



DATALOCKER H300/H350 ENTERPRISE ENCRYPTED EXTERNAL HARD DRIVE

User Guide

© 2016 DataLocker Inc. All rights reserved.

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

Ironkey™ is a registered trade mark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment 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.



CONTENTS

Quick Start	4
Mise en route	4
Kurzanleitung	5
Inicio rápido	5
クイックスタート	6
빠른 시작	6
快速入门	7
快速入門	7
About my device	8
How is it different than a regular hard drive?	8
What systems can I use it on?	9
How secure is it?	9
Product specifications	10
Recommended best practices	11
Using my device	13
Setting up the device	13
Unlocking and locking the device	14
Managing passwords	16
Accessing my secure files	17
Updating my device	18
Reformatting my device	18
Using my device on Linux	18
Finding information about my device	20
Using on-board applications	20
Managing my online account settings	22
Where can I get Help?	23

QUICK START

Enterprise devices must be set up using a Windows or Mac operating system. 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 18.

Windows & Mac Setup (Windows XP, Vista, 7, 8, 8.1, 10 or Mac OS X 10.6+)

1. Plug the device into your computer's USB port.
2. When the Device Setup window appears, follow the on-screen instructions. If this window does not appear, open it manually:
 - **Windows:** Start > This PC > Unlocker > Unlocker.exe
 - **Mac:** Finder > Unlocker > Unlocker
3. When Device Setup is complete, you can move your important files to the **PRIVATE USB** drive and they will be automatically encrypted.

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

MISE EN ROUTE

Installation avec Windows et Mac (Windows XP, Vista, 7, 8, 8.1, 10 ou Mac OS X 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 > Unlocker > Unlocker.exe
 - **Mac :** Finder > Unlocker > Unlocker
3. Lorsque l'installation du périphérique est terminée, vous pouvez déplacer vos fichiers importants vers le lecteur PRIVATE USB (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, 10 oder Mac OS X 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 > This PC > Unlocker > Unlocker.exe
 - **Mac:** Finder > Unlocker > Unlocker
3. Wenn das Geräte-Setup abgeschlossen ist, können Sie Ihre wichtigen Dateien auf das Laufwerk „PRIVATE USB“ 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, 10 o Mac 10.6 OS X 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 > Unlocker > Unlocker.exe
 - **Mac:** Finder > Unlocker > Unlocker
3. Tras finalizar la instalación del dispositivo, podrá mover sus archivos importantes a la unidad “PRIVATE USB” 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.

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、10 または Mac OS X 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] 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] > [Unlocker] > [Unlocker.exe]
 - **Mac** の場合 : [セレクト] > [Unlocker] > [Unlocker]
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「PRIVATE USB」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。

빠른 시작

Windows 및 Mac 설정 (Windows XP, Vista, 7, 8, 8.1, 10 또는 Mac OS X 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 > **Unlocker** > **Unlocker.exe**
 - **Mac:** **Finder** > **Unlocker** > **Unlocker**
3. 장치 설정이 완료되면 중요한 파일을 'PRIVATE USB' 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.

快速入门

Windows & Mac 安装（Windows XP、Vista、7、8、8.1、10 Mac OS X 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 > **Unlocker** > **Unlocker.exe**
 - **Mac**：Finder > **Unlocker** > **Unlocker**
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。

快速入门

Windows 与 Mac 设定（支援系统为：Windows XP、Vista、7、8、8.1、10 或 Mac OS X 10.6 以上版本）

1. 将装置连接到您的电脑 **USB** 连接埠。
2. 当装置设定视窗出现时，请依照画面上指示操作。
若此视窗并未出现，请手动开启：
 - **Windows**：开始 > 我的电脑 > **Unlocker** > **Unlocker.exe**
 - **Mac**：Finder > **Unlocker** > **Unlocker**
3. 当装置设定完成时，即可将您的重要档案移至「安全档案」装置，接著这些档案就会自动加密。
部分 **Windows** 系统会在您第一次连接装置后，提示您重新启动电脑。您可以放心关闭此提示且无需重新启动，因为系统并无安装任何新的驱动程序或软体。

ABOUT MY DEVICE

DataLocker® H300 Enterprise and DataLocker® H350 Enterprise are USB (Universal Serial Bus) 3.0, portable hard drive drives with built-in password security and data encryption. They are designed to be the world's most secure USB hard drives. Now you can safely carry your files and data with you wherever you go.

Figure 1: H Series hard drives

H300



H350



Once you set up your device, you will be connected to IronKey EMS, the Cloud or On-Prem server by DataLocker that manages your organization's devices. 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
- On-board applications (Malware Scanner)
- Force Read-Only mode

HOW IS IT DIFFERENT THAN A REGULAR HARD DRIVE?

FIPS 140-2 Level 3 certification (H350 only)

H350 is a FIPS-certified device so you can feel confident that you're complying with regulatory requirements.

