IRONKEY™ EMS
by DATALOCKER

DATALOCKER SENTRY EMS SECURE USB 3.0 FLASH DRIVE

User Guide

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.

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.

CONTENTS

QUICK START

Windows & Mac Setup (Windows XP, Vista, 7, 8, 8.1, 10 or Mac OS X v. 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 > 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 v. 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 > 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 v. 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 > 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 OS X v. 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 > 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 *v. 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] > [Unlocker] > [Unlocker.exe]
   - **Mac** の場合 : [セレクタ] > [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 *v. 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 > **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 *v. 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 > **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。

快速入門

Windows 與 Mac 設定 （ 支援系統為：Windows XP、 Vista、 7、 8、 8.1、 10 或 Mac OS X *v. 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 > **Unlocker** > **Unlocker.exe**
   - **Mac：Finder > Unlocker > Unlocker**
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。

ABOUT MY DEVICE

DataLocker® Sentry EMS is a USB (Universal Serial Bus) 3.0, secure portable flash drive drive with built-in password security and data encryption. Now you can safely carry your files and data with you wherever you go.

Sentry EMS devices can be managed by IronKey EMS Cloud or On-Prem server by DataLocker, allowing companies to control the applications, policies, and use of devices.

Figure 2-1 : Sentry EMS drive

HOW IS IT DIFFERENT THAN A REGULAR FLASH DRIVE?

FIPS 140-2 Level 3 certification

Sentry EMS 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.

Device Reset

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

Anti-Malware Autorun Protection (device must be activated with IronKey EMS)

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.

WHAT SYSTEMS CAN I USE IT ON?

- Windows® 10
- Windows® 8, 8.1 (No RT)
- Windows® 7 SP1
- Windows® Vista SP2
- Mac OS® X v. 10.9.x - 10.11.x

The following applications are available only on systems running Windows:

- Virtual Keyboard (English only)
- Anti-Malware Scanner (available only with devices managed by IronKey EMS)

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 22.

Table 2-1: Sentry EMS Device Specifications

Specification	Details
Capacity*	4GB, 8GB, 16GB, 32GB, 64GB
Speed**	**USB 3.0:** • 4GB: 80MB/s read, 12MB/s write • 8GB & 16GB: 165MB/s read, 22MB/s write • 32GB: 250MB/s read, 40MB/s write • 64GB: 250MB/s read, 85MB/s write **USB 2.0:** • 4GB: 30MB/s read, 12MB/s write • 8GB–64GB: 30MB/s read, 20MB/s write
Dimensions	77.9 mm x 22.2 mm x 12.05 mm
Waterproof	• Up to 4 ft. (1.2m) • Conforms to IEC 60529 IPX8 • Product must be clean and dry before use
Temperature	*Operating:* 0°C to 60°C *Storage:* -20°C to 85°C
Hardware Encryption	256-bit AES (XTS Mode)
EMI/EMC Compliance	TAA Compliant, FCC, CE, VCCI & KC, RoHS & WEEE
Certification	FIPS 140-2 level 3 certified

Table 2-1: Sentry EMS Device Specifications

Specification	Details
Hardware	USB 3.0 compliant and USB 2.0 compliant Requires 2 free drive letters
OS Compatibility	• Windows 10, Windows 8.1, Windows 8, Windows 7 (SP1), Windows Vista (SP2) • Mac OS X v.10.9.x-10.11.x
Accessibility	DataLocker Control Panel is designed to be Section 508 compliant. Users with disabilities have keyboard navigation and screen reader support.
Warranty	2 Years Limited

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

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

** Speed varies with host hardware, software and usage

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.

SUPPORT AND CONTACT INFORMATION

The following resources provide more information about DataLocker products. Please contact your Help desk or System Admin 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

GETTING STARTED

SETTING UP MY DEVICE

The setup process is the same for systems running Microsoft Windows or Mac. If your device will be managed by IronKey EMS, you must also activate the device with the management system. See "Activating my device with IronKey™ EMS" on page 13.

To set up the device

1. Plug the device into the USB port of your computer. Once the system detects your device, start the Device Setup by following the instructions for the operating system that you're running.

   Windows

   - If the **AutoPlay** window appears, under **Install or run program from your media**, click **Run Unlocker.exe**.
   - If your system does not allow AutoPlay, open Windows File Explorer and on the virtual DVD drive, double-click the **Unlocker.exe** file.

