User Guide

Sentry 5 FIPS 140-3 Level 3 (pending) certified

Sentry ONE (Managed) FIPS 140-2 Level 3 certified

Table of Contents

About This User Guide & Reference Manual

Sentry ONE is available in Standard or Managed versions. DataLocker Sentry 5 is available in a Managed version. The Standard standalone version of the device does not require a management platform, but can still optionally be managed. The Managed versions always requires a device license and can be managed by SafeConsole. SafeConsole is a secure cloud or on-premises management platform that allows your organization to manage compatible USB storage devices easily and efficiently centrally.

This guide will explain how to set up and initialize both Standard and Managed devices.

The discontinued devices Sentry EMS and Sentry 3 FIPS are also compatible with the instructions in this manual. The Sentry 3 FIPS must be updated to device software version 6.x+.

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

The DataLocker Sentry 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. More details can be found on the Product Resources page.

What Systems Can I Use It On?

- Windows™ 11, 10, 7
- macOS Intel, M1 or M2 processor
- 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.

More detailed compatibilies can also be found at: https://datalocker.com/device-updates

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. The standalone update process can only be performed on Windows. Managed devices that are running version 6.5+ can receive device software updates from SafeConsole automatically on both Windows and macOS without required elevated privileges.

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

- Latest device updates - https://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 potentially 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

Please see the accompanying product datasheet for the product specification which can be found at our Product Resources page.

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

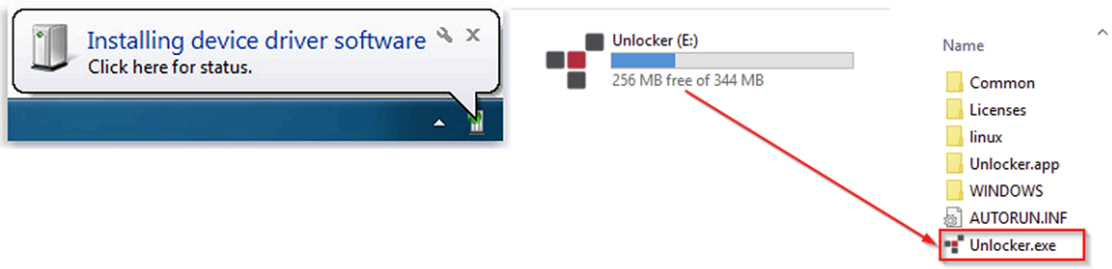
Setting Up My Device

To ensure there is ample power provided to the encrypted USB drive, insert it directly into a USB type A port on a notebook or desktop. If possible avoid connecting it to any peripheral devices that may feature a USB port, such as a keyboard or USB-powered hub as it might cause the device to be slower or not get enough power. 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 encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.
   - Windows 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 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 device will depend on if you have the Standard (Optionally Managed) or (Forced) Managed device. Initializing a Sentry Managed will require a Connection Token from your SafeConsole Administrator. SafeConsole requires a device license for activation. License sold separately. For information on how to initialize a Sentry Managed see: Setting Up A Managed Device.

