Secure. Anytime. Anywhere.

Kanguru Defender Elite200
User Manual

Model no: KDFE200

NOTICES AND INFORMATION

Please be aware of the following points before using your Kanguru Defender Elite200

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

The Kanguru Defender Elite200 is a hardware encrypted, tamper proof USB flash drive. The Defender Elite200 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 Elite200 flash drive secures your sensitive data using:

- 256-bit AES hardware encryption
- 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 Elite200 USB Flash Drive
- Quick Start Guide
- USB Extension Cable (32GB-128GB models only)

1.2 Kanguru Defender Elite200 Models

The Kanguru Defender Elite200 comes in two models, depending on your drive's capacity. Differences between the models are detailed in section 1.6 *Technical Specifications* on page 8.

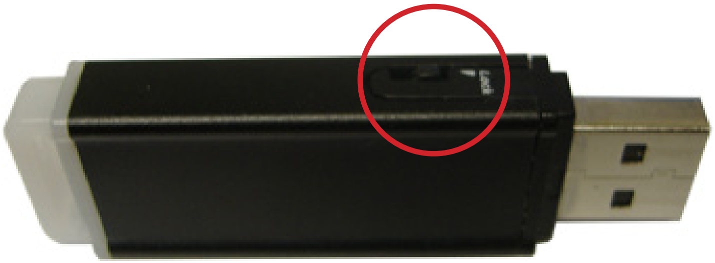
1GB - 16GB Model

32GB - 128GB Model

1.3 The Write Protect Switch

Note: The Defender Elite200's write protect switch was not considered for Common Criteria evaluation.

The Kanguru Defender Elite200 device features a physical write protect switch.



- **Unlocked -** Push the write protect switch towards the USB connector side of the device to set it in the unlocked position. When the write protect switch is set in the unlock position, the device will function normally.

- **Locked -** Push the write protect switch towards the LED side of the device to set it in the locked position. When set in the lock position, the write protect switch will prevent any data from being written to the device's secure partition.

Important! You may receive an error if you attempt to log in to your device while the write protect switch is set in the locked position. Please check and make sure that the write protect switch is set in the unlocked position when logging into the device. Once you have successfully logged in and mounted the device's secure partition, you can set the write protect switch to the locked position.

1.4 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 XP SP3, Windows Server 2003, Win Vista, Win 7, Win 8
  - ○ Max OS X 10.5 and above (compatible with Intel-based Macs only)
  - ○ Red Hat Enterprise Linux 5, Ubuntu 9/10, Linux Kernel 2.6.02 - 2.6.34
    Note: Linux Red Hat users must have Super User or Root privileges to run KDMElite200

1.5 Features

√ 256-bit AES hardware encryption
√ FIPS 140-2 (Level 2) Validated
√ Password protected data partition for your secure files
√ Does NOT require Admin privileges (except with Red Hat Enterprise Linux 5)
√ Driverless installation (Plug & Play)
√ High-strength aluminum housing
√ Tamper-proof design
√ Write protect switch
√ On-board antivirus protection
√ HIPAA Compliant
√ Sarbanes Oxley Compliant
√ GLB Compliant

Remote Management Capability

The Kanguru Defender Elite200 flash drive 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. With KRMC you will be able to:

√ Create and manage a master password for your Defender drives
√ Remotely delete all data on a managed 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

Your Kanguru Defender Elite200 does not come with KRMC enabled by default.
For more information about KRMC, visit: https://www.kanguru.com/index.php/flash-management

1.6 Technical Specifications

General Specifications

Interface	USB 2.0 (USB 1.1 compatible)
Encryption Features	Hardware based 256-bit AES encryption
OS Compatibility	Windows XP SP3*, Server 2003, Vista, 7, 8 Max OS X 10.5 and above (Intel based only) Red Hat Enterprise Linux 5, Ubuntu 9/10, Ubuntu 11, OpenSUSE11.1 Linux Kernel 2.6.02 - 2.6.34 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

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

1GB - 16GB Defender Elite200 Specifications

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 Elite200 Specifications

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 Elite200

Kanguru Defender Manager Elite200 (KDMElite200) is the client application pre-loaded on the Defender Elite200's CD-ROM partition. The user needs to login to KDMElite200 in order to access the secure, encrypted partition. KDMElite200 comes pre-installed on your Defender Elite200. No installation on your PC is necessary.

2.1 Identifying the Device Edition

Users can open the **version.ini** file located in the CD-ROM partition to verify whether the device is running a Cloud edition, Enterprise edition or No-Comms edition client.

Open the **version.ini** file in a text editor and check the line for "Product Version" and check whether the product version number ends in - 2, - 3 or - 6 suffix.

Version suffix	Edition	Description
-2	Cloud edition	The standard Defender model.
-3	Enterprise edition	Enterprise edition devices have been configured to be able to communicate with KRMC Enterprise.
-6	No-Comms edition	The No-Comms version is identical to the Cloud version but with all communication functionality disabled.

Some other general differences are identified below:

In KDM Cloud:

- Anti-Virus (AV) definitions are downloaded from Kanguru server. The list with the most current definitions is received from the Kanguru Central Server (KCS).
- Cannot be managed by KRMC Enterprise

In KDM Enterprise:

- AV definitions are downloaded from a KRMC enterprise server.
- Devices must be provisioned using UKLA - setting device properties and exporting them to a .krm file that is added in KRMC Enterprise.
- "Enterprise Edition" appears on the splash screen

In KDM No-Comms:

- There is no AV functionality.
- There is no communication to any network or internet server.
- All drive communications, including live updates for the KDM client software for the drive, are disabled.
- The drive operates in a completely offline mode, and cannot be managed by KRMC.

2.2 Running KDMElite200

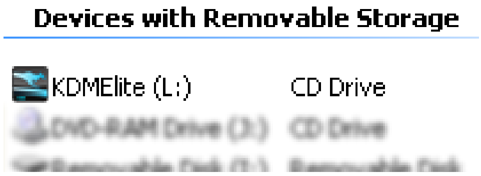
The Kanguru Defender Elite200 is compatible with multiple operating systems. Running the KDMElite200 application can be different depending on the OS your computer is running.

2.2.1 Running KDMElite200 on Windows

To run KDMElite200 from a Windows operating system, simply connect your Defender Elite200 to your computer through a USB port. The KDMElite200 application should start automatically if Autorun is enabled.

If KDMElite200 does not start automatically:

1. Open **My Computer** and open the Defender Elite200's CD-ROM partition named **KDMElite200**. The drive letter (e.g. D:, E:, F:) will depend on your computer.



Devices with Removable Storage

KDMElite (L:)	CD Drive
DVD-RAM Drive (J:)	CD Drive

2. Double-click on the **KDMElite200.exe** file to launch the KDMElite200 application.

If it is your first time running KDMElite200 you will need to complete the setup wizard in order to set your security password (see section 2.3 *The Setup Wizard* on page 15). If you have already setup your security password, you will be prompted to login (see section 2.4 *Unlocking the Security Partition* on page 21)

Caution! The **KDMElite200.exe** file needs to remain on your Defender Elite200's CD-ROM partition at all times. Always run the application from the Defender Elite200's CD-ROM partition. Do not try to copy KDMElite200 or run KDMElite200 from your computer's hard drive.

Note: Windows 7 users may not see the removable disk partition until you have logged into KDMElite200. If you are running Windows 7 and for any reason need to see the removable disk before you log into KDMElite200 please refer to the instructions on p.9.

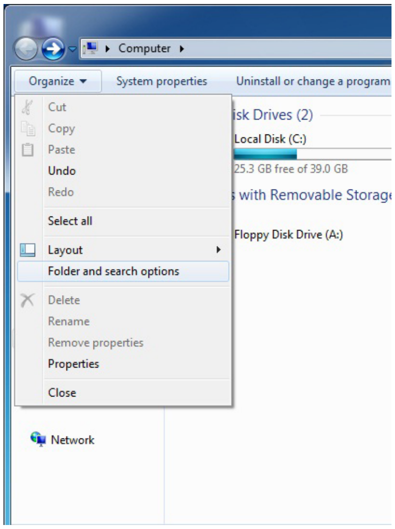
Attention Windows 7 Users

Windows 7 users may not see the removable disk partition until you have logged into KDMElite200 (see section 2.4 *Unlocking the Security Partition* on page 21 for more information). This is normal.

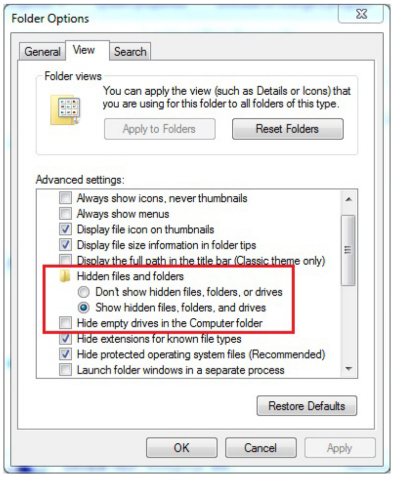
If you are running Windows 7 and for any reason need to see the removable disk before you log into KDMElite200, you will need to configure Windows in the following manner:

Note: This is user preference only. There is no need to configure Windows in order to use your device.

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



2. The Folder Options window appears. Scroll down to the option for Hidden Files and Folders and select **Show hidden files, folders, and drives**.



