

DEFENDER HDD 350™



Kanguru Defender HDD350™

User Manual



Copyright © 2020 Kanguru Solutions. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Kanguru Solutions will not be held responsible for any illegal use of this product nor any losses incurred while using this product. The user is fully responsible for any illegal actions taken.

For the latest support and drivers, visit: www.kanguru.com.

Table of Contents

Introduction	4
Box contents	4
Main Features	4
Kanguru Remote Management Console (optional)	5
1. Kanguru Defender Layout	6
2. Hardware Setup	7
3. How to Set up Kanguru Defender Manager (KDM)	8
4. Unlocking the Encrypted Drive Partition.....	10
5. Defender Command Console	11
Welcome	11
About This Device	11
Contact Information	11
AntiVirus	12
Settings: Change Password	13
Settings: KRMC	13
Settings: General	13
Settings: Help	14
6. How to Reset your Defender to Factory Default Settings.....	14
7. How to safely unmount/eject your Defender	15
8. Technical Support	16
9. Warranty and RMA Information	16



Introduction

The USB 3.0 Kanguru Defender HDD350 is an ultra-secure, tamper-proof, AES 256-bit hardware-encrypted hard drive that delivers enterprise-grade data protection with FIPS 140-2 certification. Compatible with both macOS and Windows, and available with the optional Kanguru Remote Management Console (KRMCTM), enabling organisations to maintain strict security compliance and centralised control. Its secure encrypted design isolates data from prying eyes, malware, and online threats, with no software installation or administrative rights required. Through the Kanguru Remote Management Console (KRMCTM), administrators can easily monitor, track, and enforce policies worldwide. Combining simplicity with powerful cryptographic protection, the Defender HDD350 provides organizations with complete confidence and control over sensitive data, making it an ideal solution for safeguarding information in today's demanding security environment.

The Defender contains two partitions: a read-only, CD-ROM partition and a secure, encrypted partition. The CD-ROM partition contains the login application that will allow you to access the secured partition. The secure partition is where you store your encrypted data.

Box Contents

- 1 x Kanguru Defender HDD350
- 1 x USB3 Micro-B to USB-A Cable
- 1 x USB3 Micro-B to USB-C & USB-A Combo Cable
- 1 x USB3 Micro-B to USB-A Y-Cable
- 1 x Quick Start Guide

Main Features

- FIPS 140-2 Certified (FIPS-Inside Cert 4228)
- FIPS PUB 197 validated encryption algorithm
- SuperSpeed USB 3.0 (USB 3.2 Gen 1x1)
(Note: this product is NOT compatible with USB 2.0)
- Remote Management Ready - (KRMCTM)
- Onboard Anti-Virus Protection (optional)
- Mac OS and Windows PC Compatible
- No Software Install or Administrator Rights Needed
- Tamper-proof design
- High-Strength Aluminum Housing

Kanguru Remote Management Console (optional)

Manage All of Your Secure Defender USB Drives from One Convenient Console

The Kanguru Remote Management Console (KRMCTM) is a powerful, fully-integrated platform for organizations to remotely manage all Kanguru hardware-encrypted Defender USB drives containing sensitive data anywhere in the world. KRMCTM itself never stores sensitive data—security of data solely remains within the confines of the encrypted drives. Instead, KRMCTM provides a resilient way to remotely manage and enforce security policies.

Designed for Security, Compliance, and IT Management, the KRMCTM makes it simple to monitor devices, authorize or restrict permissions, manage passwords, and even remotely disable/delete lost or stolen drives when necessary.

