

# **Kanguru Defender HDD/SSD & Defender HDD/SSD300 User Manual**

Model no:  
KDH3B, KDH3B-300F

## **NOTICES AND INFORMATION**

### **Please be aware of the following points before using your Kanguru Defender**

Copyright © 2020 Kanguru Solutions. All rights reserved.

Windows 7®, Windows 8® and Windows 10® are registered trademarks of Microsoft Inc. All other brands or product names are trademarks of their respective companies or organizations.

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 solely responsible for the copyright laws, and is fully responsible for any illegal actions taken.

### **Customer Service**

To obtain service or technical support for your system, please contact Kanguru Solutions Technical Support Department at 508-376-4245, or visit [www.Kanguru.com](http://www.Kanguru.com) for web support.

### **Legal notice**

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. 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.

### **Export Law Compliance**

Regardless of any disclosure made to Kanguru Solutions pertaining to the ultimate destination of the specific Kanguru product, you warrant that you will not export, directly or indirectly, any Kanguru product without first obtaining the approval of Kanguru Solutions and the appropriate export license from the Department of Commerce or other agency of the United States Government. Kanguru Solutions has a wide range of products and each product family has different license requirements relative to exports.

### **Defragmenting Flash Memory Warning**

Do not attempt to defragment a Kanguru Defender Solid State Drive. Flash memory does not need to be defragmented and does not gain any performance by doing so. Defragmenting your solid state drive can actually degrade the flash memory which may reduce the drive's total capacity and lifespan.

---

## TABLE OF CONTENTS

<b>1.</b>	<b>Introduction .....</b>	<b>4</b>
1.1	Package Contents.....	4
1.2	System Requirements .....	4
1.3	FIPS Approvals and Certification.....	5
1.4	Features.....	5
1.5	Technical Specifications .....	6
<b>2.</b>	<b>General Operation .....</b>	<b>7</b>
2.1	Parts and Functions.....	7
2.2	Hardware Setup .....	8
<b>3.</b>	<b>Kanguru Defender Manager.....</b>	<b>9</b>
3.1	Running KDM .....	9
3.2	Important Notice About Sleep Mode.....	10
3.3	The Setup Wizard .....	11
3.3.1	Selecting a Setup Language.....	11
3.3.2	Activating On-board Antivirus Protection.....	12
3.3.3	KRMC Cloud.....	13
3.3.4	Contact Info .....	14
3.3.5	Setting a Password.....	15
3.4	Unlocking the Security Partition .....	16
3.4.1	Resetting from the Login Screen.....	17
3.4.2	Using the Virtual Keyboard to Enter Your Password .....	18
3.5	Encrypting Files and Folders.....	19
3.6	On-board Antivirus.....	20
3.6.1	Device Scan .....	21
3.6.2	Path Scan .....	22
3.6.3	File Scan .....	23
3.7	Changing Your Password.....	24
3.8	KRMC Cloud Settings .....	25
3.9	Changing Languages .....	26
3.10	Online Documentation.....	27
3.11	About KDM .....	27
<b>4.</b>	<b>Updating Your Defender HDD.....</b>	<b>28</b>
4.1	Updating standard edition drives.....	28
4.2	Updating KRMC enterprise edition drives.....	28
4.3	Verifying the download checksum.....	29
<b>5.</b>	<b>Safely Removing Your Kanguru Defender .....</b>	<b>30</b>
5.1	Unmounting Your Defender .....	30
5.2	Safely Removing from Windows .....	31
<b>6.</b>	<b>Warranty Information .....</b>	<b>32</b>
<b>7.</b>	<b>Tech Support.....</b>	<b>32</b>
<b>8.</b>	<b>Appendix A - Proxy Support .....</b>	<b>33</b>

## 1. Introduction

The Kanguru Defender is a hardware encrypted, tamper proof drive. 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 data.

The Kanguru Defender drive secures your important data through:

- 256-bit AES hardware encryption (XTS-mode)
- Secure password protection

### 1.1 Package Contents

Please check the contents of the package you received. If any of the parts listed below are missing, please contact Kanguru Solutions (508-376-4245) and you will be shipped replacement parts immediately.

- Kanguru Defender Drive
- USB3.0 Cable
- Quick Start Guide
- Registration Form

### 1.2 System Requirements

- 1 Available USB port (USB 3.0 recommended)
- 256MB of internal DDR RAM (1GB or higher recommended)
- 500MHz internal CPU (1GHz or faster recommended)
- Supported operating system (32 and 64 bit compatible)
  - Win 7, Win 8, Win 10

*\* In line with Microsoft's End-of-Support announcement for Windows 7, Kanguru Solutions is ending support for its line of products running on the Windows 7 platform. While our products have been quality tested internally on Windows 7, we cannot guarantee normal product operation on an unsupported OS.*

## 1.3 FIPS Approvals and Certification

If you purchased a standard Defender HDD or Defender SSD, then your device uses FIPS 197 approved AES hardware encryption.

If you purchased a Defender HDD300 or Defender SSD300 (model# KDH3B-300F), then your device has also been certified to meet strict FIPS 140-2 level 2 security requirements.

## 1.4 Features

- ✓ 256-bit AES hardware encryption (XTS-mode)
- ✓ Password protected data partition for your secure files
- ✓ Does NOT require Admin privileges
- ✓ Driverless installation (Plug & Play)
- ✓ High-strength aluminum housing
- ✓ Tamper-proof design
- ✓ On-board antivirus protection

## Remote Management Capability

Kanguru Defender drives can be remotely managed using the Kanguru Remote Management Console (KRMC). KRMC is a web-based application that gives administrators a complete USB management system. KRMC is available in two different options: Customer hosted enterprise version or a Kanguru hosted Cloud version. Please contact Kanguru Solutions if you have any questions about which option would be the best fit for your organization.

With KRMC you will be able to:

- ✓ Create and manage a master password for your Defenders
- ✓ Remotely delete all data on a target drive
- ✓ Schedule actions for present or future times
- ✓ Audit at administrator and super administrator level
- ✓ Locate devices via IP address (IP Address / network location)
- ✓ Locate devices via hostname
- ✓ Create remote policy modifications like:
  - Password strength and length (e.g. 10 characters: 2 upper, 2 numbers, etc)
  - Limit invalid login attempts (e.g. 3 retries before drive is wiped)
  - Rate at which password should be changed (e.g. every 30, 60, or 90 days)
  - Change user password
  - Change master password
- ✓ Create user groups

Your Kanguru Defender does not come with KRMC enabled by default.

