KANGURU Solutions™

"Technology on the move!"

Kanguru Defender V2 Rev.2

User Manual

Copyright 2012, All Rights Reserved.

Model no: KDV2

NOTICES AND INFORMATION

Please be aware of the following points before using your Kanguru Defender V2

Copyright © 2012 Kanguru Solutions. All rights reserved.

Windows XP®, Windows Vista®, and Windows 7® 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 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 your Kanguru Defender Flash Drive. Flash memory does not need to be defragmented and does not gain any performance by doing so. Defragmenting your flash drive can actually degrade the flash memory which may reduce the drive's total capacity and lifespan.

Table of Contents

1. Introduction 4
1.1 Technical Specifications 6

2. Kanguru Defender Manager V2 7
2.1 Running KDMV2 7
2.1.1 Windows Users 7
2.1.2 Mac Users 9

2.2 The Setup Wizard 10
2.2.1 Selecting a Setup Language 10
2.2.2 Activating On-board Antivirus Protection (Windows Only) 11
2.2.3 Setting a Password 12
2.2.4 The Virtual Keyboard 13
2.2.5 KRMC Cloud 14
2.2.6 Contact Info 15
2.2.7 Resetting from the Setup Wizard 16

2.3 Logging into KDMV2 17
2.3.1 Resetting from the Login Screen 18

2.4 Encrypting Files and Folders 19

2.5 On-board Antivirus (Windows Only) 20
2.5.1 Device Scan 21
2.5.2 Path Scan 22
2.5.3 File Scan 23
2.5.4 License 24

2.6 Changing Your Password 25

2.7 Changing Languages 26

2.8 Online Documentation 27

2.9 About KDMV2 27

2.10 Unmounting Your Defender V2 28
2.10.1 Safely Removing from Windows 28
2.10.2 Safely Removing from Mac OS X 29

3. Warranty and Technical Support 29

1. Introduction

The Kanguru Defender V2 is a hardware encrypted, tamper proof USB flash drive. The Defender V2 contains two partitions: a 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 Kanguru Defender V2 flash drive secures your sensitive data using:

- 256-bit AES hardware encryption
- Secure password protection

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 V2 USB Flash Drive
- Quick Start Guide
- Registration Form
- Lanyard **Caution!** The through-hole at the bottom of the drive is designed for use with the provided lanyard only.

Features

√ 256-bit AES hardware encryption
√ FIPS 197 Validated
√ Password protected data partition for your secure files
√ Does NOT require Admin privileges
√ Driverless installation (Plug & Play)
√ High-strength aluminum housing
√ Write protect switch
√ On-board antivirus protection
√ Custom security colors available (Red, Green, Yellow, Blue, Tan, Gray)
√ HIPAA Compliant
√ Sarbanes Oxley Compliant
√ GLB Compliant

System Requirements

- 1 Available USB port (USB 2.0 Recommended)
- 256MB of internal DDR RAM or more
- 500MHz internal CPU or faster
- Operating Systems (32 and 64 bit compatible)
  - Windows 2000 SP 4, Windows XP SP 3, Windows Server 2003, Windows Vista, Windows 7
  - Mac OS X 10.5 and above (compatible with Intel-based Macs only)

Kanguru Remote Management Capability

Kanguru Defender V2 flash 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 and secutiry system.

With KRMC you will be able to:

- √ Remotely delete all data on a target drive
- √ Schedule remote actions for present or future times
- √ 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
- √ Create user groups

KRMC Compatibility

There are two versions of KRMC that you can use to manage your drives:

- **KRMC Enterprise Edition** - KRMC is hosted on the customer's own server
- **KRMC Cloud** - KRMC is hosted on a Kanguru server

The Kanguru Defender V2 is compatible with both KRMC **Enterprise Edition** as well as **Cloud**.

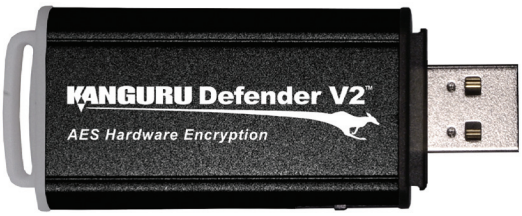
For more information about KRMC, visit: https://www.kanguru.com/index.php/flash-management

1.1 Technical Specifications

The Kanguru Defender V2 comes in two models, depending on your drive's capacity. Technical specifications are different depending on your model.

1GB - 16GB Model

32GB - 128GB Model



General Specifications

Interface	USB 2.0 (USB 1.1 compatible)
Encryption Features	Hardware based 256-bit AES encryption
OS Compatibility	Windows 2000 SP4, XP SP3, Server 2003, Vista,7 Mac OS X 10.5 and above (Intel based only) 32 and 64 bit compatible
Write Cycles	10,000 write cycles / block
Data Retention	10 years or more
Operating Temp	0°C – 70°C
Humidity Range	20% - 90%
Shock Resistance	1000G Max
Vibration	15G Peak to Peak Max

1GB - 16GB Defender V2 Specifications

Data Transfer Rate	Read: 20 - 33 MB/s Write: 10 - 13 MB/s
Weight	10g
Dimensions	64mm x 18.5mm x 9mm
Power (Read)	Max Read: 5 VDC @ 122mA
Power (Write)	Max Write: 5 VDC @ 182mA

32GB - 64GB Defender V2 Specifications

Data Transfer Rate	Read: 31 MB/s Write: 10 MB/s
Weight	15g
Dimensions	71mm x 27mm x 9mm
Power (Read)	Max Read: 5 VDC @ 150mA
Power (Write)	Max Write: 5 VDC @ 266mA

2. Kanguru Defender Manager V2

Kanguru Defender Manager V2 (referred throughout this manual as KDMV2) is the client application preloaded on the Defender V2's CD-ROM partition. The user needs to login to KDMV2 in order to access the secure, encrypted partition. KDMV2 comes pre-installed on your Defender V2. No installation on your PC is necessary.

2.1 Running KDMV2

The Kanguru Defender V2 is compatible with multiple operating systems. Steps for launching the KDMV2 application can be different depending on the operating system that your computer is running.

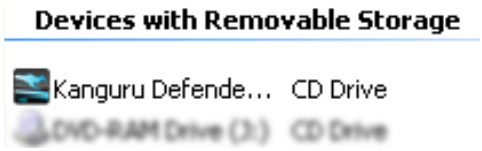
2.1.1 Windows Users

To run KDMV2, simply connect your Defender V2 to your computer through a USB port. When you connect your Defender V2, a CD-ROM partition and a removable disk partition should appear in My Computer. If you are running Windows 7 and do not see the removable disk, please refer to page 8 in this manual.

The KDMV2 application should start automatically.

If KDMV2 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 **KDMv2.exe** file to start the KDM application.