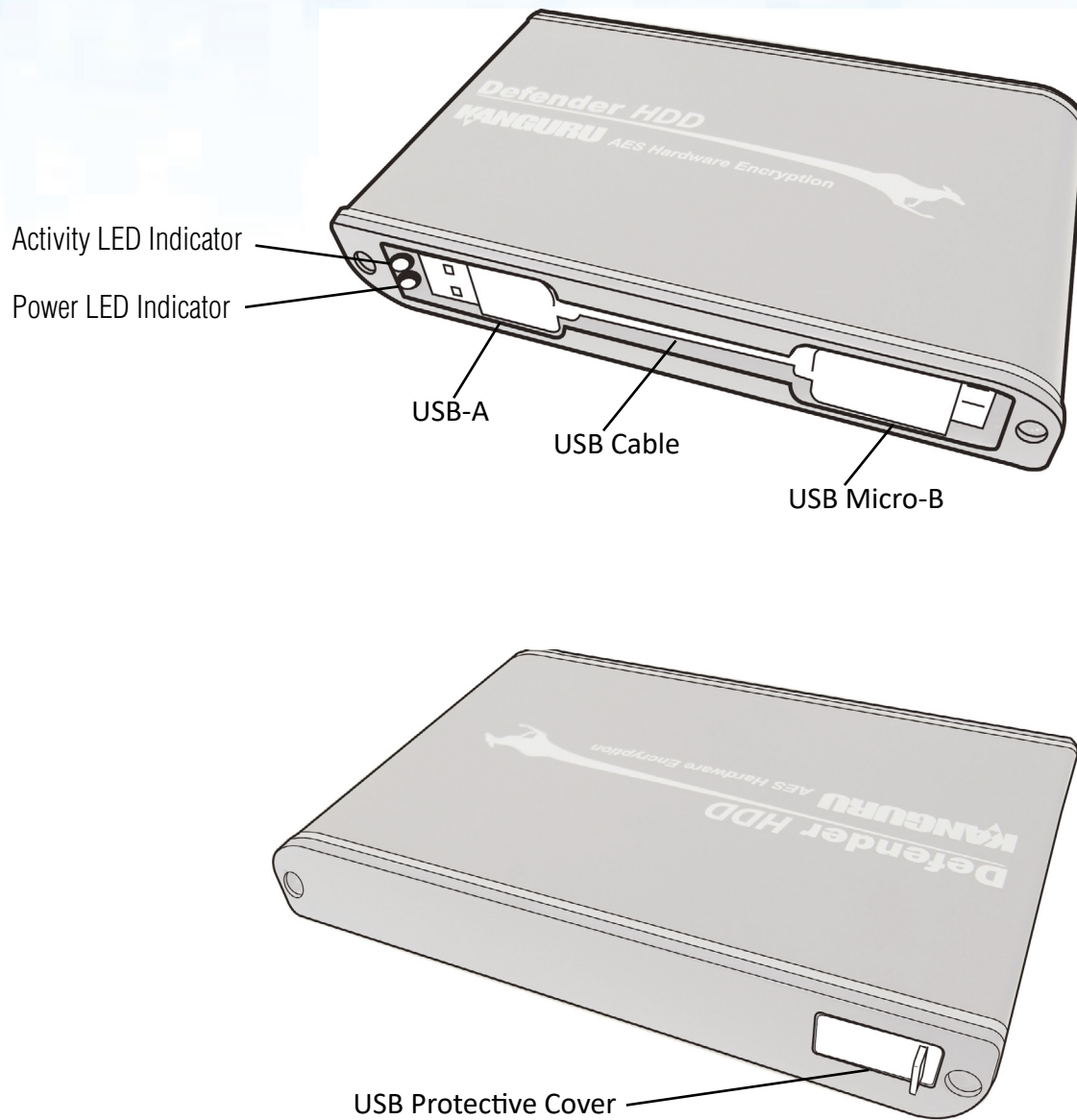
Organizations can choose between **KRMCTM-Hosted**, managed by Kanguru's high-secure servers, or the **KRMCTM On-Premise Edition**, which allows enterprises with strict compliance requirements to host the platform on their own servers. Both options provide the same powerful features while giving organizations the flexibility to select the deployment model that best fits their needs.