   Mac

   - On the Desktop, click the **Unlocker CD-ROM** icon. In the **Finder** window, click the **Unlocker** application.

2. Select a default language preference from the list. By default, device software will use the same language as your computer's operating system.

3. Review and click the check box to accept the license agreement and click **Continue**.

4. In the **Password** text box, type a device password, and then re-enter your password in the **Confirm** text box. The password protects data on the secure drive. Passwords are case-sensitive and must have at least 8 characters (including spaces).

5. Click **Continue**.

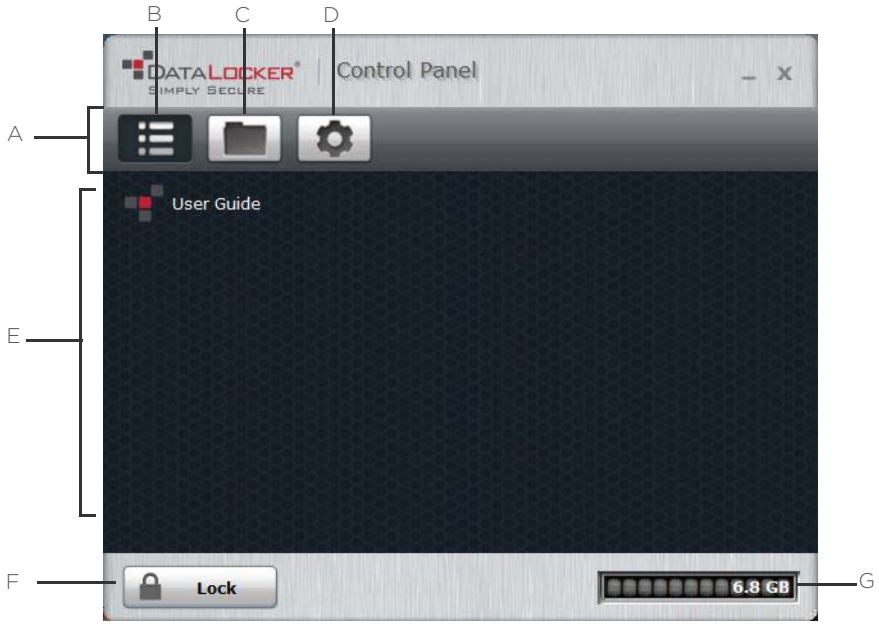
   The device initializes. Once complete, the DataLocker Control Panel opens. Your device is now ready to store and protect your data.

Note: If your device will be managed by IronKey EMS Cloud or On-Prem Server, see "Activating my device with IronKey™ EMS" on page 13.

ABOUT DATALOCKER CONTROL PANEL

DataLocker Control Panel is onboard software that lets you manage your device settings, such as changing your password, auto-lock and language preferences, or reformatting your device. You can use Control Panel to open files and applications on your device.

Figure 3-1 : DataLocker Control Panel user interface



A. Main menu bar **B.** Applications button—Displays all onboard programs or files saved to the Applications List **C.** Files button—Opens the secure drive of Sentry EMS in a file manager (Windows File Explorer or Mac Finder) **D.** Settings button—Opens the Settings page in Control Panel **E. Applications List**—displays device applications and files saved to this list **F.** Locks the secure drive (see also, "Locking the device" on page 17) **G.** Capacity Meter—Displays the space available on the secure drive

ACTIVATING MY DEVICE WITH IRONKEY™ EMS

Sentry EMS devices can be managed using IronKey™ EMS Cloud or IronKey™ EMS On-Prem server by DataLocker. IronKey EMS is sold separately. When you activate your device with IronKey EMS, features and applications are installed or applied to your device according to the settings and policies in IronKey EMS. The following list of features and applications are available with managed devices:

- *Password policies*—Your device must comply with the password policy set in IronKey EMS
- *Password reset*—Allows you to reset your device password if you forget it.
- *Auto-lock device*—Administrators can determine if your device will auto-lock after a period of inactivity.
- *Onboard applications (Malware Scanner)*—Scans your device for malware.
- *Force Read-Only mode*—Allows an administrator to force your device to open in Read-Only mode if necessary.

