

# IRONKEY

## User Guide



IronKey Enterprise H300  
Updated: September 2014

 **IRONKEY™**  
by imation

Thank you for your interest in IronKey™ Enterprise by Imation.

Imation's Mobile Security Group is committed to creating and developing the best security technologies and making them simple-to-use and widely available. Years of research and millions of dollars of development have gone into bringing this technology to you.

We are very open to user feedback and would appreciate hearing your comments, suggestions, and experiences with this product.

Feedback:

*[securityfeedback@imation.com](mailto:securityfeedback@imation.com)*

# CONTENTS

<b>Quick Start</b> .....	<b>5</b>
快速入门 .....	5
快速入門 .....	5
빠른 시작 .....	6
クイックスタート .....	6
<b>Mise en route</b> .....	<b>6</b>
<b>Kurzanleitung</b> .....	<b>7</b>
<b>Inicio rápido</b> .....	<b>7</b>
<b>About my device.</b> .....	<b>8</b>
About IronKey Enterprise H300 .....	8
How is it different than a regular hard drive? .....	8
How secure is it? .....	9
<i>Device Security</i> .....	10
<i>Application Security</i> .....	10
Product specifications .....	10
Recommended best practices .....	11
<b>How do I...?</b> .....	<b>12</b>
Set up the device .....	12
Unlock and lock the device .....	13
<i>Unlock device</i> .....	13
<i>Lock device</i> .....	14
<i>Type passwords with the Virtual Keyboard</i> .....	15
Access my device if I forget my password .....	16
Access my secure files .....	16
Encrypt and decrypt files .....	17
Update my device .....	17
Reformat my device .....	17
Use my device on Linux .....	18
<i>Use the Unlocker</i> .....	18
Find information about my device .....	20
<i>View device information</i> .....	20
<i>Determine the storage space available on the device.</i> .....	20
Use onboard applications .....	20
<i>Scan my device for malware.</i> .....	20
<i>Edit the Applications List.</i> .....	21
<i>Restore onboard applications.</i> .....	21
Manage my online account settings .....	22

<i>Change device nickname</i> .....	22
<i>Manage account settings</i> .....	22
<b>Where can I get Help?</b> .....	<b>24</b>
For more information .....	24

# QUICK START

## Windows & Mac Setup (Windows XP, Vista, 7, 8, 8.1 or Mac 10.6+)

1. Plug the device into your computer's USB 3.0 port (if unavailable, use a USB 2.0 port).
2. When the Device Setup window appears, follow the onscreen instructions.

If this window 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.

---

## 快速入门

### Windows & Mac 安装 (Windows XP、Vista、7、8、8.1 Mac 10.6 以上版本)

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 > Mac > 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。

---

## 快速入門

### Windows 與 Mac 設定 (支援系統為: Windows XP、Vista、7、8、8.1 或 Mac 10.6 以上版本)

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 > Mac > 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。

# 빠른 시작

## Windows 및 Mac 설정 (Windows XP, Vista, 7, 8, 8.1 또는 Mac 10.6 이상)

1. 컴퓨터 USB 포트에 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 > Mac > 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 시작하지 않고 메시지를 닫아도 안전합니다. 새로운 드라이버나 소프트웨어가 설치되지 않습니다.

---

# クイックスタート

## WindowsおよびMacのセットアップ (Windows XP, Vista, 7, 8, 8.1,または Mac 10.6+)

- 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] 화면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:* [セレクト] > [IronKey Unlocker] > [Mac] > [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 시스템が再起動するようにプロンプトを表示します。新しい 드라이버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。

---

# MISE EN ROUTE

## Installation avec Windows et Mac (Windows XP, Vista, 7, 8, 8.1 ou Mac 10.6+)

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 > Mac > 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.

# KURZANLEITUNG

## Geräte-Setup bei Windows und Mac (Windows XP, Vista, 7, 8, 8.1 oder Mac 10.6+)

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 > Mac > 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.

---

## INICIO RÁPIDO

### Instalación en Windows y Mac (Windows XP, Vista, 7, 8, 8.1 o Mac 10.6 o superior)

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 > Mac > 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.