Features:

- Track And Manage USB Drives Worldwide from One Convenient Console
- Self-Service Password Management
- Disable/Delete Lost Or Stolen Devices
- Automatic Global Provisioning
- Streamlined License Management
- Configure and Deploy Quickly and Easily
- Search, Audit and Report on Secure Drives
- Set Up Online & Offline Permissions
- Generate Reports
- Export Audit Logs
- Manage Password Resilience
- Notify Users And Roll Out Policy Updates
- Schedule Password Changes
- Restrict IP Addresses and Domains
- Enforce Security Policies

For more information about the Kanguru Remote Management Console visit:
<https://www.kanguru.com/pages/kanguru-remote-management-suite-for-defender-encrypted-devices>

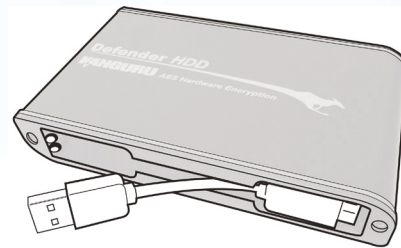
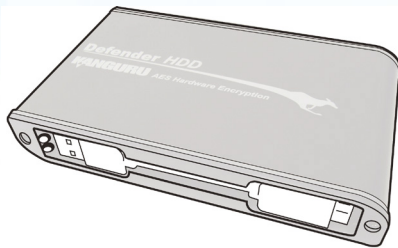
1. Kanguru Defender Layout



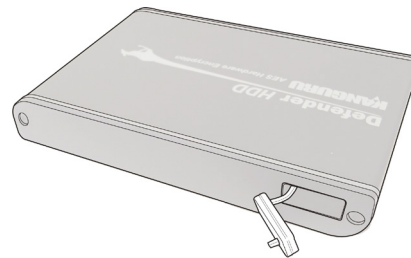
2. Hardware Setup

Follow these instructions to connect the Defender to your computer:

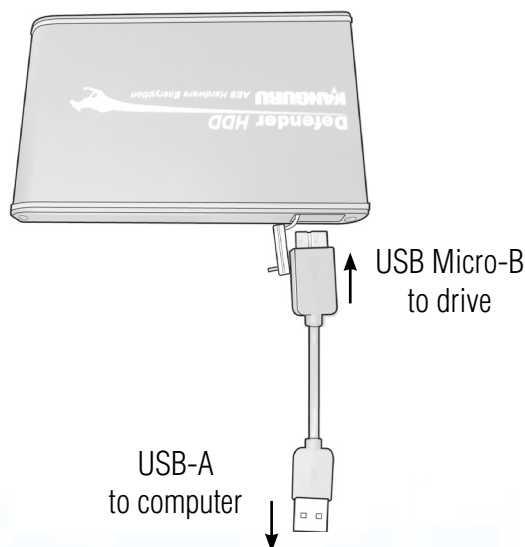
1. Remove the USB cable from the side of the Defender. The easiest way to release the cable is by pulling out the USB A side first, as shown in the image below.



2. On the other side of the drive, pull open the rubber protective USB cover to reveal the USB port.



3. Connect the USB Micro-B side of the cable to the Defender's USB port. Connect the USB-A cable to your computer. The LED indicators on the side of the drive will light up. You are now ready to begin using your Kanguru Defender drive.



Note: Connect to **USB 3.0 ports only**. If your Defender HDD is not recognized by your computer when plugged in, it may not be drawing enough power from a single USB port. Please use the provided Y-type USB cable to connect the device through two USB ports.



3. How to Set up Kanguru Defender Manager (KDM)

Kanguru Defender Manager (referred to throughout this manual as “**KDM**”) is the client program preloaded on the Defender’s CD-ROM partition. The user needs to login to KDM in order to access the secure, encrypted partition.

KDM comes pre-installed on your Defender. No installation on your PC is necessary.

Caution! The KDM.exe file needs to remain on your Defender’s CD-ROM partition at all times. Always run the application from the Defender’s CD-ROM partition. Do not try to copy KDM.exe or run KDM.exe from your computer’s hard drive.