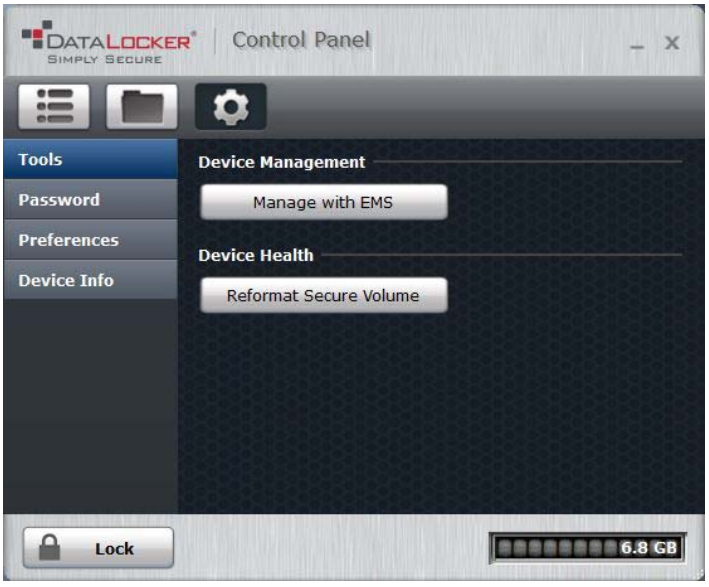
Activation pre-requisites

Before you activate your device you will need:

- The Activation Code provided by your IronKey EMS System Admin; this is typically sent in an email message.
- A network or Internet connection to IronKey EMS.
- A computer running a supported Windows or Mac operating system (see *"OS Compatibility" on page 10*).

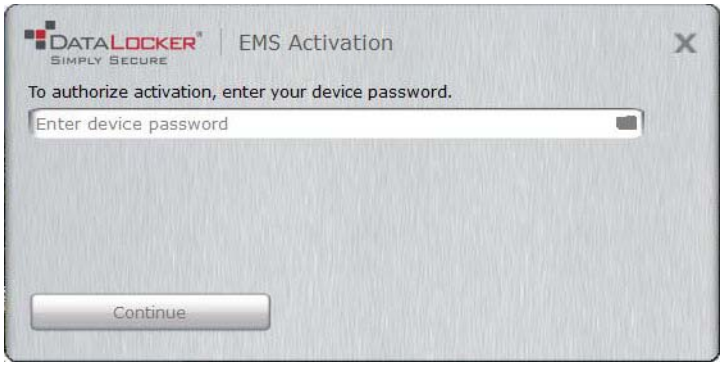
To activate your device

1. In DataLocker Control Panel, click the **Settings** button.
2. In the left sidebar, click **Tools**.
3. Under **Device Management**, click **Manage with EMS**.



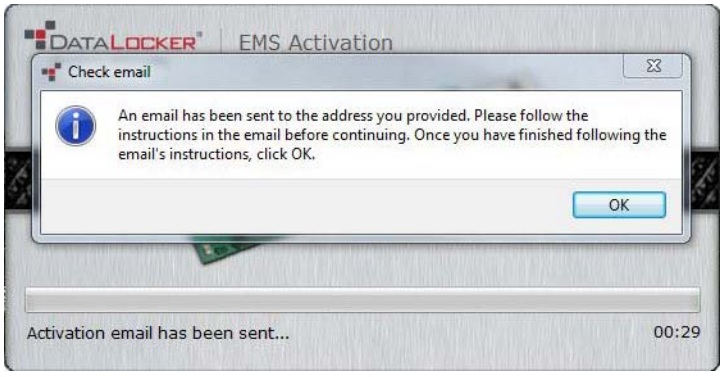
4. On the **EMS Activation** screen, type or paste the Activation Code in the **Activation Code** field. You should have received the code in an email message sent from your IronKey EMS System Admin.

5. Review and agree to the end-user license agreement, and then click **Activate**.
6. Type your device password to authorize activation.



7. On the **Change Password** screen, type a new password that conforms to the IronKey EMS password policy requirements indicated on the screen.

8. A message prompt will appear indicating that an email has been sent to you. Follow the instructions in the email and then return to this message and click **OK**; You will be asked to set up a "secret question" and "answer" that will be used to verify your identity if you have to reset your password.



9. When the successful activation message appears, click **OK** to exit the activation process.

Your device is now activated and managed by IronKey EMS. Additional applications may have been installed on your device based on the device policy settings chosen by your System Admin.

