IRONKEY™ BASIC S250/D250

User Guide

Last Updated: July15, 2016

QUICK START

English

Windows & Mac Setup

1. Plug the device into your computer's USB port (Windows Vista (SP2), 7 (SP1), 8, 8.1 or Mac 10.9.x - 10.11.x)
2. When the Device Setup window appears, follow the onscreen instructions.
   If this windows does not appear, open it manually:
   Windows: Start > My Computer > IronKey Unlocker > IronKey.exe
   Mac: Finder > IronKey Unlocker > Mac > IronKey
3. When Device Setup is complete, you can move your important files to the "Secure Files" 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.

Linux Setup

1. Plug it into your computer's USB port (Linux 2.6+)
2. Run the "ironkey" program from the device's linux folder and follow the onscreen instructions.

日本語

デバイスのセットアップ
1.デバイスをコンピューターのUSBポートに接続します。
2.「IronKey Unlocker」ドライブから、「IronKey」アプリケーションを起動します。
3.画面の指示に従い、詳細はユーザーガイドをご覧ください。
デバイスを使う準備はこれで完了です。

한국어

장치 설치
1. 컴퓨터 USB 포트로 장치를 플러그 인 하세요.
2. “IronKey Unlocker” 드라이브 상에, “IronKey” 어플리케이션을 런치하세요. 3.
화면상 설명서를 따르고 더자세한 정보는 사용자 가이드를 참조하세요. 고객님의
장치는 사용할 준비가 되었습니다.

中文

设备安装
1. 将设备插到电脑的 USB 接口。
2. 在“IronKey Unlocker”驱动器上，启动“IronKey”应用程序。
3. 按照屏幕上的说明操作。垂询详情，请阅读用户指南。您的设备可以使用了。

裝置安裝
1. 將裝置插到電腦的 USB 埠。
2. 在「IronKey Unlocker」磁碟機上，啟動「IronKey」應用程式。
3. 按照螢幕上的說明操作。垂詢詳情，請閱讀使用者指南。您的裝置可以使用了。

español

Configuración del dispositivo

1. Conecte el dispositivo en el puerto USB del ordenador.
2. En la unidad "IronKey Unlocker", ejecute la aplicación "IronKey".
3. Siga las instrucciones en pantalla y lea la Guía del usuario para más información. Su dispositivo está preparado para su uso.

français

Installation

1. Insérez le lecteur dans un port USB de l'ordinateur.
2. Lancez l'application "IronKey" à partir du lecteur "IronKey Unlocker"
3. Suivez les instructions à l'écran et consultez le guide d'utilisation pour plus d'informations.
Votre lecteur flash USB est prêt à être utilisé.

Deutsch

Geräte-Setup

1. Stecken Sie das Gerät in einen freien USB-Port des Computers.
2. Starten Sie die "IronKey"-Anwendung auf dem "IronKey Unlocker"-Laufwerk.
3. Befolgen Sie die Anweisungen auf dem Bildschirm konsultieren Sie das Benutzerhandbuch für weiterführende Informationen. Ihr Gerät ist einsatzbereit.

CONTENTS

What is it?

IronKey Basic is designed to be the world's most secure USB flash drive. Now you can safely carry your files and data with you wherever you go.

How is it different than a regular flash drive?

Hardware Encryption
Inside your device is the IronKey Cryptochip, which protects your data to the same level as highly classified government information. This security technology is always on and cannot be disabled.

Password-Protected
To access your secure data, you unlock the device with a password using the Unlocker software that is carried on the device. Do not share your password with anyone. That way, even if your device is lost or stolen, no one else can access your data.

Self-Destruct Sequence
If the Cryptochip detects physical tampering by a hacker, or if 10 consecutive incorrect password attempts have been entered, it initiates a permanent self-destruct sequence that securely erases all onboard data using flash-trash technology—***so remember your password***.

Anti-Malware Autorun Protection
Your device helps protect you from many of the latest malware threats targeting USB flash 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 central management area for accessing your files, editing your preferences, changing your device password and safely locking your device.

