Sentry K300 User Guide

DataLocker Inc.

March, 2019

Sentry K300

Contents

At A Glance

Introduction

Congratulations on your purchase of the Sentry K300™ Encrypted Flash Drive. This user manual is intended to help you configure your device. Because DataLocker is constantly updating its products, the images and text in this manual may vary slightly from the images and text displayed by your Sentry K300. These changes are minor and should not affect the ease of setup adversely.

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

- Updates: latest device updates
- Support: documentation and support

The Sentry K300 stands alone as the only platform independent, keypad, solid state flash drive to incorporate an OLED display to enable advanced security features. The display supports true alpha-numeric password based authentication and a full featured on-board menu system. With modern security policies requiring alpha-numeric passwords, the Sentry K300 is the only storage device with full support for alpha and numeric characters.

Although the Sentry K300 is extremely user friendly, it is recommended that you review this guide to ensure that you become fully acquainted with the Sentry K300 and all of its features.

About the Sentry K300

The DataLocker Sentry K300 offers affordable military-grade security with 256-bit AES hardware-based encryption in XTS mode that provides always on protection for your data. Unlike software-based encryption, the Sentry K300 cryptochip does not export encryption keys to the host PC, thereby protecting against cold-boot and malware attacks.

The Sentry K300 is completely cross-platform compatible and OS agnostic. With no software or special drivers required, the Sentry K300 works with Windows, Linux, macOS, Android phones and tablets, Chromebooks, and embedded systems - any system that can utilize USB Mass Storage. Since the Sentry K300 also has its own power supply, the device can be used as a bootable device running Windows to Go, Ubuntu Linux, the local operating system, or other portable operating systems.

Best Practices

- If the battery within the device is low or dead, charge it by plugging it into a certified USB port for 30 minutes before using the drive.
- Remove the device from the computer before using the keypad to prevent USB damage.
- The device must be completely dry before connecting to a computer.
- Only connect the device to certified USB ports.
- Safely eject the device from the operating system before removing it. For more information, see Accessing The Sentry K300.
- Use a strong password and be sure to remember it.
- Use the correct file system based on operating system and file needs. See Formatting The Sentry K300 for more information.

Product Specifications

Specification	Details
Capacity*	8GB, 16GB, 32GB, 64GB, 128GB, 256GB
Speed**	USB 3.1 Gen 1: - 8GB, 16GB, 32GB: 220MB/s Read, 100MB/s Write - 64GB, 128GB, 256GB: 220MB/S Read, 200MB/s Write USB 2.0: - All: 30MB/s read, 20MB/s write
Dimensions	101mm (L) x 22mm (W) x 13mm (H)
Weight	30.4g
Water Resistant***	IP57
Operating System Compatibility	Windows, macOS, Linux
Operating Temperature	0°C - 45°C
Storage Temperature	-20°C - 60°C
Long Term Storage Temperature (More than 1 week)	-20°C - 40°C
Warranty	3 years Limited
Hardware	USB 3.1 Gen 1 (SuperSpeed) port recommended. Backwards compatible with USB 2.0 ports (High Speed)

* Advertised capacity is approximate. Some space is required for onboard software.
** Speed varies with host hardware, software, and usage.
*** Device should be completely dry before use.

Citrix Compatibilities

The Sentry K300 is compatible with:

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

Setup

This section will guide you through the necessary steps to set up the Sentry K300 drive. It is highly recommended that you set an administrator password using alpha-numeric characters.

The default password for the device is set to *1234567*. This password allows access to the device 3 times before forcing the user to change it. Once the 3 entries with the default password have been used, the message "You must change default password" will scroll across the screen until the password is changed. Press any button to continue to the **Change Password** screen.

Note: Zeroizing the drive by using the menu option or initiating Self Destruct with too many password attempts will set the password back to the default upon reinitialization.

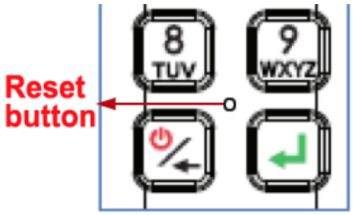
Button Roles

Enter: Perform a function

Power/Backspace: Press and hold for 3 seconds to power the Sentry K300 on or off. The device can be turned off while any screen is displayed by pressing and holding the button for 3 seconds. If the device is already on, the button will function as a backspace button, including returning to the previous screen when the **Menu** screen is displayed.

