KANGURU™
by iStorage®



Kanguru Defender HDD350™

Quick Start Guide

iStorage provides the following helpful resources:

• website: www.istorage-uk.com • email: support@istorage-uk.com • Telephone: +44 (0) 20 8991 6260

iStorage Technical Support Specialists are available from 9:00 a.m to 5:30 p.m GMT, Mon - Fri.

Quick Start Guide

Thank you for purchasing the USB 3.0 Kanguru Defender HDD350 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 (KRMC™), 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 (KRMC™), administrators can easily monitor, track, and remotely 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.

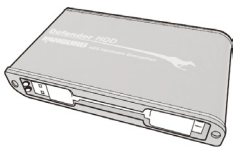
The Defender contains two partitions: a read-only, CD-ROM partition and a secure, encrypted partition. The CD-ROM partition contains the login application that will allow you to access the secured partition.The secure partition is where you store your encrypted data.

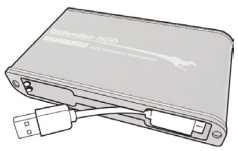
Note: This is a Quick Start Guide only. The comprehensive user manual can be downloaded from our website at: https://istorage-uk.com/product-documentation/

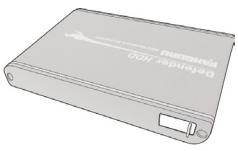
Box Contents

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

Hardware Setup









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. Alternatively, use one of the other two USB cables supplied.

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.

Note: Connect to USB 3.0 ports only, If your Defender HDD is not recognized 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.

1. 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 is necessary.

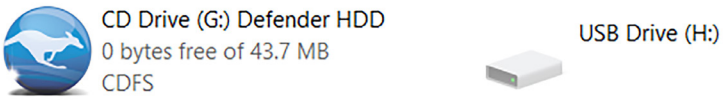
Caution! The KDM.exe file needs to remain on your Defender's CD-ROM partition at all times. Always run the application from the Defender's CD-ROM partition. Do not try to copy KDM.exe or run KDM.exe from your computer's hard drive.

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 computer. **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 below.



3. Double click on the **CD Drive Defender HDD** as seen in the above image to launch the setup wizard.

4. When you start KDM for the first time, you will be greeted by the Setup Wizard. Follow the simple instructions to setup your Defender's login password.

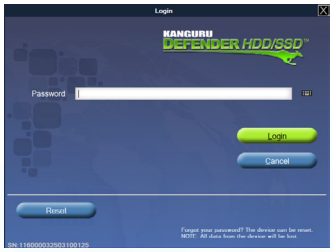
2. Unlocking the Encrypted Drive Partition

After you have set a password you will be asked to login using your password every time you run KDM.

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. Enter your password in the **Password** field.
2. Click on the **Login** button to unlock and access your encrypted drive partition.



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



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

How to Safely Remove 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 in the above image (7). Once the Defender has been unmounted/ejected, it can then be safely removed from the USB port.

A full and comprehensive user manual can be downloaded from our website at:
https://istorage-uk.com/product-documentation/

Kanguru Solutions
1360 Main Street Millis,
MA 02054, USA
www.kanguru.com
09.24.25 v.1.0 © 2020 Kanguru Solutions
Legal terms and conditions available at www.kanguru.com.