You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

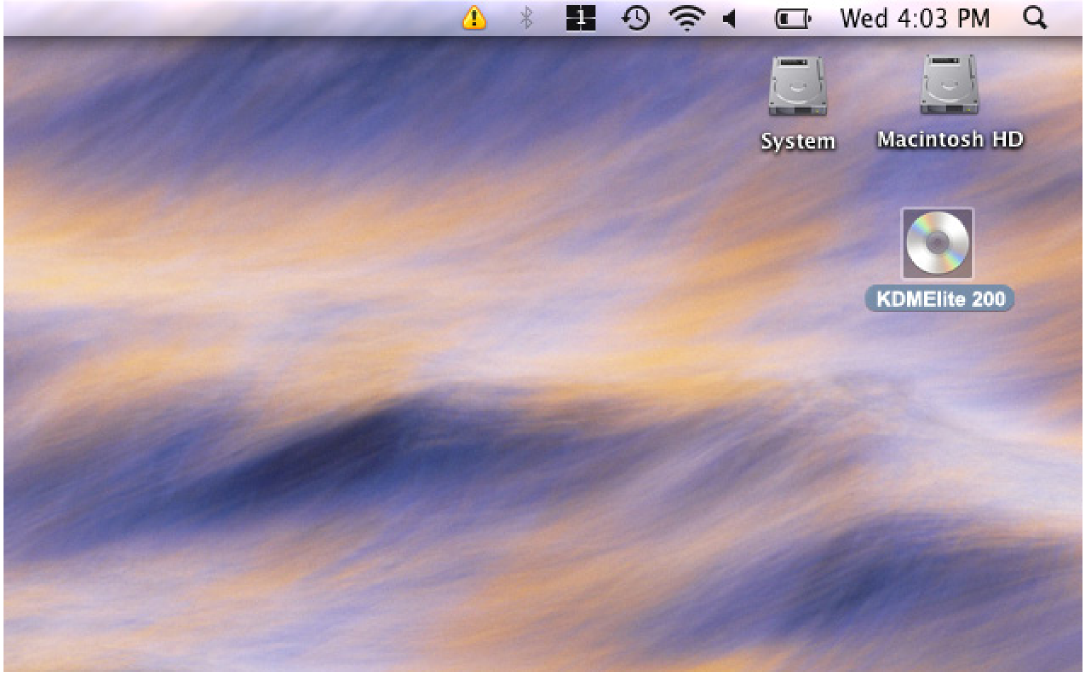
Advanced settings:

- ☐ Always show icons, never thumbnails
- ☐ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- ☐ Display the full path in the title bar (Classic theme only)
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☐ Hide empty drives in the Computer folder
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process

3. Click on the **OK** button to finish configuring Windows. The removable disk is now visible before you log into KDMElite200.

2.2.2 Running KDMElite200 on Mac OS X

To run KDMElite200 from Mac OS X, connect your Defender Elite200 to your computer through a USB port. A CD icon named 'KDMElite200' will appear on the desktop. Double click on the **KDMElite200** icon to open it.



In the window that opens, double-click on the **KDMElite200.app** file to launch the KDMElite200 application.

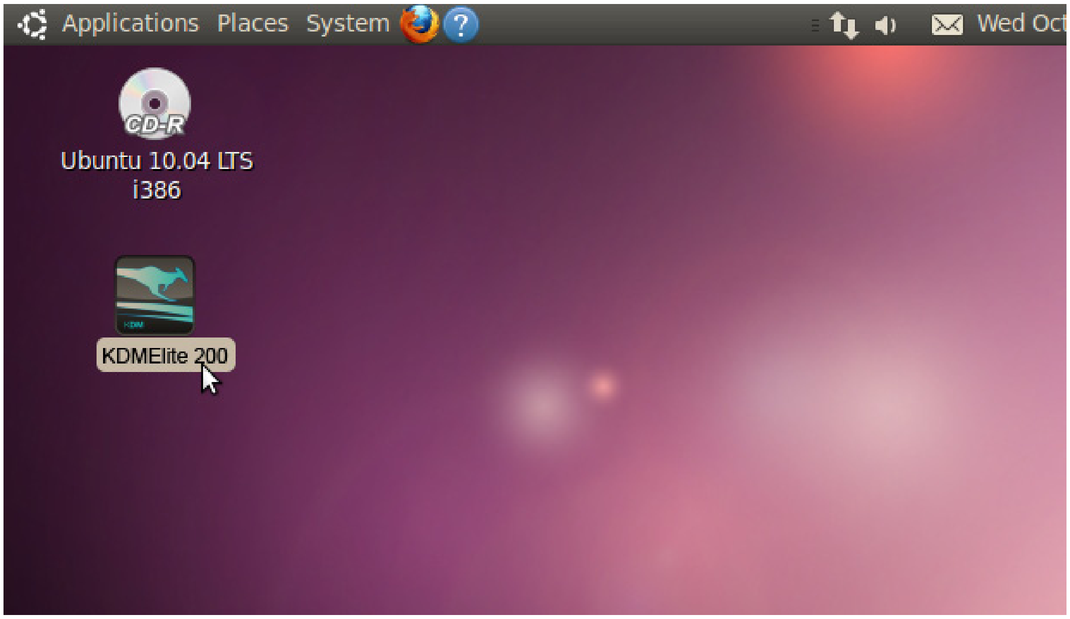
If it is your first time running KDMElite200 you will need to complete the setup wizard in order to set your security password (see section 2.3 *The Setup Wizard* on page 15). If you have already setup your security password, you will be prompted to login (see section 2.4 *Unlocking the Security Partition* on page 21).

Caution! The **KDMElite200.app** file needs to remain on your Defender Elite200's CD-ROM partition at all times. Always run the application from the Defender Elite200's CD-ROM partition. Do not try to copy KDMElite200 or run KDMElite200 from your computer's hard drive.

Note: The **KDElite200** icon is not always displayed on the desktop. If you do not see the **KDMElite200** icon on your desktop, you can locate the **KDMElite200.app** file on the CD-ROM partition through the Finder window.

2.2.3 Running KDMElite200 on Ubuntu Linux

To run KDMElite200 from a Ubuntu Linux operating system, connect your Defender Elite200 to your computer through a USB port. A ‘KDMElite200’ icon will appear on the desktop. Double click on the **KDMElite200** icon to open it.



In the window that opens, double-click on the **KDMElite200** file to launch the KDMElite200 application.

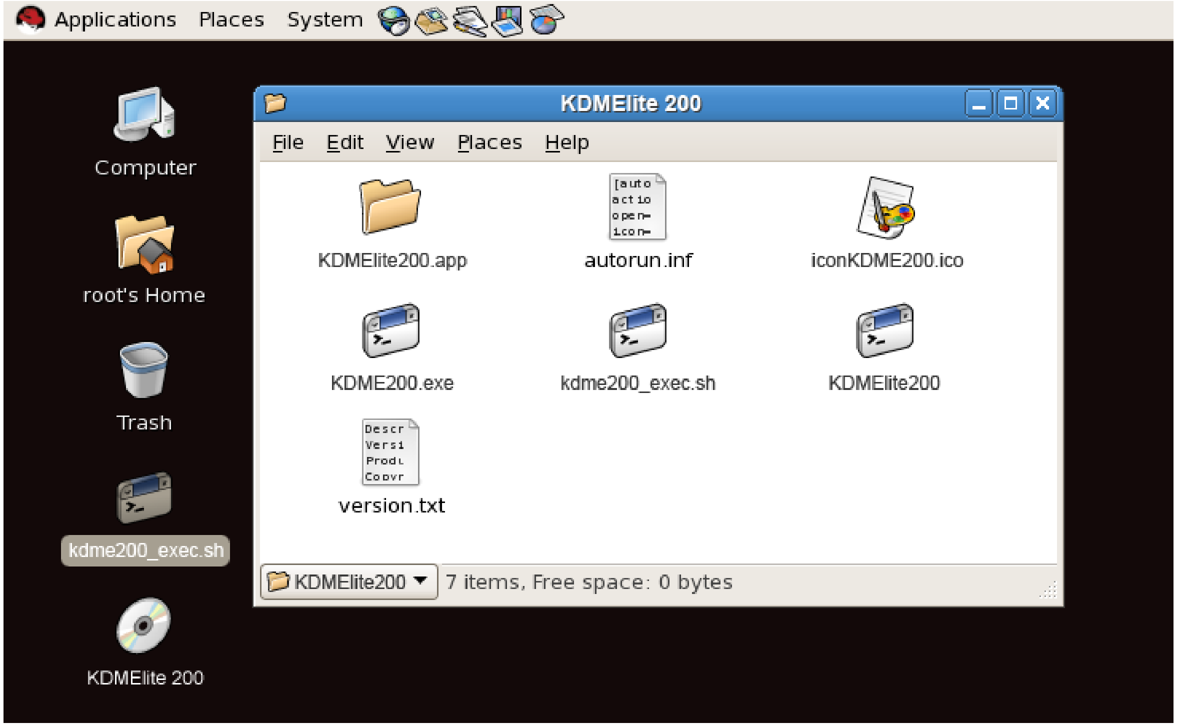
If it is your first time running KDMElite200 you will need to complete the setup wizard in order to set your security password (see section 2.3 *The Setup Wizard* on page 15). If you have already setup your security password, you will be prompted to login (see section 2.4 *Unlocking the Security Partition* on page 21).

Caution! The **KDMElite200** file needs to remain on your Defender Elite200’s CD-ROM partition at all times. Always run the application from the Defender Elite200’s CD-ROM partition. Do not try to copy KDMElite200 or run KDMElite200 from your computer’s hard drive.

2.2.4 Running KDMElite200 on Red Hat Enterprise Linux 5

Note: You must have Super User or Root privileges in order to run KDMElite200 on Red Hat Enterprise Linux 5.

To run KDMElite200 from the Red Hat Enterprise Linux 5 operating system, connect your Defender Elite200 to your computer through a USB port. A CD icon named 'KDMElite200' will appear on the desktop. If the KDMElite200 window doesn't open automatically, double click on the **KDMElite200** icon to open it.



From the window that opens, copy the **kdme200_exec.sh** shell script file to a location on your computer's local hard drive.