Zero/Up: Button will function as a **zero (0)** when the password is being entered or changed, or when the Auto Lock timeout and Minimum Password length are being defined. Button will function as **Up** on the **Selection** and **Menu** screens.

One/Down: Button will function as a **one (1)** when the password is being entered or changed, or when the Auto Lock timeout and Minimum Password length are being defined. Button will function as **Down** on the **Selection** and **Menu** screens.



Hardware Reset: Located between the four corners of eight (8), nine (9), power/backspace, and enter. Press button lightly with a dull pin tip to perform a hardware reset on a device that has become nonfunctional. This will reboot the drive if it becomes unresponsive. **Note:** Do not press this button with a sharp object at the risk of puncturing the button.

Alpha-Numeric Buttons: Secure passwords can be created using letters and/or numbers. Each button has one number and three to four letter options to choose from. Press the selected button repeatedly within 1 second until the desired character is shown in the white circle on the screen.

Unlocking Your Device

1. Press and hold the **Power** button on your Sentry K300 device until the OLED screen illuminates.
2. Enter the device password when prompted, then press **Enter**. For more information on button functionality, see Button Roles.
3. The device will display connection options. For more information on screen selection, see Screen Selection.
4. Select the appropriate option and press **Enter** to unlock the device.

   Note: If no selection is made in 60 seconds, the device will time out and power off.
5. Plug in the device. For more information, see Accessing The Sentry K300.

Screen Selection

- **Connect:** The device will connect in normal read/write mode for both an administrator or user.
- **Read Only Mode:** The device will connect to the system in read-only mode for both an administrator or user. For more information, see Read-Only Mode.
- **Boot Mode:** The device will connect in normal read/write mode by an administrator or user. For more information, see Boot Mode.

- **Menu:** The device will either connect to the Administrator Menu or the User Menu, depending on the password entered.

Note: If the last selected option was one of the 4 options above before the device was locked, the menu will highlight the same option by default the next time the drive is unlocked. If the last option selected is not on the selection menu, for example, changing the password or enabling auto lock, the menu will highlight the Connect option by default the next time the drive is unlocked.

Setting An Administrator Password

It is highly recommended that you set a new administrator password using alpha-numeric characters.

1. Unlock the device. See Unlocking Your Device for more information.
2. Locate the **Menu** screen by pressing the **Up** or **Down** key. Press **Enter** to select.
3. Press the **Up** or **Down** key to locate the **Change Password** option. Press **Enter** to select.
4. Enter the new secure password, using the alpha-numeric characters. To select a letter, press the designated key repeatedly until the desired letter shows in the white circle on the screen. Press **Enter** when desired password has been entered completely.

   Note: Be aware of your surroundings while entering a new password. The password is displayed on the screen in its entirety so the user can be sure it was correctly typed. It is not hidden from view.
5. Re-enter the new secure password to confirm. Press **Enter**.

Warning: A lost or forgotten administrator password cannot be reset or recovered without losing all the stored data.

Note: DataLocker Technical Support cannot assist with an unknown administrator password once the default password has been changed.

Setting A User Password

The Sentry K300 supports the creation of a user password. The user will have access to all data on the drive, however, the user will not be able to access certain administrative options and controls.

Note: You must change the default administrator password before creating a user password.

1. Unlock the device using the administrator password. See Unlocking Your Device for more information.
2. Locate the **Menu** screen by pressing the **Up** or **Down** key. Press **Enter** to select.
3. Press the **Up** or **Down** key to locate the **User Password** option. Press **Enter** to select.
4. Press **Create**.
5. The user password has now been enabled and set to the default password of *1234567*. This password can be entered 3 times before forcing the user to create a new password that meets the current password requirements.

Disabling A User Password

1. Unlock the device using the administrator password.
2. Locate the **Menu** screen by pressing the **Up** or **Down** key. Press **Enter** to select.
3. Press the **Up** or **Down** key to locate the **User Password** option. Press **Enter** to select.
4. Press **Disable**.
5. The user password has now been disabled.

Accessing The Sentry K300

After the device is unlocked and connected to the computer, the contents are automatically decrypted for use. The partition will be visible to the operating system like a normal flash drive.

