

Sentry ONE User Guide

DataLocker Inc.

January, 2021



Sentry ONE Standard and Managed



Contents

About This Guide	3
Quick Start	3
About My Device	3
How Is This Different Than A Regular USB Drive?	3
What Systems Can I Use It On?	4
Citrix Compatibilities	4
Updating Your Device	4
Product Specifications	4
Recommended Best Practices	5
Setting Up My Device	6
Device Access (Windows Environment)	6
Device Access (macOS Environment)	6
Standard Device Initialization	7
DataLocker Control Panel	7
Setting Up A Managed Device With SafeConsole	8
Setting Up A Managed Device With IronKey EMS	9
Strong Password	9
Using My Device - Standard And Managed Features	10
Verifying Device Security	10
Accessing My Secure Files	10
Unlocking In Read-Only Mode	10
Changing The Unlock Message	11
Locking The Device	11
Exit Control Panel On Lock	12
Typing Passwords With The Virtual Keyboard	12
Managing Passwords	13
Formatting My Device	13
Finding Information About My Device	14
Editing The Applications List	14
Resetting My Device	15
Using My Device - Managed Only Features	15
Accessing My Device If I Forget My Password	15
Restricted Files Notifications	16
Scanning My Device For Malware	16
Sanitize	17
Using ZoneBuilder In SafeConsole	17
Using My Device On Linux	18
Using The Unlocker	18
Where Can I Get Help?	19



About This Guide

DataLocker Sentry ONE is available in Standard or Managed versions. The Standard version of the Sentry ONE does not require a management platform. The Managed version requires a device license and can be managed by either SafeConsole or IronKey® EMS. Both SafeConsole and IronKey EMS are secure cloud or on-premises management platforms that allow your organization to centrally manage compatible USB (Universal Serial Bus) storage devices easily and efficiently.

This guide will explain how to setup and initialize both a Standard and Managed device.

Quick Start

Windows® & macOS® Setup

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
 - macOS: 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.

About My Device

DataLocker Sentry ONE USB 3.0 is a portable flash drive with built-in password security and data encryption. It is designed to be the world's most secure USB flash drive. Now you can safely carry your files and data with you wherever you go.



Figure 1: DataLocker Sentry ONE

How Is This Different Than A Regular USB Drive?

FIPS 140-2 Level 3 Certification - The Sentry ONE 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 with the same level of protection as highly classified government information. This security technology feature 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.



Anti-Malware Autorun Protection (Managed Only) - 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 8.1
- Windows 7
- macOS (v10.9 - 11.0.x)
- 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 only available on specific systems:

Windows Only

- Virtual Keyboard (English only)
- Device Updates

Citrix Compatibilities

The Sentry ONE and Sentry ONE Managed are compatible with:

- Citrix Virtual Apps and Desktops service on Azure
- XenApp 7.14
- XenApp 7.15 LTSR
- XenApp 7.16
- XenApp 7.17
- XenDesktop 7.14
- XenDesktop 7.15 LTSR
- XenDesktop 7.16
- XenDesktop 7.17

Updating Your Device

For the latest system compatibility, including macOS 64bit support a device update may be required. It is recommended to always update your device to the latest version.

Updated software and documentation are freely available for download at our website:

- Latest device updates - <http://datalocker.com/device-updates>
- Documentation and support - <https://support.datalocker.com>

Important: Only the latest device updates should be applied to the device. Downgrading the device to an older software or firmware version is not supported and can potential cause a loss of stored data or impair other device functionality. The latest device updates will always be available at the link above.

Product Specifications

For further details about your device, see the **Device Info** page in the DataLocker Control Panel.



Specification	Details
Capacity*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
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 & 128GB: 250MB/s read, 85MB/s write USB 2.0: - 4GB: 30MB/s read, 12MB/s write - 8GB-128GB: 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 Hardware	FIPS 140-2 level 3 certified USB 3.0 compliant and USB 2.0 compliant Requires 2 free drive letters
OS Compatibility	Windows 10, Windows 8.1, Windows 7 (SP1) macOS v.10.9.x-11.0.x Linux 2.6.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 ONE 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, usage, and applied policy.