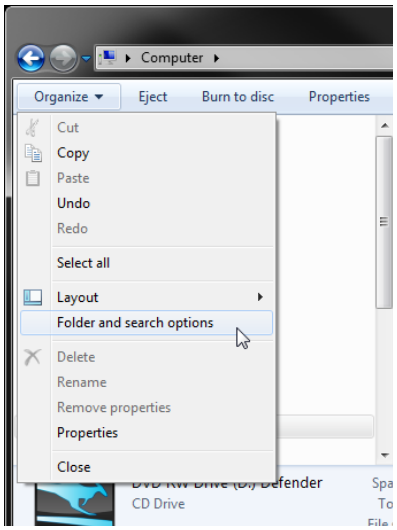
Caution! The **KDMv2.exe** file needs to remain on your Defender V2's CD-ROM partition at all times. Always run the application from the CD-ROM partition. Do not try to copy KDMV2 or run KDMV2 from your computer's local hard drive.

Attention Windows 7 Users

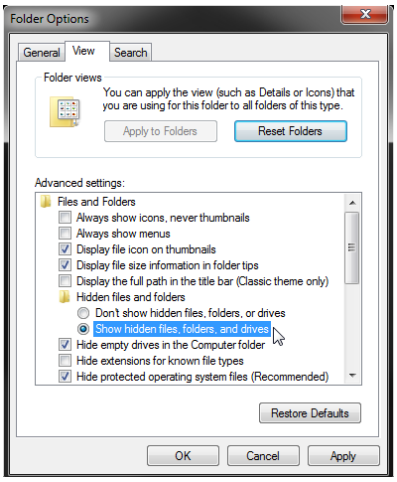
Windows 7 users may not see the removable disk partition until you have logged into KDMV2 (see section 2.3 *Logging into KDMV2* on page 17 for more information). This is normal.

If you are running Windows 7 and for any reason need to see the removable disk before you log into KDMV2, you will need to configure Windows Folder and Search Options. **Note:** This is user preference only. There is no need to configure Windows in order to use your Defender V2.

1. From My Computer, click on the **Organize** tab and then select **Folder and search options**.



2. The Folder Options window appears. Click on the **View** tab and then scroll down to the option for Hidden Files and Folders. Select **Show hidden files, folders, and drives**.

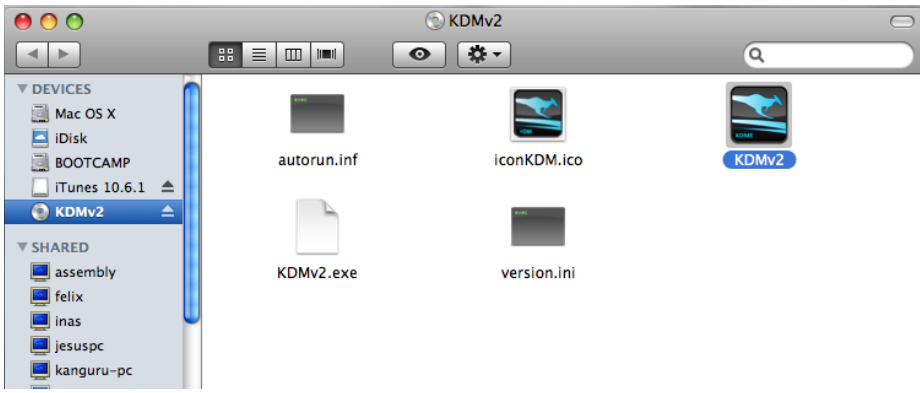


3. Click on the **OK** button to finish configuring Windows. The removable disk is now visible before you log into KDMV2.

2.1.2 Mac Users

To run KDMV2 from Mac OS X, connect your Defender V2 to your computer through a USB port. A CD icon 'KDMv2' will appear on the desktop. Double click on the KDMv2 icon to open it.

In the window that opens, double-click on the KDMv2.app file to launch the KDMV2 application.



Caution! The KDMv2.app file needs to remain on your Defender V2's CD-ROM partition at all times. Always run the application from the Defender V2's CD-ROM partition. Do not try to copy KDMv2 or run KDMv2 from your computer's hard drive.

Note: The KDMv2 icon is not always displayed on the desktop. If you do not see the KDMv2 icon on your desktop, you can locate the KDMv2.app file in the CD-Rom partition through the Finder window.

2.2 The Setup Wizard

When you start KDMV2 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 V2's secure, encrypted partition.

Note: Before you can setup your Defender V2's password, the manual write protect switch must be set to the unlock position (towards the USB connector).

2.2.1 Selecting a Setup Language

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

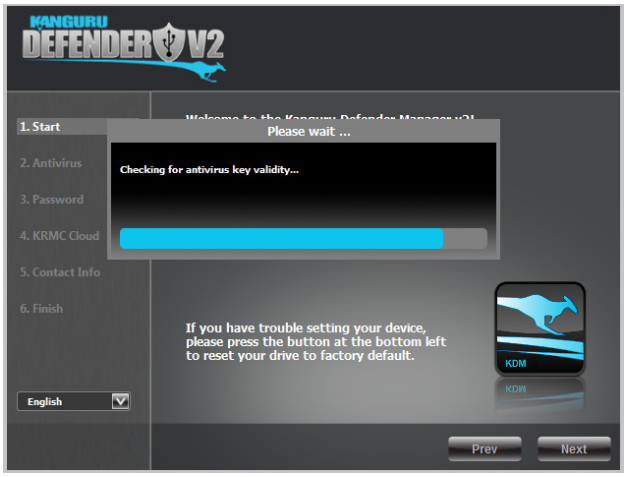
1. From the Welcome screen, click on the Language selection menu. A list of available languages will appear in a drop down menu. Select your desired language from the drop down menu. The Setup Wizard will switch to the new language.

2. Click on the **Next** button to continue to the next step.

2.2.2 Activating On-board Antivirus Protection (Windows Only)

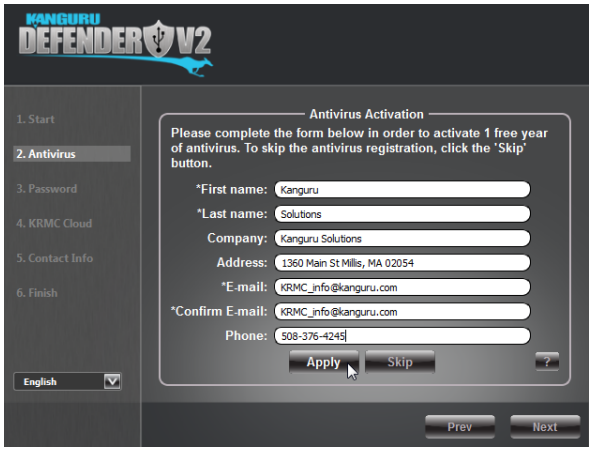
Note: This section does not apply to drives that are being managed with the Kanguru Remote Management Console (KRMC) Enterprise Edition. Antivirus for Enterprise Edition drives is activated through KRMC. If your drive is being managed by KRMC Enterprise Edition, please contact your administrator for more information.

KDMV2 will automatically check if your device has a valid antivirus license key. Your Defender V2 will need to be connected to a computer with internet access in order to register for on-board antivirus protection.



If your Defender V2 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.

