IRONKEY™ BASIC S1000 SECURE USB 3.0 FLASH DRIVE

User Guide

CONTENTS

QUICK START

Once set up, you can use your device on Windows, Mac, or Linux systems. For more information about using your device on Linux, see "Using my device on Linux" on page 16.

Windows & Mac Setup (Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.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 > My Computer > IronKey Unlocker > IronKey.exe

    • Mac: Finder > IronKey Unlocker > IronKey

3. When Device Setup is complete, you can move your important files to the IronKey Secure Files drive (IronKey USB drive for Mac) and they will be automatically encrypted.

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

Linux Setup (Linux2.6+)

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

2. Run the "ironkey.exe" program from the device's linux folder and follow the on-screen instructions.

MISE EN ROUTE

Installation avec Windows et Mac (Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x)

1. Branchez le périphérique sur le port USB de votre ordinateur.

2. Lorsque la fenêtre d'Installation du périphérique s'affiche, suivez les instructions à l'écran. Si cette fenêtre ne s'affiche pas, ouvrez-la manuellement :

    • Windows :Démarrer > Ordinateur > IronKey Unlocker > IronKey.exe

    • Mac : Finder > IronKey Unlocker > IronKey

3. Lorsque l'installation du périphérique est terminée, vous pouvez déplacer vos fichiers importants vers le lecteur Secure Files (Fichiers sécurisés). Ils seront automatiquement cryptés.

    Certains systèmes Windows vous invitent à redémarrer la première fois que vous branchez votre périphérique. Vous pouvez fermer cette invite en toute sécurité sans redémarrer, aucun nouveau pilote ou logiciel n'est installé.

Installation avec Linux (Linux 2.6+)

1. Branchez le périphérique sur le port USB de votre ordinateur.

2. Exécutez le programme ironkey.exe depuis le dossier Linux du périphérique et suivez les instructions à l'écran.

KURZANLEITUNG

Geräte-Setup bei Windows und Mac (Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x)

1. Stecken Sie das Gerät in den USB-Port Ihres Computers

2. Wenn sich das Fenster „Geräte-Setup" öffnet, folgen Sie den Anweisungen auf dem Bildschirm. Wenn sich dieses Fenster nicht öffnet, dann öffnen Sie es wie folgt manuell:

    *   Windows: Start > My Computer > IronKey Unlocker > IronKey.exe
    *   Mac: Finder > IronKey Unlocker > IronKey

3. Wenn das Geräte-Setup abgeschlossen ist, können Sie Ihre wichtigen Dateien auf das Laufwerk „Secure Files" verschieben und sie werden automatisch entschlüsselt.

    Einige Windows-Systeme werden Sie zum Neustart auffordern, wenn Sie das Ihr Gerät zum ersten Mal anschließen. Sie können diese Aufforderung sicher schließen ohne Neu zu starten – keine neuen Laufwerke oder Software werden installiert.

Geräte-Setup bei Linux (Linux 2.6+)

1. Stecken Sie das Gerät in den USB-Port Ihres Computers.

2. Führen Sie das Programm „ironkey.exe" unter dem Linux-Ordner des Geräts aus und folgen Sie den Anweisungen auf dem Bildschirm.

INICIO RÁPIDO

Instalación en Windows y Mac (Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x)

1. Conecte el dispositivo en el puerto USB de su equipo

2. Cuando aparezca la ventana Instalación del dispositivo, siga las instrucciones que se muestran en pantalla. Si no aparece, ábrala manualmente:

    *   Windows: Inicio > Equipo > IronKey Unlocker > IronKey.exe
    *   Mac: Finder > IronKey Unlocker > IronKey

3. Tras finalizar la instalación del dispositivo, podrá mover sus archivos importantes a la unidad "Secure Files" y estos se cifrarán de forma automática.

    Algunos sistemas Windows le solicitarán que reinicie el sistema tras conectar el dispositivo por primera vez. Puede cerrar este mensaje con seguridad sin reiniciar el equipo, no se instalarán drivers ni software nuevo.

Instalación en Linux (Linux 2.6 o superior)

1. Conéctelo el dispositivo en el puerto USB de su equipo.

2. Ejecute el programa "ironkey.exe" desde la carpeta de Linux del dispositivo y siga las instrucciones que se muestran en pantalla.

