KANGURU

Kanguru Defender
Secure USB Flash Drive

User Manual

For Defender Models:
- Defender 2000
- Defender 3000
- Defender Elite30
- Defender Elite200
- Defender Elite300

NOTICES AND INFORMATION

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

Copyright © 2015 Kanguru Solutions. All rights reserved.
Windows XP®, Windows Vista®, Windows 7® and Windows 8® 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

The Kanguru Defender flash drive is a hardware encrypted, tamper proof USB flash drive. The Defender flash drive 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 secure partition is where your actual data will be stored.

The Kanguru Defender 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 USB Flash Drive
- Quick Start Guide
- Registration Form

1.2 System Requirements

- 1 available USB port (USB 2.0 or higher recommended)
- 256MB of internal DDR RAM or more
- 500MHz internal CPU or faster
- For supported operating systems see

1.3 Features

- √ 256-bit AES hardware encryption
- √ Password protected secure partition for your important data
- √ Does NOT require Admin privileges (except with Red Hat Enterprise Linux 5)
- √ Driverless installation (Plug & Play)
- √ High-strength alloy housing
- √ On-board antivirus protection
- √ HIPAA compliant
- √ Sarbanes Oxley compliant
- √ GLB compliant
- √ Remote Management ready
- √ TAA compliant

1.4 Remote Management Capability

The Kanguru Defender 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:
- √ Remotely manage your Defender drives
- √ Remotely delete all data off a drive
- √ Reset user passwords
- √ 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. 6 retries before drive is wiped)
  - ○ Rate at which password should be changed (e.g. every 30, 60, or 90 days)
- √ Create user groups

You Kanguru Defender flash drive does not come with KRMC enabled by default. For more information about KRMC, visit: https://kanguru.com/remote-management/remote-management-suite.shtml

1.5 FIPS 140-2 Certified Drives

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules.

- The Defender **Elite200** and **Elite300** have been certified for **FIPS 140-2 Security Level 2**
  - ○ Security Level 2 improves upon the physical security mechanisms of the cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters within the module.

- The **Defender 2000** and **Defender 3000** have been certified for **FIPS 140-2 Security Level 3**
  - ○ In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent an intruder from gaining access to critical security parameters held within the cryptographic module. Physical security mechanisms required at Security Level 3 have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module.

1.6 Common Criteria Certified Drives

Common Criteria provides an international set of guidelines for evaluating data security products, ensuring that they meet strict, security standards for government deployments. Several specific Defender flash drives have been Common Criteria certified. For more information please refer to Appendix A - Common Criteria Certified Versions on page 48

1.7 The Write Protect Switch

Kanguru Defender Elite30, Elite200 and Elite300 flash drives have a physical write protect switch located on the edge of the drive, near the USB connector:

- **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 data from being written to the device's secure partition.

Important! For devices with a physical write protect switch, the write protect switch must be set in the intended functioning position (i.e. locked or unlocked) prior to connecting the drive to the computer.

WARNING! You may receive an error if you attempt to setup or login 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. It is highly recommended to go through the setup wizard, login and mount the device's secure partition before setting the write protect switch to the locked position.

Note: The Defender 2000 and Defender 3000 flash drives use software based write protection and do not have a physical switch. To enable the software write protection on a Defender 2000 or Defender 3000, please refer to section 2.3.2 Enabling Software Write Protection on page 21.

2. Kanguru Defender Manager

Kanguru Defender Manager (KDM) is the client program preloaded on the Defender's CD-ROM partition. The user needs to login to KDM in order to access the secure, encrypted partition. KDM comes pre-installed on your Defender flash drive. No installation to your PC is necessary.

KDM is named differently for each model:
- KDM2000 = Defender 2000
- KDM3000 = Defender 3000
- KDME30 = Defender Elite30
- KDME200 = Defender Elite200
- KDME300 = Defender Elite300

2.1 Running KDM

The Kanguru Defender flash drive is compatible with multiple operating systems. Running the KDM application can be different depending on the operating system your computer is running. For more info on which operating systems are supported by your device, please refer to Chapter 5. Technical Specifications on page 42

2.1.1 Running KDM on Windows

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

If KDM does not start automatically:
1. Open an explorer window and open the Defender's CD-ROM partition. The drive letter (e.g. D:, E:, F:) will depend on your computer.

2. Double-click on the **KDM.exe file** to launch the KDM application.
   - If it is your first time running KDM you will need to complete the setup wizard (see section 2.2 The Setup Wizard on page 13).
   - If you have already gone through the setup wizard, you will be prompted to login (see section 2.3 The Login Screen on page 20).

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

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

Attention Windows Users

Windows 7 users may not see the removable disk partition until you have logged into KDM. This is normal. If you are running Windows 7 or 8 and for any reason need to see the removable disk before you log into KDM, 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 Defender flash drive.

1. Open the **Folder and search options**.
   ○ **Windows 7** : Open My Computer, click on the **Organize tab** and then select **Folder and search options**.
   ○ **Widows 8 :** Open a explorer window, click on the **View tab**, click on **Options > Change Folder and Search Options**
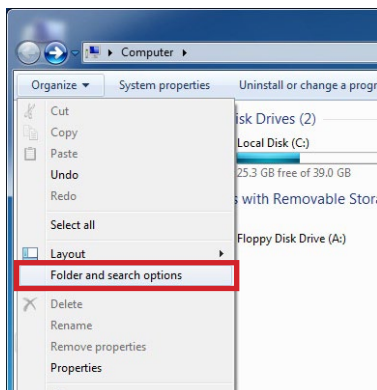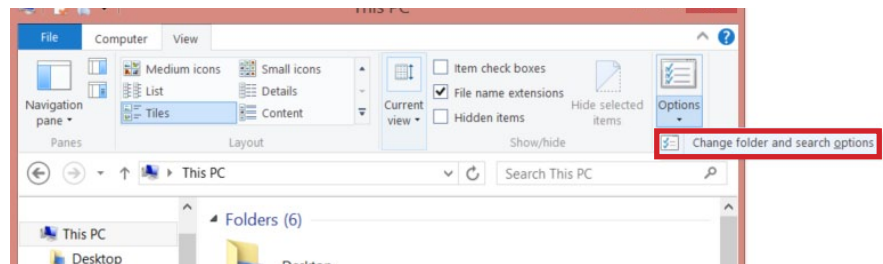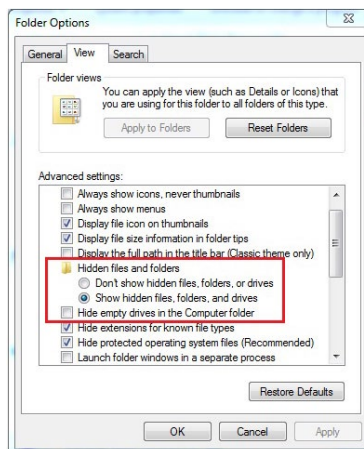