Secure Local Backup and Data Recovery
Securely back up your secure files using the onboard Secure Backup software (Windows only). It allows you to recover your data to a new IronKey Basic in case this one is ever lost or stolen.

Waterproof and Tamper-Resistant
Designed to survive the extremes, IronKey Basic's rugged metal encasing is injected with an epoxy compound that makes it not only tamper-resistant, but waterproof to military specifications (*MIL-STD-810F*).

How do I use it?

What systems can I use it on?

- Windows® 8.1
- Windows® 8
- Windows® 7 (SP1)
- Windows® Vista (SP2)
- Mac OS® X (10.9.x - 10.11.x)
- Linux (2.6+)

The computer must have a USB 2.0 port for high-speed data transfer. A USB 1.1 port or powered hub will also work, but will be slower.

Some applications are available only for specific systems:

- Secure Backup - Windows Only
- Virtual Keyboard - Windows Only
- Auto-Launch Assistant - Mac Only

How do I set up the device?

The setup process is the same for Windows and Mac systems. For Linux systems, see the details in the section later in this document.

1. Plug the IronKey device into your computer's USB port. The "Device Setup" screen appears.
   - The setup software autoruns from a virtual DVD. This screen might not appear if your computer does not allow devices to autorun. You can start it manually by:
     - WINDOWS: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe".
     - MAC: Opening the IronKey Unlocker drive in Finder and opening the IronKey application in the Mac folder.
2. Select a default language preference and agree to the end-user license agreement.

- By default, the IronKey software will use the same language as your computer's operating system.

3. Create a device password.
   - Your password is case-sensitive and must be at least 4 characters long.
4. Choose whether to enable Device Reset.
   - If you forget your password and have enabled Device Reset, the device will return to its initial state after the final password attempt (instead of self-destructing the device). When reset, all onboard data will be lost, but the device will be reusable.
   - This setting can also be enabled in the Control Panel's Settings menu; however, it cannot be configured while the device is locked.
5. The device initializes.
   - During this process, it generates the AES encryption key, creates the file system for the secure volume, and copies secure applications and files to the secure volume.
6. When initialization is complete, the IronKey Control Panel appears. Your device is then ready to protect your data and can be used on a Windows, Mac or Linux computer.

How do I unlock the device?

The unlock process is the same for Windows and Mac systems. For Linux systems, see the details in the section later in this document.

1. Plug in your device and wait for the Unlocker window to appear.
   - If the Unlocker window does not appear, you can start it manually by:
     - WINDOWS: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe".
     - MAC: Opening the IronKey Unlocker drive in Finder and opening the IronKey.app application in the Mac folder.
   - **NOTE**: On a Mac you can install the Auto-Launch Assistant, which automatically opens the Unlocker when you plug in an IronKey Basic device.
2. Enter your device password and click "Unlock". The IronKey Control Panel will appear.
   - Optionally, you can check the Read-Only Mode checkbox to unlock the device in Read-Only Mode.
   - Entering your password correctly (which is verified in hardware) will mount your secure volume with all your secure applications and files.
   - Entering the wrong password 10 consecutive times will permanently destroy the device and all your onboard data (unless Device Reset has already been enabled).
   - As a security precaution, you must unplug and reinsert the device after every three failed password attempts.

What do I do if I forget my password?

There are no backdoors to an IronKey Basic device. In other words, there is no way to unlock it if you do not have the correct password.

- If you have enabled device reset, you can reset the device back to its pre-setup state; however, all onboard data will be permanently lost.
- If you have not enabled device reset, you have only 10 password attempts before the device will permanently self-destruct. You will not be able to use the device again and your data will be erased.

How do I access my secure files?

After unlocking the device, you can access the files securely stored on the device by:

- Clicking the Files button (folder icon) in the IronKey Control Panel
- WINDOWS: Opening Windows Explorer to the "Secure Files" drive
- MAC: Opening Finder to the "Secure Files" drive

How do I encrypt and decrypt files?