Once the **kdme200_exec.sh** shell script has been copied to a local hard drive, you can execute KDMElite200 through the Terminal:

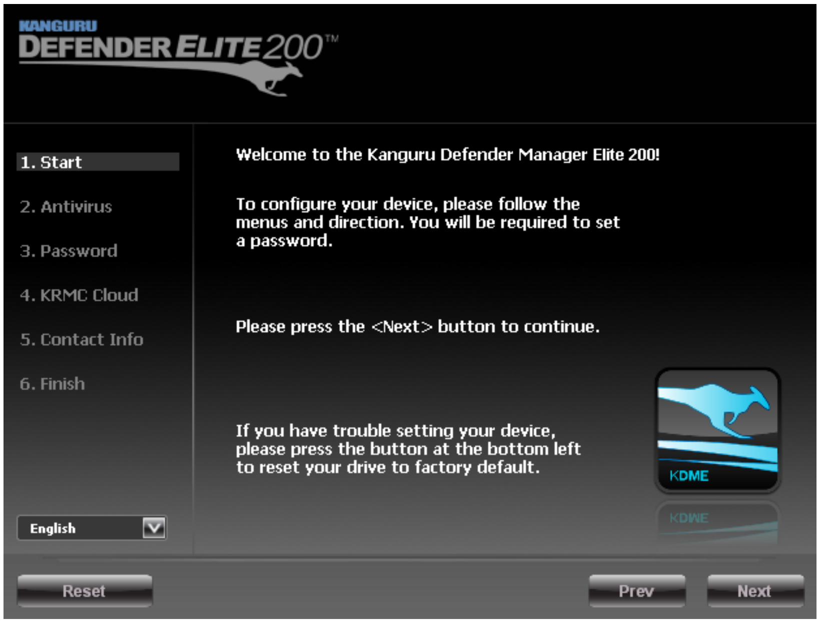
1. Open the Terminal window by clicking on **Applications** → **Accessories** → **Terminal**. The Terminal location may be different depending on which version of Red Hat you are running.
2. From the Terminal, navigate to the directory where you copied the **kdme200_exec.sh** shell script file to.
3. Type, "chmod 007 kdme200_exec.sh" to allow full execute permission.
4. Type, "./kdme200_exec.sh" to execute the shell script.

If it is your first time running KDMElite200 you will need to complete the setup wizard in order to set your security password (see section 2.3 *The Setup Wizard* on page 15). If you have already setup your security password, you will be prompted to login (see section 2.4 *Unlocking the Security Partition* on page 21).

2.3 The Setup Wizard

When you start KDMElite200 for the first time you will be greeted by the Setup Wizard. Follow the Setup Wizard instructions to create a password for your Defender Elite200's secure, encrypted partition.

Note: Before you can setup your Defender Elite200's password, the manual write-protect switch must be set to the unlock position.



Welcome to the Kanguru Defender Manager Elite 200!

To configure your device, please follow the menus and direction. You will be required to set a password.

Please press the <Next> button to continue.

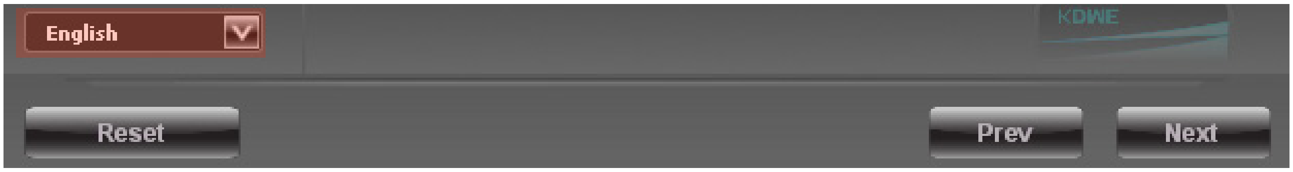
If you have trouble setting your device, please press the button at the bottom left to reset your drive to factory default.

Caution! Once the Setup Wizard has started, you should not disconnect your Defender Elite200 without either first completing the Setup Wizard or closing the Setup Wizard.

2.3.1 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 Welcome screen, click on the ☑ icon next to the Language Menu.



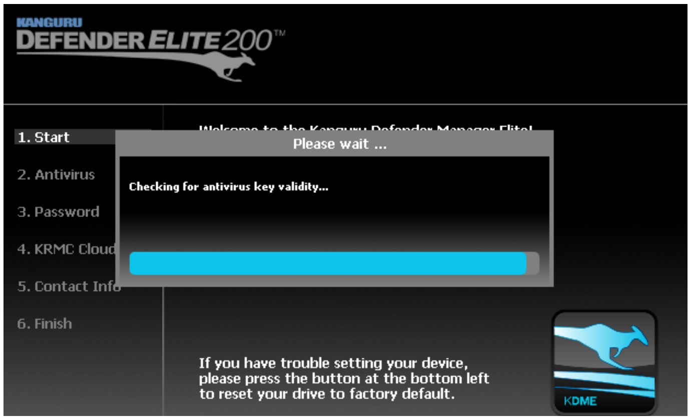
2. A list of available languages will appear in a drop down menu. Select your desired language from the drop down menu. The Setup Wizard will switch to the new language.

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

2.3.2 Activating On-board Antivirus Protection (Windows only)

Note: This section does not apply if you are running the Setup Wizard in Linux or Mac OS X.
Note: This section does not apply to Enterprise Edition devices. Antivirus for Enterprise Edition is activated by an administrator using Kanguru Remote Management Console (KRMC).
Note: This section does not apply to No-Comms Edition devices.

KDMElite200 will automatically check if your device has a valid antivirus license key.
Note: Your Defender Elite200 will need to be connected to a computer with internet access in order to register for on-board antivirus protection.



Welcome to the Kanguru Defender Manager Elite!

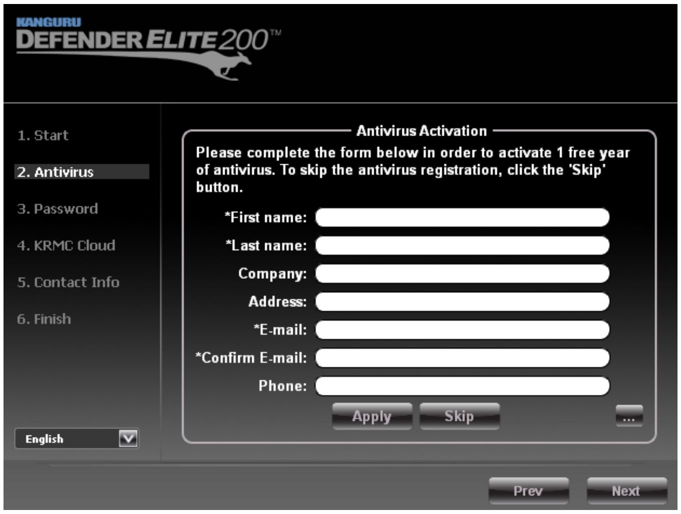
Please wait ...

Checking for antivirus key validity...

If you have trouble setting your device, please press the button at the bottom left to reset your drive to factory default.

If your Defender Elite200 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. 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.



Antivirus Activation

Please complete the form below in order to activate 1 free year of antivirus. To skip the antivirus registration, click the 'Skip' button.

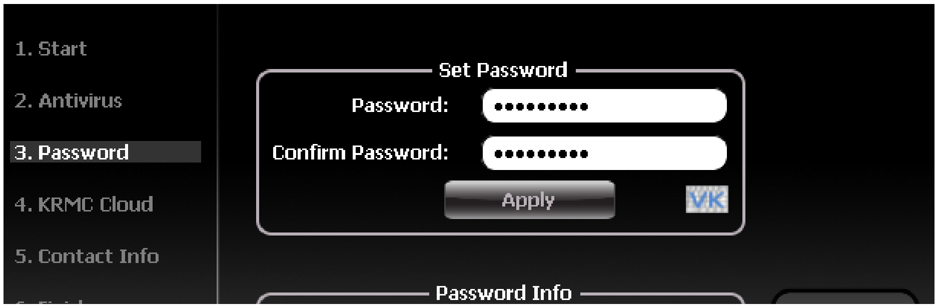
*First name:
*Last name:
Company:
Address:
*E-mail:
*Confirm E-mail:
Phone:

Click on the **Next** button to continue with setting up your Defender Elite200's security password.

2.3.3 Setting a Password

Note: Before you can set password, the manual write protect switch must be set to the unlock position (see section 1.3 *The Write Protect Switch* on page 6).

From the Set Password screen:



Password: •••••••••

Confirm Password: •••••••••

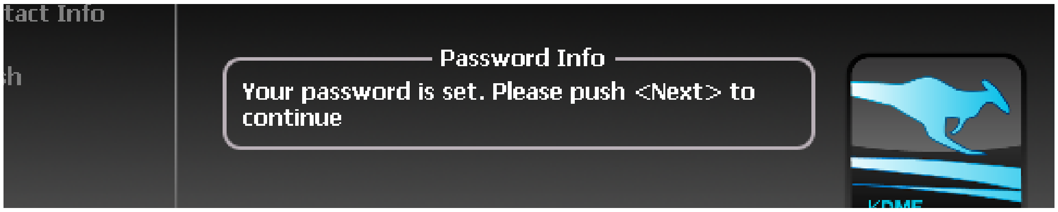
1. Enter your password in the **Password** data field. You can enter your password using KDMElite200's Virtual Keyboard by clicking the **VK** button. For more information on using the Virtual Keyboard see section 2.5 *Using the Virtual Keyboard to Enter Your Password* on page 23.