Windows 7   *Windows 8*

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

3. Click on the **OK button** to finish configuring Windows. The removable disk should now be visible before you login to KDM.

2.1.2 Running KDM on Mac OS X

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

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

- If it is your first time running KDM you will need to complete the setup wizard in order to set your security password (see section 2.2 The Setup Wizard on page 13).
- If you have already setup your security password, you will be prompted to login (see section 2.3 The Login Screen on page 20).

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

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

2.1.3 Running KDM on Ubuntu Linux

The following Defender flash drive models are supported on Linux Ubuntu:
- Defender 2000
- Defender 3000
- Defender Elite200
- Defender Elite300

To run KDM from an Ubuntu Linux operating system, connect your Defender to your computer through a USB port. A 'KDM' icon will appear on the desktop. Double click on the **KDM icon** to open it.
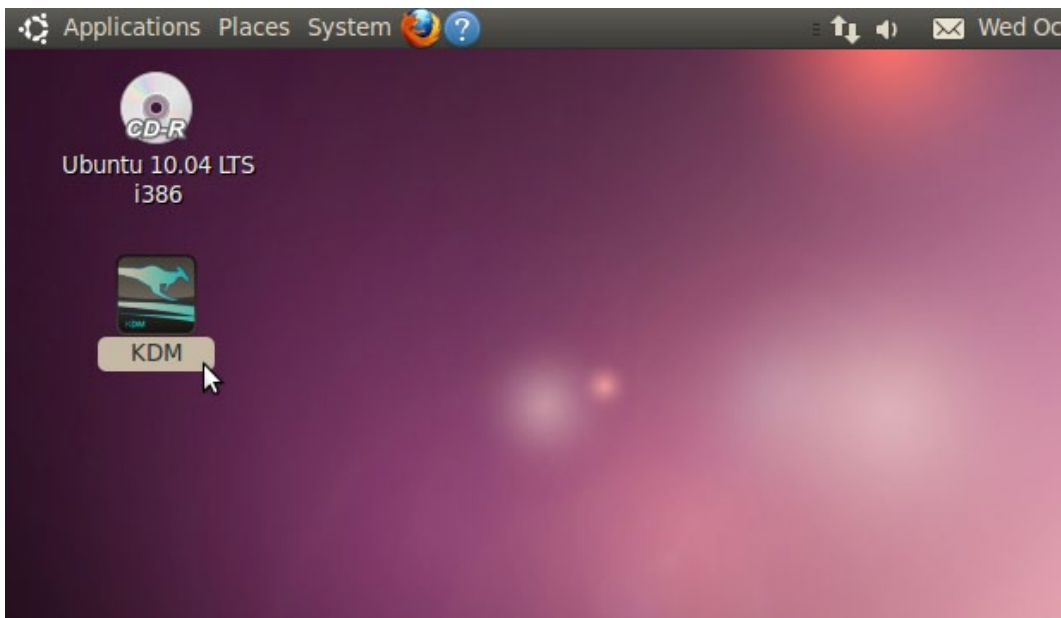
In the window that opens, double-click on the **KDM file** to launch the KDM application.

- If it is your first time running KDM you will need to complete the setup wizard in order to set your security password (see section 2.2 The Setup Wizard on page 13).
- If you have already setup your security password, you will be prompted to login (see section 2.3 The Login Screen on page 20).

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

2.1.4 Running KDM on Red Hat Enterprise Linux 5

Only the following Defender flash drive models are supported on Red Hat Enterprise Linux 5:
- Defender 2000
- Defender Elite200

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

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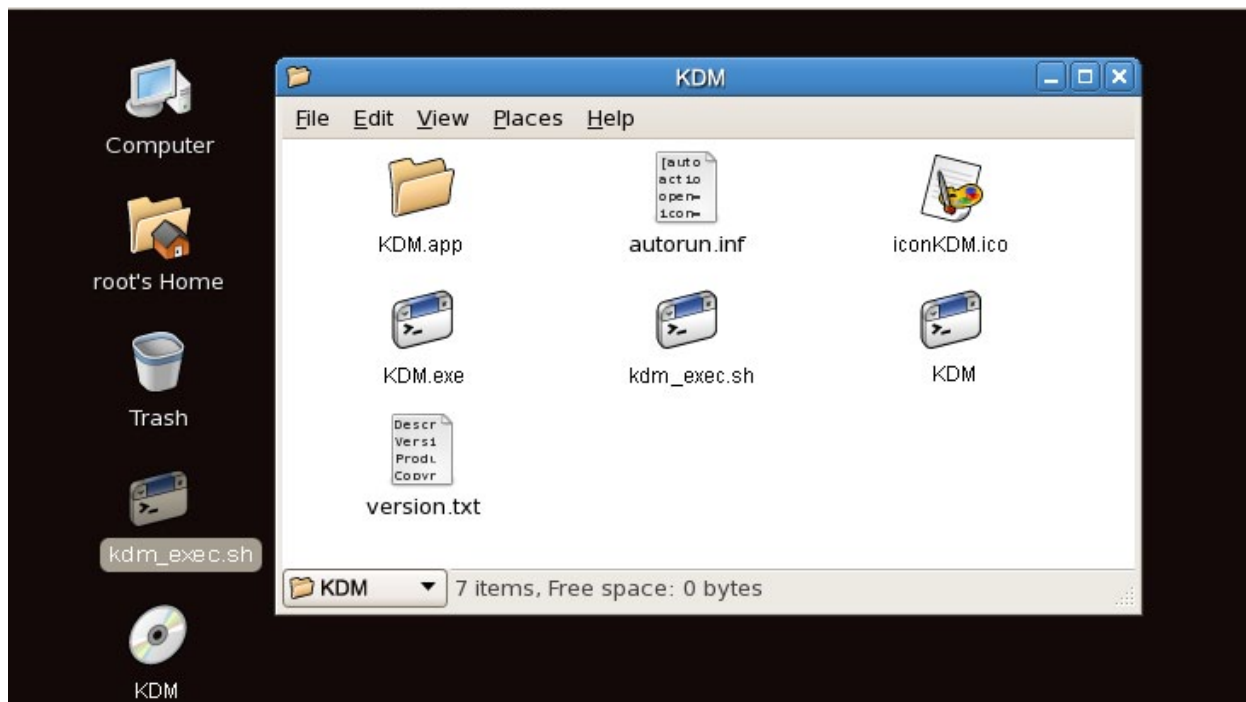