*** Limited Feature Set. No online management features.

Recommended Best Practices

1. Lock the device:

- when not in use
- before unplugging it



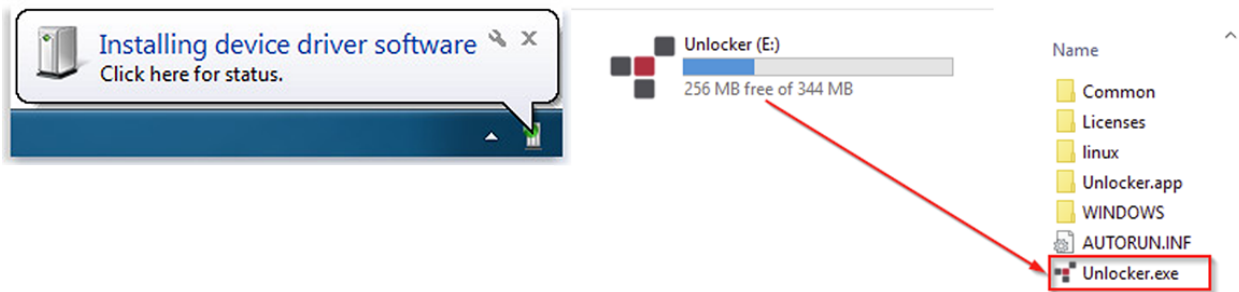
- before the system enters sleep mode
2. Never unplug the device when the indicator LED is flashing.
 3. The device password should be unique and should not be shared.
 4. Perform a computer anti-virus scan before setting up the device

Setting Up My Device

To ensure there is ample power provided to the Sentry ONE encrypted USB drive, insert it directly into a USB 2.0/3.0 port on a notebook or desktop. Avoid connecting it to any peripheral devices that may feature a USB port, such as a keyboard or USB-powered hub. Initial setup of the device must be done on a supported Windows or macOS based operating system.

Device Access (Windows Environment)

1. Plug the Sentry ONE encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.
 - Windows 7/8.1/10 users will receive a device driver notification.
 - Once the new hardware detection is complete, Windows will prompt to begin the initialization process.
2. Select the option **Unlocker.exe** inside of the Unlocker partition that can be found in File Explorer. Please note that the partition letter will vary based on the next free drive letter. The drive letter may change depending on what devices are connected. In the image below, the drive letter is E:.



Device Access (macOS Environment)

1. Plug the Sentry ONE encrypted USB drive into an available USB port on the macOS notebook or desktop and wait for the operating system to detect it.
2. Double click the **Unlocker** volume that appears on the desktop to start the initialization process.
 - If the Unlocker volume does not appear on the desktop, open Finder and locate the Unlocker volume on the left side of the Finder window (listed under Devices.) Highlight the volume and double-click the Unlocker application icon in the Finder window. This will start the initialization process.

Note: macOS may prompt for additional permissions upon initialization to access removable drives. Please allow this permission for the full functionality of the device.