   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 you will see the following message in the Password Info box:



Your password is set. Please push <Next> to continue

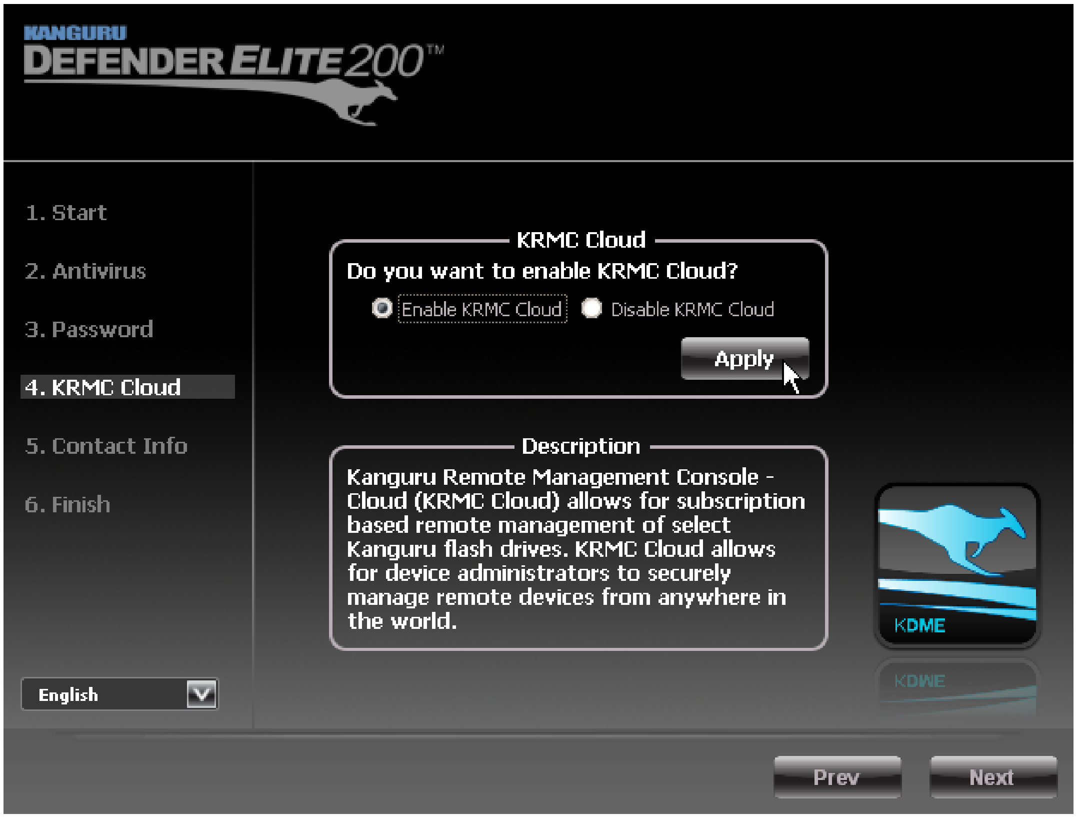
4. Click the **Next** button and KDMElite200 will automatically configure the security parameters.

Note: If you are managing your Defender Elite200 with an administrative program like KLA or KRMC, you can set a Master Password which can be used to reset the user password if it is lost or forgotten.

2.3.4 KRMC Cloud

Note: This section does not apply to Enterprise Edition devices
Note: This section does not apply to No-Comms edition devices
Note: KRMC Cloud has not been evaluated for Common Criteria.

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



KRMC Cloud

Do you want to enable KRMC Cloud?

● Enable KRMC Cloud ○ Disable KRMC Cloud

Apply

Description

Kanguru Remote Management Console - Cloud (KRMC Cloud) allows for subscription based remote management of select Kanguru flash drives. KRMC Cloud allows for device administrators to securely manage remote devices from anywhere in the world.

To Enable KRMC Cloud functionality:

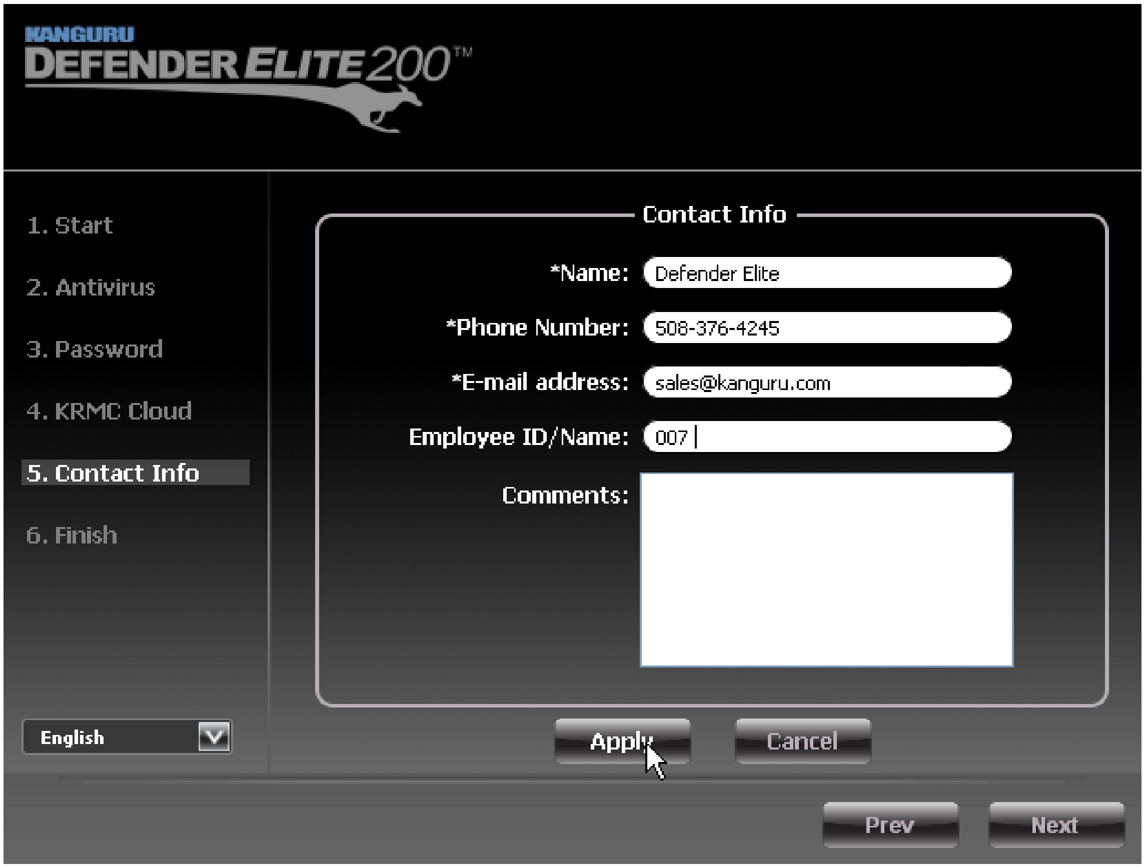
1. Select the **Enable KRMC Cloud** option and then click on the **Apply** button.
2. A dialog box will appear asking if you want to register your device with KRMC Cloud. Click on the **Yes** button.
3. Your web browser will open and direct you to the KRMC Cloud login page.
4. Purchase a license for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

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

2.3.5 Contact Info

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



*Name: Defender Elite
*Phone Number: 508-376-4245
*E-mail address: sales@kanguru.com
Employee ID/Name: 007
Comments:

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.

Congratulations! Your Defender Elite200 is now ready to use.

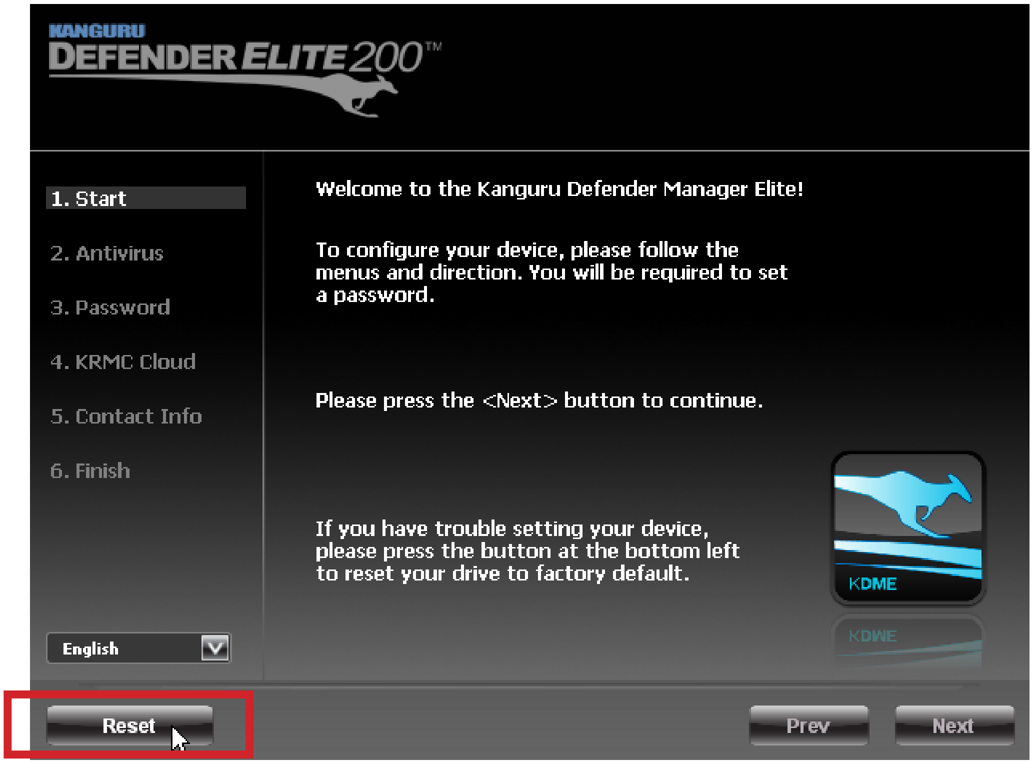
2.3.6 Resetting the Device through the Setup Wizard

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

To perform a device reset while in the Setup Wizard:

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

2. On the Welcome Screen you will see a **Reset** button in the lower-left side of the application window. Click on the **Reset** button.



Welcome to the Kanguru Defender Manager Elite!

To configure your device, please follow the menus and direction. You will be required to set a password.

Please press the <Next> button to continue.

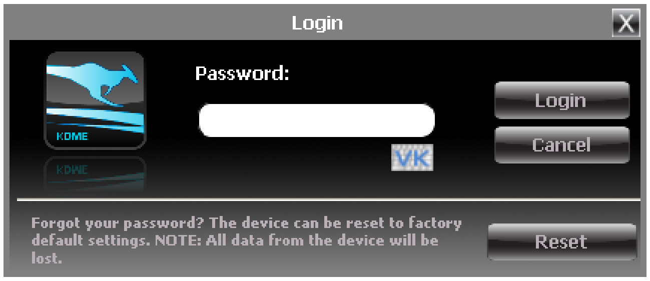
If you have trouble setting your device, please press the button at the bottom left to reset your drive to factory default.