From the window that opens, copy the **kdm_exec.sh shell script file** to a location on your computer's local hard drive.

Once the kdm_exec.sh shell script has been copied to a local hard drive, you can execute KDM 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 kdm_exec.sh shell script file to.
3. Type, "chmod 007 kdm_exec.sh" to allow full execute permission.
4. Type, "./kdm_exec.sh" to execute the shell script.
   - If it is your first time running KDM you will need to complete the setup wizard in order to set your security password (see section 2.2 The Setup Wizard on page 13).
   - If you have already setup your security password, you will be prompted to login (see section 2.3 The Login Screen on page 20).

2.2 The Setup Wizard

When you start KDM for the first time you will be greeted by the Setup Wizard. Follow the Setup Wizard instructions to create a security password for your Defender's secure, encrypted partition.
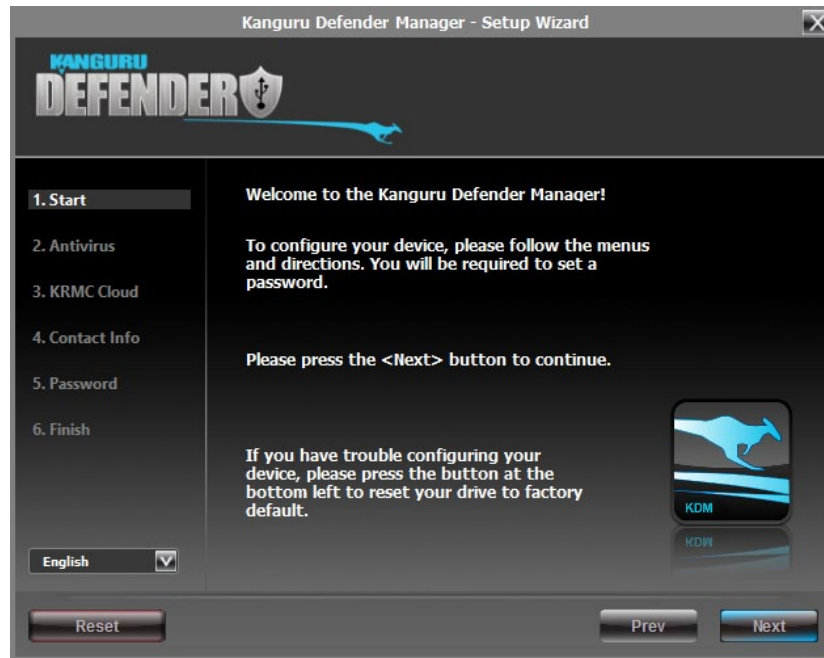
Caution! Once the Setup Wizard has started, you should not disconnect your Defender flash drive without either first completing the Setup Wizard or closing the Setup Wizard by clicking on the **X button**.

2.2.1 Selecting a Setup Language

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

1. From the Welcome screen, click on the ▼ **icon** in 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.

2.2.2 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**.

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.

2.2.3 Activating On-board Antivirus Protection (Windows only)

This section does not apply if you are running the Setup Wizard in Linux or Mac OS X. This section does not apply to Enterprise Edition users. Antivirus for Enterprise Edition is activated through Kanguru Remote Management Console (KRMC). Enterprise Edition users, please contact your administrator.

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

KDM will automatically check during the Setup Wizard for a valid antivirus license key.
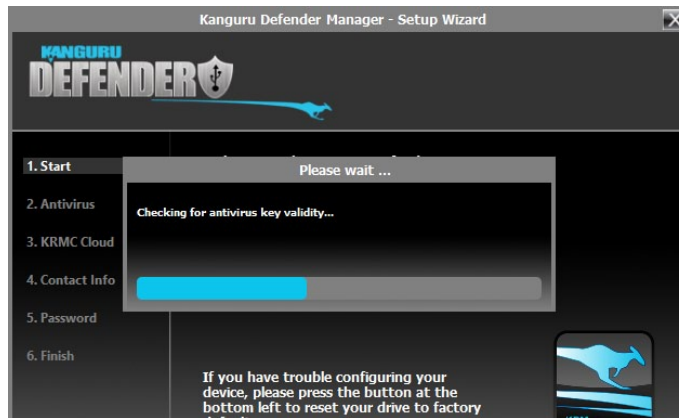
If your Defender flash drive does not already have a valid antivirus license key, then you must fill out the registration form with the required information and then click on the **Apply button** to activate your free antivirus trial.