For more information about KRMC, visit: <https://www.kanguru.com/index.php/flash-management>

## 1.5 Technical Specifications

### General Specifications

Interface	USB3.0 5Gbps (backwards compatible with USB2.0)
Encryption Features	Hardware based 256-bit AES encryption (XTS-mode)
Drive interface	SATA II 3Gbps
Operating Temp	32°F ~ 158°F (0°C – 70°C)
Dimensions	5.5" x 3.5" x 1"

### Kanguru Defender HDD

Capacities <sup>1</sup>	500GB, 1TB, 2TB
Rotation Speed	5400
Cache Size	8MB
Reliability	750,000 hrs
Access Time	8.5 - 11ms
Weight	10.3 oz

### Kanguru Defender SSD

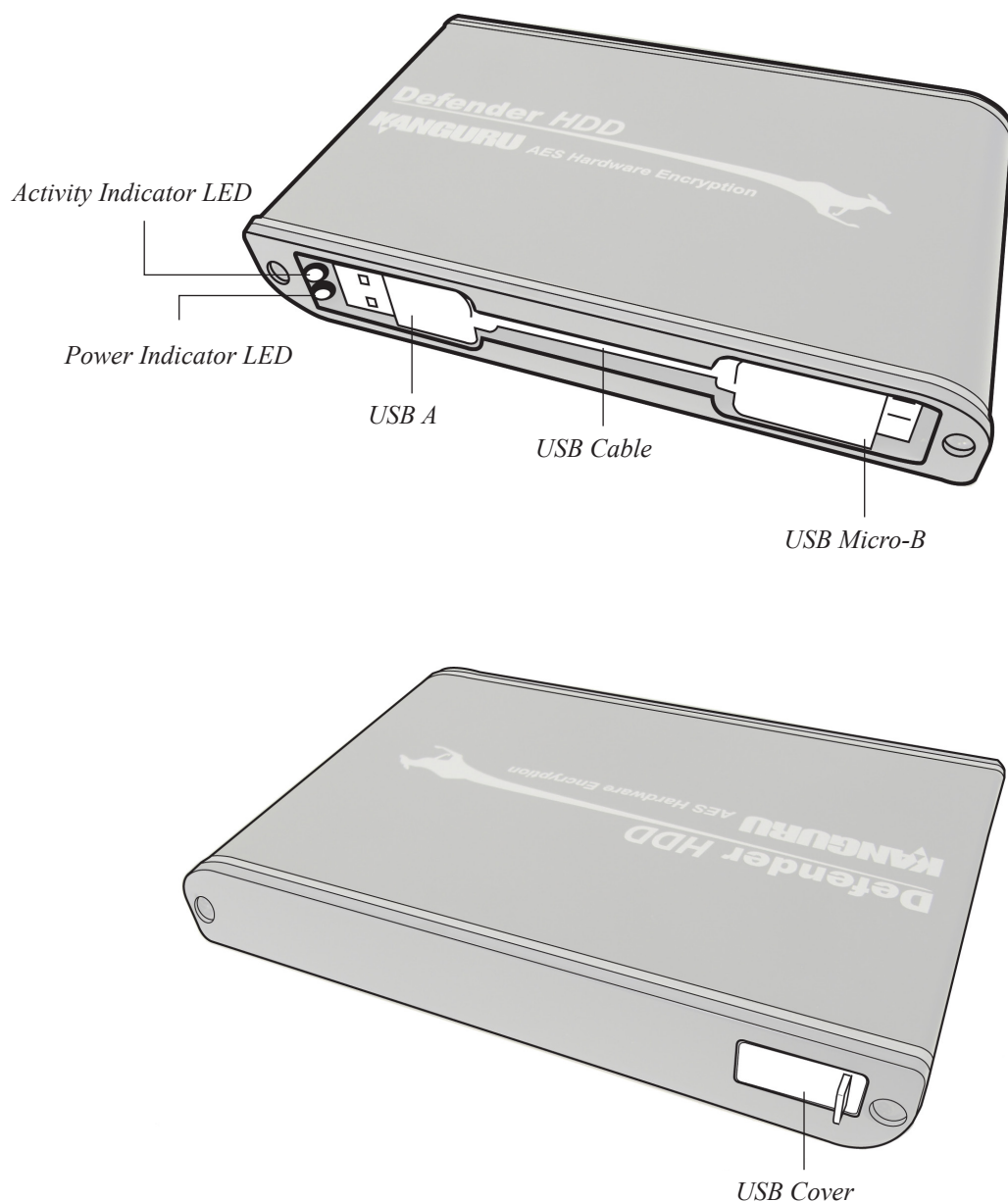
Capacities <sup>1</sup>	256GB, 480GB
Write Cycles	10,000 write cycles / block
Mean Time Between Failure	1,000,000 hours
Access Time	0.4ms
Weight	9.6 oz

<sup>1</sup> Kanguru Solutions defines a gigabyte (GB) as 1,000,000,000 bytes.

## 2. General Operation

This chapter contains information on how to use your Kanguru Defender. Please read these sections carefully.

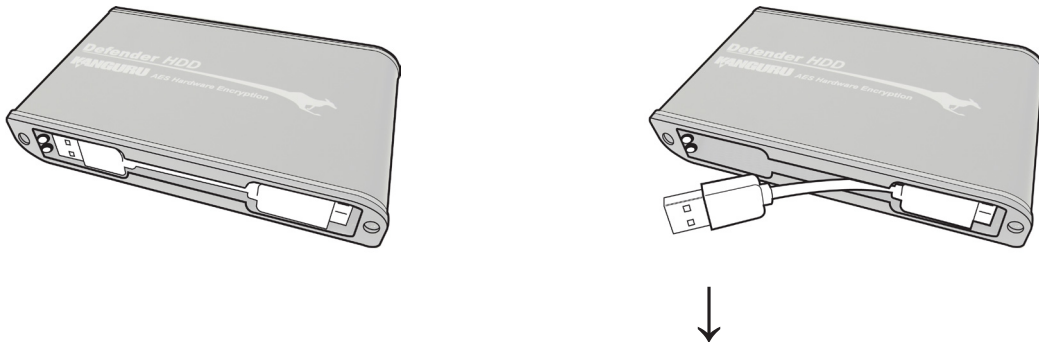
### 2.1 Parts and Functions



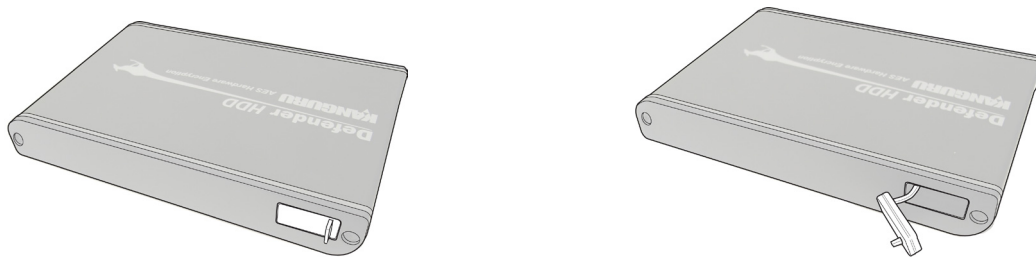
## 2.2 Hardware Setup

Follow these instructions to connect the Defender drive to your computer:

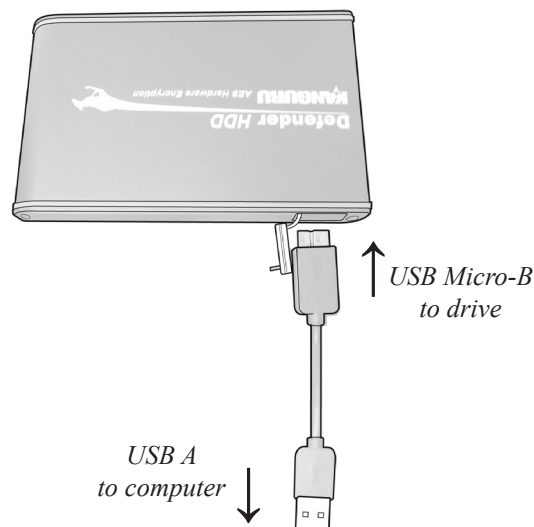
1. Remove the USB cable from the side of the Defender. The easiest way to release the cable is by pulling out the USB A side first, as shown in the image below.



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



3. Connect the Micro B side of the USB cable to the Defender's USB port. Connect the A side of the USB 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:** 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. Kanguru Defender Manager

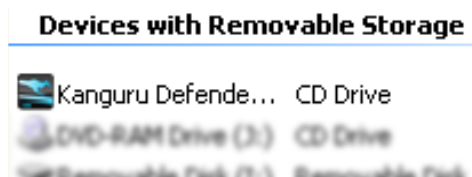
Kanguru Defender Manager (referred to throughout this manual as “KDM”) is the client program preloaded on the Defender’s CD-ROM partition. The user needs to login to KDM in order to access the secure, encrypted partition. KDM comes pre-installed on your Defender drive. No installation on your PC is necessary.

#### 3.1 Running KDM

To run KDM from a Windows operating system, simply connect your Defender drive to your computer through a USB port. The KDM application should start automatically if Autorun is enabled.

If KDM does not start automatically:

1. Open **My Computer** and open the Defender’s CD-ROM partition. The drive letter (e.g. D:, E:, F:) will depend on your computer.



2. Double-click on the **KDM.exe** file to launch the KDM application.

If it is your first time running KDM you will need to complete the setup wizard in order to set your security password (see section [3.3 The Setup Wizard on page 11](#)). If you have already setup your security password, you will be prompted to login (see section [3.4 Unlocking the Security Partition on page 16](#))

**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.

**Note:** You may not see the removable disk partition until you have logged into KDM.

### **3.2 Important Notice About Sleep Mode**

Do not leave KDM running on a computer that is going into Sleep Mode.

If you are still logged into KDM when a computer goes into sleep, it may lead to unexpected behavior which could potentially corrupt your data in a worst case scenario.

It is strongly advised not to leave a device unattended while logged in for any extended period of time, especially if the computer the device is connected to is configured to automatically go into Sleep Mode after a period of inactivity.

It is recommended that Sleep Mode be disabled on any computer that the Defender HDD/SSD is being used on.

If it is not possible to disable Sleep Mode, then be sure to logout of KDM once you are done using the device.

### 3.3 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.



**Caution!** Once the Setup Wizard has started, you should not disconnect your Defender without either first completing the Setup Wizard or closing the Setup Wizard by clicking on the **X** button.

#### 3.3.1 Selecting a Setup Language

The default language for the Setup Wizard is set to English. To run the Setup Wizard in a different language:

1. From the Start screen, click on the  icon next to the Language Menu.



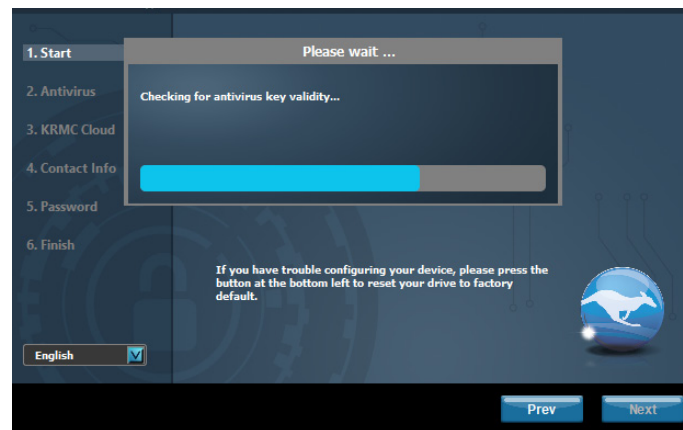
2. A list of available languages will appear in a drop down menu. Select your desired language from the drop down menu. The Setup Wizard will switch to the new language.
3. Click on the **Next** button to continue to the next step.

### 3.3.2 Activating On-board Antivirus Protection

**Note:** This section does not apply to Enterprise Edition users. Antivirus for Enterprise Edition is activated through Kanguru Remote Management Console (KRMC). Enterprise Edition users, please contact your administrator.

KDM will automatically check if your device has a valid antivirus license key.

**Note:** Your Defender will need to be connected to a computer with internet access in order to register for on-board antivirus protection.



If your Defender does not already have a valid antivirus license key, then you must fill out the following registration form with the required information and then click on the **Apply** button in order to activate your one (1) year of free antivirus protection.

Click on the **Skip** button if you do not wish to activate antivirus protection.

**Important!** If you decide to skip activating your antivirus now, you will not be able to activate it in the future without first resetting your drive to the factory default setting.



Click on the **Next** button to continue with setting up your Defender's security password.

### 3.3.3 KRCM Cloud

**Note:** This section does not apply to Enterprise Edition users.

Kanguru Defender drives can be remotely managed using the Kanguru Remote Management Console (KRCM). KRCM Cloud is hosted on Kanguru's server and can be enabled on any non-Enterprise Defender drive.