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 be required to restart the Setup Wizard.

2.4 Unlocking the Security Partition

Anytime you run KDMElite200, you will be asked to login using your security password. You need to provide the correct security password in order to access the Defender Elite200's secure partition.



Forgot your password? The device can be reset to factory default settings. NOTE: All data from the device will be lost.

When the login screen appears:

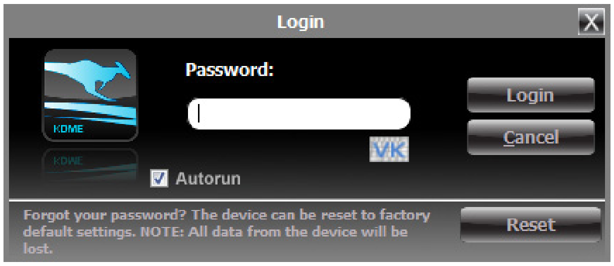
1. Enter your password in the **Password** field.
2. Click on the **Login** button.

Caution! If you enter your password incorrectly six times in a row (six is the default setting, 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 Elite200 or manually running KDMElite200.exe will bring the login window back.

Once you have successfully logged in to KDMElite200, the Defender Elite200's secure partition will be accessible through My Computer or Windows Explorer. For more information on accessing the secure partition, see section 2.6 *Encrypting Files and Folders* on page 24.

Caution! Once KDMElite200 has started, you should never disconnect your device without first closing KDMElite200 properly by clicking the KDMElite200 task bar icon and selecting **Unmount Kanguru Defender** as described in section 2.13 *Unmounting Your Defender Elite200* on page 33.

Note: If your Defender 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.



☑ Autorun

Forgot your password? The device can be reset to factory default settings. NOTE: All data from the device will be lost.

2.4.1 Resetting from the Login Screen

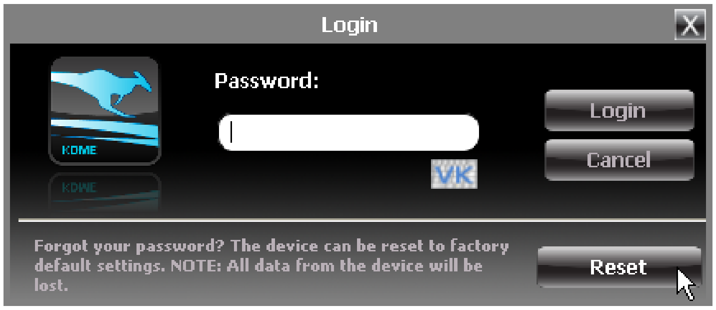
In the event you have forgotten your password, you can use the Reset to Factory Default function to reset your password. This function will restore the device to the factory settings, erasing all saved passwords and data residing on the device's secure partition.

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

To reset your Defender Elite200 to the factory default:

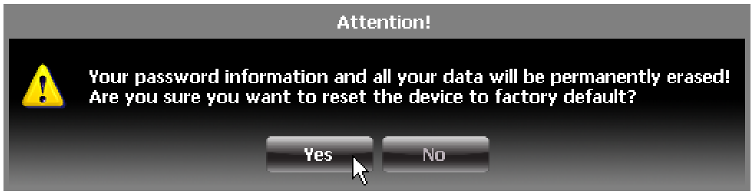
1. Start KDMElite200.

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



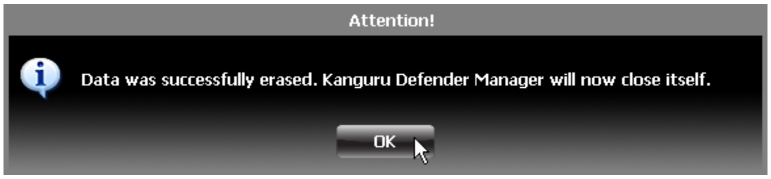
Forgot your password? The device can be reset to factory default settings. NOTE: All data from the device will be lost.

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



Your password information and all your data will be permanently erased! Are you sure you want to reset the device to factory default?

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.



Data was successfully erased. Kanguru Defender Manager will now close itself.

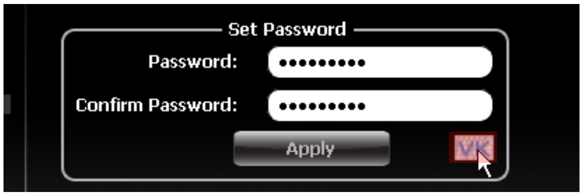
The next time you run KDMElite200, you will have to complete the Setup Wizard again before you are able to access the secure partition. Please see section 2.3 *The Setup Wizard* on page 15 for instructions on completing the Setup Wizard.

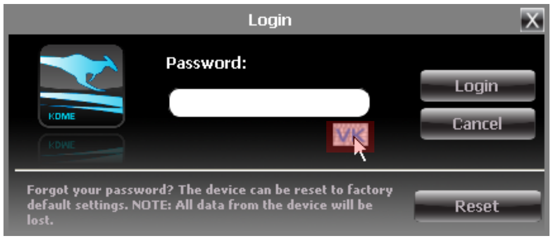
2.5 Using the Virtual Keyboard to Enter Your Password

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.

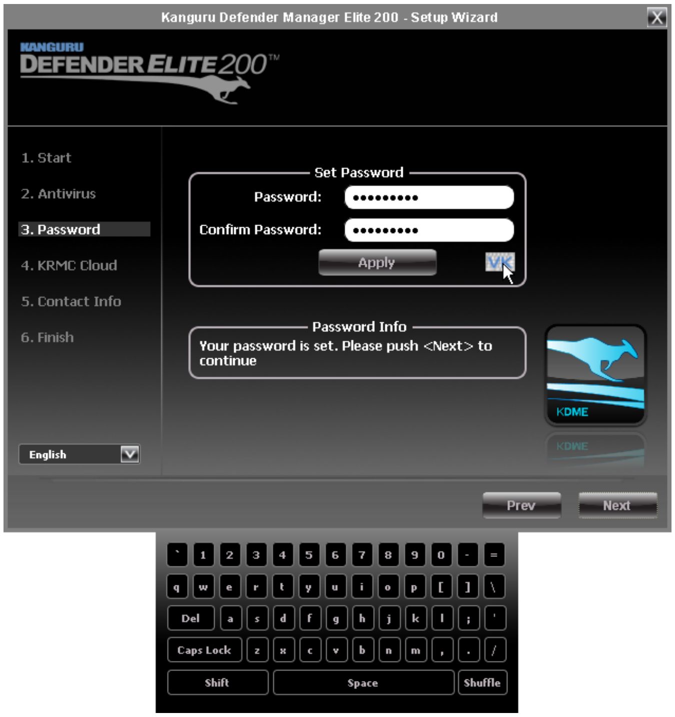
To use the virtual keyboard to enter your password:

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


Set Password
Password: •••••••••
Confirm Password: •••••••••

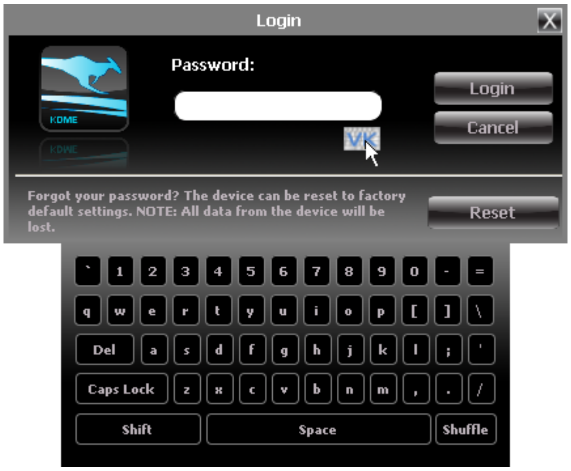

Login
Password:
Forgot your password? The device can be reset to factory default settings. NOTE: All data from the device will be lost.

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


Kanguru Defender Manager Elite 200 - Setup Wizard

Set Password
Password: •••••••••
Confirm Password: •••••••••

Password Info
Your password is set. Please push <Next> to continue
` 1 2 3 4 5 6 7 8 9 0 - =
q w e r t y u i o p [ ] \
Del a s d f g h j k l ; '
Caps Lock z x c v b n m , . /
Shift Space Shuffle


Login
Password:
Forgot your password? The device can be reset to factory default settings. NOTE: All data from the device will be lost.
KDME
Login
Cancel
VK
Reset
` 1 2 3 4 5 6 7 8 9 0 - =
q w e r t y u i o p [ ] \
Del a s d f g h j k l ; '
Caps Lock z x c v b n m , . /
Shift Space Shuffle

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 layout. Randomizing the keyboard layout protects your password from mouse tracking programs designed to thwart virtual keyboards.

2.6 Encrypting Files and Folders

A key feature of the Defender Elite200 is drag & drop encryption; allowing you to simply drag files that you want to encrypt directly onto the drive. The Defender Elite200 automatically encrypts these files as they are transferred to the secure partition, ensuring that your data stays safe and private.

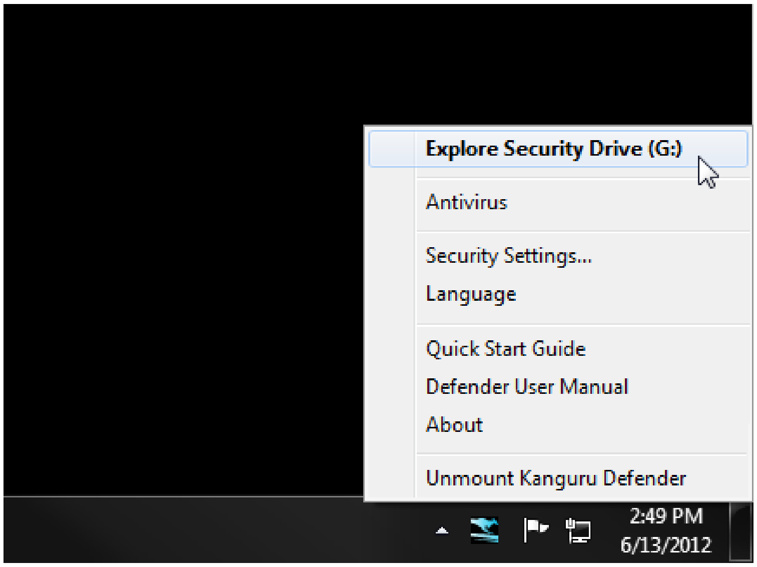
To open the secure partition:

1. Start KDMElite200.

2. Login to KDMElite200 to gain access to the secure partition.

3. Click on the KDMElite200 icon located in the task bar and then select **Explore Security Drive** from the popup menu.

Note: Linux users must right-click on the KDMElite200 icon in the task bar.