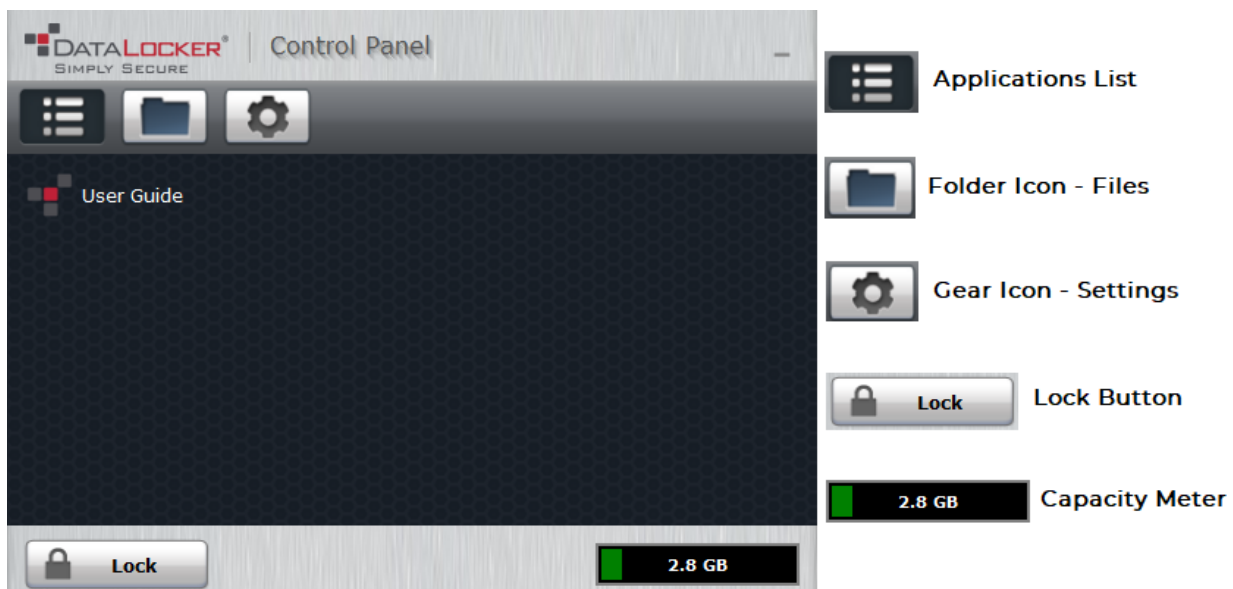


Standard Device Initialization

Initialization of your Sentry ONE device will depend on if you have the **Standard** (Optionally Managed) or (Forced) **Managed** device. Initializing a Sentry ONE Managed will require an Activation Code or Connection Token from your IronKey EMS or SafeConsole Administrator. IronKey EMS and SafeConsole require a device license for activation. *License sold separately.* For information on how to initialize a Sentry ONE Managed see: [Setting Up A Managed Device](#).

1. Select a language preference from the list. By default, device software will use the same language as your computer's operating system (if available).
2. Review the license agreement, check the checkbox to accept it, and click **Continue**.
3. In the Password text box, type a device password, then re-enter your password in the Confirm text box. The password protects the data on the secure drive. Passwords are case-sensitive and must have at least 8 characters along with more requirements if **Strong Password** is enabled.
4. If initializing on Windows, you will be given the option of formatting the PRIVATE_USB drive as either FAT32 or exFAT. For more information, see [Formatting My Device](#).
5. Click **Continue**. The device will finish initializing. Once complete, the DataLocker Control Panel will open. Your device is now ready to store and protect your data.

DataLocker Control Panel



Upgrading My Device From Standard To Managed (Windows And macOS Systems Only)

If notified by your System Administrator, you can upgrade your DataLocker Sentry ONE Standard device to a Managed device. Managed devices are compatible with SafeConsole or IronKey EMS. When you upgrade your device, you will be required to activate it using a Connection Token or Activation Code, provided by your administrator. An internet connection is required to complete this process.

Important: Only start the upgrade process if your System Administrator has asked you to activate your device with SafeConsole or IronKey EMS. Upgrading a device is not reversible. Once managed,



the device will remain managed, even after a reset.

To upgrade from Standard to Managed:

1. When you receive the Connection Token or Activation Code from your System Administrator, start the DataLocker Control Panel and click **Settings (Gear Icon)**. See the [DataLocker Control Panel](#) for more information.
2. In the left sidebar, click **Tools**, then click **Manage Device**.
3. Paste the Connection Token or Activation Code in the Activation text box.
4. Follow the on-screen instructions.
5. Additional applications may be installed on your device based on the device policy settings chosen by your System Administrator. You may also be required to change your password so it conforms to the password security policy set for managed devices in your organization.

Setting Up A Managed Device With SafeConsole

The initialization process will begin by allowing the device to be ready to communicate with the SafeConsole server. The steps needed to register a Sentry ONE Managed to SafeConsole will depend on the policies that your administrator is enforcing. Not all options will be shown.

A SafeConsole Connection Token will be needed. The SafeConsole Connection Token is obtained by the System Administrator through the Quick Connect Guide, located inside of the SafeConsole user interface.

Users without access to a Management Server, please contact sales: sales@datalocker.com / +1(913)310-9088

1. Enter the SafeConsole Connection Token that is obtained in the steps above. Review the license agreement, check the checkbox to accept it, and click **Activate** in the bottom left-hand corner.
 - **Optionally Enabled Policies** - These policies may or may not be enabled by your System Administrator. They will appear during device registration if they have been enabled.
 - Confirm Ownership of the device: Enter the Windows username and password that is associated with the login credentials of the computer the device is plugged into.
 - Custom Device Information: Required information about you or your device. The required fields will vary.
 - Unique User Token: This token is directly associated with the end user's account and will be provided by the System Administrator.
 - Administrator Registration Approval: The System Administrator may require their approval to proceed with device registration.
2. Enter a secure Password and Confirm it. Once the password created meets the requirements listed to the right side of the input fields, click **Continue**. The requirements of this password will depend on the policy selected by your administrator. Passwords are case-sensitive and must have at least 8 characters along with more requirements if **Strong Password** is enabled.
3. Choose a Secure Volume File System (see [Formatting My Device](#)) and click **Continue**.
4. The device will now finalize the setup process and be ready for use. Access the Encrypted Storage by clicking the **Folder Icon** in the top menu. The settings of the device can be accessed and altered by clicking the **Gear Icon**. See the [DataLocker Control Panel](#) for more information.