Click on the **Skip button** if you do not wish to activate antivirus protection. If you decide not to activate your antivirus at this point, you will not be able to activate it in the future without first resetting your drive back to the factory default setting.
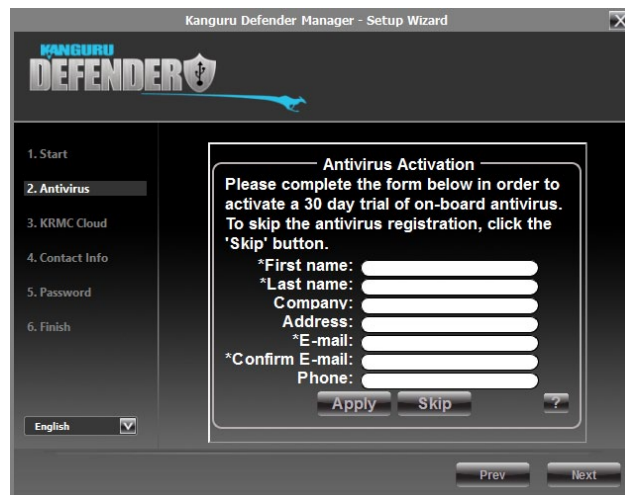
Click on the **Next button** to continue with setting up your Defender's security password.

2.2.4 KRMC Cloud

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

Kanguru Defender flash 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 flash drive.

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 instructing you to enter your KRMC Cloud Account ID. Click on the **OK button**.
3. Enter your KRMC Cloud Account ID in the field provided, and then click on the **Register button.** This will register your device with your KRMC Cloud account.

Note: If you have not purchased a KRMC Cloud license and do not have a KRMC Cloud Account ID then please contact Kanguru Sales to purchase a KRMC Cloud license. If you have a KRMC Cloud account but do not remember your KRMC Cloud Account ID, please contact Kanguru Technical Support.

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.

2.2.5 Contact Info

If you chose to manage your drive using KRMC Cloud, then the information entered in the Contact Info window will automatically be imported to the KRMC Cloud server when you register your drive. If you did not enable KRMC Cloud then you can skip this step.

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


Fill in your information in the appropriate fields and then click on the **Apply button**. Any field that appear with a * next to it is a mandatory field and must be filled out.

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.

2.2.6 Setting a Password

From the Set Password screen:
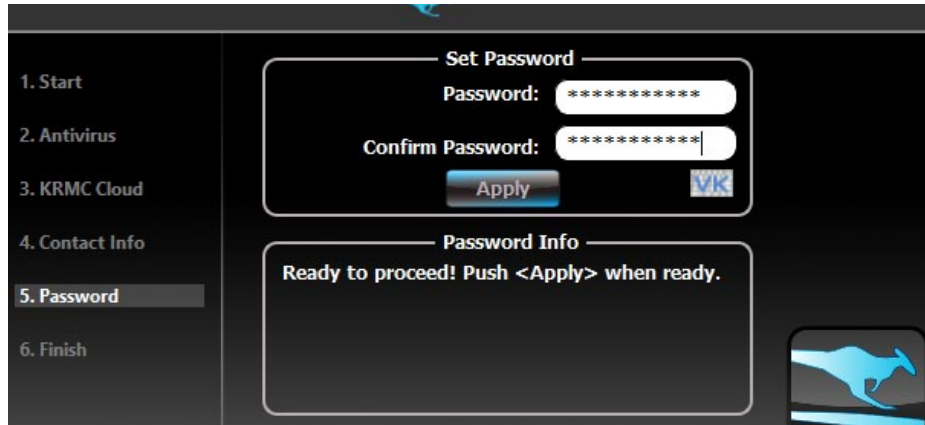
1. Enter your password in the 'Password' field. You can enter your password using KDM's Virtual Keyboard by clicking the **VK button**. For more information on using the Virtual Keyboard see section 2.3.4 Using the Virtual Keyboard to Enter Your Password on page 23.

   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:
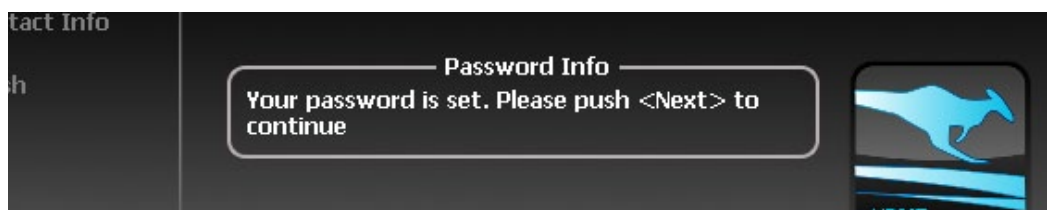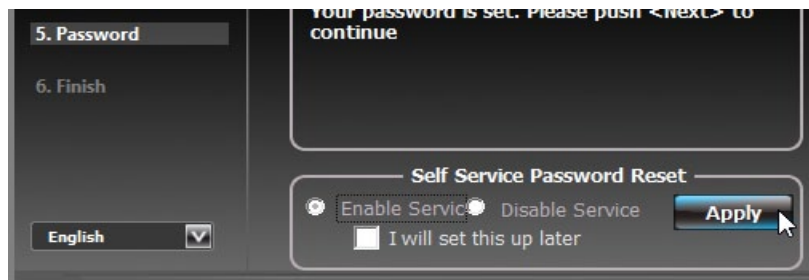

4. Click the **Next button** and KDM will automatically configure the security parameters.

2.2.7 Enabling Self Service Password Reset

Enabling Self Service Password Reset (SSPR) functionality will allow you to reset your Defender's password without first needing to wipe the data stored in the secure partition. The SSPR feature is a subscription service and requires a license key. If you do not have a license key, either contact Kanguru to purchase one, or select the **Disable Service option** and then click on the **Apply button**.

If you decide to enable the SSPR service:

1. Select the **Enable Service option** and then click on the **Apply button**.
   Note: If you want to enable SSPR but have not yet purchased your SSPR subscription, you can select 'I will set this up later' and then click on the **Next button**.

2. Next you'll need to designate an email address that you can have a password reset link sent to in case you forget your login password. Enter your email in the corresponding fields.