# About my device

IronKey Enterprise H300 is designed to be the world's most secure USB hard drive. Now you can safely carry your files and data with you wherever you go.

## About IronKey Enterprise H300

IronKey™ Enterprise H300 is a USB (Universal Serial Bus) portable hard drive with built-in password security and data encryption.

Your device (once setup) will be connected to the IronKey Enterprise Management System that protects your organization's data. Device applications and features are configured by the System Administrator. Some settings that are described in this guide may not be available to you if the administrator has not enabled them for your device.

### Device features with administrative control

- » Password policies
- » Password Reset
- » Auto-locking device
- » Onboard applications (Malware Scanner)
- » Force Read-Only mode

## How is it different than a regular hard 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 a specified number of consecutive 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.**

### **Anti-Malware Autorun Protection**

Your device is capable of protecting 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, editing your preferences, changing your device password and safely locking your device.

### **Online account**

Your online account allows you to use some applications and features, such as resetting a password.

## **What systems can I use it on?**

- » Windows® 8.1
- » Windows® 8
- » Windows® 7
- » Windows® Vista
- » Windows® XP (SP2+)
- » Mac OS® X (10.6+)
- » Linux (2.6 or higher)—Note: The Linux CLI Unlocker does not support any features that require network access, for example changing your password.

The device supports USB 3.0 Super Speed. As a minimum, the computer must have a USB 2.0 port (high-speed).

Some applications are available only for specific systems:

- » **Windows Only**
  - Virtual Keyboard (English only)
  - Anti Malware
  - Device updates
- » **Mac Only**—Auto-Launch Assistant

## **How secure is it?**

IronKey Enterprise H300 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 encryption keys, 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 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 the password is verified in hardware
- » Password try-counter implemented in tamper-resistant hardware
- » Once the password try-count is exceeded, the device will initiate a permanent self-destruct sequence.
- » 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 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.

# Product specifications

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

Specification	Details
Hard Drive Capacity*	500 GB and 1 TB
Dimensions	124.6mm X 86.6mm X 26.8mm
Weight	500GB: 10.8 oz (306 grams) 1TB: 11.6 oz (328 grams)
Operating Temperature	5C, 55C
Operating Shock	400 G (2ms) / 900 G (1ms)
Hardware Encryption	<ul style="list-style-type: none"> <li>• Data: 256-bit AES (XTS Mode)</li> <li>• Hardware: 256-bit AES</li> <li>• Hashing: 256-bit SHA</li> <li>• PKI: 2048-bit RSA</li> </ul>
File System Support	<ul style="list-style-type: none"> <li>• FAT32 (Default)</li> <li>• NTFS (Windows only)</li> </ul>
EMI/EMC Compliance	USA FCC, Europe CE, Canada ICES, Australia C-Tick, Taiwan BSMI, Japan VCCI, Korea KCC KCC ID: MISP-REM-WKY-H300
Hardware	USB 3.0 (Super Speed) recommended, 2.0 (High-Speed)
Hardware accessories	USB 3.0 Type A to Micro B cable
OS Compatibility	<ul style="list-style-type: none"> <li>• Windows XP (SP2+), Windows Vista, Windows 7, or Windows 8, Windows 8.1</li> <li>• Mac 10.6+</li> <li>• Unlocker for Linux (2.6 or higher, x86)</li> </ul>
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.

IronKey Enterprise H300 devices do not require any software or drivers to be installed.

*\* Advertised capacity is approximate. Some space is required for onboard software.*

## Recommended best practices

- » Create an online account (if applicable) so that you can:
  - reset a forgotten device password
- » Lock the device
  - when not in use
  - before unplugging it
  - before the 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 do I...?

## Set up the device

The setup process is the same for Windows and Mac systems.

1. Plug the IronKey device into your computer's USB port. The "Device Setup" screen appears. The setup software runs automatically from public volume. This screen may 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 IronKey Unlocker folder.
2. Type the Activation Code. You should have received the code in an email message sent from your Administrator.
3. Select a default language preference, agree to the end-user license agreement, and then click the "Activate" button.