USING MY DEVICE

The following section provides information about common device tasks including:

- Unlocking the device
- Locking the device
- Managing passwords
- Accessing my secure files
- Reformatting my device
- Viewing device information
- Scanning my device for malware
- Editing the Applications List

UNLOCKING THE DEVICE

Once you enter the correct password, the device will mount the secure volume with all your secure applications and files. If you enter an incorrect password 10 consecutive times, the device will be reset and all onboard data will be erased.

Unlocking in Read-Only Mode

Unlocking your device in a read-only state prevents files from being modified or infected with malware, for example, when using the device on an untrusted computer. In Read-Only Mode you cannot add, modify or erase files on the device, this includes reformatting the device and restoring applications or editing the Applications List. For devices managed by IronKey EMS, a System Admin can also force your device to unlock in a read-only state.

To unlock the device

1. Insert the device in 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

   - If the **AutoPlay** window appears, under **Install or run program from your media**, click **Run Unlocker.exe**.
   - If your system does not allow AutoPlay, open Windows Explorer and on the virtual DVD drive, double-click the **Unlocker.exe** file.

   Mac

   - On the Desktop, click the **Unlocker CD-ROM** icon. In the **Finder** window, click the **Unlocker** application.
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 19.

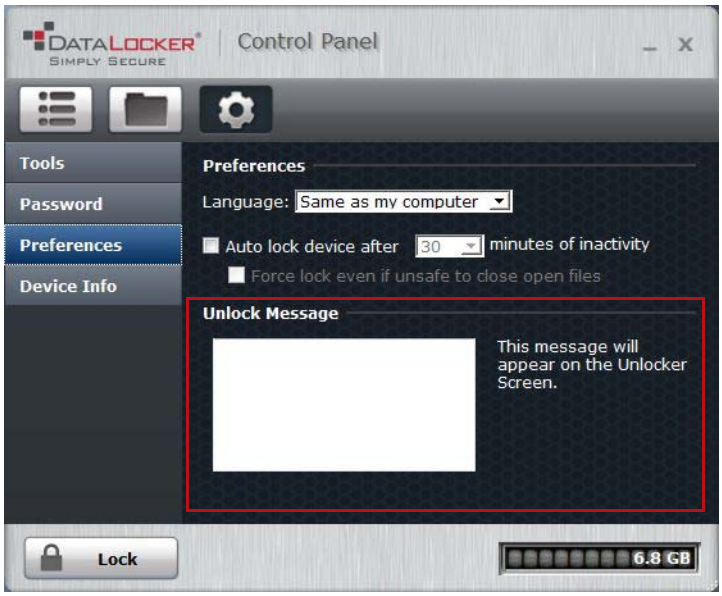
Note: To exit Read-Only mode, lock your device and click to clear the **Read-Only Mode** check box the next time you unlock it.

Changing the Unlock message

The Unlock message is custom text that displays in the Unlocker window when you unlock the device. You can 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. If your device is managed by IronKey EMS, this feature is only available if enabled in the device policy by the System Admin.

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 not in use to prevent unwanted access to your secure files. You can manually lock the device or set the device to automatically lock after a specified period of inactivity. If your device is managed by IronKey EMS, auto-locking the device must be enabled in policy by your System Admin.

By default, to prevent potential file corruption, your device will not lock if applications or files on the drive are open. Close any open onboard 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 them 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: If your device is managed by IronKey EMS, it 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 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

Secure password management includes regularly changing your password. Make sure you remember your device password. If you forget it, see "Accessing my data if I forget my device password" on page 20.

If your device is managed by IronKey EMS, password policy settings are determined by an administrator. 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.

You can use the Virtual Keyboard instead of the real keyboard to type your password, see "Typing passwords with the Virtual Keyboard" on page 19.

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

The Virtual Keyboard helps protect your device password from keylogging and screenlogging spyware by letting you click out letters and numbers instead of typing them on a keyboard, bypassing 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 data if I forget my device password

If your device is *not* managed by IronKey EMS, there is no way to unlock it if you do not know the password; your only option is to reset the device back to its pre-setup state, *all onboard data will be permanently lost*. If your device *is* managed by IronKey EMS, you can reset your password if you have password reset privileges; these are granted by an IronKey EMS System Admin. All onboard data is maintained. Otherwise, you must reset the device or contact your System Admin. The following figure displays the Password screen in Control Panel Settings for a managed device where the Password Reset option is enabled.