To Enable KRCM Cloud functionality:

1. Select the **Enable KRCM Cloud** option and then click on the **Apply** button.
2. A dialog box will appear confirming that KRCM Cloud was enabled on your device. Click **OK**.
3. Enter the KRCM Cloud Account ID for the account that you are registering this device with.
4. Click on **Register**

If you choose not to remotely manage your Defender using KRCM Cloud, select the **Disable KRCM Cloud** option and then click on the **Apply** button.

**Important!** You will not be able to enable KRCM Cloud functionality again, unless you reset your drive to the factory default.

Click on the **Next** button to continue setting up your drive.

### 3.3.4 Contact Info

**Note:** This section does not apply to Enterprise Edition users.



The image shows the 'Contact Info' screen of the Kanguru Defender HDD/SSD setup utility. The interface has a dark blue background with a green kangaroo logo. At the top left, it says 'KANGURU DEFENDER HDD/SSD™', 'USB 3.0', and 'AES 256-Bit Hardware Encryption'. At the top right, it says 'Hardware Encrypted USB'. On the left side, there is a vertical list of steps: 1. Start, 2. Antivirus, 3. KRMC Cloud, 4. Contact Info (highlighted), 5. Password, and 6. Finish. Below this list is a language dropdown menu set to 'English'. The main area is titled 'Contact Info' and contains several input fields: '\*Device Name:', 'Employee ID/Name:', '\*Phone Number:', '\*E-Mail:', 'Department:', and 'Comments:'. At the bottom of the form are 'Apply' and 'Cancel' buttons. At the very bottom of the screen are 'Prev' and 'Next' buttons.

Your contact info will be saved to the drive. If you are managing your drive using KRMC Cloud, the information entered here will be automatically be imported to the KRMC Cloud server when you register your drive.

Fill in your information in the appropriate fields and then click on the **Apply** button. A window will appear confirming that your data has been saved. Click on the **OK** button to close the window and then click on the **Next** button to finish setting up your drive.

### 3.3.5 Setting a Password

From the Set Password screen:

The screenshot displays the 'Set Password' screen of the KANGURU setup wizard. On the left, a sidebar lists the steps: 1. Start, 2. Antivirus, 3. KRM Cloud, 4. Contact Info, 5. Password (selected), and 6. Finish. Below the sidebar is a language selector set to 'English'. The main content area is divided into two panels. The top panel, titled 'Set Password', contains two input fields: 'Password' and 'Confirm Password', both filled with asterisks. To the right of these fields is a blue 'VK' button. Below the fields is a green 'Apply' button. The bottom panel, titled 'Password Info', lists password requirements with green checkmarks indicating they are met: 'Passwords match', '8 characters', '1 uppercase letters', '0 lowercase letters', '1 numerals', and '0 special characters'. At the bottom right of the screen are 'Prev' and 'Next' buttons.

1. Enter your password in the **Password** data field. You can enter your password using KDM's Virtual Keyboard by clicking the **VK** button. For more information on using the Virtual Keyboard see [section 3.4.2 Using the Virtual Keyboard to Enter Your Password on page 18](#).

**Note:** For security reasons, it is recommended that you incorporate letters, numbers and symbols to achieve maximum security.

2. Enter the same password in the **Confirm Password** field for verification. If your passwords do not match or there is any other issue with the password which you have entered in the Set Password section, an explanation will be visible in the **Password Info** window.

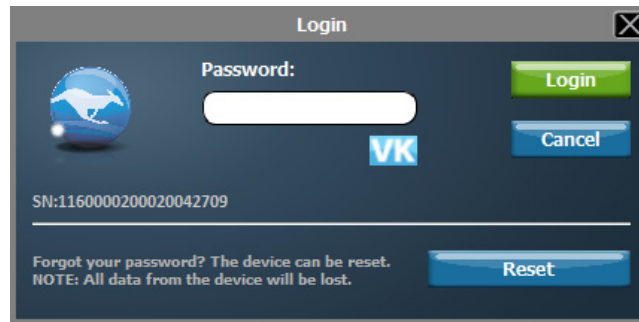
**Note:** The **Password Info** window will inform you if there are any password requirements. It updates in real time. Disregard the messages in the **Password Info** box until you have finished entering your password into both the **Password** and **Confirm Password** fields.

3. Click on the **Apply** button to set your password. Once the password has been set, click on the **Next** button.

Congratulations! Your device is now set up and ready for use. Click on the **Finish** button to complete the Setup Wizard and start using your device.

### 3.4 Unlocking the Security Partition

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



When the login screen appears:

1. Enter your password in the **Password** field.
2. Click on the **Login** button.

**Caution!** If you exceed the number of allowed incorrect password entries (6 entries is the default setting, but this may be different depending on your setup), for security purposes any data stored on the secure partition will automatically be erased. You will be issued an on-screen warning when you have one attempt remaining, to prevent accidental erasure. To cancel the login process, click on the **Cancel** button. Unplugging and then reinserting your Defender or manually running KDM.exe will bring the login window back.

Once you have successfully logged in to KDM, the Defender's secure partition will be accessible through My Computer or Windows Explorer. For more information on accessing the secure partition, see section [3.5 Encrypting Files and Folders on page 19](#).

**Caution!** Once KDM has started, you should never disconnect your device without first closing the KDM application by clicking the KDM task bar icon and selecting **Unmount Kanguru Defender** as described in section [5.1 Unmounting Your Defender on page 30](#).

**Note:** If your Defender drive is being managed by KRMC, you may see an **Autorun** checkbox in the Login window. This means that your administrator has configured your drive to auto-execute a file saved on your drive's secure partition every time you successfully login. You can disable the Autorun functionality by unchecking this box.



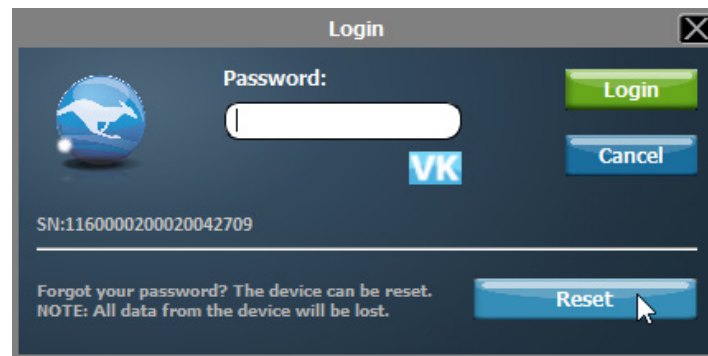
### 3.4.1 Resetting from the Login Screen

In the event you have forgotten your password, you can use the ‘Reset to Factory Default’ function to reset your password. This function will restore the device to the factory settings, erasing all saved passwords and data residing on the device’s secure partition.