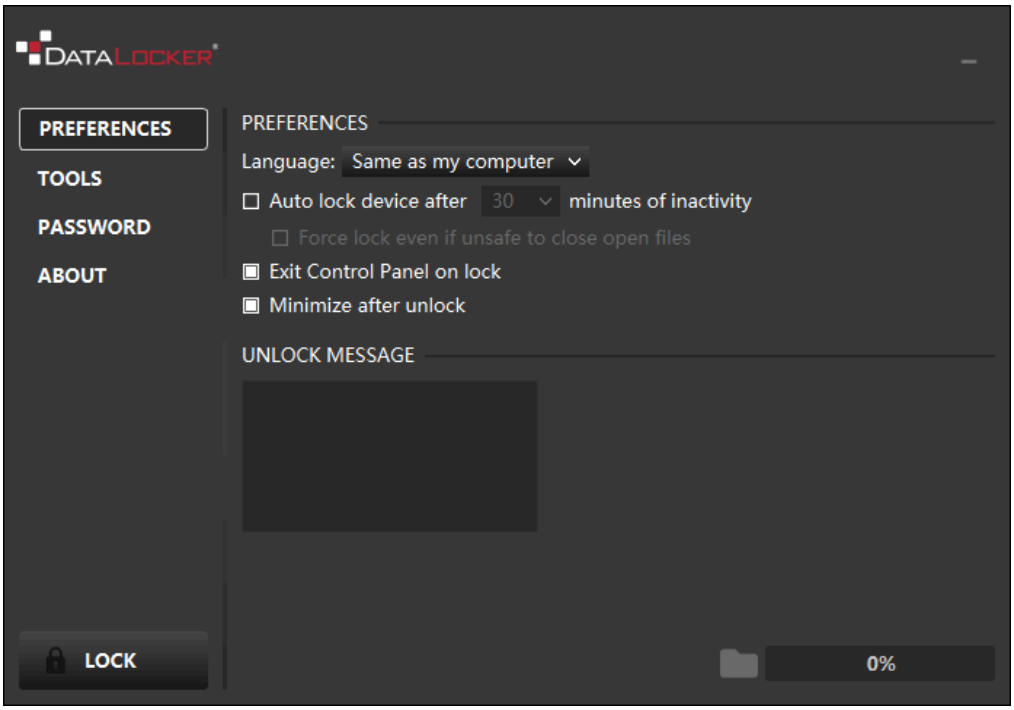
1. Select a language preference from the list. By default, device software will use the same language as your computer's operating system (if available).

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.

4. 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



Screenshot of Unlocker.exe running, also referred to as the DataLocker Control Panel

Upgrading My Device From Standard To Managed

If notified by your System Administrator, you can upgrade your DataLocker Sentry Standard device to a Managed device using a Windows or macOS host. Managed devices are compatible with SafeConsole. When you upgrade your device, you will be required to activate it using a Connection Token, 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. 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 from your System Administrator, start the DataLocker Control Panel.
2. In the left sidebar, click Tools, then click Manage Device.
3. Paste the Connection Token in the 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.

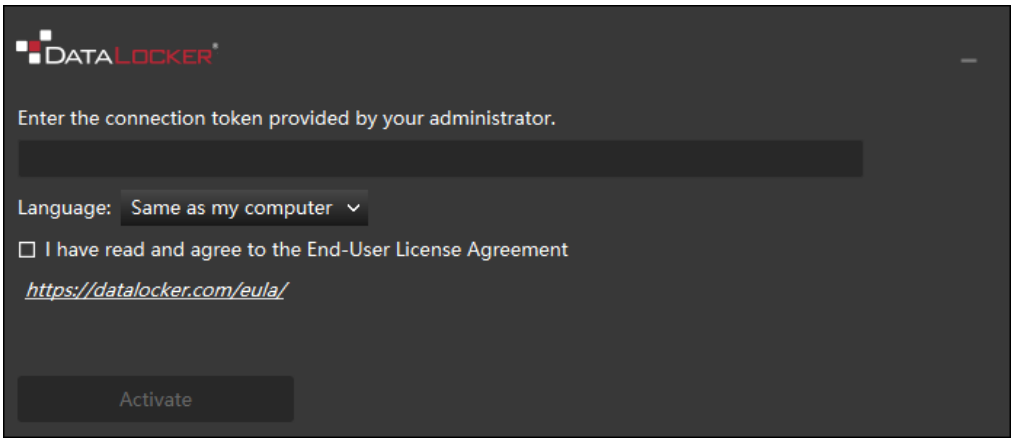
Setting Up A Managed Device With SafeConsole

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 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. The device will now finalize the setup process and be ready for use. Access the Encrypted Storage by clicking the Folder Icon in the lower right corner.