The Setup Wizard

When you start KDM for the first time you will be greeted by the Setup Wizard. Follow the Setup Wizard instructions to create a security password for your Defender’s secure, encrypted partition.

1. Connect the Defender to a USB 3.0 port on your PC. **Note:** This device does not work on USB 2.0 ports.
2. Two drives appear, one containing the KDM.exe launcher and the other providing access to the encrypted drive partition, both marked by drive letters (e.g. G, H,...) as seen in image 1 below.

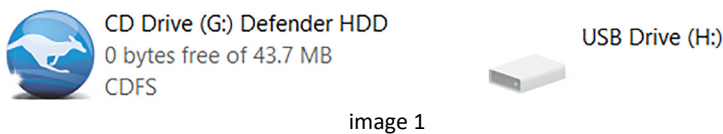


image 1

3. Double click on the CD Drive Defender HDD (image 1) to launch the setup wizard.
4. Click Next to continue (image 2).



image 2

5. Enter your name, phone number and e-mail (image 3), then click on **Apply** and **Next** to continue.



image 3

6. You will receive an e-mail containing an activation code. Enter your **Code** (image 4), Click **OK** and then **Next** to continue.



image 4

Note: The **Code** input field only appears when setting up KDM for the first time or when setting KDM with a different email address. If you set up KDM after a 'factory reset' using the same email as the initial setup, the **Code** input field is not required and will not appear.

7. Create and confirm a **password** that meet the requirements as set out in image 5, click **Save** and then **Finish**.

Note: For security reasons, click the **keyboard icon** (image 5) to open the **virtual keyboard** as shown below. We recommend using the virtual keyboard when creating a new password and whenever you log in to the KDM.



image 5

After you have set your password you will be asked to login as described in **Section 4** 'Unlocking the Encrypted Drive Partition'.



4. Unlocking the Encrypted Drive Partition

8. After you have set a password you will be asked to login using your password every time you run KDM. You need to provide the correct password in order to access the Defender's encrypted drive partition.

Note: The Login screen is accesible by double-clicking on the CD Drive Defender HDD partition.

To unlock and access the Defender's encrypted drive partition;

1. Open **Virtual Keyboard**
2. Enter your password in the **Password** field.
3. Click on the **Login** button to unlock and access your encrypted drive partition.
4. **Caution!** Using the **Reset** to 'Factory Default' function will format and wipe all data off the encrypted drive partition! All personal data on the device will be lost! Refer to **Section 6** 'How to Reset your Defender to Factory Default Settings'.

Note: After performing a reset, you must repeat the steps in **Section 3**, How to Set Up Kanguru Defender Manager (KDM), before you can use the drive again.



image 6

1. Open Virtual Keyboard
2. Password
3. Login
4. Reset

Note: If your Defender is remotely managed via the Kangauru Remote Management Console (**KRMC**), the Reset button is disabled and will not be visible. Only an Administrator can perform a remote reset on your device.

Caution! The Defender is configured to allow a maximum of **7 (seven)** consecutive incorrect password entries. All data stored on the secure partition will automatically be erased if this number is exceeded. You will be issued an on-screen warning (image 7) when you have one attempt remaining, to prevent accidental erasure.

Note: If the Defender is reset after **7 (seven)** consecutive incorrect password attempts, you must repeat the steps in **Section 3**, How to Set Up Kanguru Defender Manager (KDM), before you can use the drive again. If your Defender is remotely managed via the Kangauru Remote Management Console (**KRMC**), the Administrator can perform a remote password reset on your device.

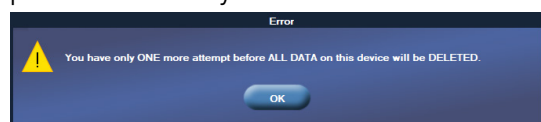


image 7

Once you have successfully logged in to KDM, the Defender's secure encrypted partition will be unlocked and ready for use, the '**Kanguru Defender HDD Command Console**' will launch automatically as shown in **Section 5** 'Defender Command Console' image 8.