クイックスタート

Windows および Mac のセットアップ (*Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x*)

1. デバイスをコンピューターの USB ポートに挿入します。

2. [デバイスのセットアップ] 画面が表示されたら、画面上の指示に従ってください。

   この画面が表示されない場合は、手動で開いてください。

   - Windows の場合 :[スタート] > [マイ コンピューター] > [IronKey Unlocker] > [IronKey.exe]

   - Mac の場合 : [セレクタ] > [IronKey Unlocker] > [IronKey]

3. デバイスのセットアップが完了したら、重要なファイルを「Secure Files」ドライブに移動させることができ、そこで自動的に暗号化されます。

   デバイスを初めて挿し込むと、Windows システムが再起動するようにプロンプトを表示します。新しいドライバーまたはソフトウェアがインストールされていない場合、再起動することなくそのプロンプトを安全に閉じることができます。

Linux セットアップ (Linux 2.6+)

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. デバイスの linux フォルダーから「ironkey.exe」を実行し、画面の指示に従います。

빠른 시작

Windows 및 Mac 설정 (*Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x*)

1. 컴퓨터 USB 포트로 장치를 꽂습니다.

2. 장치 설정 창이 나타나면 화면의 지침을 따릅니다.

   이 창이 나타나지 않으면 다음과 같이 수동으로 엽니다.

   - Windows: 시작 > 내 컴퓨터 > IronKey Unlocker > IronKey.exe
   - Mac: Finder > IronKey Unlocker > IronKey

3. 장치 설정이 완료되면 중요한 파일을 'Secure File' 드라이브로 이동할 수 있습니다. 이동한 파일은 자동으로 암호화됩니다.

   일부 Windows 시스템에서는 장치를 처음으로 꽂으면 다시 시작하라는 메시지를 표시합니다. 다시 시작하지않고 메시지를 닫아도 안전합니다. 새로운 드라이버나 소프트웨어가 설치되지 않습니다.

Linux 설정 (Linux 2.6 이상)

1. 컴퓨터의 USB 포트에 꽂습니다.

2. 장치의 linux 폴더에서 'ironkey.exe' 프로그램을 실행하고 화면의 지침을 따릅니다.

快速入门

Windows & Mac **安装** （*Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x*）

1. 将设备插到电脑 USB 接口。

2. 显示设备安装窗口后，按屏幕上的说明进行操作。

   如果窗口未显示，可手动将其打开：

   - Windows： 开始 > 我的电脑 > IronKey Unlocker > IronKey.exe
   - Mac：Finder > IronKey Unlocker > IronKey

3. 设备安装完成后，可以将重要文件移动到 "安全文件" 驱动器中，文件会自动加密

   首次插入设备后，某 Windows 系统会提示重新启动 您可以放心关闭此提示，且无需重新启动，因为系统并未安装任何新的驱动程序或软件。

Linux **安装** （Linux 2.6 **以上版本**）

1. 将设备插到电脑 USB 接口。

2. 从设备 linux 文件夹中运行 "ironkey.exe" 程序，并按屏幕上的说明进行操作

快速入門

Windows **與** Mac **設定** （*Windows 10, 8/8.1, 7 (SP1), Vista (SP2) or Mac OSX 10.9.x - 10.11.x*）

1. 將裝置連接到您的電腦 USB 連接埠。

2. 當裝置設定視窗出現時，請依照畫面上指示操作。

   若此視窗並未出現，請手動開啟：

   - Windows： 開始 > 我的電腦 > IronKey Unlocker > IronKey.exe
   - Mac：Finder > IronKey Unlocker >IronKey

3. 當裝置設定完成時，即可將您的重要檔案移至 「安全檔案」裝置，接著這些檔案就會自動加密。

   部分 Windows 系統會在您第一次連接裝置後，提示您重新啟動電腦。您可以放心關閉此提示且無需重新啟動，因為系統並無安裝任何新的驅動程式或軟體。

Linux **設定** （**支援系統為**：Linux 2.6 **以上版本**）將裝
置連接到您的電腦 USB 連接埠。

從裝置內的 linux 資料夾執行 「ironkey.exe」應用程式並依照畫面上指示操作。

ABOUT MY DEVICE

IronKey™ Basic S1000 is a USB (Universal Serial Bus) 3.0, portable flash drive with built-in password security and data encryption. IronKey Basic S1000 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.

Figure 1: S1000 device

HOW IS IT DIFFERENT THAN A REGULAR FLASH DRIVE?

FIPS 140-2 Level 3 certification
IronKey Basic S1000 has FIPS certification so you can feel confident that you're complying with regulatory requirements.

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, or if ten incorrect password attempts have been entered, it initiates a permanent self-destruct sequence that securely erases all onboard data (unless you set your device to reset)—so remember your password.