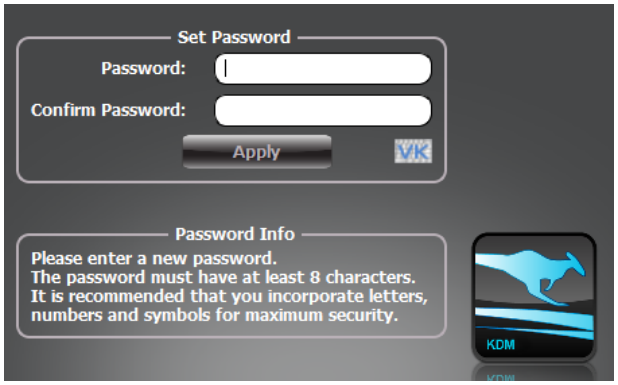


Click on the **Next** button to continue with setting up your Defender V2's security password.

2.2.3 Setting a Password

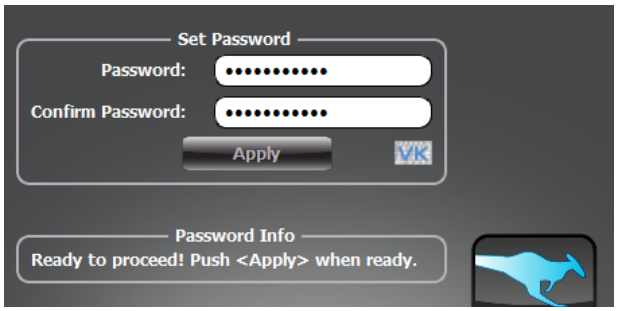
Your password is used to login to your Defender V2's secure partition after you have completed the Setup Wizard. To create your login password from the Set Password screen:

1. Enter your password in the **Password** data field. **Note:** For security reasons, it is recommended that you incorporate letters, numbers and symbols to achieve maximum security.

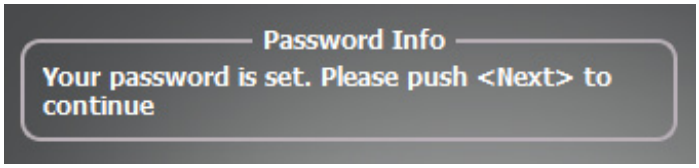


The Password Info window will inform you if there are any password requirements. It updates in real time. Disregard the messages in the Password Info box until you have finished entering your password into both the Password and Confirm Password fields.

2. Enter the same password in the **Confirm Password** field for verification. If the passwords you entered match, you will receive a notification in the Password Info box.



3. Click on the **Apply** button to set your password. Once the password has been set you will see the following message in the Password Info box:



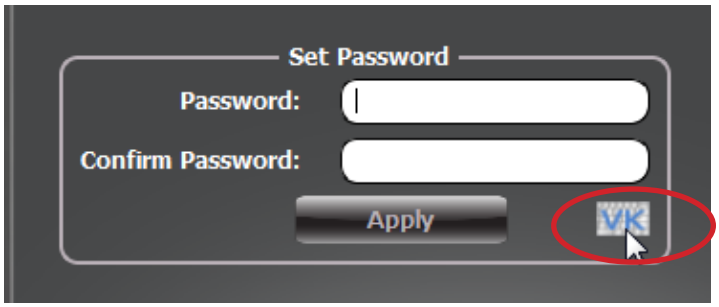
4. Click the **Next** button. KDMV2 will automatically configure the security parameters and complete the setup process.

2.2.4 The Virtual Keyboard

The virtual keyboard feature can be accessed when you are entering your Defender's password (see section 2.2.3 *Setting a Password* on page 12). It can be used when entering your password to prevent any keylogging applications from recording your key strokes.

To use the virtual keyboard to enter your password:

1. From the Set Password screen click on **VK** button. It is located near the bottom right of the Confirm Password field.



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

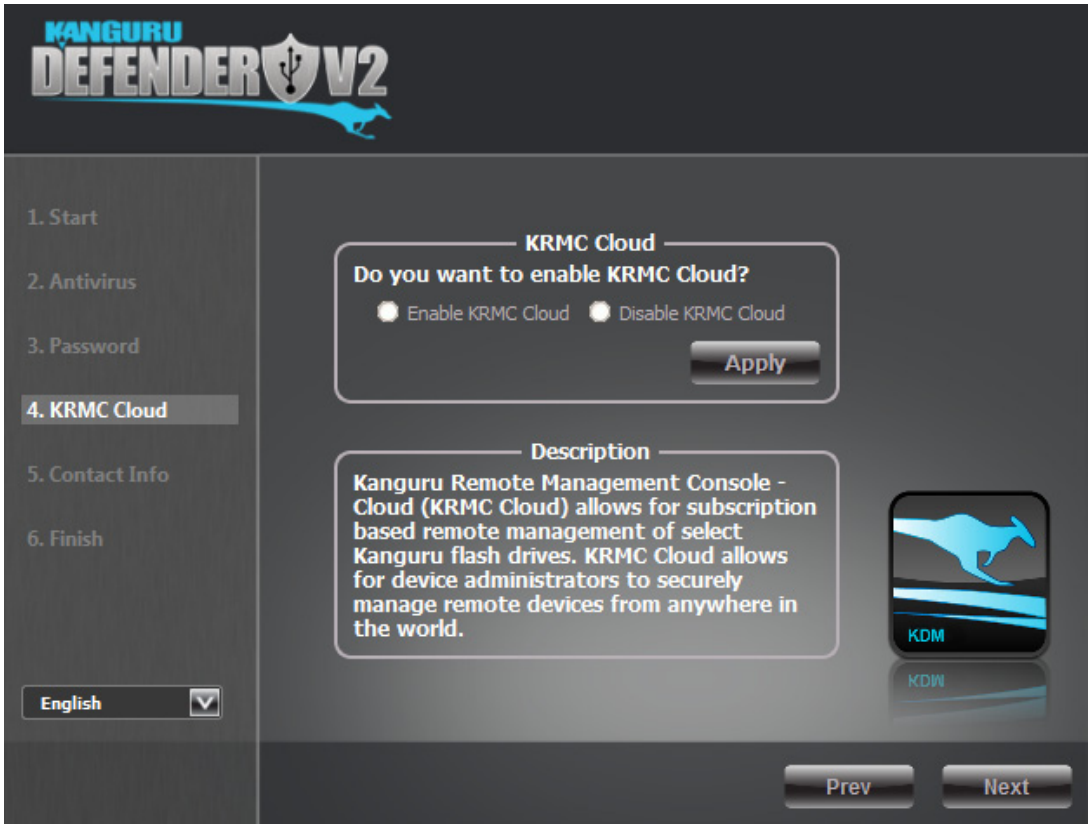
3. Click on the **VK** button again to close the virtual keyboard.

Note: You can click on the **Shuffle** key on the bottom right corner of the virtual keyboard to randomize the virtual keyboard's layout to prevent mouse tracking software from spying your password.

2.2.5 KRMC Cloud

Note: This section does not apply to Defender V2 drives that are being managed with the Kanguru Remote Management Console (KRMC) Enterprise Edition.