Setting Up A Managed Device With IronKey EMS

The initialization process will begin by allowing the device to be ready to communicate with the IronKey EMS server. **NOTE:** Functionality of Managed Sentry ONE Devices varies depending on whether the device is managed by SafeConsole or IronKey EMS. Some functionality in this guide will pertain exclusively to SafeConsole Managed Sentry ONE Devices. Examples include Anti-Malware Quarantine, Device Santize and Restricted File notifications.

An IronKey EMS Activation Code will be needed. The IronKey EMS Activation Code is obtained by the System Administrator through the IronKey EMS Console. This code can also be emailed to the end user.

Users without access to a Management Server, please contact sales: sales@datalocker.com / +1(913)310-9088

1. Enter the IronKey EMS Activation Code that is obtained in the steps above. Review the license agreement, check the checkbox to accept it, and click **Activate** in the bottom left-hand corner.
2. Enter a secure Password and Confirm it. Once the password created meets the requirements listed to the right side of the input fields, click **Continue**.
3. Depending on the policy created by your System Administrator, you may be required to create an Online Account. An email will be provided to the end user with the instructions on how to create an online account. After the account has been confirmed, click **OK**.
 - The user will receive an Online Account Error message if the online account has not been created or there was an issue while attempting to verify the account.
4. Choose a Secure Volume File System (see [Formatting My Device](#)) and click **Continue**.
5. The device will now finalize the setup process and be ready for use. Access the encrypted storage by clicking the **Folder Icon** in the top menu. The settings of the device can be accessed and altered by clicking the **Gear Icon**. See the [DataLocker Control Panel](#) for more information.

Strong Password

While creating or changing the password for the device there is an option to enable **Enforce Strong Password**. For Managed devices this option may be configured or enforced by your System Administrator. When enabled the following rules are checked against all potential passwords.

- Must be at least eight (8) characters in length.
- Must include characters from at least three (3) of the following character classes:
 - ASCII digits (0123456789) **Note:** If the last character of the password is an ASCII digit, then it does not count as an ASCII digit for this restriction.
 - lowercase ASCII (abc...xyz)
 - uppercase ASCII (ABC...XYZ) **Note:** If the first character of the password is an uppercase ASCII letter, then it is not counted as an uppercase ASCII letter for this restriction.
 - non-alphanumeric ASCII (!@#\$, etc)
 - non-ASCII characters

Strong Password Examples

Example Passwords	Results
password	Failed: 8 characters long, however, only contains 1 unique character class (lowercase ASCII).



Example Passwords	Results
Password1	Failed: 9 characters long, however the Capital 'P' and '1' do not count toward the unique character classes, leaving only lowercase ASCII.
pa\$\$Word	Pass: 8 characters long. Contains lowercase ASCII, uppercase ASCII, and non-alphanumeric ASCII.

Note: These passwords are for examples only and should not be used when setting up the device.

Using My Device - Standard And Managed Features

Verifying Device Security

If a secure USB storage device has been lost or unattended it should be verified as per the following user guidance. The secure USB storage device shall be discarded if it may be suspected that an attacker has tampered with the device or if the self test fails.

- Verify the secure USB storage device visually, that it doesn't have marks or new scratches that might indicate tampering.
- Verify that the secure USB storage device is physically intact by slightly twisting it.
- Verify that the secure USB storage device weighs about 30 grams.
- Verify when plugged into a computer that the blue indicator light on the secure USB storage device blinks (the correct frequency is 3 times per second at initial connection and during read/write operations).
- Verify that the secure USB storage device is showing as a DVD-RW and a storage partition is not mounted until the device is unlocked
- Verify that the device software on the virtual DVD-RW drive is issued by DataLocker Inc before executing it.

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 them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, "always-on" security.