3. Enter your SSPR license key in the 'Enter License Key' field and then click on the **Send button**. Your SSPR license key should have been e-mailed to you when you purchased your SSPR subscription. Contact Kanguru if you did not receive your SSPR license.

4. An email containing your activation code will be sent to the email address you entered above. Enter the activation code into the 'Enter Activation Code' field and then click on the **Activate button**.
   Note: The activation code field is case sensitive. Please enter your activation code exactly as it appears in the email that you received from Kanguru.

5. Click on the **OK button** to close the window, and then click on the **Next button**.

Congratulations! Your Defender flash drive is now setup and ready to use.

2.3 The Login Screen

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

When the login screen appears:
1. Enter your password in the 'Password' field.
2. Click on the **Login button**.

Caution! By default, if you enter your password incorrectly six times in a row any data stored on the secure partition will automatically be erased for security purposes. 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 flash drive or manually restarting KDM.exe will bring the login window back.

Once you have successfully logged in to KDM, the Defender's secure partition will be accessible through My Computer or Windows Explorer. For more information on accessing the secure partition, see section 2.4.1 Encrypting Files and Folders on page 25.

Caution! Once KDM has started, you should never disconnect your device without first closing KDM properly by clicking the **KDM task bar icon** and selecting **Unmount Kanguru Defender** as described in section 2.7 Unmounting Your Defender on page 37.

### 2.3.1 Enabling and Disabling Autorun Functionality

If your Defender flash 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.

2.3.2 Enabling Software Write Protection

Unlike other Defender models, the Defender 2000 and Defender 3000 do not have a physical write protect switch, but rather use software write protection.

To enable write protection on a Defender 2000 or Defender 3000 device, click on box for **Enable write protection** in the login window.
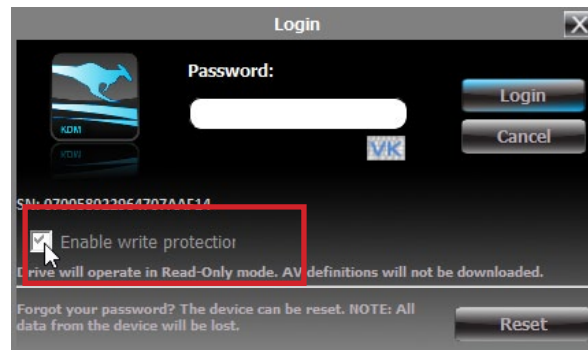
When you login to your device, you will not be able to write to or modify any files on the secure partition.

To disable write protection, you must unmount the secure partition, restart KDM and then uncheck the **Enable write protection box** the next time you are at the login screen.

2.3.3 Resetting You Device from the Login Screen

In the event you have forgotten your password and do not have the Self Service Password Reset functionality enabled, 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. **Note:** The Reset function may be disabled if your device is managed by KRMC or KLA.

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 flash drive to the factory default:

1. From the login screen, click on the **Reset button**.
    Note: If the **Reset button** is not visible then your device is likely managed by KRMC or KLA. Please check with your administrator.

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

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


The next time you run KDM, you will have to go through the Setup Wizard again before you are able to access the secure partition. Please see section for instructions on completing the Setup Wizard.

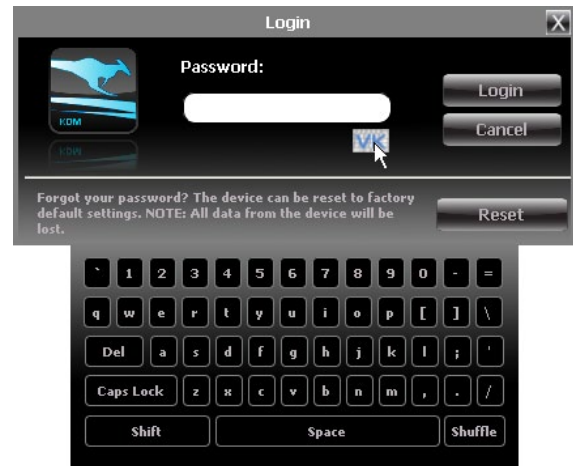## 2.3.4 Using the Virtual Keyboard to Enter Your Password

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 the **VK button** which is located near the password entry field.
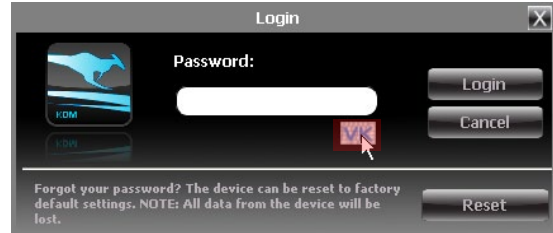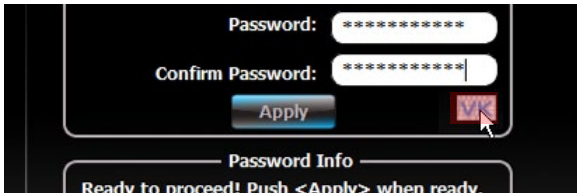
2. The virtual keyboard will appear below the Setup Wizard window. Click on the keys on the virtual keyboard to enter your password.

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

Note: You can click on the **Shuffle key** 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.
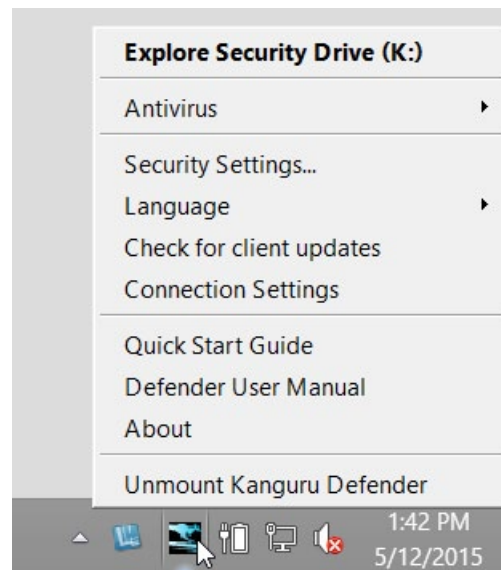
2.4 The KDM Taskbar Menu

The KDM Taskbar menu provides a simple user interface that allows you to use and configure your Defender device.