The Kanguru Defender V2 can be remotely managed using the Kanguru Remote Management Console (KRMC). KRMC Cloud is hosted on Kanguru's server and KRMC Cloud functionality must be enabled on the drive in order for it to be managed by KRMC.



To Enable KRMC Cloud functionality:

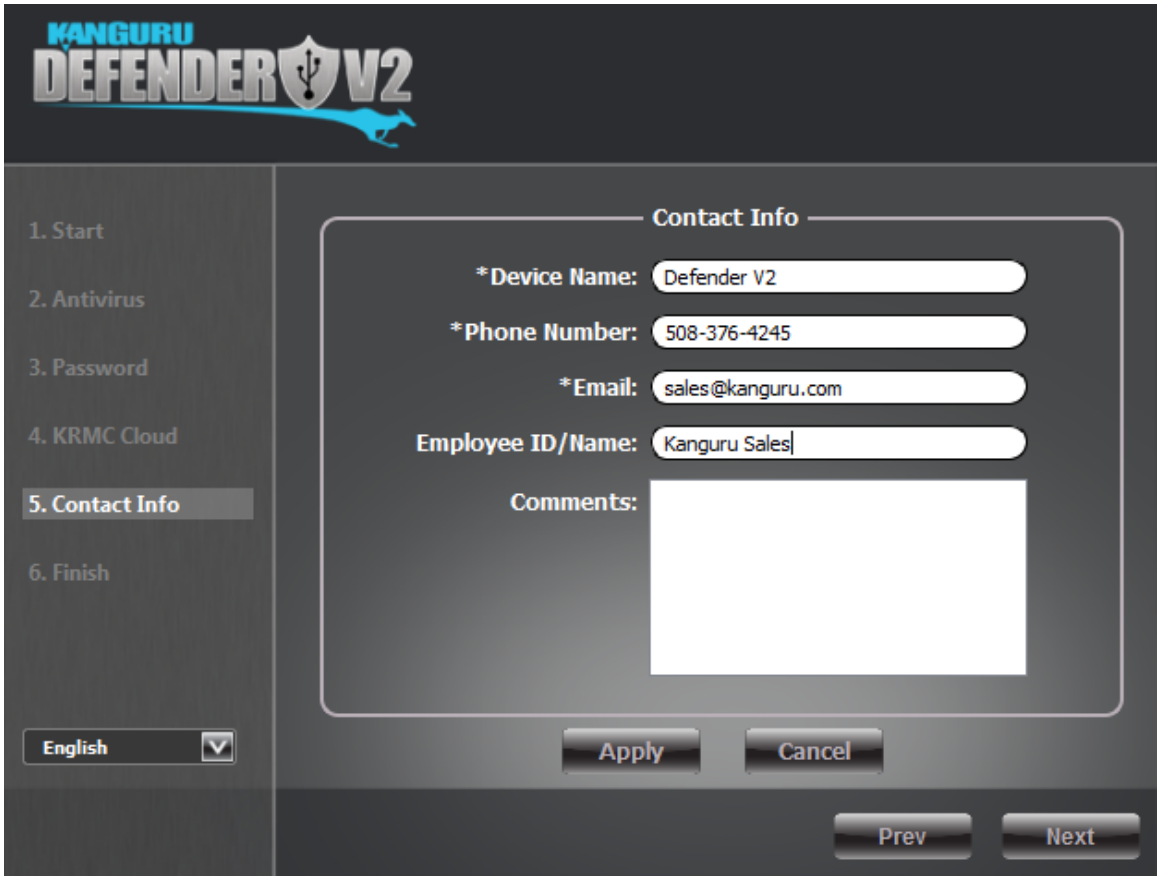
1. Select the **Enable KRMC Cloud** option and then click on the **Apply** button.
2. A dialog box will appear asking if you want to register your device with KRMC Cloud. Click on the **Yes** button.
3. Your web browser will open and direct you to the KRMC Cloud login page.
4. Purchase a license for your drive in order to use it with KRMC Cloud.

If you choose not to remotely manage your Defender using KRMC Cloud, select the **Disable KRMC Cloud** option and then click on the **Apply** button. You will not be able to enable KRMC Cloud functionality again, unless you reset your drive to the factory default.

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

2.2.6 Contact Info

Note: This section does not apply to drives that are being managed with the Kanguru Remote Management Console (KRMC) Enterprise Edition.



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 Defender V2 with KRMC Cloud.

Fill in your information in the appropriate fields (Device Name**,** Phone Number and Email are required 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.

Congratulations! Your Kanguru Defender V2 is now ready for use.

2.2.7 Resetting from the Setup Wizard

If you experience any problems while running the Setup Wizard, you may have to perform a device reset before you can complete the setup process.

Caution! Performing the reset function will format the device's secure encrypted partition. All data stored on the secure partition will be lost.

To perform a device reset during the Setup Wizard:

1. From anywhere in the Setup Wizard, click on the **Prev** button until you return to the Start screen.

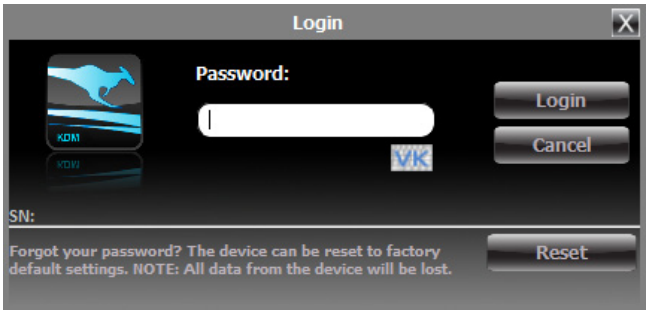
2. On the Start screen you will see a **Reset** button located at the bottom of the window. Click on the **Reset** button.

3. A dialog box appears asking you to confirm the reset. Click on **Yes** to reset your device to the factory default settings.

After the device has been reset to the factory default setting you will need to complete the Setup Wizard again before you are able to access the Defender V2's secure partition.

2.3 Logging into KDMV2

Anytime you run KDMV2, you will be asked to login using your security password. You need to provide the correct security password in order to access the Defender V2'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 enter your password incorrectly seven times in a row (seven times is the default setting; actual number of attempts may vary 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 V2 or manually running KDMv2.exe will bring the login window back.

Once you have successfully logged in to KDMV2, the Defender's secure partition will be accessible through My Computer or Windows Explorer. For more information on accessing the secure partition, see section 2.4 *Encrypting Files and Folders* on page 19.

Caution! Once KDMV2 has started, you should never disconnect your device without first closing KDMV2 properly by clicking the KDMV2 taskbar icon and selecting **Unmount Kanguru Defender** as described in section 2.10 *Unmounting Your Defender V2* on page 28.

Note: If your Defender V2 drive is being managed by KRMC, you may see an **Autorun** checkbox. 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.