Strong Password

For Managed devices this "Strong Password" option may be 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

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 Folder Icon in the lower right corner 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, 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 predefined message and disable the ability for it to be changed or created.

To change the Unlock Message:

1. In the DataLocker Control Panel, click Preferences in the left sidebar.
2. Type the message text in the Unlock Message field. The text must fit in the space provided (approximately 6 lines and 200 characters).

Minimize Control Panel on unlock

When your device is unlocked, the Control Panel is minimized to the taskbar automatically. If desired, the Control Panel can remain displayed after the user unlocks the device.

To disable Minimize after unlock:

1. In the DataLocker Control Panel, click Preferences in the left sidebar.
2. Click the Checkbox for Minimize after unlock.

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.
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. In the DataLocker Control Panel, click Preferences in the left sidebar.
2. Click the Checkbox for Exit Control Panel on lock.

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.

To change your password:

1. Unlock your device.
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 by your System Administrator.
5. Click Change Password.

Reformatting My Device

Your device is automatically formatted as FAT32 during initialization.

Reformat options are for Windows operating systems only - macOS will automatically reformat 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 perform a quick format and provide an empty drive, but will not erase your device password and settings. To completely clean the media between uses select sanitize or reset. Sanitize and reset will perform a cryptographic erasure that will permanently erase any content on the secure storage partition.

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.
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 full your device is. . The color of the bar changes based on how much space is used: green 0-49%, yellow 50-79%, red 80-100%. The text on the Capacity Meter displays how much space is used.

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

To view device information:

1. Unlock your device and 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.

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. You will need to contact your administrator to obtain this code. You may be required to provide the request code and serial number to your System Administrator. Your System Administrator's email and phone number might 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 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 by your System Administrator.

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 back 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.
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.
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.
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.

If you are not intending to manage your device with SafeConsole you can set up your device on Linux. The device will then be able to unlock on Linux, macOS and Windows. This requires Linux Unlocker v6.7.0+.

For managed devices they 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 to 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/parameters, for example:

```
Unlocker_64.exe
```

This will prompt you to either set up your device or prompt you for the device password to unlock the drive. If you have multiple devices, you must specify which one you want to unlock.

These are the available parameters for the device software:

```
Options:

  -h, -help        help

  -u, -unlock      unlock device

  -l, -lock        lock device

  -ro, -readonly   unlock as read only

  -cp, -changepwd  change password [unmanaged devices only]
```

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
```

If the device is unmanaged and has not been used, you enter the setup by running the device software with no parameters, for example:

```
Unlocker_64.exe:
```

These are the available setup prompts:

The device can, after a setup on Linux, be used on Windows and macOS, but it cannot be managed by SafeConsole.

```
Linux Unlocker v6.7.0

----------------------------

The device is not set up.

Do you want to set-up the device? (Y/n)
```

Proceed by pressing enter or Y/n, then provide:

```
New password:

Confirm new password:
```

DEVICE SET-UP

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 SafeConsole, you will not be able to unlock the device.
   - ZoneBuilder is currently not supported under Linux and can also cause the device to be blocked.

Example Linux prompts

Getting 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 tickets, information, knowledgebase articles, and video tutorials
datalocker.com: General information
datalocker.com/warranty: Warranty information

Document Version

The latest version of this document resides at
https://media.datalocker.com/manuals/sentry/DataLocker_Sentry_ONE_User_Guide.pdf

https://media.datalocker.com/manuals/sentry/DataLocker_Sentry_5_User_Guide.pdf

This document was compiled on Jan 17, 2024, v3

Notices

DataLocker is continuously updating its products, the images and text in this manual may vary slightly from the images and text displayed by your device. These changes are minor and should not adversely affect the ease of setup.

Disclaimer

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, DataLocker Sentry, and the DataLocker logo are registered trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. All rights reserved.

Patents

Patent: **datalocker.com/patents**

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.