To access your secure files:

1. Click **Files** on menu bar of the DataLocker Control Panel.
 - Windows: Opens Windows Explorer to the PRIVATE_USB drive.
 - macOS: 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.

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

Unlocking In Read-Only Mode

You can unlock your device in a read-only state so that files cannot be altered 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. Managed devices can be forced to unlock in a read-only state by an administrator.

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 in Read-Only Mode:

1. Insert the device into the USB port of the host computer and run the **Unlocker.exe**.
2. Check the **Read-Only Checkbox** below the password entry box.
3. Type your device password and click **Unlock**. The DataLocker Control Panel will appear with the text *Read-Only Mode* at the bottom.

Changing The Unlock Message

The Unlock Message is custom text that displays in the Unlocker window when you unlock the device. This feature allows you to customize the message that displays. For example, adding classification labels can help identify which documents can be saved to the device due to company policy. For managed devices, System Administrators have the ability to set a pre-defined message and disable the ability for it to be changed or created.

To change the Unlock Message:

1. In the DataLocker Control Panel, click **Settings** 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 in the space provided (approximately 7 lines and 200 characters).

Locking The Device

Lock your device when you are not using it to prevent unwanted access to your secure files on the drive. You can manually lock the device or you can set the device to automatically lock after a specified period of inactivity. For Managed devices, this feature may or may not be enabled by your System Administrator.

Caution: 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.

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 (Windows only).

To manually lock the device:

1. Click **Lock** in the bottom left-hand corner of the DataLocker Control Panel to safely lock your device.
 - You can also use the keyboard shortcut: **CTRL + L** (Windows only), or right-click the **DataLocker Icon** in the system tray and click **Lock Device**.

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



To set a device to automatically lock:

1. Unlock your device and click **Settings** on the menu bar in the DataLocker Control Panel.
2. Click **Preferences** in the left sidebar.
3. Click the **Checkbox** 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.

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, 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.

Exit Control Panel On Lock

When your device is locked, the Control Panel will close automatically. To unlock the device and access the Control Panel, you will need to run the Unlocker application again. If desired, the Control Panel can be set to return to the Unlock screen after the user locks the device.

To disable **Exit Control Panel on lock**:

1. Unlock your device and click **Settings** on the menu bar in the DataLocker Control Panel.
2. Click **Preferences** in the left sidebar.
3. Click the **Checkbox** for Exit Control Panel on lock.

Typing Passwords With The Virtual Keyboard

If you are unlocking your device on an unfamiliar computer and are concerned about keylogging and screen logging 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 screen loggers.

Note: This feature uses a standard QWERTY key set. It is available on Windows only and 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 the 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.

Hint: Click **Randomize** to arrange the keys in a random order. This helps protect against screen loggers.

Note: When you click a key in the Virtual Keyboard, all of the keys briefly go blank. This feature prevents screen loggers from capturing what you clicked. To disable this feature, click the icon (beside the Exit button) and choose **Disable Screen Logger Protection**.



Managing Passwords

You can change your password on your device by accessing the Password tab in the DataLocker Control Panel.

For Managed devices, password policy settings are determined by your System 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.

Note: When a password is required, for example, when logging into the device or during a manual password change operation, you can use the Virtual Keyboard instead of the actual keyboard to type the password.

To change your password:

1. Unlock your device and click **Settings** 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. Passwords are case-sensitive and must have at least 8 characters along with more requirements if **Strong Password** is enabled.
5. Click **Change Password**.

Formatting My Device

Your device will need to be formatted during initialization, before it can be used to store files.

If initializing on Windows, you will be given the option of formatting the PRIVATE_USB drive as either FAT32 or exFAT.

Options are for Windows operating systems only - macOS will automatically format to FAT32

- **FAT32**
 - Pros: Cross-platform compatible (Windows, macOS, and Linux)
 - Cons: Limited individual file size of 4GB
- **exFAT**
 - Pros: No file size limitations
 - Cons: Microsoft restricts usage by license obligations

After initialization, reformatting the PRIVATE_USB drive will erase all your files and your Application List, but will not erase your device password and settings.

Important: Before you reformat the device, back up your PRIVATE_USB drive to a separate location, for example, to cloud storage or your computer.

Note: For managed devices, the System Administrator may limit the ability to reformat drives if a filesystem already exists on the drive.