Hardware Encryption

The Cryptochip in your device protects your data to the same level as highly classified government information. This security technology is always on and cannot be disabled.

Password-Protected

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

Self-Destruct Sequence

If the Cryptochip detects physical tampering, 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—*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 DataLocker Control Panel, a program for accessing your files, managing your device and editing your preferences, changing your device password, and safely locking your device. Enterprise device users can also access their online account (if applicable) and admin users can open the Admin Console from the Control Panel.

Online account

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

WHAT SYSTEMS CAN I USE IT ON?

- Windows® 10
- Windows® 8.1
- Windows® 8
- Windows® 7
- Windows® Vista
- Windows® XP (SP2+)
- Mac OS® X (10.6 or higher)
- Linux (2.6 or higher)—**Note:** The Linux CLI Unlocker does not support any features that require network access, for example setting up your device or changing your password.

Some applications are available only on specific systems:**Windows Only**

- Virtual Keyboard (English only)
- Anti-Malware Scanner
- Device updates

Mac Only

- Auto-Launch Assistant

HOW SECURE IS IT?

H300 and H350 devices have 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 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, 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 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 further details about your device, see the **Device Info** page in the DataLocker Control Panel. See “To view device information” on page 20.

Table 1: H300 and H350 Device Specifications

Specification	Details
Hard Drive Capacity*	500GB, 1TB, 2TB
Dimensions	124.6mm (L) x 86.6mm (W) x 26.8mm (H)

Table 1: H300 and H350 Device Specifications

Specification	Details
Weight	500GB: 10.8 oz (306 grams) 1TB: 11.6 oz (328 grams) 2TB: 11.8 oz (334 grams)
Operating Temperature	5C, 55C
Operating Shock	400 G (2ms) / 900 G (1ms)
Hardware Encryption	<ul style="list-style-type: none"> • 256-bit AES (XTS Mode) • Hardware: 256-bit AES • Hashing: 256-bit SHA • PKI: 2048-bit RSA
File System Support	<ul style="list-style-type: none"> • FAT32 (Default) • NTFS (Windows only)
EMI/EMC Compliance	USA FCC, Europe CE, Canada ICES, Australia C-Tick Taiwan BSMI, Japan VCCI, Korea KCC (KCC ID: MSIP-REM-WKY-H300) (KCC ID:MSIP-REM-WKY-H350)
Certification	FIPS 140-2 level 3 certified (applies to H350 only)
Hardware	<ul style="list-style-type: none"> • USB 3.0 (SuperSpeed) port recommended, As a minimum, the computer must have a USB 2.0 port (high-speed).
Hardware accessories	USB 3.0 Type A to Micro B cable
OS Compatibility	<ul style="list-style-type: none"> • Windows 10, Windows 8.1, Windows 8, Windows 7, Windows XP (SP2+), Windows Vista • Mac OS X (10.6 or higher) • Linux (2.6 or higher, x86)
Accessibility	DataLocker Control Panel is designed to be Section 508 compliant. Users with disabilities have keyboard navigation and screen reader support.
Warranty	5 Years Limited

Designed and assembled in the U.S.A.

H300/H350 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

1. Create an online account (if applicable) so that you can reset a forgotten device password.
2. Lock the device (see “Locking the device” on page 15)
 - when not in use
 - before unplugging it
 - before the system enters sleep mode

3. Never unplug the device when the LED is on.
4. Never share your device password.
5. Perform a computer anti-virus scan before setting up the device.

USING MY DEVICE

SETTING UP THE DEVICE

Devices managed by IronKey™ EMS must be set up using a Windows or Mac operating system. 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

1. Plug the USB cable into the device and insert the cable 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 **Unlocker** drive in **This PC** and double-clicking the **Unlocker.exe** file.
- **Mac:** Opening the **Unlocker** drive in **Finder** and then opening the **Unlocker** 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 14.

2. Type or paste 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 **Activate**. By default, device software will use the same language as your computer's operating system.
4. Type a device password and confirm it, and then click **Continue**.
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 **Continue**. Your online account is required to reset your device password.
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 choosing and answering a "secret question". The secret question will be used to verify your identity if you have to reset your password.
7. Once you have set up your online account, click **OK** in the message prompt to proceed with the device setup.
8. 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.
9. 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 DataLocker 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 device to systems running only Windows and Mac.

Installing the Auto-Launch Assistant (Mac only)

Installing the Auto-Launch Assistant will automatically open the 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 19. 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—defined by the administrator—will permanently destroy the device and all your onboard 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. Administrators can also force your device to unlock in a read-only state.

When working in this mode, the DataLocker 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 **Unlocker** drive in **This PC** and double-clicking the **Unlocker.exe** file.
 - Mac: Opening the **Unlocker** drive in Finder, and then opening the **Unlocker** 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 14.
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 DataLocker Control Panel will appear.