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 Elite200's secure partition are only accessible after you have successfully logged into KDMElite200.

2.7 On-board Antivirus (Windows only)

Note: This section does not apply to No-Comms edition devices

You must register your device with Kanguru Solutions in order to take advantage of the Defender Elite200's on-board antivirus functions (see section 2.3.2 *Activating On-board Antivirus Protection (Windows only)* on page 16).

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 Elite200 are scanned for viruses and malware.

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 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.

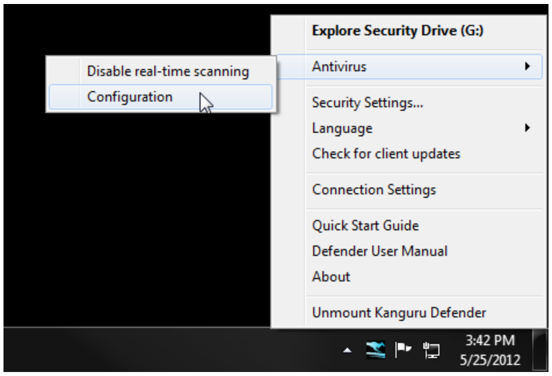
Virus definitions are stored in the 'System' folder on the secure partition. If these files are deleted, they will be automatically re-downloaded. If the device is reset to the factory default, these files will be deleted and will need to be re-downloaded.

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:

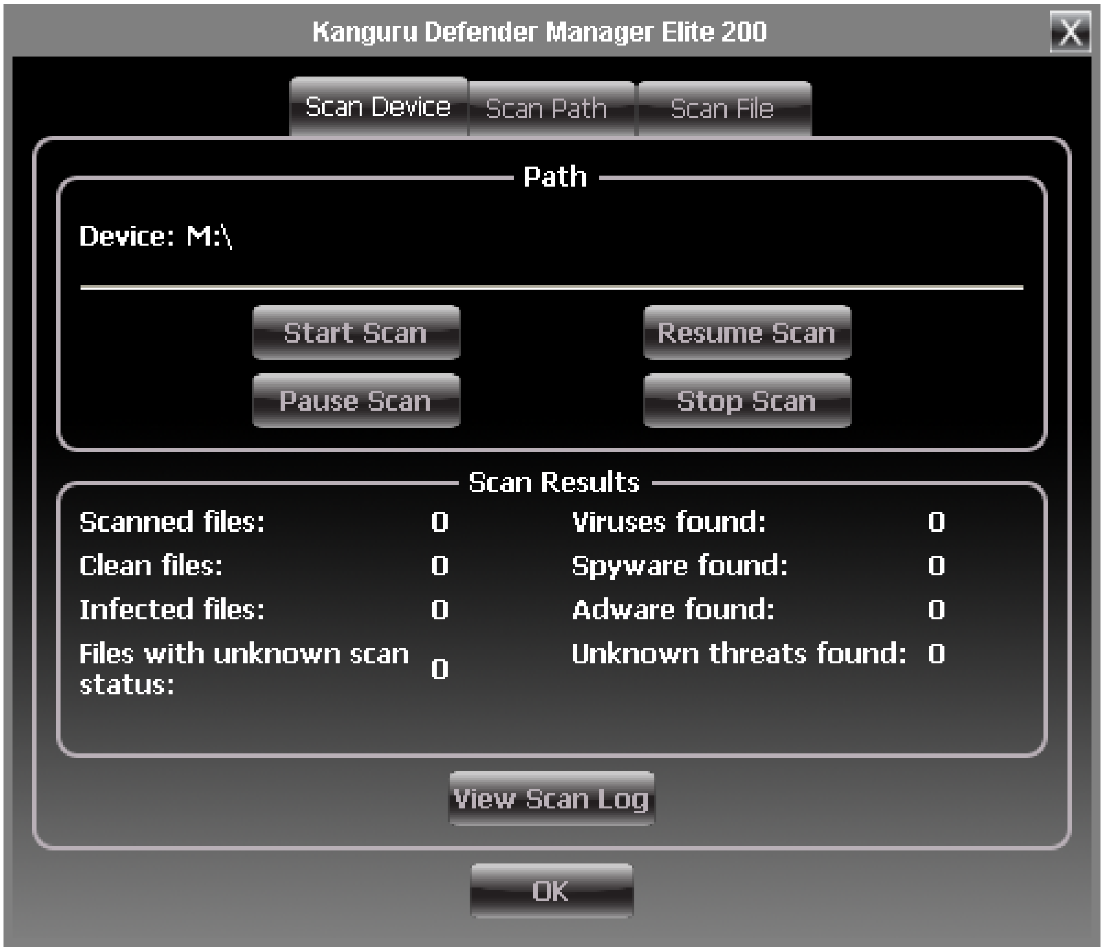
1. Right-click on the KDMElite200 icon located in the task bar.
2. Select **Antivirus** from the popup menu and then click on **Configuration** from the submenu.



The antivirus console appears.

2.7.1 Device Scan

The antivirus console allows you to scan your Defender Elite200 for known viruses and malware.



Device: M:\

Scanned files:	0	Viruses found:	0
Clean files:	0	Spyware found:	0
Infected files:	0	Adware found:	0
Files with unknown scan status:	0	Unknown threats found:	0

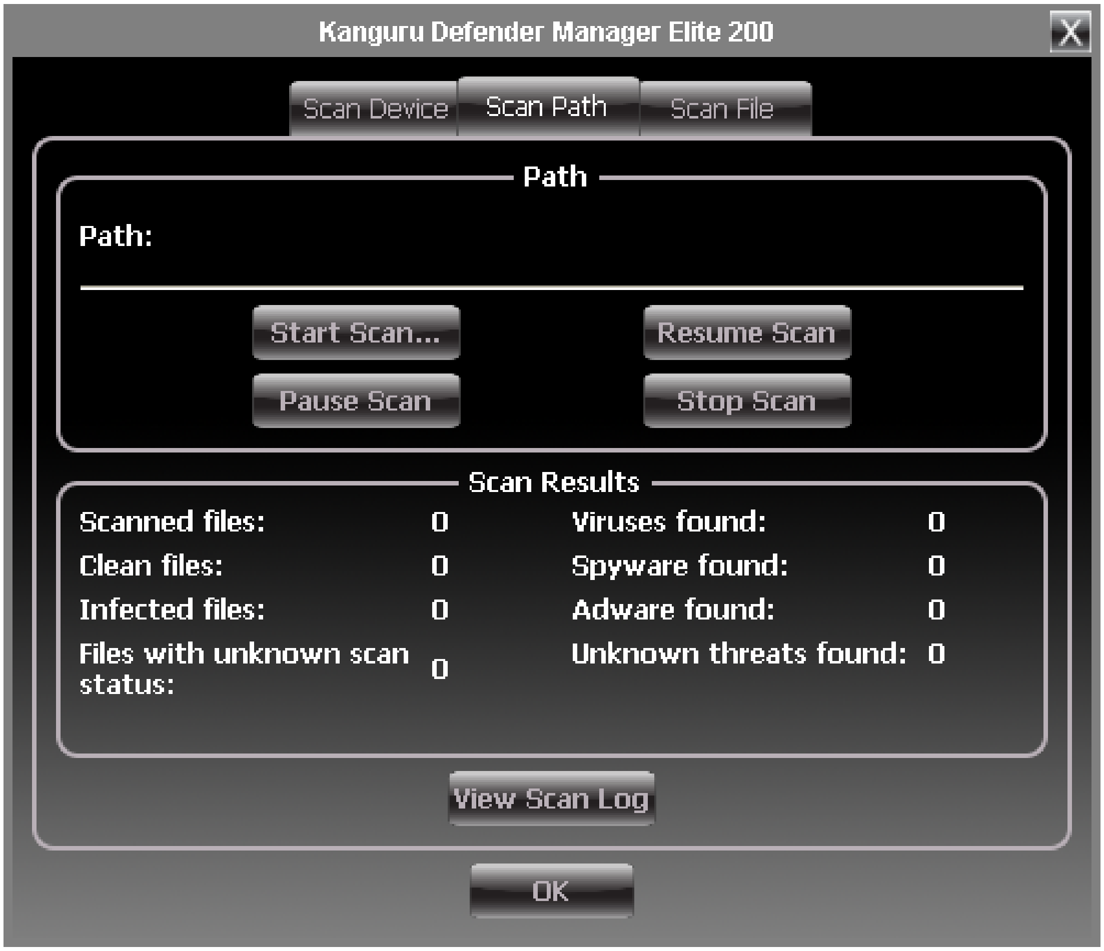
To scan your Defender Elite200:

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 Elite200.
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.

2.7.2 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.