Caution! Before unplugging the Defender from the USB port, always ensure that you unmount/eject the secured partition by clicking the '**Logout**' button , as shown in **Section 5** 'Defender Command Console' (Image 8). Once the Defender has been unmounted/ejected, it can then be safely removed from the USB port.

5. Defender Command Console

After a successful login, the Defender's Command Console will launch, as shown in Image 8.

• Welcome



1. About This Device
2. Contact Info
3. AntiVirus
4. Settings - Change Password/KRMC/General
5. Help
6. View Encrypted Files
7. Logout  - Eject/Unmount
8. Collapse the Command Console

Caution! Before unplugging the Defender from the USB port, always ensure that you unmount/eject the secured partition by clicking the 'Logout' button , as shown in Image 8. Once the Defender has been unmounted/ejected, it can then be safely removed from the USB port.

• About This Device



• Contact Information

The Name, Phone Number, and Email fields are automatically filled with the details you provided during setup.



• AntiVirus

Safeguard your data with confidence. Choose a 1, 2, or 3-Year Kanguru Endpoint Protection (Anti-Virus/Anti-Malware) subscription license for your Kanguru Defender® Secure USB drive. Enjoy world-class protection that detects and eliminates threats before files are transferred to your drive, ensuring your Kanguru Defender® encrypted USB drive remains uncompromised.

To purchase your license, click on the 'Get AV' button (image 11) to activate Endpoint Protection on your device as seen below in image 12.



image 11



image 12

AntiVirus Scan:

1. Scan the whole drive
2. Select and scan any folder
3. Select and scan any file
4. Delete the file If an infection is detected
5. Disinfect the file if an infection is detected
6. Click '**Run Scan**' to start scanning
7. View Scan Log

Under the License tab (image 13) are details of your AV License, including date of last automatic AV definition update and how to renew your license.



image 13

• Settings

Change Password:

To change your password, fill in the fields shown in Image 14 and click **Save**. If the change is successful, a confirmation window will appear (Image 15). Click **OK** to proceed.

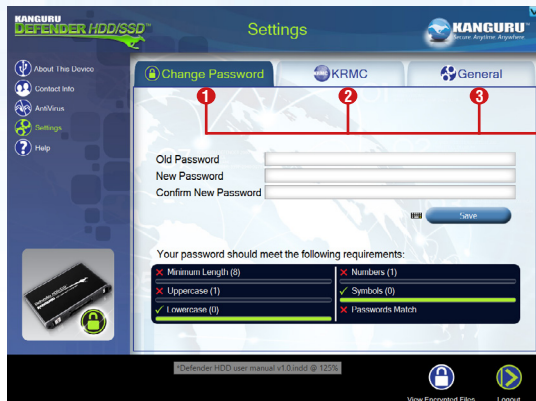


image 14

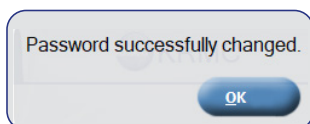


image 15

Setting Tabs

1. Change Password - refer to image 14
2. Kanguru Remote Management Console (KRM) - refer to image 16
3. General - refer to image 17

• Settings

KRM:



image 16

1. To Enable KRM Cloud functionality click on the '**Enable KRM**' button, the 'Remote Management' logo will visibly light up.
2. Enter your **Cloud ID**. **Note:** Ensure '**Enable KRM**' is active as described above (1).
3. Click the '**Verify**' button to access KRM cloud functionality.
4. For more information on KRM and how to purchase, click on the '**Buy KRM**' button.

• Settings

General:

If your computer connects to the internet through a proxy server and KDM cannot detect the server address, you will need to manually enter the proxy address, type, and credentials (image 17).



image 17



• Settings

Help:

Helpful links and technical support contact details.



image 18

Caution! Before unplugging the Defender from the USB port, always click **Logout**  to unmount/eject the secured partition. Once it has been unmounted/ejected, you can safely remove the Defender from the USB port.