By default, IronKey software will use the same language as your computer's operating system.
4. Type a device password and confirm it, and then click the "Continue" button.

Your password is case-sensitive and must comply with the password policy set by the administrator.
5. If you are prompted to provide an email address for an online account, enter it now and click the "Continue" button.
6. A message prompt will appear indicating that an email has been sent to you. Follow the instructions in the email to set up your online account; this includes creating a "secret question".

Your online account is required to reset your device password.
7. Once you have set up your online account, click OK in the message prompt to proceed with the device setup.

On the Device Setup screen, select the file system for the secure volume. Mac and Linux operating systems do not support an NTFS file system.
8. Click the "Continue" button. 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.
9. 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. Some policies set by the administrator may restrict use of the product to systems running only Windows and Mac.

If you want to add or modify the message that displays on the Unlocker screen, see “Create a message that displays in the Unlocker” on page 14.

# Unlock and lock the device

## UNLOCK DEVICE

The unlock process is the same for Windows and Mac systems. For Linux systems, see “Use my device on Linux” on page 18.

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 application in the IronKey Unlocker folder.
  - **NOTE:** On a Mac you can install the Auto-Launch Assistant, which automatically opens the Unlocker when you plug in an IronKey Enterprise H300 device.
2. Type your device password and click “Unlock”. The IronKey Control Panel will appear.
  - Optionally, you can click 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 a consecutive number of times—depends on the password settings defined by the administrator— will permanently destroy the device and all your onboard data.
  - As a security precaution, you must unplug and reinsert the device after every three failed password attempts.

### Unlock the device in Read-Only mode

You can unlock your device in a read-only state so that files cannot be edited on your secure hard drive. For example, say that you want to access a file on your device while using an untrusted or unknown computer; unlocking your device in Read-Only Mode will prevent any malware on that machine from infecting your device or modifying your files. Administrators can also set your device to unlock in a read-only state.

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

- » You will see a message in the Control Panel that indicates 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.
- » 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.

### **Create a message that displays in the Unlocker**

This feature, if enabled by the System Admin, allows you to create a message that appears on the IronKey Unlocker window. For example, you can provide contact information so that if you lose your device, someone will know how to return it to you.

1. Unlock your device and click the “Settings” button in the menu bar.
2. Click the “Preferences” button in the left sidebar.
3. Enter text in the “Unlock Message” field.  
Your message text must fit the space provided (approximately 7 lines and 200 characters).


### **Automatically launch the Unlocker on a Mac**

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

1. Unlock your device and click the “Settings” button in the menu bar.
2. On the “Tools” side bar, click the “Install Auto-Launch Assistant” button.

**TIP:** To uninstall it, click on the “Uninstall Auto-Launch Assistant” button

## **LOCK 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 want the device to automatically lock when not in use, see “Set device to automatically lock” on page 14.

**NOTE:** 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 any open onboard applications and files and retry locking the device.

**NOTE:** An administrator can remotely disable your device if necessary. Disabling an unlocked device will automatically lock the device. You cannot unlock the device unless the System Admin re-enables the device.

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

### **Set device to automatically lock**

If enabled by your System Admin, 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 the “Settings” button in the menu bar.
2. Click the “Preferences” button in the left sidebar.
3. Click the checkbox for auto-locking the device and set the time-out for either 5, 15, 30, 60, 120, or 180 minutes.

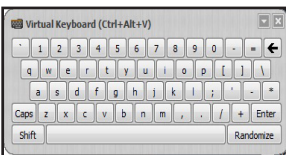
If a secure file has been opened, it may not be safe to lock the device; otherwise, you may lose the file changes or corrupt the file. The device will continue to try to lock in this situation, but will not force the application to quit. You can configure the setting to force the device to lock; however,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

**IMPORTANT:** Forcing a device to lock can result in data loss. 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 run CHKDSK

1. Unlock the device.
2. Use the following keyboard shortcut to bring up the “Run” prompt:  
WINDOWS LOGO BUTTON + R.
3. Type “CMD” and press ENTER.
4. From the command prompt, type CHKDSK, 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. Use data recovery software if necessary in order to recover your files.