Everything you store on your IronKey Basic device will be encrypted. Since the device has a built in Cryptochip, all of the encryption and decryption is done for you "on-the-fly", giving you the convenience of working as you normally would with a regular flash drive, while providing strong and "always-on" security.

- Simply drag a file onto the Secure Files drive and it is automatically encrypted.
- Files opened from the Secure Files drive are automatically decrypted right as you open them.

How do I use the Control Panel?

The IronKey Control Panel appears as soon as you unlock the device. It is a central location for:

- Accessing your secure files
- Launching Secure Backup software (Windows only)
- Configuring your device settings
- Changing your device password
- Reformatting your device
- Safely locking your device

NOTE: The IronKey Control Panel is available for Windows and Mac systems only.

QUICKLY ASSESSING SECURE FILES

Click the Files button in the Control Panel to open Windows Explorer (or Finder on the Mac) to the Secure Files drive.

LOCKING THE DEVICE

Click the Lock button in the bottom left of the Control Panel to safely lock your device. You can also use the keyboard shortcut: CTRL + L

If you have applications or files open on the Secure Files drive, you might not be able to lock your device (this prevents potential file corruption). Close open onboard applications and files and try again to lock the device.

TIP: Once the device is locked, you can safely unplug the device. However, do not unplug the device when it is unlocked.

DETERMINE HOW MUCH SPACE IS AVAILABLE ON THE DEVICE

The Capacity Meter at the bottom right of the Control Panel provides current information about how much data storage is available on your device. The green bar graph represents how full the device is (e.g. the meter will be fully green when the device is full), while the white text on the Capacity Meter displays how much free space remains.

USING THE APPLICATIONS LIST

The Applications List is the area where you can quickly launch onboard applications and files.

To edit the Applications List:

1. Unlock your device. The Control Panel will appear with the Applications List selected by default.
   - If you already have the Control Panel open, you can click the Applications button in the menu bar to view the Applications List.
2. Drag a file from the desktop to the Applications List area to add it to the list.
3. Right-click anywhere in the Application List to access the options menu, which allows you to add, rename, sort or delete items in the list.

Some things to know about the Applications List:

- Items in the list are shortcuts to actual files. Managing the items in the list does not alter the actual file.
- Any file can be added to the list, including documents, images, and batch files.
- For items that are not applications, the operating system opens the item with the default program associated with that filetype.
- Items that are Windows executables will be hidden from view on the Mac. Similarly, Mac application files will be hidden from view on Windows computers.

CONFIGURING DEVICE RESET AND SELF-DESTRUCTION

By default, your device will self-destruct after 10 consecutive incorrect password attempts. Self-destruction is thorough (i.e. every block of data is erased) and permanent (i.e. you can never use the device again). Self-destruction is the most secure way to protect your data.

You can configure your device to reset instead of self-destructing. This allows you to continue using your device if you forget your password; however, after the device is reset, all of your onboard data will still be lost.

To configure this setting:

1. Unlock your device
2. Click on the Settings button in the menu bar
3. Click on Password button in the left sidebar
4. Toggle the checkbox in the Device Reset area

NOTE: Device Reset is an important security feature of the product, and changing this setting requires you to enter your password.

CHANGING THE DEVICE PASSWORD

1. Unlock your device and click on the Settings button in the menu bar
2. Click on the Password button 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 the "Change Password" button

NOTE: If you created backups with the Secure Backup application, restoring those backups will require you to enter the device password that was current at the time of back up.

TIP: Changing your password on a regular basis is a good security practice. However, be especially careful to remember your device password.

INSTALLING THE AUTO-LAUNCH ASSISTANT ON A MAC

Installing the Auto-Launch Assistant will automatically open the IronKey Unlocker when you plug in your device on that computer. This feature is only available on a Mac.

1. Unlock your device and click on the Settings button in the menu bar
2. To install it, click on the "Install Auto-Launch Assistant" button
3. To uninstall it, click on the "Uninstall Auto-Launch Assistant" button

REFORMATTING THE DEVICE

Reformatting the Secure Files drive will erase all your secure files and your Application List, but it will not erase your device password and settings.