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.

Waterproof and Tamper-Resistant

Designed to survive the extremes, the rugged metal encasing is injected with an epoxy compound that makes it not only tamper-resistant, but waterproof to military specifications (MIL-STD-810F).

WHAT SYSTEMS CAN I USE IT ON?

- Windows$^®$ 10
- Windows$^®$ 8/8.1
- Windows$^®$ 7 (SP1)
- Windows$^®$ Vista (SP2)
- Mac OS$^®$ X (10.9.x - 10.11.x)
- Linux (2.6+)

Some applications are available only on specific systems:

Windows Only

- Virtual Keyboard (English only)

Mac Only

- Auto-Launch Assistant

HOW SECURE IS IT?

The IronKey Basic S1000 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.

The 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, it destroys the Cryptochip, making the stored encrypted files inaccessible.

We strive to be very open about the security architecture and technology that we use in designing and building this product. 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 on-board 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 the password is verified in hardware
- Password try-counter implemented in tamper-resistant hardware
- Once the password try-count is exceeded, by default, the device will be reset and all data will be erased. Resetting a device puts the device back to its original factory state. If you disable the device reset setting in the Control Panel, the device will self-destruct when the password try-count is exceeded.
- Sensitive data and settings are stored in hardware

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 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). Only after the password is validated, is the AES key available for encryption. The password try-counter is also implemented in hardware to prevent memory rewind attacks.

PRODUCT SPECIFICATIONS

For further details about your device, see the Device Info page in the IronKey Control Panel. See "To view device information" on page 18.

Table 1: S1000 Device Specifications

Specification	Details
Capacity	4G, 8G, 16G, 32G, 64G, 128G
Dimensions	82mm X 21.1mm X 9.1mm
Weight	1.12 oz (32 grams)
Operating Temperature	0C, 70C
Operating Shock	16 G rms
Hardware Encryption	256-bit AES (XTS Mode)
EMI/EMC Compliance	USA FCC, Europe CE, Canada ICES, Australia C-Tick Taiwan BSMI, Japan VCCI, Korea KCC (KCC ID: MSIP-REM-WKY-S1000)
Certification	FIPS 140-2 level 3 certified

Table 1: S1000 Device Specifications

Specification	Details
Hardware	• USB 3.0 (SuperSpeed) port recommended, As a minimum, the computer must have a USB 2.0 port (high-speed). • Water-resistant MIL-STD-810F • Dust-resistant • Shock-resistant • Ruggedized
OS Compatibility	• Windows 10, Windows 8/8.1, Windows 7 (SP1) or Windows Vista (SP2) • Mac OS X (10.9.x - 10.11.x) Unlocker for Linux (2.6+)
Accessibility	IronKey Control Panel is designed to be Section 508 compliant. Users with disabilities have keyboard navigation and screen reader support.

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

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 on.

3. Never share your device password.

4. Perform a computer anti-virus scan before setting up the device.

USING MY DEVICE

SETTING UP THE DEVICE

Once set up, you can use your device on Windows, Mac, or Linux systems. The setup process is the same for systems running a Microsoft Windows or Mac operating system. To set up the device using Linux, see "Setting up the device on Linux" on page 16.

To setup the device

1. Plug the IronKey device into your computer's USB port. The Device Setup screen appears.

   The setup software runs automatically from the public volume. This screen may not appear if your computer does not allow devices to autorun. You can start it manually by:
   - Windows: Opening the IronKey Unlocker drive in My Computer and double-clicking the IronKey.exe file.
   - Mac: Opening the IronKey Unlocker drive in Finder and then opening the IronKey application. You can install the Auto-Launch Assistant, so that the Unlocker will automatically open when you plug in a device. See "Installing the Auto-Launch Assistant (Mac only)" on page 11.

2. Select a default language preference, agree to the end-user license agreement, and then click Unlock.

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

3. Type a device password and confirm it, and then click Continue.

   Your password is case-sensitive and must have at least 4 characters (including spaces).

4. Select Reset the device... if you do not want the device to self-destruct if the wrong password is entered 10 consecutive times.

5. Click Continue. 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.

   When the initialization is complete, the IronKey Control Panel appears. Your device is now ready to protect your data and can be used on a Windows, Mac or Linux computer.

Installing the Auto-Launch Assistant (Mac only)

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

To install the Auto-Launch Assistant

1. Unlock your device and click the Settings [⚙] button on the menu bar.

2. Click Tools from the left side bar, and then click Install Auto-Launch Assistant.

Tip: To uninstall the Assistant, click Uninstall Auto-Launch Assistant.