To reformat a device:

1. Unlock your device and click **Settings** 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**.



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 click **Settings** on the menu bar of the DataLocker Control Panel.
2. Click **Device Info** in the left sidebar.

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

- Model Number
- Hardware ID
- Serial Number
- Software Version
- Firmware Version
- Release Date
- Secure Files Drive Letter
- Unlocker Drive Letter
- Operating System and System administrative Privileges
- Management Console

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.

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

Editing The Applications List

The Applications List, located in the DataLocker 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. For managed devices, this feature may be disabled by your System Administrator.

To edit the Applications List:

1. Unlock your device. The DataLocker Control Panel will appear with the Applications List selected by default.
2. If the DataLocker Control Panel is already open, click the **Applications Icon** 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, Tile, or Sort Alphabetically.

Functions of 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 macOS. Similarly, macOS application files will be hidden from view on Windows computers.

Resetting My Device

Your device can be reverted back to factory settings. This will securely wipe all data from the device and a new security key will be created for the next use.

For Managed devices, your System Administrator may have this option disabled. Contact your administrator if you need to reset your device.

Resetting your device:

1. Unlock your device.
2. Right-click on the **DataLocker Icon** in the system tray.
3. Click **Reset Device**.

To prevent accidental device resets a popup will ask to enter a random four digits. After entering the confirmation, the device will now be reset back to factory settings.

Note: If the device was originally standard and connected to a management server, the management requirements will still be enforced even after a reset.

Using My Device - Managed Only Features

Accessing My Device If I Forget My Password

If you forget your password and an administrator has granted you password reset privileges, you can reset it. If your administrator has not granted password reset privileges, you must contact your administrator for help resetting your password.

To reset your password:

1. Plug in your device and start the Unlocker.
2. Click **Password Help**.
3. Depending on the management platform, you may receive an email with instructions on how to obtain your recovery code. Otherwise, you will need to contact your administrator to obtain this code. In the latter case, you may be required to provide the request code and serial number to your System Administrator. Your System Administrator's email and phone number should be provided for your convenience. Clicking the email address will open up your default email client and pre-populate this information to be sent.
4. Once received the recovery code will need to be copied and pasted exactly as it is given to you. Incorrect codes count against the ten unlock attempts before the device is reset.
5. Type your new password (or use the Virtual Keyboard) and confirm it in the fields provided, then click **Change Password**. **Note:** Passwords are case-sensitive and must have at least 8 characters along with more requirements if **Strong Password** is enabled.

Warning: If the device is currently offline from the management server a warning will be shown that the new password will not be able to be backed up until the device is unlocked while online. If you believe this message is shown in error, please contact your System Administrator immediately.



Restricted Files Notifications

If enabled by your SafeConsole administrator, your device may restrict certain files from being saved to the secure storage. When an affected file is restricted, you will receive a notification containing the file's name. If desired, you can disable these notifications.

NOTE: Affected files will still be restricted when notifications are disabled.

To disable restricted files notifications:

1. Unlock your device and click **Settings** on the menu bar in the DataLocker Control Panel.
2. Click **Preferences** in the left sidebar.
3. Click the **Checkbox** for Show restricted files notifications.

Scanning My Device For Malware

If enabled by your SafeConsole administrator, the Malware Scanner is a self-cleaning technology that detects and quarantines malware on your device. 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, scans your device, then reports and cleans any malware that is found.

Your system administrator may require the anti-malware definition to be updated before the device can be unlocked. In this event, the full anti-malware definition will need to be downloaded to a temporary folder on the local computer before the password can be entered. This can increase the time it takes to unlock the device based on the host computer's networking connection and the size of malware updates needed.

Some things to know about scanning your device:

- The scanner runs automatically when you unlock your device.
- It scans all onboard files (compressed and uncompressed).
- It will report and delete any detected malware.
- (Optional) If your SafeConsole Administrator has enabled Quarantine, it may quarantine any malware it finds. See [Restoring or Deleting a Quarantined File](#) for more information.
- 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 of the last update is displayed in the Control Panel.
- If the scanner becomes too far out of date, it will need to download a large file to bring it back up-to-date.

Restoring or Deleting a Quarantined File

If your SafeConsole administrator has enabled Quarantine, you will have the option of restoring or deleting detected malware. This process helps when McAfee® detects a valid document as malware.

NOTE: Depending on the size of infected files, Quarantine may not be available. If the file cannot be quarantined, it will be deleted. Deleted files cannot be restored using the following process.