Path:

Scanned files:	0	Viruses found:	0
Clean files:	0	Spyware found:	0
Infected files:	0	Adware found:	0
Files with unknown scan status:	0	Unknown threats found:	0

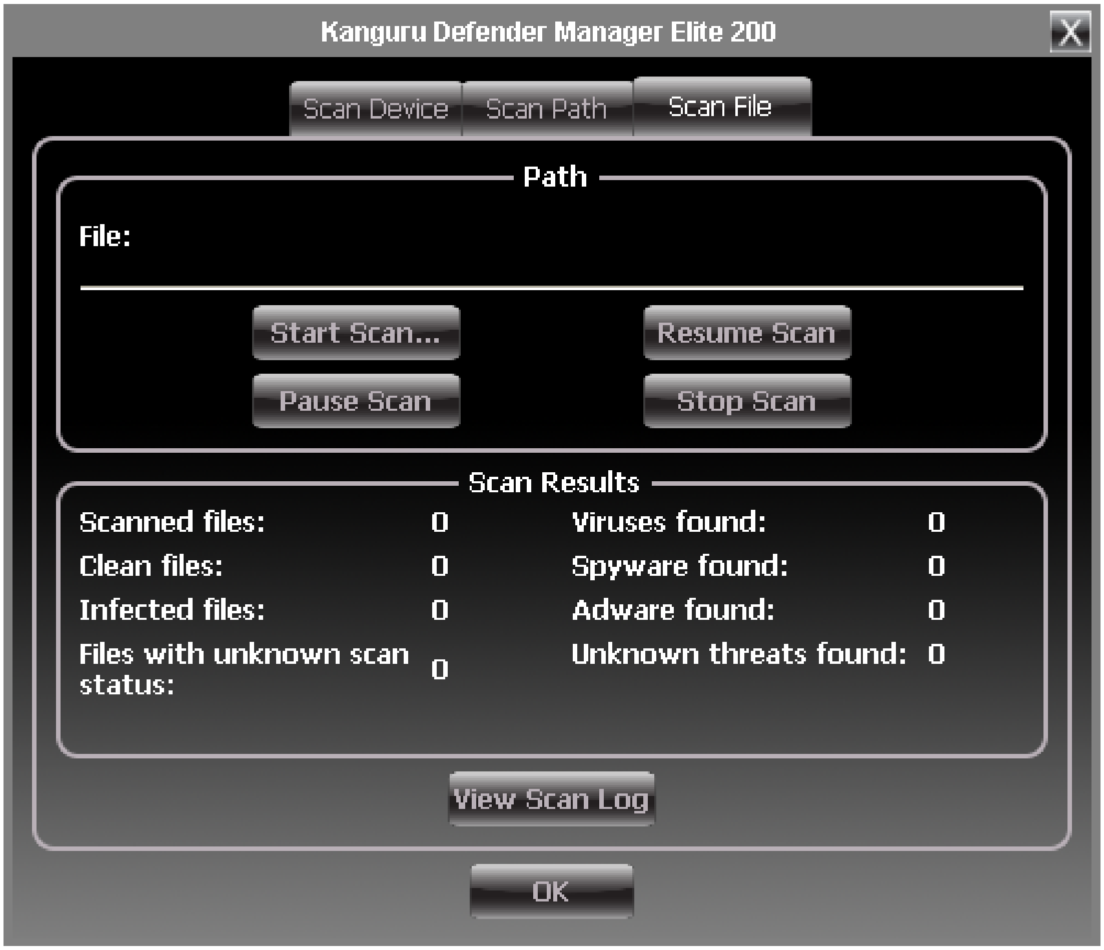
To scan a path on your computer:

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.

2.7.3 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.



File:

Scanned files:	0	Viruses found:	0
Clean files:	0	Spyware found:	0
Infected files:	0	Adware found:	0
Files with unknown scan status:	0	Unknown threats found:	0

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.

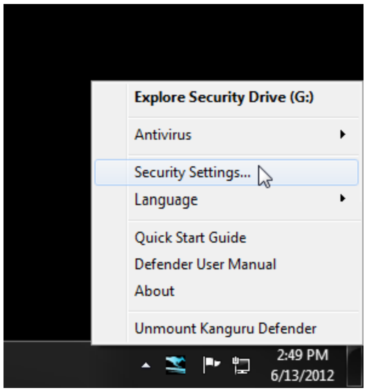
2.8 Changing Your Password

You can change your security password through the Security Settings.

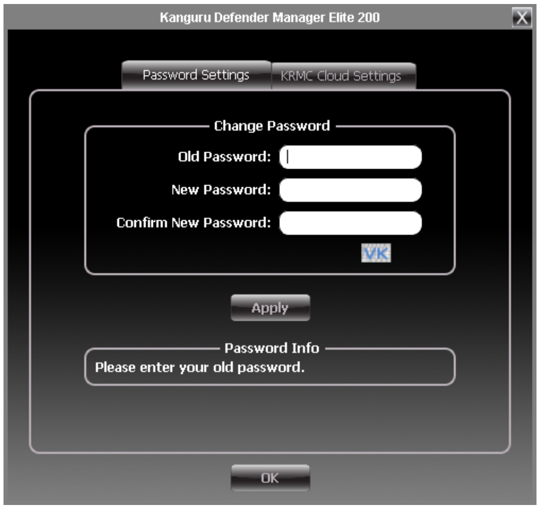
To change your password:

1. Click on the KDMElite200 icon located in the task bar and then select **Security Settings…** from the popup menu.

Note: Linux users must right-click on the KDMElite200 icon in the task bar.



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.



Please enter your old password.

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 complete setting your new password.

2.9 KRMC Cloud Settings

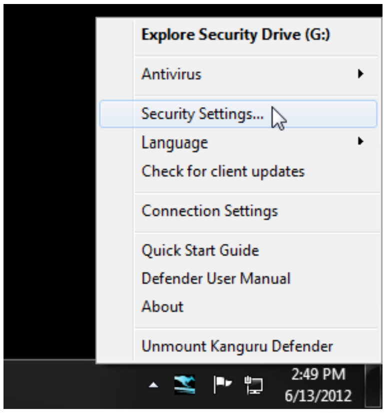
Note: This section does not apply to Enterprise Edition users.
Note: This section does not apply to No-Comms edition devices
Note: KRMC Cloud has not been evaluated for Common Criteria.

You can enable or disable KRMC Cloud functionality through the Security Settings.

To change your device's KRMC functionality:

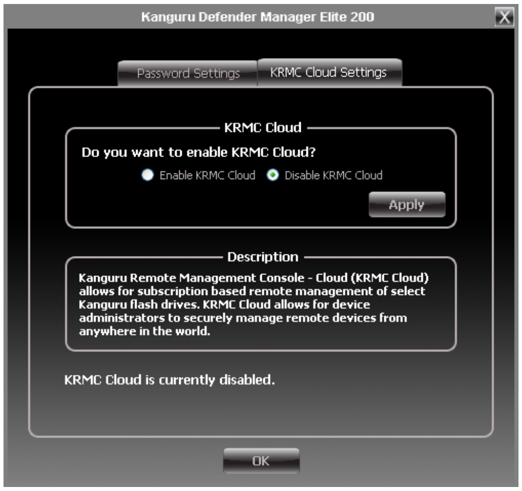
1. Click on the KDMElite200 icon located in the task bar and then select **Security Settings…** from the popup menu.

Note: Linux users must right-click on the KDMElite200 icon in the task bar.



2. The Password Settings window opens. Click on the KRMC Cloud Settings tab at the top of the window to enter the KRMC Cloud Settings window.

3. Enable or Disable KRMC Cloud by selecting the appropriate radio button and then click on the **Apply** button.



Do you want to enable KRMC Cloud?

○ Enable KRMC Cloud ● Disable KRMC Cloud

Kanguru Remote Management Console - Cloud (KRMC Cloud) allows for subscription based remote management of select Kanguru flash drives. KRMC Cloud allows for device administrators to securely manage remote devices from anywhere in the world.

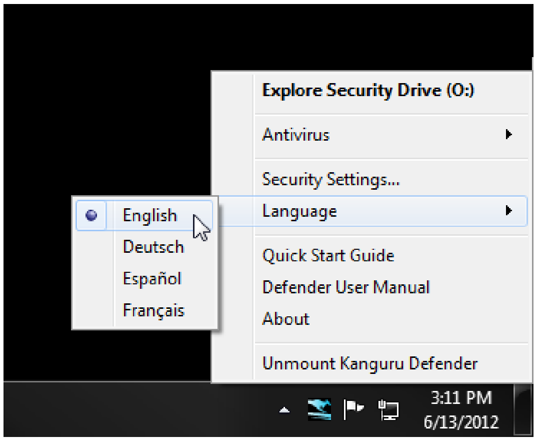
KRMC Cloud is currently disabled.

2.10 Changing Languages

KDMElite200 supports several languages. The KDMElite200 language is set to English by default.

To change the language:

1. Right -click on the KDMElite200 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. Click on the desired language from the submenu that you want KDMElite200 to be displayed in.

2.11 Online Documentation

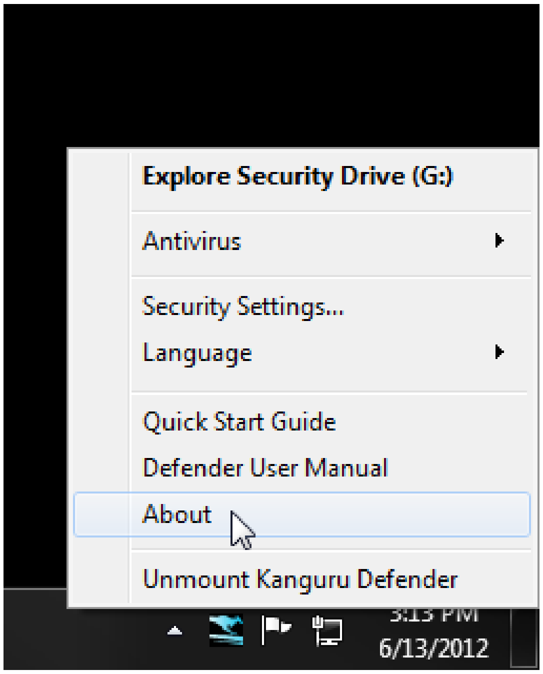
You can download digital copies of the Kanguru Defender Elite200's documentation from the internet.