1. Unlock your device and click on the Settings button in the menu bar
2. Click on the "Reformat Secure Volume" button

TIP: Back up your data prior to reformatting; otherwise, it will be erased.

CREATING A MESSAGE THAT IS DISPLAYED IN THE UNLOCKER

This feature allows you to create a message that appears on the IronKey Unlocker window. For example, in the event that you lose your device, someone can return it to you if you provide your contact information.

1. Unlock your device and click on the Settings button in the menu bar
2. Click on the Preferences button in the left sidebar
3. Enter text in the Unlock Message field

You can only enter a long a message as will fit in the space provided (approximately 7 lines and 200 characters).

AUTO-LOCKING THE DEVICE IF IT IS LEFT UNATTENDED

You can set a device time-out to automatically lock your device after a specified period of inactivity. This will help prevent others from accessing your secure files.

1. Unlock your device and click on the Settings button in the menu bar
2. Click on the Preferences button in the left sidebar
3. Toggle the checkbox for auto-locking the device and set the time-out for either 5, 15, 30, 60, 120, or 180 minutes.

If a secure file has been opened, it may not be safe to lock the device; otherwise, the file changes may be lost or the file corrupted. The device will continue to try to lock in this situation, but will not force quit the application. You can configure the setting to force the device to lock; however, you risk the potential loss of data of any opened and modified files.

NOTE: Force locking can result in data loss. If your files have become corrupt due to a force lock or unplugging the device before locking, you might be able to recover the files by running CHKDSK and using data recovery software. For example,

1. Unlock the device
2. Use the following keyboard shortcut to bring up the "Run" prompt: WINDOWS BUTTON + R
3. Type in "`CMD`" and press enter
4. From the command prompt, type in CHKDSK and then the Secure files drive letter, and then "`/F /R`". For example, if the Secure Files drive letter is G, you would enter:
    - `CHKDSK G: /F /R`
5. You may also need to use data recovery software in order to recovery your files

VIEWING DEVICE INFORMATION

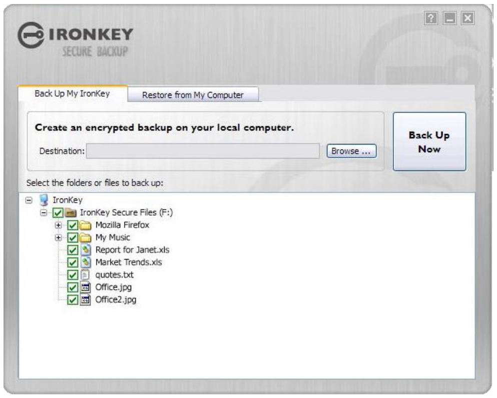
1. Unlock your device and click on the Settings button in the menu bar
2. Click on the "Device Info" button in the left sidebar

On this screen you can view details about your device, including:

- Model number
- Serial number,
- Software and firmware versions
- Secure files drive letter
- Operating System and system administrative privileges

You can also click the copy button to copy the device information to the clipboard for your email, forum posting or support request.

How do I use the Secure Backup software?



Create an encrypted backup on your local computer.

Select the folders or files to back up:

- IronKey
  - ☑ IronKey Secure Files (F:)
    - ☑ Mozilla Firefox
    - ☑ My Music
    - ☑ Report for Janet.xls
    - ☑ Market Trends.xls
    - ☑ quotes.txt
    - ☑ Office.jpg
    - ☑ Office2.jpg

If your device is lost or stolen:

- No one can access your data without the password
- You can restore an encrypted backup of your data to a new or existing IronKey Basic device by using the Secure Backup software (Windows only, English only)

Secure Backup works by saving an encrypted backup of some or all of your onboard files to your local computer or network fileshare. You use the same application to restore one or all of your files.