## TYPE 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 keyset and is available on Windows only. The language preference for the device must be set to English.

You can start the Virtual Keyboard in a couple of ways:

1. Click the Virtual Keyboard  icon in a password field on the IronKey Unlocker or Control Panel. The Virtual Keyboard appears.
  - Alternatively, when the keyboard focus is in a password field 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 located. 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. If you do not want to use this feature, you can disable it in the options menu beside the “Close” button.

## Access my device if I forget my password

If you forget your password, you can reset it if an administrator has granted you password reset privileges. Otherwise, you must contact your administrator.

1. Plug in your device and launch the Unlocker.
2. Click the “Password Help” button.
3. On the Password Help prompt, click the “Reset Password” button. An email will be sent to the email address provided during account setup with instructions on how to proceed.
4. After you complete the instructions in the email message, click the “Continue” button.
5. Type your new password, or use the Virtual Keyboard, and confirm the password in the fields provided, then click the “Change Password” button.

## Change my password

Password settings are determined by an 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.

It is a good security practice to regularly change your password. However, be especially careful to remember your device password.

1. Unlock your device and click the “Settings” button in the menu bar.
2. Click 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.

## 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 menu bar of the IronKey Control Panel.
- WINDOWS: Opening Windows Explorer to the “Secure Files” drive.
- MAC: Opening Finder to the “Secure Files” drive.

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

## Encrypt and decrypt files

Everything you store on your IronKey Enterprise H300 device is 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 hard drive, while providing strong and “always-on” security.

- Drag a file onto the Secure Files drive to automatically encrypt it.
- Files opened from the Secure Files drive are automatically decrypted as you open them.

## Update my device

You can securely update software and firmware on your device through signed updates that are verified in hardware. Updating your device allows you to take advantage of new features and enhancements as they become available.

1. Unlock your device and click the “Settings” button on the menu bar of the IronKey Control Panel.
2. Click the “Tools” sidebar and in the Updates section, click the “Check for Updates” button.
3. If an update is available, click “Download” to install it.

**NOTE:** You must use a computer running Windows to download software updates.

**TIP:** You can check for updates automatically each time you unlock your device by clicking the “Automatically check for updates” checkbox. If your administrator has already set this option, the checkbox will appear enabled and dimmed.

## Reformat my 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 the “Settings” button in the menu bar.
2. Under Device Health, select the file format and click the “Reformat Secure Volume” button.

**IMPORTANT:** Back up your Secure Files drive to a separate location (for example, to cloud storage or your computer) before you reformat the device.

# Use my device on Linux

You can use your IronKey Enterprise H300 device on several distributions of Linux (x86 systems only with kernel version 2.6 or higher). However, you must set up the device using a Windows or Mac operating system. Some policies set by the administrator may restrict the use of the product to systems running only Windows and Mac.

## USE THE UNLOCKER

Use the Unlocker for Linux to access your files and securely transfer files from and between Windows, Mac, and Linux computers.

Depending on your Linux distribution, you may need root privileges to use the program “`ironkey.exe`” found in the Linux folder of the public volume. If you have only one IronKey Enterprise H300 device attached to the system, run the program from a command shell with no arguments (for example, `ironkey`). If you have multiple IronKey Enterprise H300 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`.

### 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 IronKey Enterprise H300 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 on any IronKey Enterprise H300 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.

## Find information about my device

### VIEW DEVICE INFORMATION

1. Unlock your device and click the “Settings” button in the menu bar.
2. Click 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
- Release Date
- Secure files drive letter
- Unlocker drive letter
- Operating System and system administrative privileges

**TIP:** You can also click the “Copy” button to copy the device information to the clipboard for pasting in an email or support request.

### DETERMINE THE STORAGE SPACE 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 (for example, the meter will be totally green when the device is full), while the white text on the Capacity Meter displays how much free space remains.