Figure 4-1 : Password Reset settings in Control Panel

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 it.

To reset your password (applies only to devices managed by IronKey EMS)

1. Plug in your device and start the Unlocker window.
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 device activation with IronKey EMS.
4. Follow the instructions in the email message and then return to the Unlocker window. Enter the password recovery code and click **Continue**.
5. Type your new password (or use the Virtual Keyboard) and confirm the password in the fields provided, then click **Change Password**.

Note: If your EMS account setup is not complete, or you do not have an email address associated with your user account in EMS, or if you cannot access your email message, contact your system administrator.

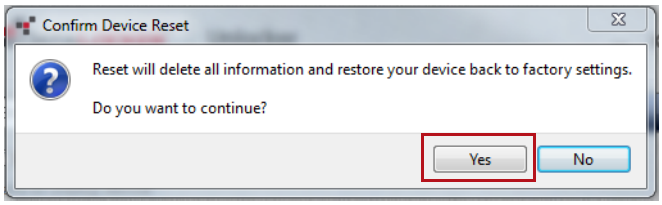
To reset your device

1. Plug in your device and wait for the operating system to detect it.

2. In the Notification area of the Windows taskbar, right-click the DataLocker icon and click **Reset Device**.

If you are using a Mac, click the DataLocker icon in the Menu bar and choose **Reset Device**.

3. A confirmation message will display to indicate that you are about to reset your device. If you're sure you want to reset it, click **Yes**. *Important: All data will be lost and your device will be reset to factory settings.*



Note: As a security feature to prevent unauthorized access to device data, your device will automatically reset to a factory state if 10 consecutive incorrect login attempts are entered.

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 flash 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**.

REFORMATTING MY DEVICE

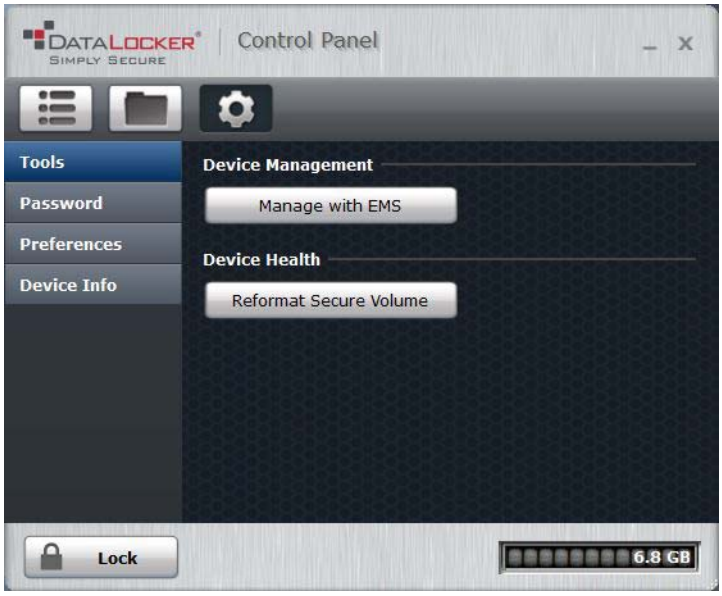
Reformatting the secure volume will erase all your files and your Applications List, but it will not erase your device password and settings.

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**.



VIEWING DEVICE INFORMATION

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.

Figure 4-2 : Capacity meter in Control Panel

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 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.

SCANNING MY DEVICE FOR MALWARE

Malware Scanner is available only when enabled by your System Admin for devices managed by IronKey EMS. Malware Scanner is a self-cleaning technology that detects and removes malware from your device. Powered by the McAfee® Anti-Virus and Anti-Malware signature database, it is updated regularly to protect your device from the latest malware threats.

Malware Scanner:

- Runs automatically when you unlock your device.
- Scans any running system processes and all onboard files (compressed and uncompressed).
- Reports and cleans any malware that it finds.

Updating Malware Scanner

The scanner is automatically updated before each scan to protect you from the latest malware threats. Requirements for updating:

- An Internet connection.
- A minimum of 135 MB of free space on the device to accommodate the downloaded malware signature files.

Note: 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 (see Figure 3-1 on page 12), is the area where you can quickly launch onboard 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 Applications 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 onboard applications (managed devices only)

You can restore onboard 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**.