When you login to KDM, the KDM icon appears in the taskbar area. To access the KDM Taskbar menu, simply click on the **KDM icon**.

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

2.4.1 Encrypting Files and Folders

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

To open the secure partition:

1. Start KDM.

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

3. Click on the **KDM icon** located in the task bar and then select **'Explore Security Drive'** from the popup menu.
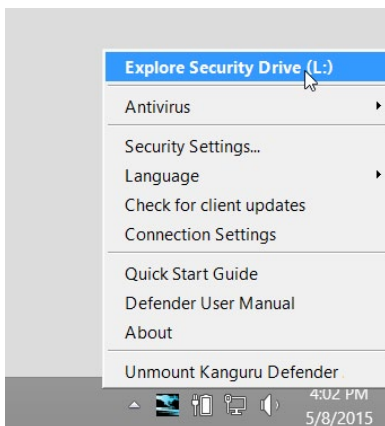
The secure partition appears in a new window. We recommend using either the drag & drop action, right-click copy/paste action, or the shortcut keys (Ctrl+C and Ctrl+V) to copy and paste files and folders directly to and from the secure partition.

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

2.4.2 Enabling On-board Antivirus (Windows only)

Defender flash drives support on-board, antivirus functionality. The onboard anti-virus feature is a subscription based service and requires a license key. If you do not have a license key you can either contact Kanguru to purchase an antivirus license, or you can fill out the antivirus activation form during the Setup Wizard to obtain a 30-day free trial license (see section 2.2.3 Activating On-board Antivirus Protection (Windows only) on page 15).

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

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.

2.4.3 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 **KDM icon** located in the task bar.
   Note: Linux users must right-click on the **KDM icon** in the task bar.

2. Select 'Antivirus' from the popup menu and then click on '**Configuration'** from the submenu.
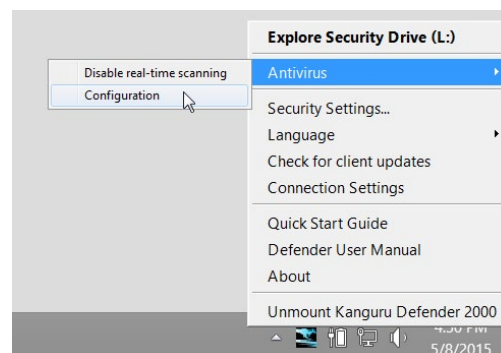
The antivirus console appears.

2.4.3.1 Device Scan

The antivirus menu allows you to scan your Defender for known viruses and malware.
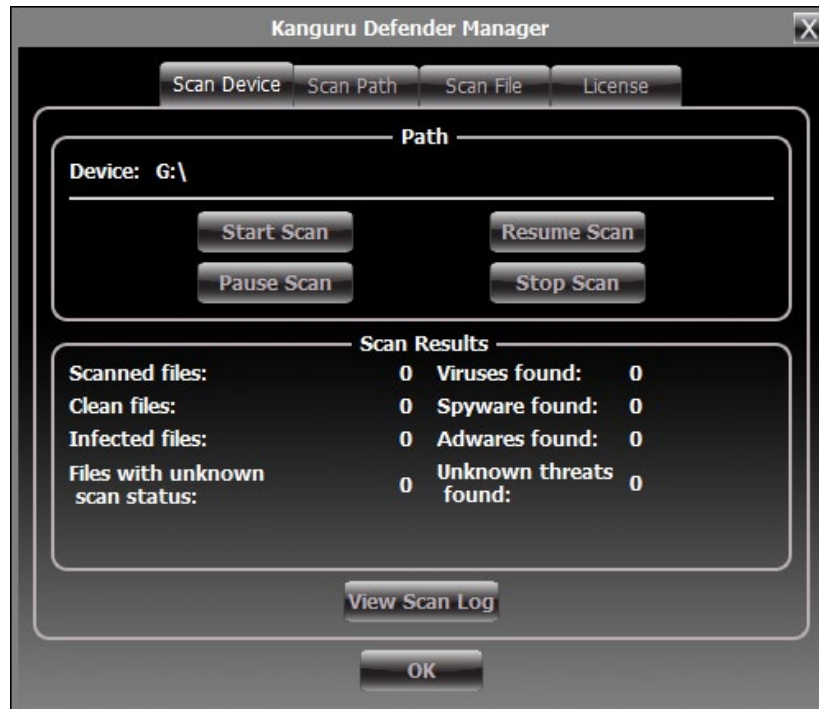
To scan your Defender:
1. Click on the **Scan Device tab** at the top of the antivirus menu.
2. Click on the **Start Scan** button to begin scanning your Defender device.
3. Once the scan has started:
    ○ Click on the **Pause Scan button** to pause the scan process. Click on the **Resume Scan button** 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 menu.