Before connecting your device, you must first unlock it using the keypad. For more information, see Unlocking Your Device.

Accessing On Windows

1. Open **This PC**.
2. Scroll to the **Devices and drives** section.
3. Double click the Sentry K300 drive.

   Note: Drive name will vary based on the volume name inputted during formatting.

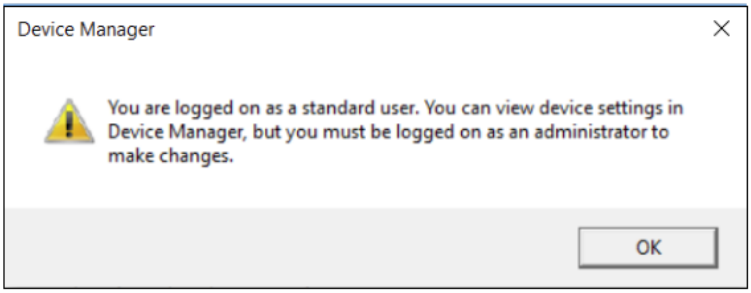
Disabling Windows 10 Power Save

By default, Windows 10 attempts to shut off USB devices after a set period of inactivity. If the Sentry K300 is put into this low power state, the drive will automatically lock the drive and require reauthentication. To disable this feature of Windows, follow the steps below.

Note: You will need to complete the following steps once for each drive plugged into your computer.

1. Log in as a local administrator on your computer.

   Note: If you are not an administrator you will receive a warning indicating you won't be able to make changes when you open Device Manager. Please contact your administrator for further assistance.



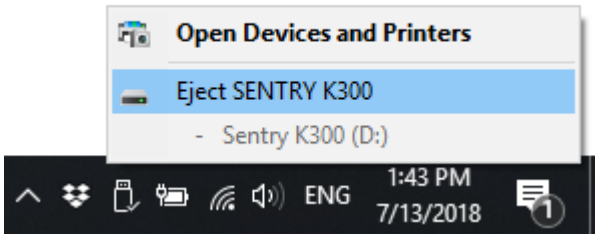
2. Unlock your Sentry K300 device and plug it into the computer.
3. Open **Device Manager** (Click the windows button and type "device manager").
4. Click on the arrow next to Universal Serial Bus controllers.
5. Right click on **USB Mass Storage Device**.
6. Click **Properties**.
7. Go to the **Power Management** tab.
8. Uncheck "Allow the computer to turn off this device to save power".
9. Click **OK**.

Disconnecting The Device

To ensure the security of your data, please safely eject your Sentry K300 device.

To safely eject:

1. Look for the USB icon in your taskbar. If you don't see it, click the arrow to expand the menu.
2. Right click the icon and click "Eject SENTRY K300" Your private partition will be displayed underneath the Sentry K300 listing and will eject with the USB drive.



Accessing On macOS

Note: The Sentry K300 is formatted as NTFS by default from the factory. Before using the device on your macOS system, you will need to reformat the drive. For more information, see Formatting the Sentry K300.

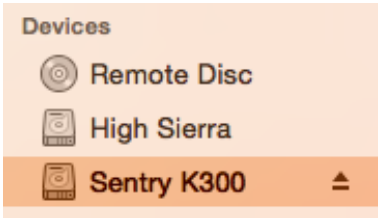
1. If the drive does not appear on your desktop, open **Finder**.
2. Scroll to the **Devices** section.
3. Click the Sentry K300 drive.

   Note: Drive name will vary based on the volume name inputted during formatting.

Disconnecting The Device

To ensure the security of your data, please safely eject your Sentry K300 device.

To safely eject, click and drag the Sentry K300 drive icon on your desktop to the trash can. If you do not see the icon on your desktop, open **Finder** and click the **Eject** button next to the Sentry K300 drive.



Accessing On Linux

Most recent distributions of Linux operating systems will mount a flash drive automatically when plugged in. You should see the device in your file manager as Sentry K300. If you are unable to view the Sentry K300, you can mount the device manually using the following commands.

1. Poll the system to find connected storage devices using one of the following commands:

   ```
   lsblk
   sudo blkid
   sudo fdisk -1
   ```

   The partition should look similar to `/dev/sdb1`

2. Create mount point.

   ```
   sudo mkdir /media/k300
   ```

3. Mount Sentry K300

   Using the partition found in step 1, substitute the following command:

   ```
   sudo mount /dev/sdb1 /media/k300
   ```

   You are now able to copy files to the `/media/k300` folder. Copied files will be saved to the device.