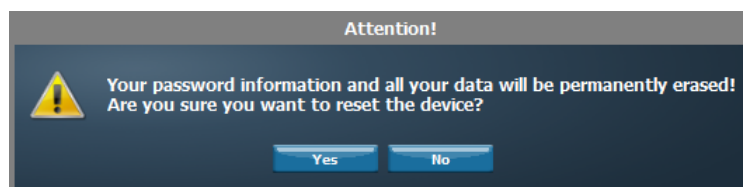
**Caution!** Using the ‘Reset to Factory Default’ function will format and wipe all data off the secure partition ! All personal data on the device will be lost!

To reset your Defender to the factory default:

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



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



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 complete the reset.

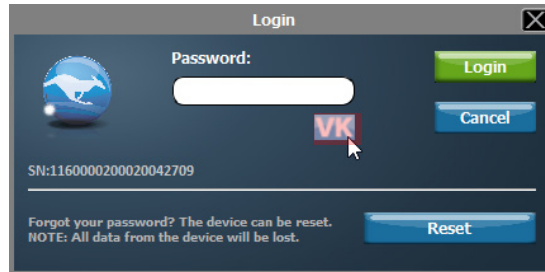
The next time you run KDM, you will have to complete the Setup Wizard again before you are able to access the secure partition. Please see section [3.3 The Setup Wizard on page 11](#) for instructions on completing the Setup Wizard.

### 3.4.2 Using the Virtual Keyboard to Enter Your Password

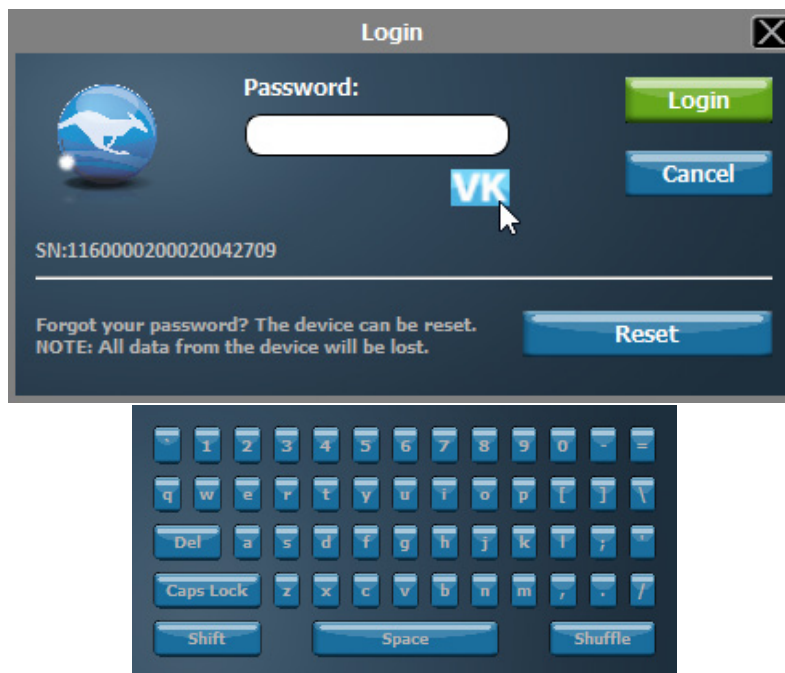
The virtual keyboard feature can be accessed anytime you are required to enter your password in order to prevent key logging applications from recording your key strokes and potentially stealing your password.

To use the virtual keyboard to enter your password:

1. Click on **VK** button which is located near the password entry field.



2. The virtual keyboard will appear below the Setup Wizard window. Click on the keys on the virtual keyboard to enter your password.




3. Click on the **VK** button again to close the virtual keyboard.

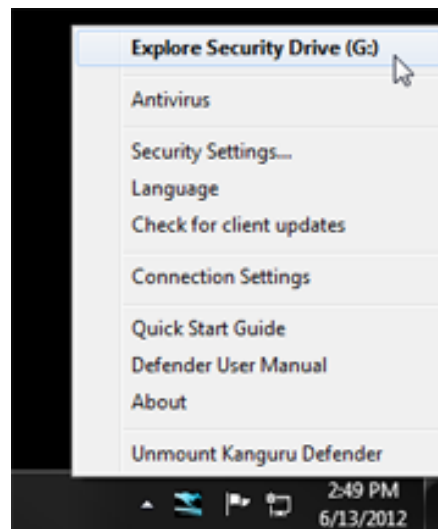
**Note:** You can click on the **Shuffle** key located at the bottom, right-hand corner of the virtual keyboard to randomize the virtual keyboard layout. Shuffling the keyboard layout protects your password from mouse tracking applications designed to thwart virtual keyboards.

### 3.5 Encrypting Files and Folders

A key feature of the Defender is drag & drop encryption; allowing you to simply drag files directly onto the drive. The Defender automatically encrypts these files as they are transferred to the secure partition, ensuring that your data stays safe and private.

To open the secure partition:

1. Start KDM.
2. Login to KDM to gain access to the secure partition.
3. Click on the KDM icon  located in the task bar and then select **Explore Security Drive** from the popup menu.



The Defender's security partition opens in a new window.

We recommend using either the drag & drop action, right-click copy/paste action, or the shortcut keys (Ctrl+C and Ctrl+V) to copy and paste files and folders directly to and from the secure partition.

**Note:** Data saved on the Defender's secure partition are only accessible after you have successfully logged into KDM.

### 3.6 On-board Antivirus

You must register your device with Kanguru Solutions in order to take advantage of the Defender's on-board antivirus features (see section [3.3.2 Activating On-board Antivirus Protection on page 12](#)).

Once your on-board antivirus has been activated, real-time virus scanning is automatically enabled whenever you log into your device. All files copied to the Defender are scanned for viruses and malware.


**Note:** If the device is connected to a computer with internet access, updates for the latest virus definitions are downloaded automatically after you login to KDM. If you disconnect your Defender before the latest update has finished downloading, the Defender will save your place and continue the download the next time it is connected to a computer with internet access.