6. How to Reset your Defender to Default Factory Settings

If you forget your password, you can reset the Defender using the **Reset** function. This action resets and restores the device to its default factory settings and permanently deletes all passwords and data from the secure partition.

Caution! Using the 'Reset to Factory Default' function will format and wipe all data off the secure partition! All personal data on the device will be lost!

To reset your Defender to the factory default:

1. Start KDM.
2. When the login screen appears, click on the **Reset** button (image 19).

Note: Resetting the Defender is not possible if the device is being remotely managed through the Kanguru Remote Management Console (**KRMC**). Only the Administrator is able to remotely Reset your device!

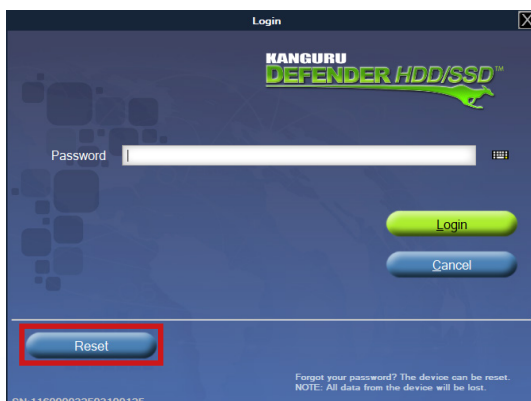


image 19

3. When you are prompted to confirm the reset, click on the **Yes** button (image 20).

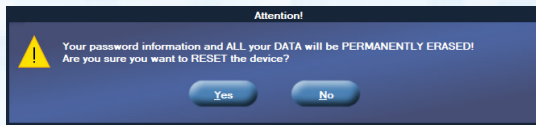


image 20

4. When your password and data stored on the secure partition have been erased, the following message will appear. Click on the **OK** button to finish.

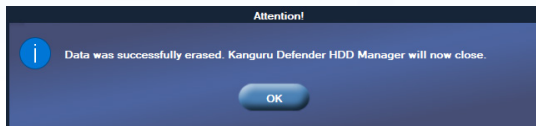


image 21

How to set up KDM after a Reset

The next time you run KDM, you will have to complete the Setup Wizard as described in '**Section 3 - How to Set up Kanguru Defender Manager (KDM)**' before you are able to access the secure encrypted drive partition.

7. How to safely unmount/eject your Defender

Caution! Before unplugging the Defender from the USB port, always ensure that you unmount/eject the secured partition by clicking the '**Logout**' button , as shown below (image 22). Once the Defender has been unmounted/ejected, it can then be safely removed from the USB port.



image 22

8. Technical Support

If you experience any problems installing your Kanguru product or have any technical questions regarding any of our products, please call our tech support department. Our tech support is free and available Monday thru Friday, 9am to 5pm EST.

Call 1-508-376-4245

Or visit our website at www.Kanguru.com

9. Warranty and RMA information

Kanguru Solutions guarantees that every Kanguru Defender will be free from defects in workmanship and materials for 3 years from the date of purchase. This warranty does not apply if, in the judgment of Kanguru Solutions, the product fails due to damage from handling, accident, abuse, misuse, or if it has been used in a manner not conforming to the product's instructions, has been modified in any way, or the warranty labels have been removed. If the product proves defective during this warranty period, call Kanguru Solutions Technical Support in order to obtain a Return Material Authorization required for service. When returning a product, mark the RMA number clearly on the outside of the package, and include a copy of your original proof of purchase. In no event shall Kanguru Solutions' liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. Kanguru Solutions offers no refunds for its products after 30 days of purchase. Kanguru Solutions makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Kanguru Solutions reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

DEFENDER HDD 350™



KANGURU™
by **iStorage®**

Kanguru Solutions

1360 Main Street Millis,
MA 02054, USA

www.kanguru.com

09.10.25 v.1.0 © 2020 Kanguru Solutions

Legal terms and conditions available at www.kanguru.com.