To disconnect:

Eject the device by using the graphical file manager, if available, or run the following command:

```
`sudo umount /media/k300`
```

Accessing On Other Systems

The Sentry K300 can be used on other systems that support USB mass storage devices. Once the device has been authenticated with the administrator or user password and connected to the system, it will mount like any other USB mass storage device. Please refer to the product manual of the system for more information.

Features

Device Information

To see information about the device without logging into it, press and hold the **Power** button for 3 seconds. Before entering the password, press **Enter**. Use the **Up** and **Down** arrow keys to see different information.

Device information shown:

- Device Name
- Firmware Version
- Capacity
- Alpha-numeric Serial Number
- QR Code Serial Number
- Certificated Logo
- Patent

Read-Only Mode

This option protects the contents of the drive by not allowing users to alter or add files. This feature can be enabled in two different capacities.

- **All users and administrators:** Can be enabled by the administrator and user in the Screen Selection Menu. Enabling this feature here will force the device to launch in Read-Only Mode until the device is locked. This is helpful when using unknown computers.
- **Users only:** Can be enabled by the administrator in the Administrator Menu. Enabling this feature here will force the device to launch in Read-Only Mode for **Users only** until the feature is turned off. For more information on finding the Administrator Menu, see Administrator Menu Screen Options.

Boot Mode

After authentication, selecting Boot Mode from the Selection Screen allows you to boot an operating system, such as Windows To Go, from the Sentry K300. In this mode, the device can lose momentary connection with the computer and remain unlocked. Only select Boot Mode when planning to run an operating system from the Sentry K300. For a more secure connection, it is recommended to use **Connect Mode**, unless Boot Mode is specifically needed.

If Boot Mode is selected and the device is connected to an operating system like a normal flash drive, it will automatically be remounted after safely ejecting. To lock your device, physically remove it from the computer.

To use boot mode:

1. Install an operating system on the drive. During installation of an operating system to the Sentry K300, the drive does not need to be in Boot Mode. For installation instructions, please refer to the portable operating system's guide.
2. Safely eject the drive from the computer.
3. Power the device back on and log in using either the administrator or user password.
4. Select **Boot Mode** on the Selection Screen.

5. Plug in your device and power on the computer. You will need to select the Sentry K300 as the boot device, which may require changes to your computer's BIOS settings.

Note: Special precautions should be taken to ensure the Sentry K300 does not get disconnected from the host system. If the computer goes to sleep, the device may be locked, which may cause loss of access to the operating system on the drive. By default, Windows To Go in Windows 10 disables the suspended states.

Self Destruct

Self destruct functionality is enabled by default on the device and cannot be disabled. After 20 incorrect password attempts, the device will wipe all data and return the drive to factory settings. The message "Incorrect Password", along with the current incorrect password count, will scroll across the screen each time an incorrect password attempt is made. Press **Enter** to display device information or press any other button to return to the password entry screen.

After each 5 consecutive incorrect password attempts, the device will power off. Pressing the **Power** button will allow the user to continue entering passwords.

After 17 and 18 consecutive incorrect password attempts, the message "Brute Force detected! All data will be deleted." will scroll across the screen. After the 19th attempt, the message "Self Destruct will begin with next failed login" will scroll across the screen.

Once the 20th consecutive incorrect password attempt has been made, the device will display "Hacking detected. All data has been deleted." The device will then power off by pressing any button.

Note: After the 20th incorrect password attempt, all data is wiped from the drive and it will be reset to factory settings. The drive will need to be reinitialized upon the next use.

Zeroize

Zeroizing the device will wipe all data on the drive and return the device to factory settings.

To Zeroize the Sentry K300:

1. Power on the device by pressing the **Power** button.
2. Enter the administrator password on the device.

   Note: Only administrators can initiate a Zeroize action. Users will not see this option.
3. Locate the **Menu** screen by pressing the **Up** or **Down** key. Press **Enter** to select.
4. Press the **Up** or **Down** key to locate the **Zeroize** option. Press **Enter** to select.
5. Select **Yes**, then press **Enter** to initiate.
6. Device will ask "All saved data will be deleted. Continue?" Select **Continue**, then press **Enter**.
7. Device will ask "Warning! Verify to Continue?" Select **Continue**, then press **Enter**.
8. Device will show message "System data has been deleted." Press any key to continue.
9. The device will now power off automatically.
10. To reinitialize your Sentry K300 device, see Setting Up The Sentry K300 After Zeroize below.