UNLOCKING AND LOCKING THE DEVICE

Unlocking the device

The unlock process is the same for Windows and Mac systems. For Linux systems, see "Use my device on Linux" on page 18. Once you enter the correct password, the device will mount the secure volume with all your secure applications and files. Exceeding the number of incorrect password attempts will, by default, reset the device. If you disabled this setting, the device will self-destruct and you will lose all on-board data.

Note: As a security precaution, you must unplug and reinsert the device after every three failed password attempts.

Unlocking in Read-Only Mode

You can unlock your device in a read-only state so that files cannot be edited 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, restore applications or edit the Applications list, or edit files on the drive.

To unlock the device

1.   Insert the device into the USB port of the host computer, 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 double-clicking the Iron-Key.exe.
      • Mac: Opening the IronKey Unlocker drive in Finder, and then opening the IronKey application. If you installed the Auto-Launch Assistant, the Unlocker will automatically open when you plug in a device. See "Installing the Auto-Launch Assistant (Mac only)" on page 11.

2.   If you want to unlock your device in Read-Only Mode, click the Read-Only check box.

3.   Type your device password and click Unlock. The IronKey Control Panel will appear.

Tip: You can also use the virtual keyboard (Windows and English only) to type your password, see "Typing passwords with the Virtual Keyboard" on page 14.

Changing the Unlock message

The Unlock message is custom text that displays in the Unlocker window when you unlock the device. This feature allows you to customize the message that displays for example, to add contact information so that if you lose your device someone will know how to return it to you.

To change the Unlock message

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

2.   Click Preferences in the left sidebar.

3.   Type the message text in the Unlock Message field. The text must fit 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.

By default, to prevent potential file corruption, your device will not lock if applications or files on the drive are open. Close any open applications or files before locking the device.

Caution: If you configure auto-lock to force the device to lock, any open files may lose changes or become corrupt as a result of the forced lock operation. Unplugging the device while it is unlocked may also result in loss or corruption of data on the device.

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.

To manually lock the device

• Click the Lock button in the bottom left of the Control Panel to safely lock your device.

Tip: You can also use the keyboard shortcut: CTRL + L or right-click the IronKey icon from the system tray and click Lock Device.

To set a device to automatically lock

1. Unlock your device and in the IronKey Control Panel, click the Settings button on the menu bar.
2. Click Preferences in the left sidebar.
3. Click the check box 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.

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 can result in loss of data to any open and unsaved files.

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 drive letter, and then "/F /R".

   For example, if the IronKey Secure Files drive letter is G, you would type:

   ```
   CHKDSK G: /F /R
   ```
5. Use data recovery software if necessary in order to recover your files.

MANAGING PASSWORDS

It is a good security practice to regularly change your password. However, be especially careful to remember your device password. If you forget it, there is no way to unlock the device.

When a password is required, for example when logging in to the device or during a password change operation, you can use the Virtual Keyboard instead of the real keyboard to type the password, see "Typing passwords with the Virtual Keyboard" on page 14.

To change your password

1. Unlock your device and click the Settings [⚙] button 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.

Typing passwords with the Virtual Keyboard

If you are unlocking your device on an unfamiliar computer and are concerned about keylogging and screenlogging spyware, use the Virtual Keyboard. It helps protect 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.

Note: This feature uses a standard QWERTY key set and is available on Windows only. The language preference for the device must be set to English.

To type a password using the Virtual Keyboard

1. Open the Virtual Keyboard by doing one of the following actions:
   - In a password field, click the Virtual Keyboard icon [⌨].
   - When the keyboard focus is in a password field, press CTRL+ALT+ V.
2. Click the keys to type your password, and then click ENTER.

   You can also use the Virtual Keyboard in conjunction with the actual keyboard, so that you type some characters and click some characters.

Tip: Click the Randomize button to arrange the keys in a random manner. This helps protect against screenloggers.

Note: 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. To disable this feature, click the ▼ icon (beside the Exit button) and choose Disable screenlogger protection.

Accessing my device if I forget my password

There are no back doors 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 on-board 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.

ACCESSING MY SECURE FILES

After unlocking the device, you can access your secure files. Since the device has a built-in Cryptochip, files are automatically encrypted and decrypted "on-the-fly" when you save or open a file on the drive. This technology gives you the convenience of working as you normally would with a regular flash drive, while providing strong, "always-on" security.