2.3.1 Resetting from the Login Screen

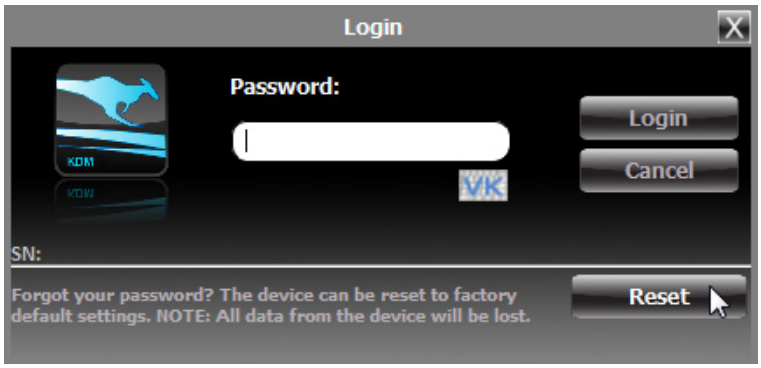
In the event you have forgotten your password, you can use the Reset to Factory Default function to reset your password. This function will restore the device to the factory settings, erasing all saved passwords and data residing on the device's secure partition.

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

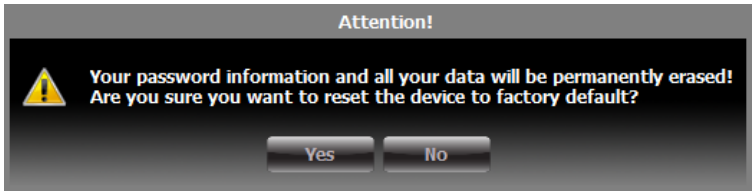
To reset your Defender V2 to the factory default:

1. Start KDMV2.

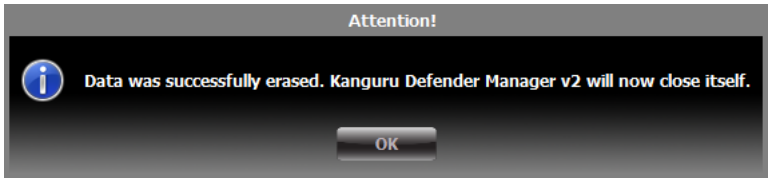
2. When the login screen appears, click on the **Reset** button.



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 KDMV2, you will have to complete the Setup Wizard again before you are able to access the secure partition.

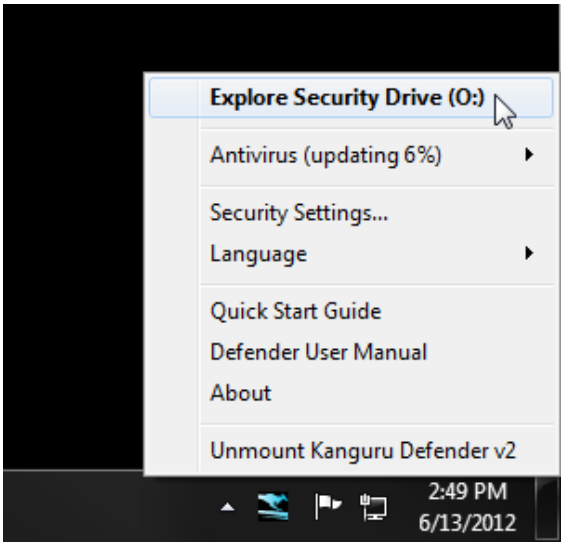
2.4 Encrypting Files and Folders

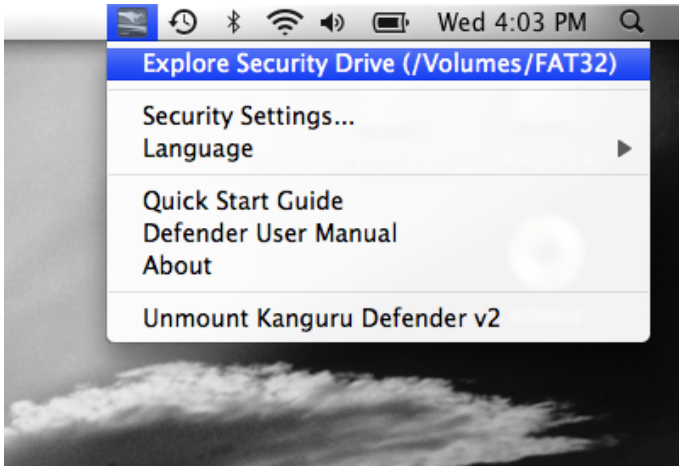
A key feature of the Defender V2 is drag & drop encryption; allowing you to simply drag files that you want to encrypt onto the drive using the standard Windows Explorer interface. The Defender V2 automatically encrypts these files as they are transferred to the secure partition, ensuring that your data stays safe and private.

To open the secure partition:

1. Login to KDMV2 to gain access to the secure partition.

2. Click on the KDMV2 icon located in the taskbar and then select **Explore Security Drive** from the popup menu.





Alternatively, you can access the secure partition through My Computer or through Windows Explorer.

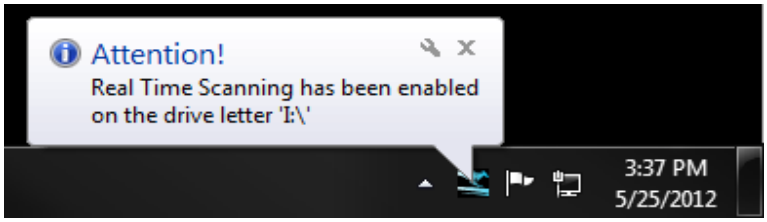
We recommend using either the drag & drop action, right-click copy/paste action, or the shortcut keys (Ctrl+C and Ctrl+V) to copy and paste files and folders directly to and from the secure partition.

Note: Data saved on the Defender V2's secure partition are only accessible after you have successfully logged into KDMV2.

2.5 On-board Antivirus (Windows Only)

You must register your device with Kanguru Solutions in order to take advantage of the Defender V2's on-board antivirus functions (see section 2.2.2 *Activating On-board Antivirus Protection (Windows Only)* on page 11).

Once your on-board antivirus has been activated, real-time virus scanning is automatically enabled whenever you log into your device.



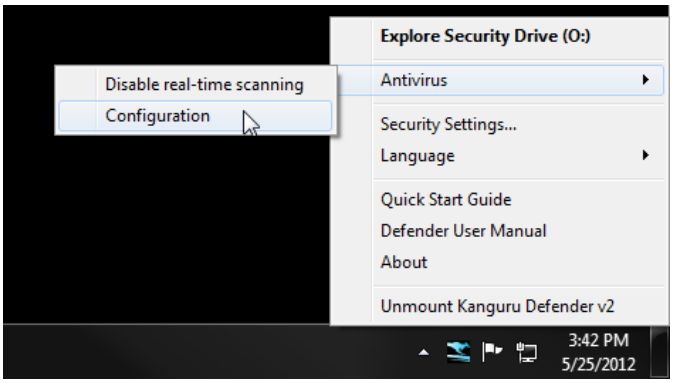
Note: Updates for the latest the virus definitions are downloaded automatically when the device is connected to a computer with internet access. If you disconnect your Defender V2 before the latest update has finished downloading, the Defender V2 will save your place and continue the download the next 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. **Do not delete the 'System' folder or save any data besides virus definitions to it.**

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. Click on the KDMV2 icon located in the taskbar.
2. Select **Antivirus** from the popup menu and then click on **Configuration** from the submenu.