Setting Up The Sentry K300 After Zeroize

Setting up your device after a Zeroize command has been initiated is much like setting up a new drive.

1. Power on the device by pressing the **Power** button.
2. Device will ask "Initialize the device?" Select **Yes**, then press **Enter**.
3. Device will ask "All saved data will be deleted. Continue?" Select **Yes**, then press **Enter**.
4. Device will ask "Warning! Verify to Continue?" Select **Yes**, then press **Enter**.
5. The device will ask you to plug it in by showing an image of a plugged in device on the screen.

   Warning: Do not power off or unplug the device at this step. The device will move to the next step automatically when it's finished initializing.
6. Device will show the message "The initialized password is '1234567' ". Unplug the device and press any key to continue.
7. Device will show the message "You must reformat the drive." Press any key to continue.
8. The device will power off and back on automatically. The password entry screen will be displayed when it is finished restarting. Enter the default password of *1234567*.
9. Format the Sentry K300 on your system and it will then be ready for use. See Formatting The Sentry K300 for more information.

Screensaver Mode

The device is programmed to turn off the screen after 10 seconds of either no use or the waiting/connection screen. This prevents screen burn-in. To turn the screen back on, press any key. This setting cannot be turned off.

Inactivity Mode

The device is programmed to power off after 60 seconds of inactivity. To power back on, press the **Power** button. This setting cannot be turned off.

Note: The device will not power off while connected to the computer. The screen may turn off after 10 seconds to prevent screen burn-in, however, you can revive it by pressing any key.

Administrator Menu Screen Options

- **Change Password:** Change the administrator password.
- **User Password:** Create or disable the user password. See Setting A User Password.
- **Strong Password:** Enforce strong password requirements for new password changes and will affect both administrator and user passwords. This should be enabled before enabling the user password.

Requirements:

  - 8 characters
  - 1 letter
  - no consecutive numbers
  - no consecutive letters

- **Minimum Password Length:** Can be set to require 7-30 password characters for all new passwords.
- **Read-Only Mode:** Force the drive to unlock in read-only mode after unlocking with the user password. The user is unable to write to the drive without the administrator password.
- **Auto Lock:** Set the amount of inactivity time (in minutes) before the device automatically locks. The maximum number of minutes that cane be entered is 180.
- **Zeroize:** Wipe all data on the drive and return the device to factory settings. The device will need to to be re-initialized and formatted before use.

User Menu Screen Options

- **Change Password:** Change the user password.
- **Auto Lock:** Set the amount of inactivity time (in minutes) before the device automatically locks. The maximum number of minutes that cane be entered is 180.

Formatting The Sentry K300

Selecting The Correct File System

Your device is formatted as **NTFS** from the factory.

The Sentry K300 can be reformatted to any file system of your choosing to accommodate a different operating system or to remove file size restrictions. Not all file systems are available on all operating systems.

Recommended file systems:

- FAT32
  - Pros: Cross-platform compatible (Windows, macOS, and Linux)
  - Cons: Limited individual file size of 4GB
- NTFS
  - Pros: No file size limitations
  - Cons: Limited cross-platform compatibility - Windows, macOS (read-only), and Linux (read-only)
- exFAT
  - Pros: No file size limitations
  - Cons: Not supported by legacy operating systems

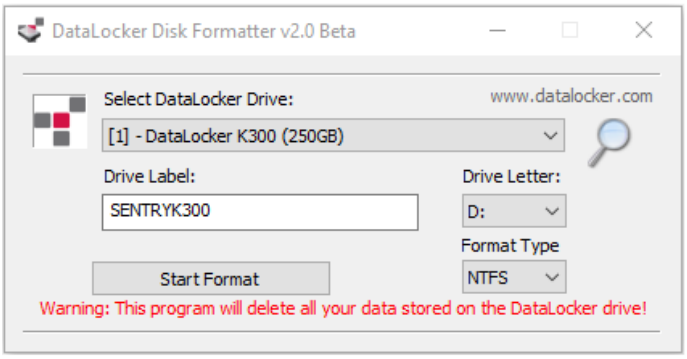
Note: Reformatting your Sentry K300 drive will erase all your files but will not erase your device password and settings. This should not be used as a method of securely erasing files. To securely erase your files, perform a Zeroize function. For more information, see the Zeroize section.

