

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

6. Exit Control Panel on Lock

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

To disable Exit Control Panel on lock:

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

2. Click Preferences in the left sidebar.

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

Managing Passwords

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

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

Note: When a password is required, for example, when logging into the device or during a manual password change operation, you can use the Virtual Keyboard instead of the actual keyboard to type the password.

To change your password:

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

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

3. Enter your current password in the field provided.

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

5. Click Change Password.

Formatting My Device

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

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

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

- FAT32

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

- exFAT

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

- NTFS

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

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

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

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

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

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

Finding Information About My Device

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

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

To view device information:

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

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

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

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

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

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

Resetting My Device

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

Resetting your device:

1. Unlock your device.

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

3. Click Reset Device.

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

Using My Device on Linux

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

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

Using The Unlocker

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

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

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

These are the available parameters for the device software:

```
Options:

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

Note: Unlocker_xx.exe only unlocks the IRONKEY SECURE FILES USB; 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-mounting the device does not automatically lock the IRONKEY SECURE FILES USB. To lock the device, you must either unmount and physically remove (unplug) it, or run:

- Unlocker_xx.exe -l

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

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

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

4. Permissions

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

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

   • You might need root user permissions.

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

Where Can I Get Help?

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

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

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

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

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

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

Document No. S1000B11062023