BACKING UP FILES FROMYOUR DEVICE

1. Click the "Secure Backup" button in the IronKey Control Panel to open the program (Windows only)
   - The Secure Backup window should appear, displaying the Secure Files drive.
2. Select the files you want to back up.
3. Check the checkboxes next the files you want to back up.
   - A green checkmark means all files in this folder and all sub-folders will be backed up
   - A red minus sign means only some of the files in this folder or its subfolders will be backed up
4. Select the destination folder for the backed up files.
   - The location of the backup can be an existing folder, a new folder, or a separate drive (e.g. a network fileshare)
5. Click "Backup Now". The files will be encrypted and backed up.

NOTE: While the files are securely encrypted, the filenames will not be. Zipping the files to be backed up first will hide the file names.

NOTE: Do not add, alter, or delete the backed up files or it could prevent you from being able to restore them later.

RESTORING BACKED UP FILES TOYOUR DEVICE

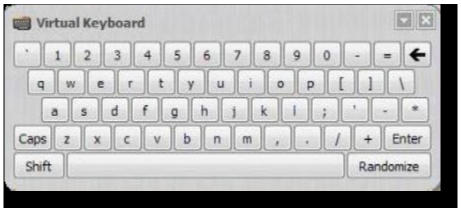
1. Click the "Secure Backup" button in the IronKey Control Panel to open the program (Windows only)
   - The Secure Backup window should appear, displaying the Secure Files drive.
2. Select the "Restore from My Computer" tab.
3. Select the destination folder you had chosen previously when backing up your data.

- Make sure to select the folder that contains the backup, not files or folders within that folder.

4. Select which files/folders to restore and click “Restore Now”. Restored files will overwrite existing files of the same name on the Secure Files drive.

NOTE: If the data was backed up from a different IronKey Basic device, you will have to supply the device password for that device in order to restore the files to a different device.

How do I use the Virtual Keyboard?


Virtual Keyboard
` 1 2 3 4 5 6 7 8 9 0 - = ←
q w e r t y u i o p [ ] \
a s d f g h j k l ; ' - *
Caps z x c v b n m , . / + Enter
Shift
Randomize

If you are unlocking your device on an unfamiliar computer and are concerned about keylogging and screenlogging spyware, use the IronKey Virtual Keyboard. It helps protects your device password by letting you click out letters and numbers. The underlying techniques in the Virtual Keyboard will bypass many trojans, keyloggers, and screenloggers.

The Virtual Keyboard can be launched a couple of ways:

- In places where you enter a password into the device (e.g. the Unlocker, changing your device password, setting up your device), click the Virtual Keyboard icon
- When the keyboard focus is in a password field, use the keyboard shortcut CTRL+ALT+ V

NOTE: This feature is available on Windows only and uses a standard QWERTY keyset.

1. Click the Virtual Keyboard icon in a password field on the IronKey Unlocker or Control Panel. The Virtual Keyboard appears.
   - Alternatively, you can press CTRL+ALT+ V
2. Click the keys to type your password. Click “Enter” when you are finished.
   - You can use the Virtual Keyboard in conjunction with the actual keyboard, so that you type some characters and click some characters.
   - You can also optionally click the “Randomize” button to randomize where the keys are. This helps protect against screenloggers.
3. When you click a key in the Virtual Keyboard, all of the keys briefly go blank. This feature prevents screenloggers from capturing what you clicked.
   - If you do not want to use this feature, you can disable it in the options menu next to the close button.

How do I use Read-Only Mode?

You can unlock your device in a read-only state such that files on your Secure Files drive cannot be edited. An example of when this is useful is when you want to access a file on your device while using an untrusted or unknown computer. If you unlock your device in Read-Only Mode, malware on that machine cannot infect your device or modify your files.

1. Plug in your device and launch the Unlocker
2. Check the “Read-Only Mode” checkbox
3. Unlock your device

» You will see a message in the Control Panel that you are in Read-Only Mode.

» When you unlock your device in Read-Only Mode, you will remain in Read-Only Mode until you lock your device.