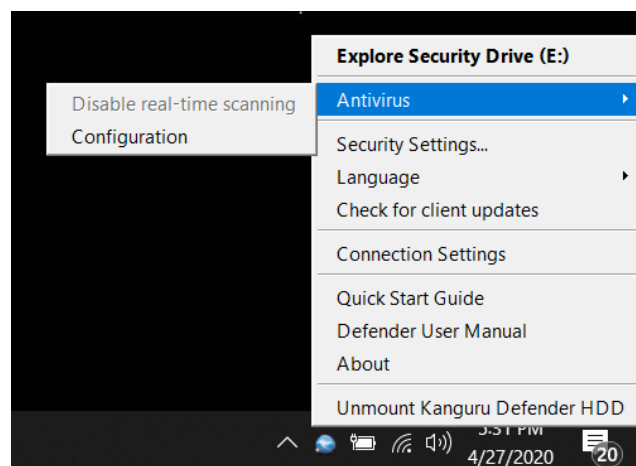
Virus definitions are stored in the 'System' folder on the secure partition. If these files are deleted, they will be automatically re-downloaded. If the device is reset to the factory default, these files will be deleted and will need to be re-downloaded.

**Caution!** Do not store any data in the 'System' folder. Any data saved here that does not pertain to virus definitions will be automatically deleted.

#### The Onboard Antivirus console

You can access the on-board antivirus console to scan your device, a path or a file. To open the antivirus console:

1. Right-click on the KDM icon  located in the task bar.
2. Select **Antivirus** from the popup menu and then click on **Configuration** from the submenu.



The antivirus console appears.

### 3.6.1 Device Scan

The antivirus console allows you to scan your Defender for known viruses and malware.



To scan your Defender:

1. Click on the **Scan Device** tab at the top of the antivirus console.
2. Click on the **Start Scan** button to begin scanning your Defender.
3. Once the scan has started:
  - Click on the **Pause Scan** button to pause the scan process. Click on the **Resume Scan** button to resume the scan.
  - Click on the **Stop Scan** button to cancel the scan process.
4. The scan results will appear in the **Scan Results** window.
5. Click on the **View Scan Log** button to view a log of the previous scan.
6. Click on the **OK** button to close the antivirus console.

### 3.6.2 Path Scan

The antivirus console allows you to scan any path on your computer for known viruses and malware.

**Note:** The **Scan Path** feature can be disabled on Enterprise Edition drives, please contact your administrator for more information.



To scan a path on your computer:

1. Click on the **Scan Path** tab at the top of the antivirus console.
2. Click on the **Start Scan** button and then select a path on your computer to begin scanning.
3. Once the scan has started:
  - Click on the **Pause Scan** button to pause the scan process. Click on the **Resume Scan** button to resume the scan.
  - Click on the **Stop Scan** button to cancel the scan process.
4. The scan results will appear in the **Scan Results** window.
5. Click on the **View Scan Log** button to view a log of the previous scan.
6. Click on the **OK** button to close the antivirus console.

### 3.6.3 File Scan

The antivirus console allows you to scan any file on your computer for known viruses and malware.

**Note:** The **Scan File** feature can be disabled on Enterprise Edition drives, please contact your administrator for more information.




To scan a file:

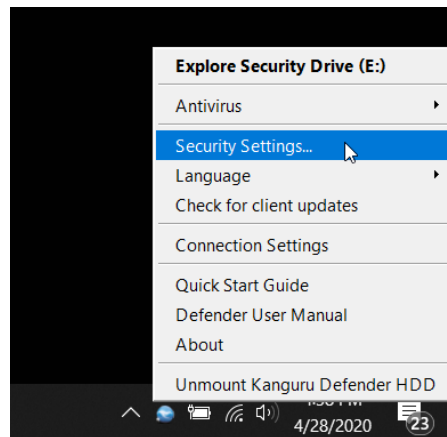
1. Click on the **Scan File** tab at the top of the antivirus console.
2. Click on the **Start Scan** button and then select a file to begin scanning.
3. Once the scan has started:
  - Click on the **Pause Scan** button to pause the scan process. Click on the **Resume Scan** button to resume the scan.
  - Click on the **Stop Scan** button to cancel the scan process.
4. The scan results will appear in the **Scan Results** window.
5. Click on the **Advanced Info** button to view a log of the previous scan.
6. Click on the **OK** button to close the antivirus console.

### 3.7 Changing Your Password

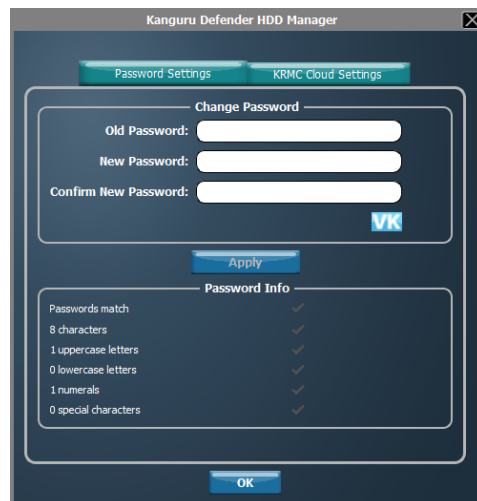
You can change your security password through the Security Settings.

To change your password:

1. Click on the KDM icon  located in the task bar and then select **Security Settings...** from the popup menu.



2. The Password Settings window opens. Enter your current password in the **Old Password** field. Enter your new password in the **New Password** field and then enter it again in the **Confirm New Password** field.



3. When you are ready to proceed, click on the **Apply** button to set your new password.
4. Once your new password has been set, a confirmation window appears informing you that your password has been successfully changed. Click on the **OK** button to finish setting your new password.




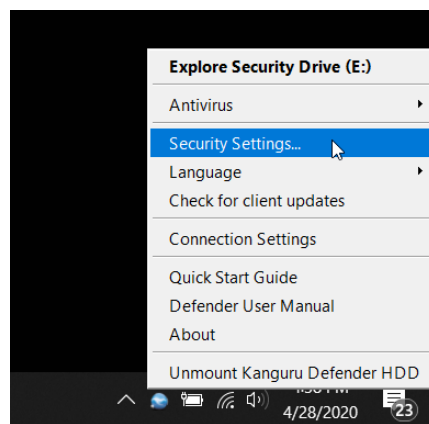
### 3.8 KRMCloud Settings

**Note:** This section does not apply to Enterprise Edition users.

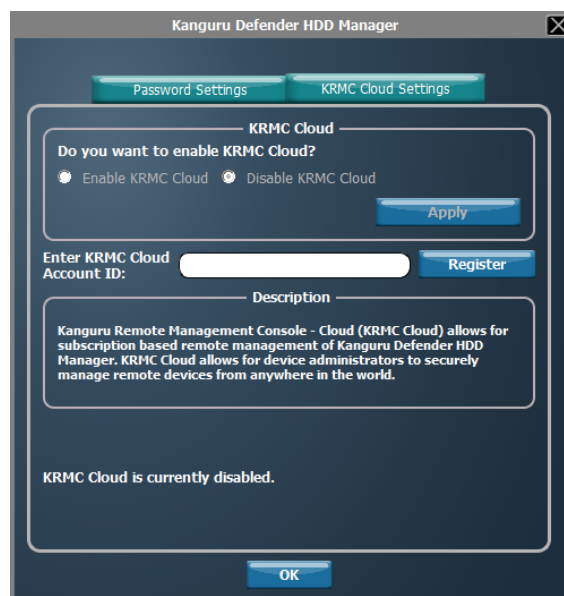
You can enable or disable KRMCloud functionality through the Security Settings.