The antivirus console appears.

2.5.1 Device Scan

The antivirus console allows you to scan your Defender V2 for known viruses and malware.

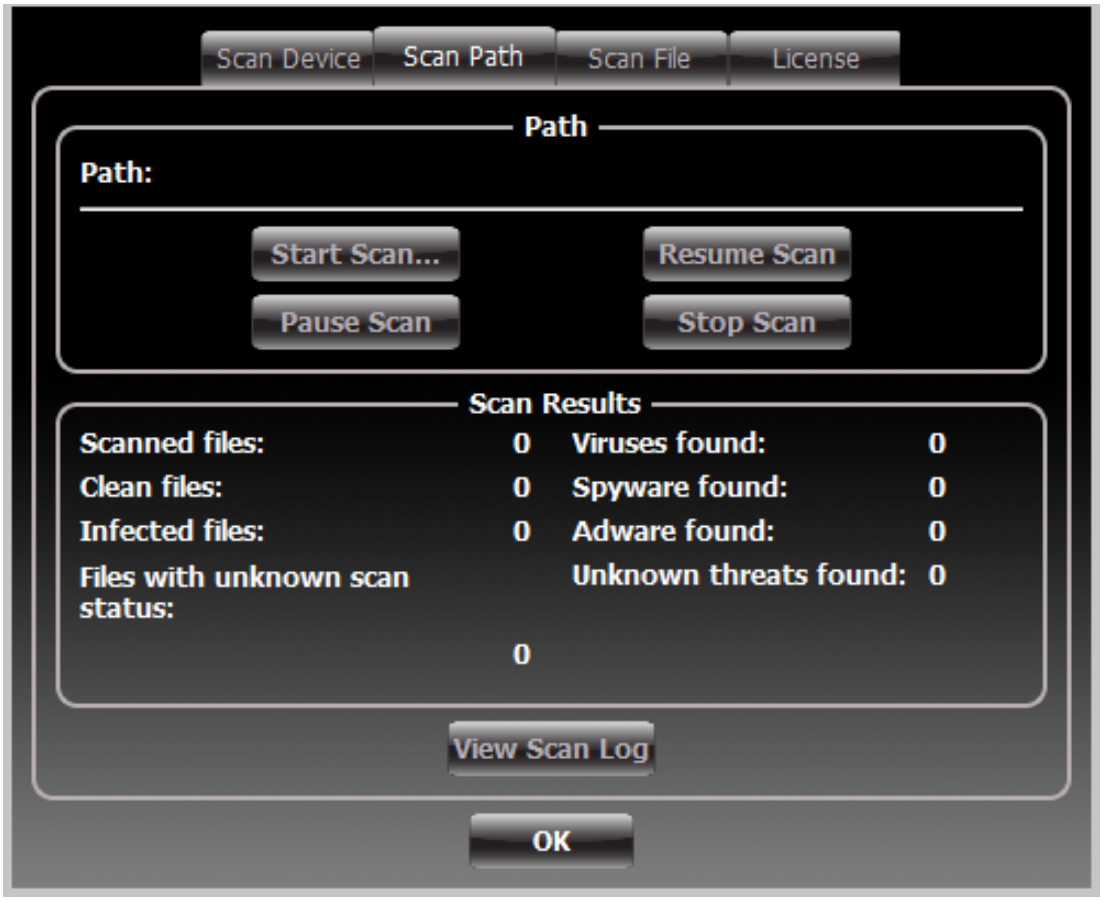
To scan your Defender V2:

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 V2.
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.

2.5.2 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.



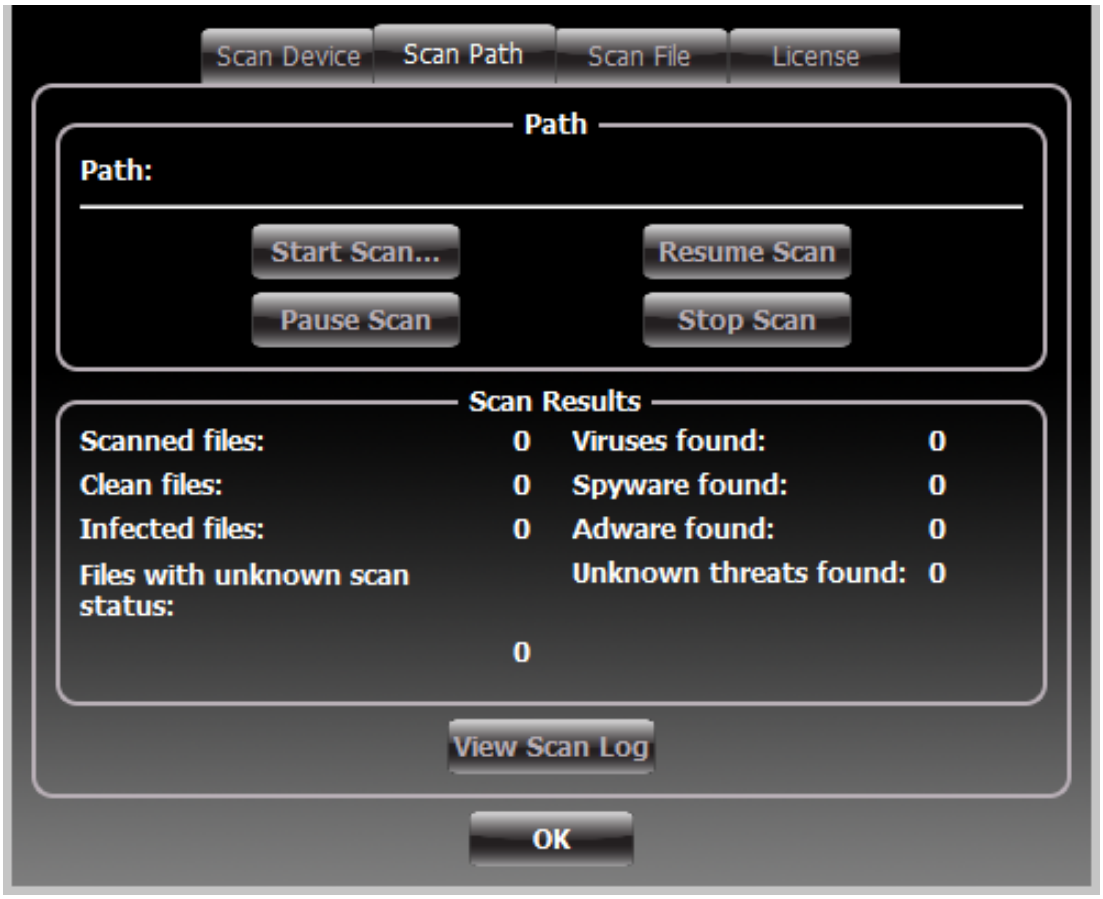
To scan a path on your computer:

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.