» Note that some features are not available in Read-Only Mode because they require modifying files on your device. Examples of unavailable features include reformatting, restoring applications, editing files on the Secure Files drive, and editing the Applications List.

» To unlock your device in Read-Only Mode on Linux, enter: `ironkey --readonly`

How do I use the device on Linux?

If you prefer to use a Linux computer, you can use your IronKey Basic device on several distributions of Linux (x86 systems only with kernel version 2.6+).

SETTING UP THE DEVICE ON LINUX

1. Plug it into your computer’s USB port and run the ironkey program from the device’s linux folder.
   - The device mounts as a virtual DVD.
   - You must start the Unlocker manually by going to the linux folder and running ironkey.
2. Agree to the license agreement.
   - Press Q (Quit) to exit or press Y (Yes) to agree to the terms.
3. Create a device password.
   - Your password is case-sensitive and must be at least 4 characters long .
4. You can also choose to enable Device Reset, which will allow you to reset the device (instead of self-destructing the device) in case you forget your password. When reset, all onboard data will be lost, but the device will be reusable.
5. The device initializes. During this process, it generates the AES encryption key, and creates the file system for the secure volume.
6. When this is complete, your device is ready for use.

USING THE UNLOCKER ON LINUX

Use the Unlocker for Linux to access your files and change your device password on Linux, allowing you to securely transfer files from and between Windows, Mac, and Linux computers.

Depending on your Linux distribution, you might need root privileges to use the program "`ironkey`" found in the Linux folder of the mounted virtual DVD. If you have only one IronKey Basic attached to the system, simply run the program from a command shell with no arguments (e.g. `ironkey`). If you have multiple IronKey Basic devices, you must specify which one you want to unlock.

NOTE: `ironkey` only unlocks the secure volume; 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 `ironkey`.

To change the password of the device named "devicename," enter:

```
ironkey --changepwd [devicename]
```

To lock the IronKey named "devicename," enter:

```
ironkey --lock [devicename]
```

To unlock the IronKey in Read-Only Mode, enter:

```
ironkey --readonly
```

To unlock the IronKey with the password "devicepassword," enter:

```
ironkey --password [devicepassword]
```

Simply unmounting the device does not automatically lock the secure volume. To lock the device, you must either unmount and physically remove (unplug) it, or else run:

```
ironkey --lock
```

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

1. Kernel Version must be 2.6 or higher

If you compile your own kernel, you must include the following in it:

```
» DeviceDrivers->SCSIDeviceSupport-><*>SCSICDROMSupport
» DeviceDrivers-><*> Support for Host-side USB
» DeviceDrivers-><*> USB device filesystem
» DeviceDrivers-><*> EHCI HCD (USB 2.0) support
» DeviceDrivers-><*> UHCI HCD (most Intel and VIA) support
» DeviceDrivers-><*> USB Mass Storage Support
```

The kernels that are included by default in most major distributions already have these features, so if you are using the default kernel that comes with a supported distribution you do not need to take any other action.

Also, on 64-bit linux systems the 32-bit libraries must be installed in order to run the `ironkey` program. Consult the distribution's help resources for assistance and more information.

2. Mounting problems

- 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>
```

- The name of the mounted device varies depending on the distribution. The names of the IronKey Basic devices can be discovered by running:

```
ironkey --show
```

3. Permissions

- You must have permissions to mount external/usb/flash devices
- You must have permissions to run executables off the device's virtual DVD in order to launch the Unlocker
- You might need root user permissions

See the Linux folder on the device's virtual DVD for information about how to set up permissions to allow non-root users to access their IronKey Basic devices. All of these methods require that the system administrator take (one time) action to enable access; after that, ordinary users can lock, unlock, and change passwords on any IronKey Basic devices they plug in.

4. Supported distributions

Not all distributions of Linux are supported. Please visit *http://support.ironkey.com* for the latest list of supported distributions.

5.The IronKey Unlocker for Linux only supports x86 systems at this time.

Best Practices

- Lock the device
  - when not in use
  - before unplugging it
  - before system enters sleep mode
- Never unplug the device when the LED is on
- Never share your device password
- Perform a computer anti-virus scan before setting up the device

How does it work?

Technical and Security Notes

IronKey Basic has been designed from the ground up with security in mind. A combination of advanced security technologies are used to ensure that only you can access your data. Additionally, it has been designed to be physically secure, to prevent hardware-level attacks and tampering, as well as to make the device rugged and long-lasting.

This IronKey Cryptochip is hardened against physical attacks such as power attacks and bus sniffing. It is physically impossible to tamper with its protected data or reset the password counter. If the Cryptochip detects a physical attack from a hacker, it destroys the encryption keys, making the stored encrypted files inaccessible.

We are endeavoring to be very open about the security architecture and technology that we use in designing and building this product. There is no hocus-pocus or handwaving here.We use established cryptographic algorithms, we develop threat models, and we perform security analyses (internal and third party) of our systems all the way through design, development and deployment.

DEVICE SECURITY

Data Encryption Keys

- AES key generated by onboard Random Number Generator
- AES key generated at initialization time and encrypted with hash of user password
- No backdoors: AES key cannot be decrypted without the user password
- AES key never leaves the hardware and is not stored in NAND flash

Data Protection

- Secure volume does not mount until password is verified in hardware
- Password try-counter implemented in tamper-resistant hardware
- Once password try-count is exceeded, all data is erased by hardware
- Secure box architecture accessible only to firmware to store sensitive data and settings

Physical Security

- Solid, rugged metal case
- Encryption keys stored in the tamper-resistant Cryptochip
- All chips are protected by black epoxy-based potting compound
- Exceeds military waterproof standards (MIL-STD-810F)

APPLICATION SECURITY

Device Password Protection

- USB command channel encryption to protect device communications
- Password-in-memory protection to protect against cold-boot and other attacks
- Virtual Keyboard to protect against keyloggers and screenloggers

The device password is hashed using salted SHA-256 before being transmitted to the device firmware over a secure and unique USB channel. It is stored in an extremely inaccessible location in the protected Cryptochip hardware. The hashed password is validated in hardware (there is no "getPassword" function that can retrieve the hashed password), and only after the password is validated is the AES encryption key decrypted. The password try-counter is also implemented in hardware to prevent memory rewind attacks. Typing your password incorrectly too many times initiates a permanent "flash-trash" self-destruct sequence, which is run in hardware rather than using software, ensuring the ultimate protection for your data.

ADDITIONAL NOTES

Section 508 Compliance

The IronKey Control Panel is designed to be Section 508 compliant. Users with disabilities have keyboard navigation and screen reader support.

Product Specifications

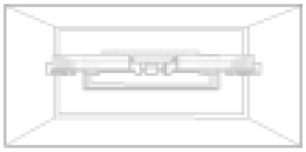
For details about your device, see “Device Info” in the Control Panel settings.

CAPACITY*
Up to 64GB, depending on the model

DIMENSIONS
75mm X 19mm X 9mm

WEIGHT
0.8 oz

WATERPROOF
MIL-STD-810F



OPERATING TEMPERATURE
0C, 70C

OPERATING SHOCK
16G rms

ENCRYPTION
Hardware: 256-bit AES
Hashing: 256-bit SHA
PKI: 2048-bit RSA

FIPS CERTIFICATIONS
See *www.ironkey.com/en-US/website/certification-and-compliance* for details.

HARDWARE
USB 2.0 (High-Speed) port recommended, USB 1.1

OS COMPATIBILITY
Windows XP (SP2+), Vista, 7, 8, or 8.1
Mac 10.5+
Unlocker for Linux (2.6+, x86)

Designed and Assembled in the U.S.A.
IronKey Basic devices do not require any software or drivers to be installed.

** Advertised capacity is approximate and not all of it will be available for storage. Some space is required for onboard software.*

Where Can I Get Help?

Where can I go for more info?

support.ironkey.com	Support information, knowledgebase and video tutorials
www.ironkey.com	General information

Support Contact Information

http://support.ironkey.com/