## Use onboard applications

Your administrator determines the applications that are installed on your device.

### SCAN MY DEVICE FOR MALWARE

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

## Some things to know about scanning your device:

- » The scanner runs automatically when you unlock your device.
  - It scans any running system processes and all onboard files (compressed and uncompressed) .
  - It reports and cleans any malware that it finds.
- » 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 it was last updated 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.

## EDIT THE APPLICATIONS LIST

The Applications List is the area where you can quickly launch onboard applications and files. Items in the list are shortcuts to actual files. Managing the items in the list does not alter the actual file.

1. Unlock your device. The Control Panel will appear with the Applications List selected by default.
2. If the Control Panel is already open, click the “Applications” button in the menu bar to view the Applications List. Do one of the following:
  - **To add a file or application shortcut**—Drag a file from the desktop to the Applications List area to add it to the list.
  - **To add, rename, sort or delete items in the list**—Right-click anywhere in the Application List and choose the action from the options menu.
  - **To change the way icons appear in the list**—Right-click anywhere in the Application list and choose, “Large icons”, “List”, or “Tile”.

## Some things to know about the Applications List:

- » You can add any file 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 file type.
- » 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.

## RESTORE ONBOARD APPLICATIONS

You can restore your onboard applications if they are ever erased or corrupted (Windows only).

1. Unlock your device, and click the “Settings” button on the menu bar of the IronKey Control Panel.
2. Click the “Tools” button in the left sidebar and then, under Device Health, click the “Restore Onboard Apps” button.

## Manage my online account settings

**NOTE:** You may not have an online account if your System Administrator has not enabled this feature. Online accounts are typically created during device setup. You must have an online account to use features such as resetting a password.

Your device supports advanced cryptographic authentication using strong PKI key pairs generated in the Cryptochip. When you log into your online account from your device, it uses these unique keys as your digital identity credentials. This locks down your account so that you must have both your device and your password in order to gain access. In other words, only you can access your online account, even if someone stole your device or password.

### To log on to your online account

1. Unlock your device and click the “Settings” button on the menu bar of the Control Panel.
2. Click the “Account” button in the left sidebar.
3. Click the “Manage Account Settings” button.

## CHANGE DEVICE NICKNAME

If you own more than one IronKey Enterprise H300 device, you can create nicknames for each device. Names help you tell the devices apart from each other.

1. Log on to your online account.
2. On the “My IronKeys” tab, click the “Edit” button beside the device whose nickname you want to change.
3. Type a new nickname in the box and click the “Save” button.

## MANAGE ACCOUNT SETTINGS

The following table describes some tasks you can perform when you log on to your online account.

- Access your online account and then follow the steps in the table below.

Task	Description
Review account activity	Click “Account Dashboard” to monitor recent events such as logins, failed password attempts and so on.

Set up email alerts	Click “Account Alerts” to have email alert notices sent to you when specific activities occur, such as an incorrect secret question attempt. You can also sign up to be notified of new IronKey product announcements.
Edit Secret Questions and Answers	Click the “Edit” button to modify your Secret Question responses that you provided during the setup of your online account. You can also edit time zone data.

**NOTE:** You cannot update email addresses in your online profile unless you are a System Administrator.

# Where can I get Help?

## For more information

[support.ironkey.com](http://support.ironkey.com)

[securityfeedback@imation.com](mailto:securityfeedback@imation.com)

<https://www.ironkey.com>

Support information, knowledgebase and video tutorials

Product feedback and feature requests

General information

Please contact your Help desk or System Administrator if you have further questions.

*NOTE: Imation 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 Imation on the issue discussed as of the date of publication. Imation cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. Imation makes no warranties, expressed or implied, in this document. Imation, the Imation logo, IronKey and the IronKey logo are trademarks of Imation Corp. and its subsidiaries. All other trademarks are the property of their respective owners.

© 2014 Imation Corp. All rights reserved. IK-H300-USR02-1.0

### 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 into 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.*

### Industry Canada

*This Class B digital apparatus complies with Canadian ICES-003.*

*Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.*