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

Formatting On Windows

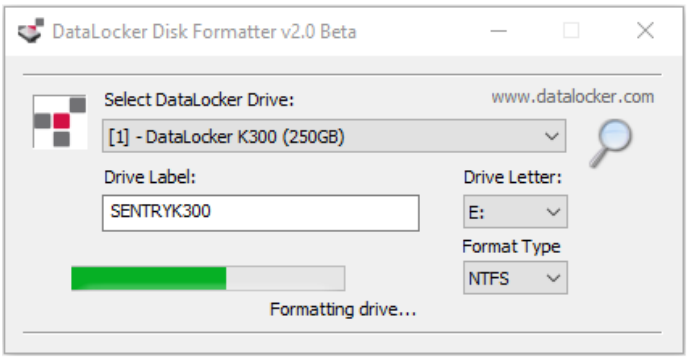
1. Unlock your device using the administrator password. For more information, see Unlocking Your Device.
2. Connect the device to your Windows computer.
3. Download the **DataLocker Disk Formatter Tool**, which can be found here.
4. Run the **DataLocker_Disk_Formatter.exe**. The formatting tool will automatically find the Sentry K300 device.

5. Select the **Drive Letter** and **Format Type**, and rename your **Drive Label**.

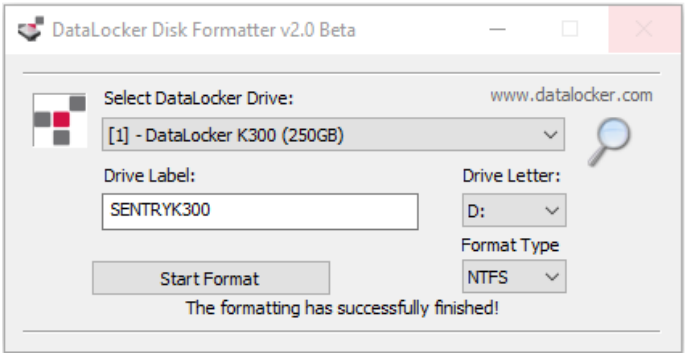


6. Click **Start Format**.
7. The formatting tool will show **Formatting drive...**

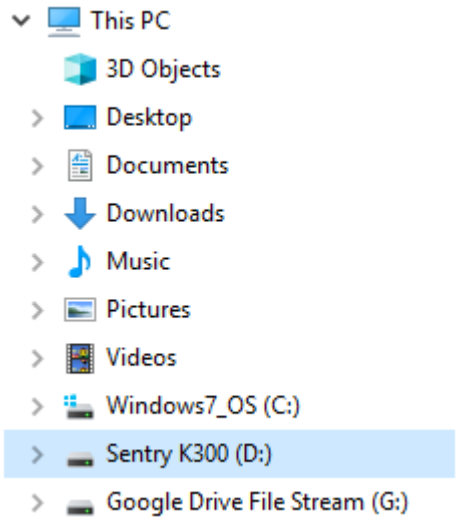
   Note: Windows may recognize that the drive needs to be formatted after the formatting tool has already started. Feel free to close any popups from Windows that say the drive needs to be formatted.



8. When finished, the formatting tool should display the message "**The formatting has successfully finished!**"

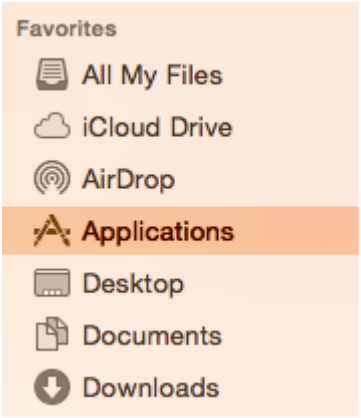


Your Sentry K300 will now appear under **This PC**.