2.5.3 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.

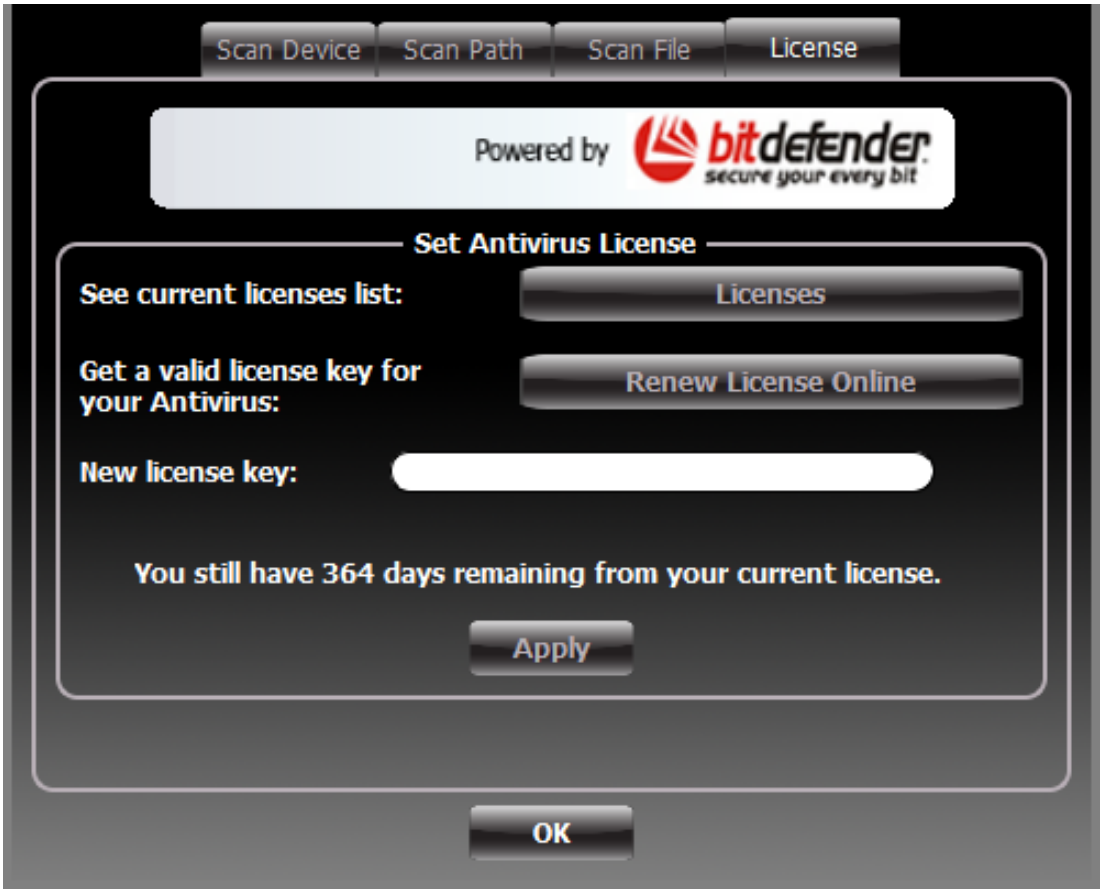


To scan a file:

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 **View Scan Log** button to view a log of the previous scan.
6. Click on the **OK** button to close the antivirus console.

2.5.4 License

The antivirus console allows you to manage your antivirus license.



To check your antivirus license:

1. Click on the **License** tab at the top of the antivirus console.
2. Click on the **Licenses** button to see your current antivirus license.

If you do not have a valid license key:

1. Click on the **Renew Licenses Online** button to obtain a valid license key for your antivirus (this option may not be available).
2. Enter your license key in the **New License Key** field.
3. Click on the **Apply** button to apply your license key.
4. Click on the **OK** button to close the antivirus console.

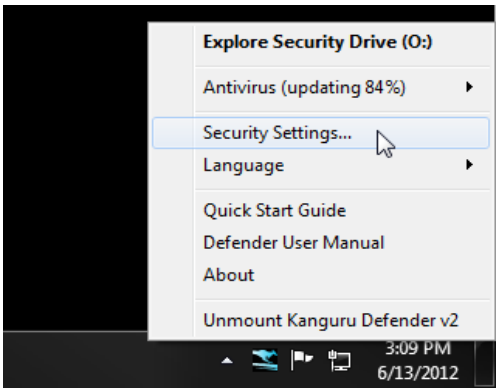
2.6 Changing Your Password

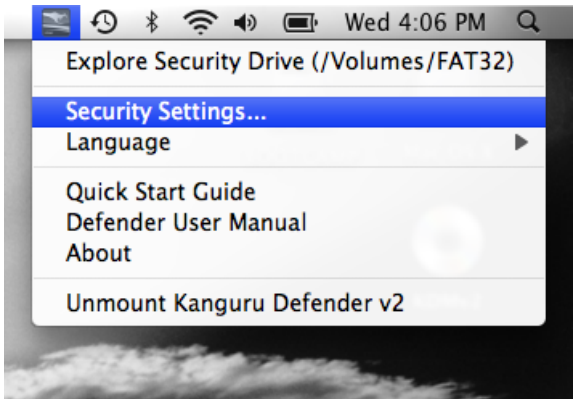
You can change your security password through Security Settings.

To change your password:

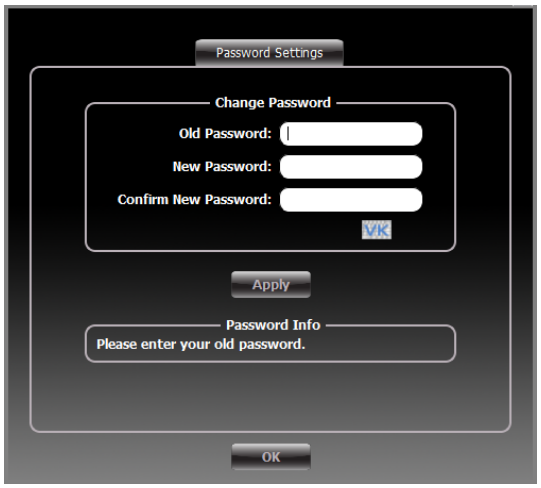
1. Login to KDMV2 to gain access to the secure partition.

2. Click on the KDMV2 icon located in the taskbar and then select **Security Settings…** from the popup menu.





3. 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.



4. When you are ready to proceed, click on the **Apply** button to set your new password.

5. 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 set your new password.