2.4.3.2 Path Scan

The antivirus menu 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.
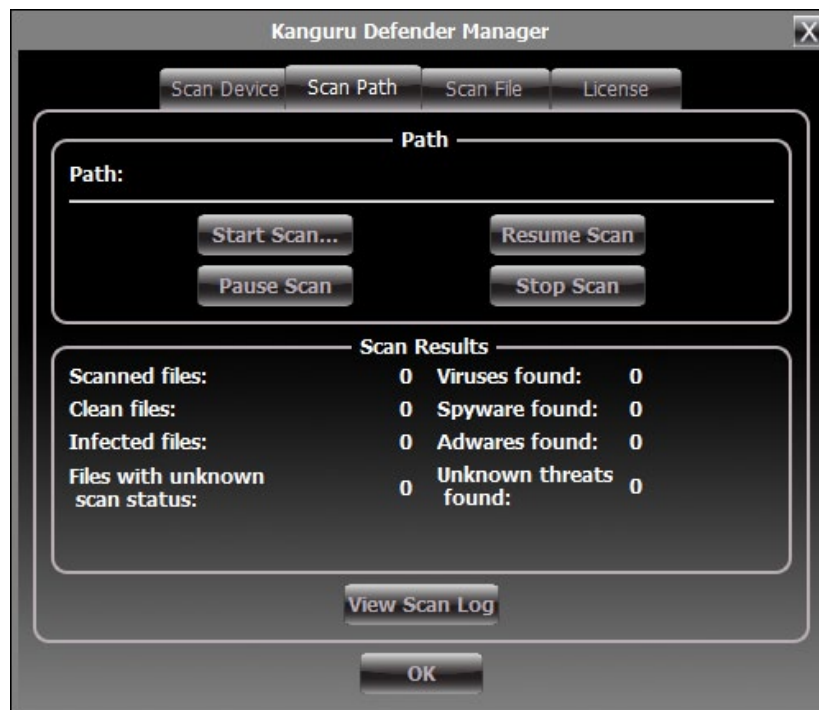
To scan a path on your computer:
1. Click on the **Scan Path tab** at the top of the antivirus menu.
2. Click on the **Start Scan button** and then select a path on your computer to begin scanning.
3. Once the scan has started:
    ○ Click on the **Pause Scan button** to pause the scan process. Click 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 menu.

2.4.3.3 File Scan

The antivirus menu 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.
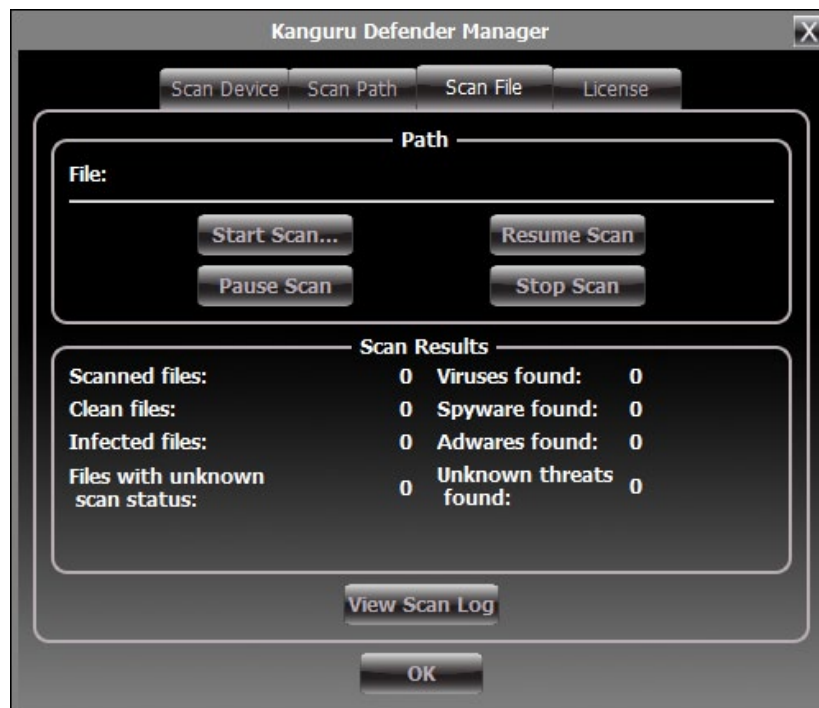

To scan a file:
1. Click on the **Scan File tab** at the top of the antivirus menu.
2. Click on the **Start Scan button** and then select a file to begin scanning.
3. Once the scan has started:
    ○ Click on the **Pause Scan button** to pause the scan process. Click on the **Resume Scan button** to 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 menu.

2.4.3.4 Antivirus License

The antivirus menu allows you to view your antivirus license information and also renew your subscription. You can view the number of days remaining on your current antivirus license

- Click on the **Licenses button** to see your current antivirus license number.
- Click on the **Renew License Online button** to purchase a one-year antivirus license subscription from Kanguru's online store.

Once you have purchased or renewed your antivirus license, you will receive a new antivirus license key as well as a customer ID. Enter your new license key and customer ID in the appropriate fields and then click on the **Verify ID button**.

Your antivirus license will be activated once your customer ID and antivirus license key have been verified. Click on the **OK button** to close the antivirus menu.

2.4.4 Changing Your Password

You can change your security password through the Security Settings.

To change your password:

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

    Note: Linux users must right-click on the **KDM icon** in the task bar.
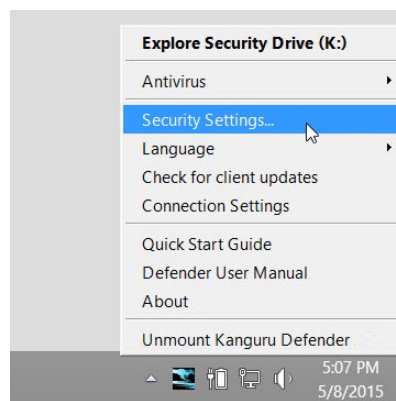
2. The 'Password Settings' window opens. Enter your current password in the 'Old Password' field. Enter your new password in the 'New Password field' and then enter it again in the 'Confirm New Password' field.
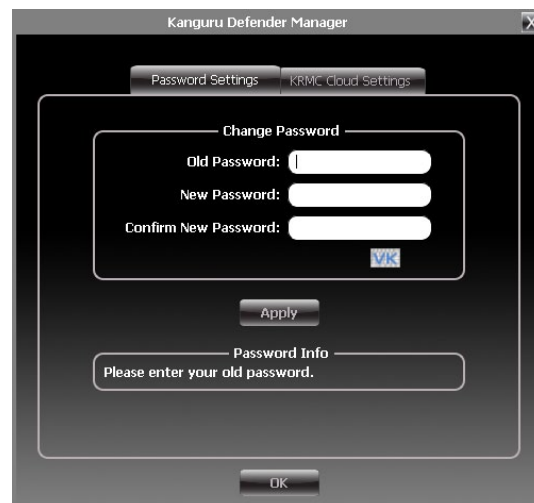
3. When you are ready to proceed, click on the **Apply button** to set your new password.