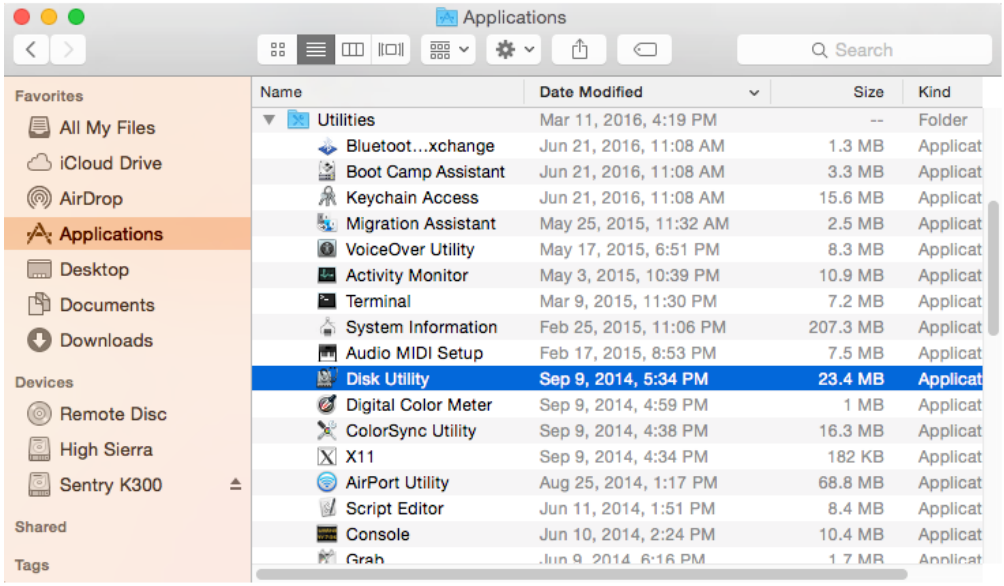


Formatting On macOS

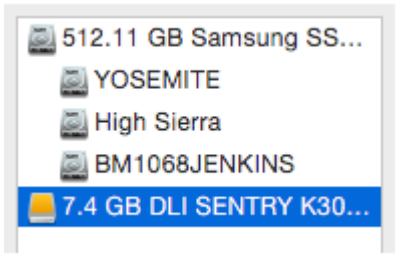
1. Unlock your device using the administrator password. For more information, see Unlocking Your Device.
2. Connect the device to your macOS computer.
3. Go to **Applications** under Finder.



4. Click on **Utilities**, then double click **Disk Utility**.

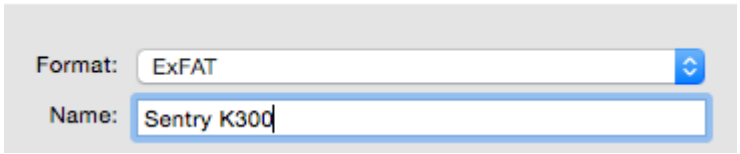


5. Select the Sentry K300 disk.



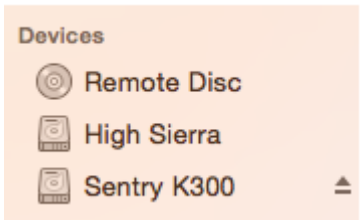
6. Click the **Erase** tab.

7. Choose the new file system from the dropdown and rename your disk label.



8. Click **Erase**.

   Your Sentry K300 will now appear under **Devices**.



Formatting On Linux

The Sentry K300 is platform independent, capable of being run with 100% compatibility on most systems. For optimal Linux or Unix based system compatibility, we recommend using at least the Linux 2.6.31 Kernel (released 9 September 2009), which implemented the xHCI specification for USB 3.0. Although older versions should work, they might run in USB 2.0 mode, which can be significantly slower.

In most newer distributions the drive should automatically mount. To format the drive, first enter terminal, then list detected hard disks using

```
# fdisk -l | grep '^Disk'
```

Your configuration may vary. For this example, we'll assume the disk is at /dev/sdb

You will then type:

```
# fdisk /dev/sdb
```

Follow the instructions in fdisk to create a new partition.

Finally you'll use the mkfs command to format the disk for Linux. Here, we use ext4.

```
# mkfs.ext4 /dev/sdb1
```

If you want to rename the drive, use the e2label command.

```
# e2label /dev/sdb1 /DataLocker
```

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

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, 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.

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.