To change your device's KRMCloud functionality:

1. Click on the KDM icon  located in the task bar and then select **Security Settings...** from the popup menu.




2. The Password Settings window opens. Click on the **KRMCloud Settings** tab at the top of the window to enter the KRMCloud Settings window.
3. Enable or Disable KRMCloud by selecting the appropriate radio button and then click on the **Apply** button.

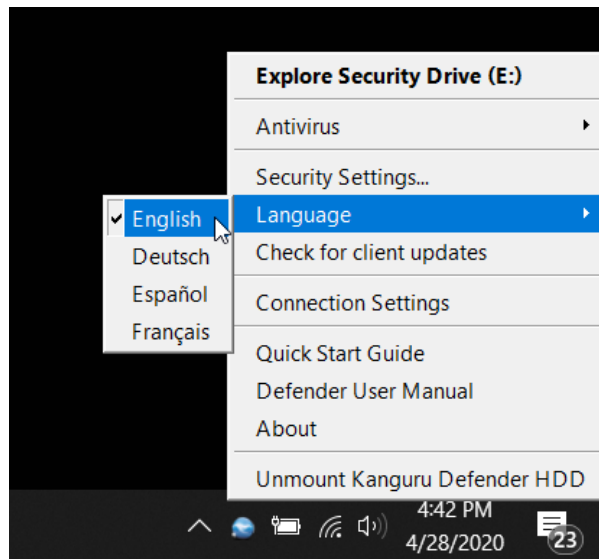


### 3.9 Changing Languages

KDM supports several languages. The language is set to English by default.

To change the language:

1. Right -click on the KDM icon  located in the task bar and then hover your cursor over the **Language** option in the popup menu. A list of available languages appears.



2. From the submenu, click on the desired language that you want the KDM application to be displayed in.


### 3.10 Online Documentation

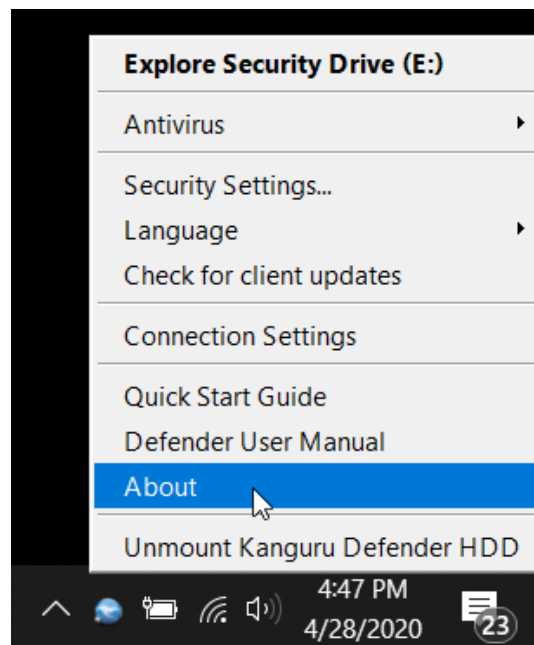
You can download digital copies of the Kanguru Defender's documentation from the internet.

To download your Defender's documentation, right-click on the KDM icon  located in the task bar.

- Click on **Quick Start Guide** to download a digital copy of the Defender's Quick Start Guide.
- Click on **Defender User Manual** to download a digital copy of the Defender's User Manual

### 3.11 About KDM

To view information regarding the version of KDM currently installed on your device, right-click on the KDM icon  located in the task bar and then select **About**.



## 4. Updating Your Defender HDD

Updates for your Defender HDD's client application may be released from time to time. To view the version of the KDM client application currently running on your drive, see section [3.11 About KDM on page 27](#).

Please check whether your Defender HDD is being managed by Kanguru Remote Management Console (KRMC), as the update process is different for enterprise edition and standard edition drives.

### 4.1 Updating standard edition drives

Standard edition Defender HDD drives will automatically check the Kanguru Central Server (KCS) for client updates. Once you have successfully logged into your Defender HDD's secure partition, KDM will check KCS for any available client updates. If an update is available, you will receive a pop-up notification with instructions for downloading the updater file.

**Note:** The drive will only check KCS if it is connected to a computer with internet access.

Standard edition Defender HDD users can also manually search and download available client updaters from the Kanguru Support site. Defender HDD client updaters can be found under the 'USB Client Software Updates' forum in the 'Software Downloads and Updaters' section ([support.kanguru.com](http://support.kanguru.com)).

### 4.2 Updating KRMC enterprise edition drives

Enterprise edition Defender HDD drives are managed by the Kanguru Remote Management Console (KRMC). Updaters for enterprise edition Defender HDD drives are available for download from the Kanguru Support site. The KRMC system administrator is granted access to the enterprise edition downloads when their KRMC order is processed. Enterprise edition updaters can be found under the 'KRMC Enterprise' forum in the 'Software Downloads and Updaters' section ([support.kanguru.com](http://support.kanguru.com)).

Once you have downloaded your enterprise edition updater, you can create an 'Upgrade Client Application' action in KRMC to deploy the update to all of your managed drives remotely.

**Note:** Only KRMC administrators are given access to download the enterprise edition updaters.

### 4.3 Verifying the download checksum

To verify the integrity of the KDM updater that you downloaded, please use the SHA256 Checksum tool. The SHA256 Checksum tool will generate a 64-character checksum which can be verified against the checksum list published by Kanguru Solutions. This ensures that the updater file was downloaded correctly and wasn't altered.