To download your Defender Elite200's documentation, right-click on the KDMElite200 icon located in the task bar

- Click on **Quick Start Guide** to download a digital copy of the Defender Elite200's Quick Start Guide.
- Click on **Defender User Manual** to download a digital copy of the Defender Elite200's User Manual

2.12 About KDMElite200

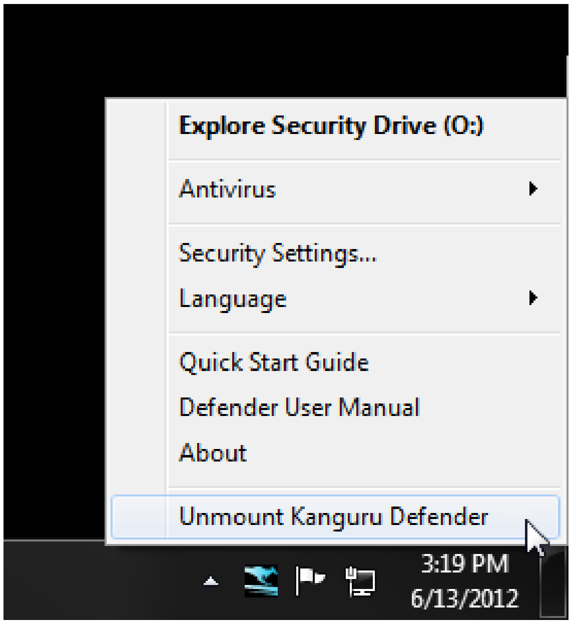
To view information regarding the version of KDMElite200 currently installed on your device, right-click on the KDMElite200 icon located in the task bar and then select **About**.


Explore Security Drive (G:)
Antivirus ▸
Security Settings...
Language ▸
Quick Start Guide
Defender User Manual
About
Unmount Kanguru Defender
3:13 PM
6/13/2012

2.13 Unmounting Your Defender Elite200

When you unmount your Defender Elite200, the KDMElite200 application will close and the secure partition containing your encrypted data will be inaccessible until you log into KDMElite200 again.

To unmount your Defender Elite200, right-click on the KDMElite200 icon located in the task bar and then select **Unmount Kanguru Defender.**



The KDMElite200 icon in the task bar will disappear and the Defender Elite200's secure partition will no longer be accessible.

Caution! Do not disconnect the Kanguru Defender Elite200 without first properly unmounting your device as detailed in this section and then safely removing the device from your computer as described in chapter 4. *Safely Removing Your Kanguru Defender Elite200* on page 36. Doing so may result in file damage or data corruption.

3. Updating Your Defender Elite200

Updates for your Defender Elite200 flash drive's client application may be released from time to time. To view the version of the KDMElite200 client application currently running on your drive, see section 2.12 *About KDMElite200* on page 32.

You must identify which Defender Elite200 edition device you are updating, as the update process is different for enterprise edition, cloud edition and No-Comms edition drives. Please refer to section 2.1 *Identifying the Device Edition* on page 9 for more information on identifying your device edition.

3.1 Updating Cloud Edition Drives

Cloud edition Defender Elite200 drives will automatically check the Kanguru Central Server (KCS) for client updates. Once you have successfully logged into your Defender Elite200's secure partition, KDMElite200 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.

Cloud edition Defender Elite200 users can also manually search and download available client updaters from the Kanguru Support site. Defender Elite200 client updaters can be found under the 'USB Client Software Updates' forum in the 'Software Downloads and Updaters' section (support.kanguru.com).

3.2 Updating KRMC Enterprise Edition Drives

Enterprise edition Defender Elite200 drives are managed by the Kanguru Remote Management Console (KRMC). Updaters for enterprise edition Defender Elite200 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).

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

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

3.3 Updating No-Comms edition drives

No-Comms edition Defender 2000 users must manually search and download available client updaters from the Kanguru Support site. Defender 2000 client updaters can be found under the 'USB Client Software Updates' forum in the 'Software Downloads and Updaters' section (support.kanguru.com).

3.4 Verifying the download checksum

To verify the integrity of the KDMElite200 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:

1. Download the SHA256 Checksum tool from the Kanguru Solutions' support site.
2. Save the SHA256 Checksum tool to the same directory that KDMElite200 updater file is saved in.
3. Open a command prompt window by clicking on **Start → All Programs → Accessories → Command Prompt.**
4. Within the command prompt window, navigate to the directory containing your KDMElite200 updater file and the SHA256 Checksum tool.
5. Type "sha256.exe <filename.exe>", where <filename.exe> is the name of the updater file that you are checking.
6. Press the **Enter** key. A 64-character string appears. This is the SHA256 checksum of the updater.
7. 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.

4. Safely Removing Your Kanguru Defender Elite200

Before unplugging the Defender Elite200 from the USB port, you should always make sure that you have unmounted the secured partition (see section 2.13 *Unmounting Your Defender Elite200* on page 33). After the Defender has been unmounted, you should use you operating system's method for safely removing a USB device.

4.1 Safely Removing from Windows

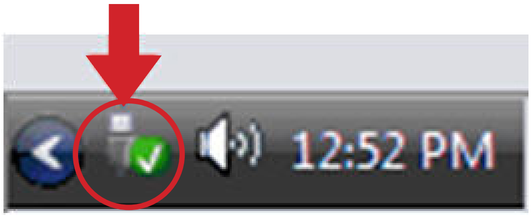
Caution! Be sure that the secure partition has been unmounted before attempting to remove the Defender drive. See section 2.13 *Unmounting Your Defender Elite200* on page 33.

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

To safely remove your Defender Elite200:

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

Note: The icon may look different depending on which version of Windows you are running.



2. A popup menu appears listing all USB devices connected to your computer. Select the Defender Elite200 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 your Defender Elite200.

If a message saying "The device cannot be stopped right now" appears, please make sure that any windows or applications accessing the Defender Elite200 are closed and then try again.

4.2 Safely Removing from Mac OS X

Caution! Be sure that the secure partition has been unmounted before attempting to remove the Defender drive. See section 2.13 *Unmounting Your Defender Elite200* on page 33.

To remove the Defender drive, click and drag the **KDMElite200 icon** from the desktop into the trash can icon. When you start dragging the KDMElite200 icon, the trash can icon will turn into an eject icon.

Alternatively, you can right-click on the **KDMElite200 icon** from the desktop and then select 'Eject' from the pop-up menu.

Once the KDMElite200 icon no longer appears on your desktop then it is safe to disconnect your Defender Elite200.

4.3 Safely Removing from Linux

Caution! Be sure that the secure partition has been unmounted before attempting to remove the Defender drive. See section 2.13 *Unmounting Your Defender Elite200* on page 33.

To remove the Defender drive, right-click the **KDMElite200 icon** on the desktop and then click on **Eject** from the popup menu. Once the KDMElite200 icon no longer appears on your desktop then it is safe to disconnect your Defender Elite200.

5. 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.

6. Tech Support

If you experience any problems using your Kanguru Defender Elite200 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

Appendix A - Common Criteria Certified Versions

The Common Criteria for Information Technology Security Evaluation, referred to more commonly as Common Criteria, is an international standard for computer security. Common Criteria provides an international set of guidelines for evaluating data security products, ensuring that they meet strict, security standards for government deployments.

Defender Elite200s with the following specifications have been certified by Common Criteria:

- Client software version : **2.0.0.0**
- Firmware version : **02.03.10**

Important! Defender Elite200s running these specific client software and firmware versions have been certified by Common Criteria. If you update the client software version to a newer version, your device will no longer be Common Criteria certified.

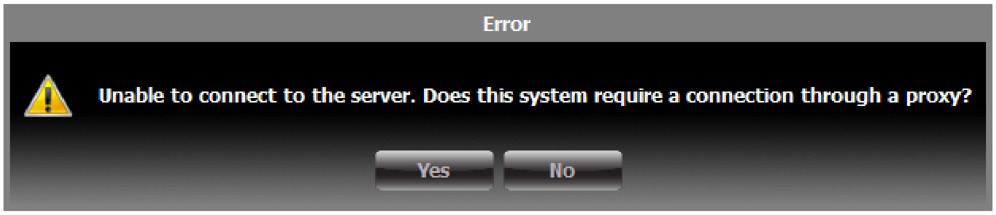
The Defender Elite200's firmware version is specific to the device's hardware. The firmware version is not accessible to the user. You are not able to view, update or modify the firmware version on your Defender Elite200 in any way.

Updates to the Defender Elite200's client software are released by Kanguru Solutions regularly. To prevent you from accidentally updating your device to a non-Common Criteria certified client version, the client application's auto-update feature has been disabled on Common Criteria certified Defender Elite200s. For more information about updating your Defender Elite200's client software version, please see Chapter 3. *Updating Your Defender Elite200* on page 34.

Appendix B - Proxy Support

If your computer uses a proxy server to access the internet, the correct proxy information will need to be configured in KDMElite200.

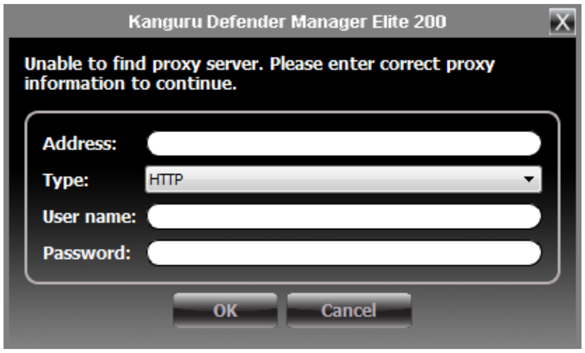
If the KDMElite200 client application cannot connect to the internet you will see the following error message:



Unable to connect to the server. Does this system require a connection through a proxy?

If the computer that the Defender Elite200 is connected to uses a proxy server to access the internet, click on the **Yes** button. KDMElite200 will try to read the proxy server information from the computer's configuration.

- If KDMElite200 is able to determine your proxy server's address and no authentication is required then KDMElite200 will read this information and connect to the internet as normal.
- If KDMElite200 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 KDMElite200 is unable to determine your proxy server's address then you will need to enter the proxy server address, proxy type and credentials:



Unable to find proxy server. Please enter correct proxy information to continue.

Address:
Type: HTTP
User name:
Password:

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 KDMElite200 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 Elite200 is connected to that connects to the internet through a proxy server.

KANGURU™

Secure. Anytime. Anywhere.

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

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