Tip: You can also use the virtual keyboard (runs in Windows and is English only) to type your password, see “Typing passwords with the Virtual Keyboard” on page 16.

Changing the Unlock message

The Unlock message is custom text that displays in the Unlocker window when you unlock the device. This feature, if enabled in policy by the System Admin, 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 DataLocker 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, if enabled in policy by your System Admin, 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 on-board 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 DataLocker icon in the system tray and click **Lock Device**.

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

To set a device to automatically lock

1. Unlock your device and in the DataLocker 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.

Note: 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 **PRIVATE USB** drive letter, and then **"/F /R"**.
For example, if the **PRIVATE USB** 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

Password policy 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. If you forget your password, see “Accessing my device if I forget my password” on page 17.

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 16.

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. It is available on Windows only. The language preference for the device must be set to English.

To type a password using the Virtual Keyboard (Windows only)

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

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



This check box will only appear if your administrator has enabled Password Reset for your device. Password Reset allows you to reset your password if you forget the code at device login.


To reset your password

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

ACCESSING MY SECURE FILES

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

To access my secure files

1. Click the **Files**  button on menu bar of the DataLocker Control Panel.
 - **Windows:** Opens Windows Explorer to the **PRIVATE USB** drive.
 - **Mac:** Opens **Finder** to the **PRIVATE USB** drive.
2. Do one of the following:
 - To open a file, double-click the file on the **PRIVATE USB** drive.
 - To save a file, drag the file from your computer to the **PRIVATE USB** drive.


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

UPDATING 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.

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

To update the device

1. Unlock your device and click the **Settings**  button on the menu bar of the DataLocker Control Panel.
2. From the left sidebar, click **Tools**.
3. In the **Updates** section, click **Check for Updates**.
4. If an update is available, click **Download** to start the install process and follow the instructions on-screen.

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

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 DataLocker Control Panel.
2. Click **Tools** on the left sidebar.
3. Under **Device Health**, select the file format and click **Reformat Secure Volume**.

USING MY DEVICE ON LINUX

You can use your device on several distributions of Linux (x86 systems only with kernel version 2.6 or higher). Enterprise devices must be set up using a Windows or Mac operating system, see “Setting up the device” on page 13. Also, some policies, set by the administrator, may restrict the use of the device to systems running only Windows or Mac.

Using the Unlocker

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

Note: `unlocker.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 `unlocker.exe`.

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

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

To unlock the device, enter:

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

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

`unlocker.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:

`unlocker.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 `unlocker.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:
`unlocker.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, unlock, and change passwords on any devices they plug in.

4. Supported distributions

Not all distributions of Linux are supported. Please visit <http://support.datalocker.com> for the latest list of supported distributions.

5. The 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 DataLocker Control Panel, to see how much storage space is still available on your device. The green bar graph represents how full the device is (for example, the meter will be totally green when the device is full). The white text on the Capacity Meter displays how much free space remains.



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

To view device information

1. Unlock your device and in the DataLocker 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

Note: To visit the DataLocker website or access more information about legal notices or certifications for DataLocker 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.

USING ON-BOARD APPLICATIONS

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

Scanning my device for malware


If enabled by your System Administrator, the Malware Scanner is a self-cleaning technology that detects and removes malware that gets on your device from an infected file or computer. 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.

Editing the Applications List

The Applications List, located in the Control Panel, is the area where you can quickly launch on-board applications and files. Items that appear in the list are shortcuts to the actual files. Managing the list items 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 on 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. You can also right-click the Applications List area and click **Add Application**.
 - **To rename or delete list items**—Right-click the application or file and choose the action from the menu.
 - **To sort or change the way icons appear in the list**—Right-click anywhere in the Application list and choose, **Large icons**, **List**, or **Tile**, or **Sort Alphabetically**.

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.

Restoring on-board applications

You can restore on-board applications installed by IronKey EMS if they are ever erased or become corrupt (Windows only).


1. Unlock your device, and click the **Settings**  button on the menu bar of the DataLocker Control Panel.
2. Click **Tools** in the left sidebar. Under **Device Health**, click **Restore Onboard Apps**.

MANAGING MY ONLINE ACCOUNT SETTINGS

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 your device or password is stolen.

To log in to your online account

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

Changing the device nickname

If you own more than one Enterprise 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 Devices** tab, click the **Edit** button beside the device for which you want to change the nickname.
3. Type a new nickname in the box and click the **Save** button.

Managing online account settings

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

Log on to 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 product announcements.
Edit Secret Questions and Answers	On the Account Settings tab, 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?

The following resources provide more information about DataLocker products. Please contact your Help desk or System Administrator if you have further questions.

- support.datalocker.com—Support information, knowledge base and video tutorials
- support@datalocker.com—Product feedback and feature requests
- www.datalocker.com—General information