The SHA256 Checksum tool and a list of valid checksum values can be found on Kanguru's Support site: <https://kanguru.zendesk.com/entries/21747773-sha256-checksum-utility>

To view and verify your download's checksum:

3. Download the SHA256 Checksum tool from the Kanguru Solutions' support site.
4. Save the SHA256 Checksum tool to the same directory that KDM updater file is saved in.
5. Open a command prompt window by clicking on **Start** → **All Programs** → **Accessories** → **Command Prompt**.
6. Within the command prompt window, navigate to the directory containing your KDM updater file and the SHA256 Checksum tool.
7. Type "sha256.exe <filename.exe>", where <filename.exe> is the name of the updater file that you are checking.
8. Press the **Enter** key. A 64-character string appears. This is the SHA256 checksum of the updater.
9. Verify that the checksum generated by the SHA256 Checksum tool matches the checksum published by Kanguru Solutions for your updater version.

If the checksum generated by the SHA256 Checksum tool matches the checksum published, then your updater downloaded correctly. If the checksum generated does not match the checksum published by Kanguru Solutions, please delete the updater from your computer and download it again.

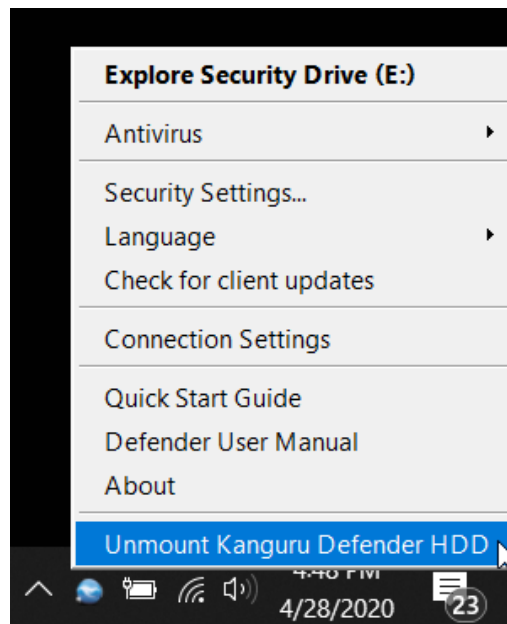
## 5. Safely Removing Your Kanguru Defender

Before unplugging the Defender from the USB port, you should always make sure that you have unmounted the secured partition. After the Defender has been unmounted, you should use your operating system's method for safely removing a USB device.

### 5.1 Unmounting Your Defender

When you unmount your Defender, the KDM application will close and the secure partition containing your encrypted data will be inaccessible until you log into KDM again.

To unmount your Defender, right-click on the KDM icon  located in the task bar and then select **Unmount Kanguru Defender**.



The KDM icon in the task bar will disappear and the Defender's secure partition will no longer be accessible.

**Caution!** Do not disconnect the Kanguru Defender without first properly unmounting your device as detailed in this section and then safely removing the device from your computer. Doing so may result in file damage or data corruption.

## 5.2 Safely Removing from Windows

**Caution!** Be sure that the secure partition has been unmounted before attempting to remove the Defender drive. See section [5.1 Unmounting Your Defender on page 30](#).

Please use the Windows ‘Safely Remove Hardware’ function before disconnecting your Defender drive.

To safely remove the Defender:

1. Click on the **Safely Remove Hardware icon** located in the task bar.



2. A popup menu appears listing all USB devices connected to your computer. Select the Defender from the menu (it will appear with two drive letters).

A message will appear indicating that the portable storage device can be safely removed. You can now disconnect the Defender.

If a message saying “The device cannot be stopped right now” appears, please make sure that any windows or applications accessing the Defender are closed and then try again.

## **6. Warranty Information**

This product carries a 3-year warranty from the date of purchase. Kanguru Solutions is not responsible for any damages incurred in the shipping process. Any claims for loss or damage must be made to the carrier directly. Claims for shipping errors should be reported to Kanguru Solutions within three (3) working days or receipt of merchandise.

## **7. Tech Support**

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

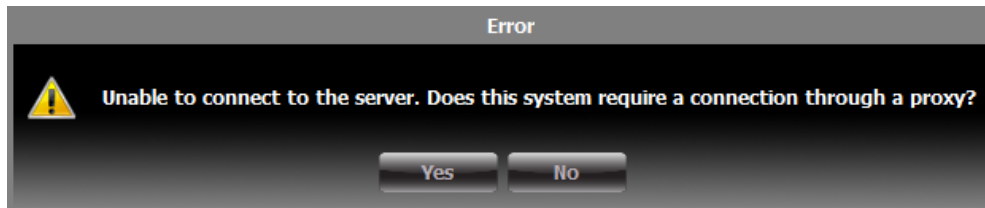
Call 1-508-376-4245 or  
Visit our website at [www.Kanguru.com](http://www.Kanguru.com)



## Appendix A - Proxy Support

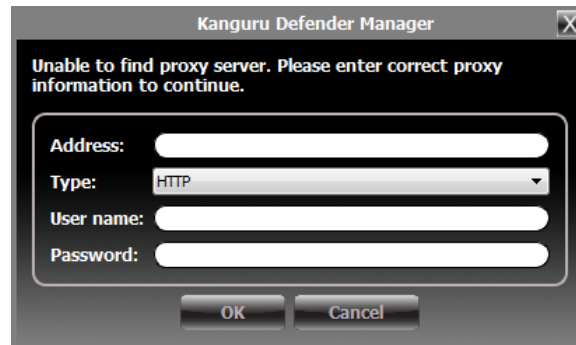
If your computer uses a proxy server to access the internet, the correct proxy information will need to be configured in KDM.

If the KDM client application cannot connect to the internet you will see the following error message:



If the computer that the Defender is connected to uses a proxy server to access the internet, click on the **Yes** button. KDM will try to read the proxy server information from the computer's configuration.

- If KDM is able to determine your proxy server's address and no authentication is required then KDM will read this information and connect to the internet as normal.
- If KDM is able to determine your proxy server's address but the proxy requires authentication then you will need to enter your credentials in the window that appears.
- If KDM is unable to determine your proxy server's address then you will need to enter the proxy server address, proxy type and credentials:



Enter the proxy address and the port to connect to in the address field (e.g. 192.168.0.193:8080 or proxycomp:8080). Select your proxy type and then enter your credentials. If KDM is able to connect to the proxy server using those credentials then the authentication information is saved in an encrypted proxy settings file.

**Note:** Proxy information must be configured once for each computer the Defender HDD/SSD is connected to that connects to the internet through a proxy server.



Kanguru Solutions  
1360 Main Street  
Millis, MA 02054  
[www.kanguru.com](http://www.kanguru.com)

04.28.20 v1.8 © 2020 Kanguru Solutions

Legal terms and conditions available at [www.kanguru.com](http://www.kanguru.com). Please review and agree before use. Thank you.