If a file is detected as infected, a warning dialog will be shown with the option to lock the drive at that time. Quarantined files remain on the device in an encrypted state to prevent further execution.

To view quarantined files:



1. Unlock your device and click **Settings** in the DataLocker Control Panel.
2. Click **Quarantine** on the left sidebar.

Selecting a file from the list will display additional details including, Threat Name, Threat Type, anti-malware definition version, and the date of quarantine. After the file is selected files can either be Restored or Deleted.

Restored files will be exempt from automatic scanning while the device is currently unlocked. The file will be scanned during the next unlock or if a manual scan is selected from the **Anti-Malware** tab. If the anti-malware definitions still determine that the file is infected, it will quarantine the file once again.

Deleted files will be permanently deleted.

Sanitize

Sanitize allows for the contents of the encrypted drive to be securely erased. This is accomplished by erasing the encryption key that the drive uses to access files on the Secure Volume while still retaining the connection to SafeConsole.

Warning: Performing this action will completely erase all data on the Secure Volume. This action is permanent.

The ability to sanitize a drive depends on the settings configured by your SafeConsole administrator. If allowed your drive can be sanitized by the following steps:

1. Unlock your device and open the device Control Panel by launching **Unlocker.exe**.
2. Right click the system tray icon for the Control Panel and select **Sanitize Device**.
3. Enter the numbers prompted in the dialog box to confirm that all data can be wiped from the drive.
4. The device will reset. Unplug and plug your device back into your workstation.
5. Launch **Unlocker.exe** and input the device password.

Using ZoneBuilder In SafeConsole

If enabled by your System Administrator, ZoneBuilder is a SafeConsole tool used to create a Trusted Zone of computers. It can be used to restrict device access to computers within the Trusted Zone, and if enabled, can automatically unlock your device, which eliminates the need to enter your password.

If your administrator chooses to enable this policy, you may be required to trust the account.

Trusting the account:

1. Unlock your device and click **Settings** in the DataLocker Control Panel.
2. Click **Zone Builder** on the left sidebar.
3. Click **Trust This Account**.
4. Enter the password for the device and click **OK**. Your account will now show up in the Trusted Accounts box.

Your account is now in the Trusted Zone of computers. Depending on the policy set by your System Administrator, you may have restricted device access outside of the Trusted Zone or when offline. Your device may also be set to automatically unlock on trusted computers.

To remove a trusted account, simply highlight the account you wish to remove and click **Remove**.



Using My Device On Linux

You can use your device on several distributions of Linux. There are two executables in the linux folder, Unlocker_32.exe and Unlocker_64.exe. For this guide, replace Unlocker_xx.exe with the executable that is compatible with your system.

The device must be previously set up using a Windows or macOS operating system. See [Setting Up My Device](#) for more information. Some Managed device policies, set by the System Administrator, may restrict usage of the device to systems only running Windows or macOS operating systems.

Using The Unlocker

Use the Unlocker_xx.exe for Linux to access your files. Depending on your Linux distribution, you may need root privileges to use the program Unlocker_xx.exe found in the Linux folder of the mounted public volume. If the binary files inside the linux folder are not mounted with the executed bit then the files will need to be copied the computer's local file system and the execute bit manually added by using the following commands.

- `chmod +x Unlocker_32.exe`
- `chmod +x Unlocker_64.exe`

If you have only one device attached to the system, run the program from a command shell with no arguments (for example, `Unlocker_xx.exe`). This will then prompt you for your device password to unlock the drive. If you have multiple devices, you must specify which one you want to unlock.

Note: Unlocker_xx.exe only unlocks the PRIVATE_USB; 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_xx.exe.

Simply un-mounting the device does not automatically lock the PRIVATE_USB. To lock the device, you must either unmount and physically remove (unplug) it, or run:

- `Unlocker_xx.exe -l`

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

1. Kernel Version must be 2.6 or higher
2. Mounting
 - 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.
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.
4. The Unlocker for Linux supports x86 and x86_64 systems.
5. Policies that will block the device
 - If the device is disabled within the policy settings in either SafeConsole or IronKey EMS, you will not be able to unlock the device.



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: Information, knowledgebase articles, and video tutorials
- support@datalocker.com: Feedback and feature requests
- datalocker.com: General information
- datalocker.com/warranty: Warranty information



© 2021 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 trademark 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 to 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.