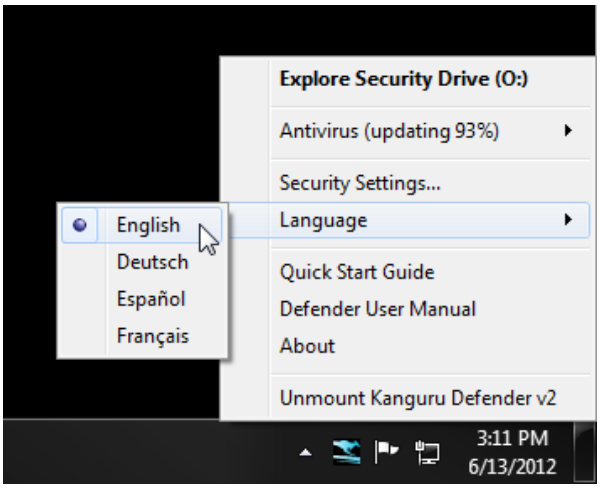
2.7 Changing Languages

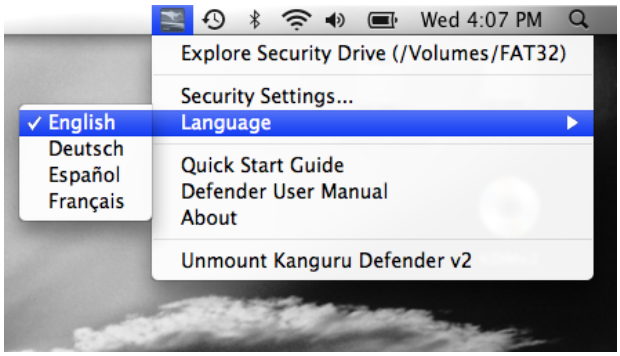
KDMV2 supports several languages. The KDMV2 language is set to English by default.

To change the language:

1. Login to KDMV2 to gain access to the secure partition.

2. Click on the KDMV2 icon located in the taskbar and then hover your cursor over the **Language** option in the popup menu. A list of available languages appears.





3. Click on the desired language from the submenu that you want KDMV2 to be displayed in.

2.8 Online Documentation

You can download digital copies of the Kanguru Defender V2's documentation from the internet.

To download your Defender V2's documentation:

1. Login to KDMV2 to gain access to the secure partition.

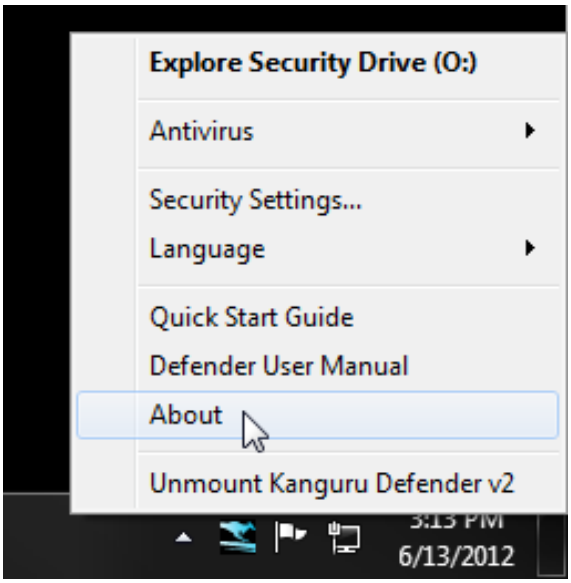
2. Click on the KDMV2 icon located in the taskbar
   - Click on **Quick Start Guide** to download a digital copy of the Defender's Quick Start Guide.
   - Click on **Defender User Manual** to download a digital copy of the Defender's User Manual

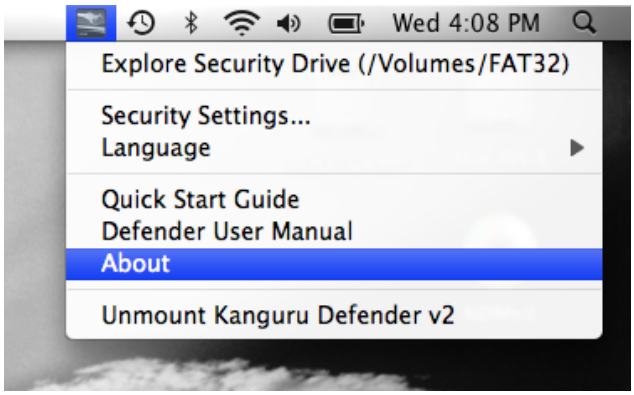
2.9 About KDMV2

To view information regarding the version of KDMV2 currently installed on your device:

1. Login to KDMV2 to gain access to the secure partition.

2. Click on the KDMV2 icon located in the taskbar and then select **About**.





A window appears showing the version of KDMV2 currently running. This information is particularly useful when calling in for technical support.

2.10 Unmounting Your Defender V2

When you unmount the Defender V2, the KDMV2 application will close and the secure partition containing your encrypted data will be inaccessible until you log into KDMV2 again.

Caution! Do not disconnect the Defender V2 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.

2.10.1 Safely Removing from Windows

To unmount your Defender Basic, click on the KDMV2 icon located in the taskbar and then select **Unmount Kanguru Defender V2.**

The KDMV2 icon in the taskbar will disappear and the secure partition will no longer be accessible from My Computer or Windows Explorer.

After the Defender V2 has been unmounted, use the Windows 'Safely Remove Hardware' function before removing your drive. To safely remove your Defender V2, click on the Safely Remove Hardware icon located in the taskbar. The icon may look different depending on your version of Windows.

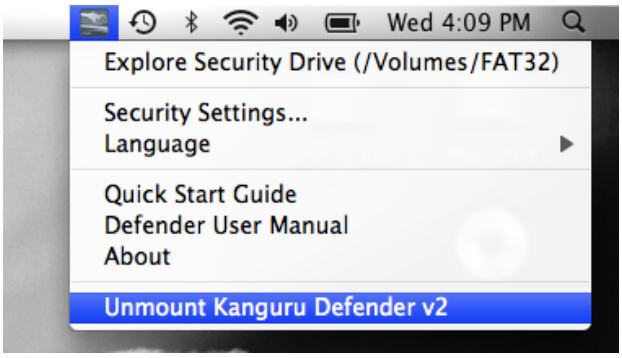
Windows XP / 2000

Windows Vista / 7

A popup menu appears listing all USB devices connected to your computer. Select the Defender V2 from the list (it will appear with two drive letters). A message will appear indicating that the portable storage device can be safely removed. If a message saying "The device cannot be stopped right now" appears, please make sure any windows or applications accessing the Defender V2 are closed and then try again.

2.10.2 Safely Removing from Mac OS X

To unmount your Defender Basic, click on the KDMV2 icon located in the status menu and then select **Unmount Kanguru Defender V2.**



The KDMV2 icon in the taskbar will disappear and the secure partition will no longer be accessible.

Once the Defender V2 has been unmounted, click and drag the KDMv2 icon from the desktop into the trash can icon. When you start dragging the KDMv2 icon, the trash can icon will change to an eject symbol.

Once the KDMv2 icon disappears from your desktop you can safely disconnect your Defender V2 from the USB port.

3. Warranty and Technical Support

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.

If you experience any problems using your Kanguru Defender V2 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

Kanguru Solutions
1360 Main Street
Millis, MA 02054
www.kanguru.com

06.13.12 v2.0 © 2012 Kanguru Solutions

Legal terms and conditions available at www.kanguru.com. Please review and agree before use. Thank you.