To access my secure files

1. Click the Files ⬛ button on menu bar of the IronKey Control Panel.
   - Windows: Opens Windows Explorer to the IronKey Secure Files drive.
   - Mac: Opens Finder to the IronKey USB drive.

2. Do one of the following:
   - To open a file, double-click the file on the IronKey Secure Files drive (IronKey USB drive for Mac).
   - To save a file, drag the file from your computer to the IronKey Secure Files drive (IronKey USB drive for Mac).

Tip: You can also access your files by right-clicking the IronKey icon on the Windows taskbar and clicking Secure Files.

UPGRADING MY DEVICE FROM BASIC TO ENTERPRISE

If notified by your system administrator, you can upgrade your IronKey Basic device to an Enterprise device. Enterprise devices are managed by an IronKey Enterprise Management System. When you upgrade your device, you will be required to activate it using an activation code provided by your administrator. An Internet connection is required to complete this process. See the IronKey Enterprise User Guide on your device for information about Enterprise features.

Important: Only start the upgrade process if your system administrator has asked you to activate your device with IronKey Enterprise.

To upgrade from Basic to Enterprise

1. When you receive the Activation Code from your system administrator, start the IronKey Control Panel and click the Settings ⚙ button.
2. In the left sidebar, click Tools and then click Upgrade to Enterprise.
3. Paste the Activation Code in the Enterprise Activation text box (Windows and Mac systems only).
4. Follow the on-screen instructions.
5. Additional applications may be installed on your device based on the device policy settings chosen by your system administrator. You may also be required to change your password so that it conforms to the password security policy set for Enterprise devices in your organization.

REFORMATTING MY DEVICE

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

Important: Before you reformat the device, back up your secure volume to a separate location (for example, to cloud storage or your computer).

To reformat a device

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

2.   Click Tools on the left sidebar.

3.   Under Device Health, click Reformat Secure Volume.

USING MY DEVICE ON LINUX

You can set up and use your device on several distributions of Linux (x86 systems only with kernel version 2.6 or higher).

Setting up the device on Linux

1.   Plug it into your computer's USB port and start the Unlocker by running the ironkey.exe program from the linux folder on the device.

     The device mounts as a drive.

2.   Accept 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.   Enable Device Reset if you want the device to reset instead of self-destructing if you exceed the number of password attempts allowed. A device reset operation erases all on-board data, but unlike self-destruct, does not render the device unusable.

5.   The device initializes. During this process, it generates the AES encryption key, and creates the file system for the secure volume.

     When this process is complete, your device is ready for use.

Using the Unlocker

Use the Unlocker for Linux to access your files and change your device password on Linux. Depending on your Linux distribution, you may need root privileges to use the program "`ironkey.exe`" found in the Linux folder of the mounted public volume. If you have only one IronKey device attached to the system, run the program from a command shell with no arguments (for example, `ironkey.exe`). If you have multiple devices, you must specify which one you want to unlock.

Note: `ironkey.exe` 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.exe`.

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

```
ironkey.exe --changepwd [devicename]
```

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

```
ironkey.exe --readonly
```
When prompted, type your password.

To unlock the device, enter:

`ironkey.exe --unlock` When prompted, type your password.

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

`ironkey.exe --lock`

Simply unmounting the device does not automatically lock the secure volume.

To lock the device when more than one device is in use, enter:

`ironkey.exe --lock [devicename]` where devicename is the name of the device you want to 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.exe` 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 devices can be discovered by running:

        `ironkey.exe --show`

3. Permissions

- You must have permissions to mount external/usb/devices.
- You must have permissions to run an executable file from the public volume in order to launch the Unlocker.
- You might need root user permissions.

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

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.

This Capacity Meter indicates that there is 92.5 GB of free space available on the drive.
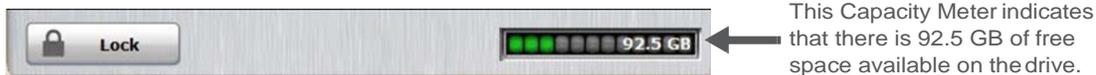
For general information about your device, see the Device Info page.

To view device information

1.   Unlock your device and in the IronKey Control Panel, click the Settings [⚙] button on the menu bar.
2.   Click Device Info in the left sidebar.

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

- Model number
- Serial number
- Software and firmware version
- Release Date
- Secure Files drive letter
- Unlocker drive letter
- Operating System and system administrative privileges

3.   If you want 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.

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

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.

- *support.ironkey.com*—Support information, knowledge base and video tutorials
- *www.ironkey.com*—General information