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 close the 'Password Setting' window.

2.4.4.1 Self Service Password Reset

Self Service Password Reset (SSPR) functionality will allow you to reset your Defender's password without needing to wipe the data stored in the secure partition. The SSPR feature is a subscription based service and requires a license key. If you do not have a license key, please contact Kanguru to purchase one.

If you decide to enable the SSPR service:

1. Select the **Enable Service option** and then click on the **Apply button**.
   Note: This section is not available if you have already enabled SSPR during the setup wizard (see section).

2. Next you'll need to designate an email address that you can have a password reset link sent to, in case you forget your login password. Enter your email in the corresponding fields.

3. Enter your SSPR license key in the 'Enter License Key' field and then click on the **Send button**. Your SSPR license key should have been emailed to you when you purchased your SSPR subscription. Contact Kanguru if you did not receive your SSPR license.

4. An email containing your activation code will be sent to the email address you entered above. Enter the activation code into the 'Enter Activation Code' field and then click on the **Activate button**.
   Note: The activation code field is case sensitive. You must enter your activation code exactly as it appears in the email that you received from Kanguru.

5. Click on the **OK button** to close the window. SSPR is now enabled.

2.4.5 KRMC Cloud Settings

You can enable or disable KRMC Cloud functionality through the Security Settings. **Note:** This section does not apply to Enterprise Edition users or if you have already enabled KRMC Cloud.
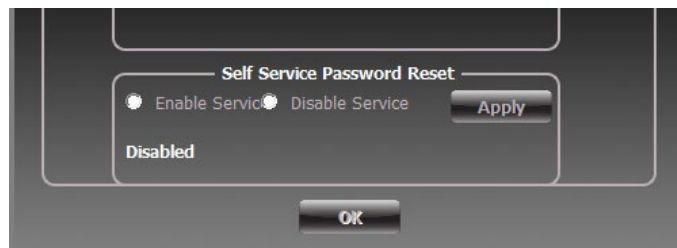
To change your device's KRMC functionality:

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

    Note: Linux users must right-click on the **KDM 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 clicking on the appropriate radio button and then click on the **Apply button**.
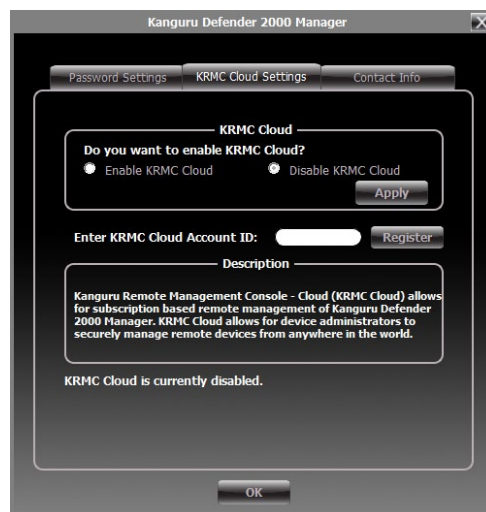
4. If you are choosing to enable KRMC Cloud, enter your KRMC Cloud Account ID and then click on the **Register button.**

2.4.6 Changing Languages

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

To change the language:

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

    Note: Linux users must right-click on the **KDM icon** in the task bar.
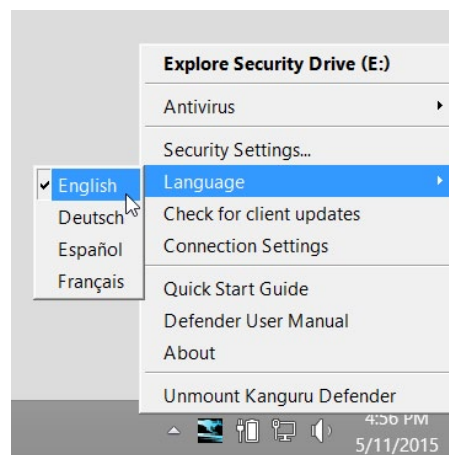
2. Click on the desired language that you want KDM to be displayed in.

2.4.7 Connection Settings and Configuring a Proxy Server

If your computer uses a proxy server to access the internet and KDM is unable to determine your proxy server's address then you will need to enter the proxy server address, proxy type and credentials.

To configure your proxy serer settings:

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

   Note: Linux users must right-click on the **KDM icon** in the task bar.
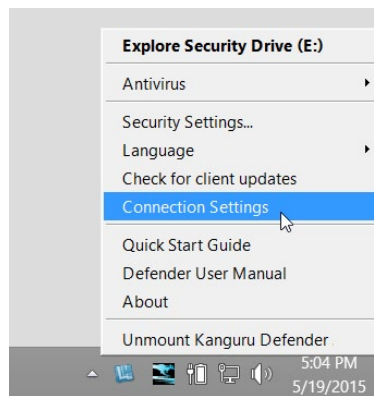
2. The 'connection preferences' window appears.
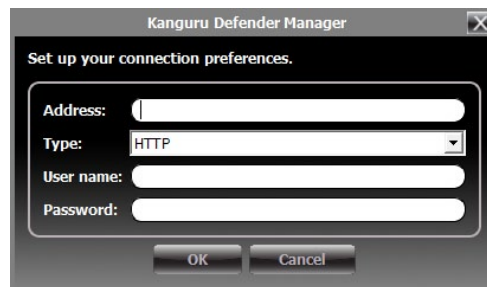
3. Enter the proxy address and the port to connect to in the 'Address' field (e.g. 192.168.0.193:8080 or proxycomp:8080).

4. Select the proxy type from the drop down menu.

5. Enter your credentials in the 'User name' and 'Password' fields.

6. Click the **OK button** to save the proxy configuration.

If KDM is able to connect to the proxy server using those credentials then the authentication information is saved in an encrypted proxy settings file on the host computer.

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

2.5 Online Documentation

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

To download your Defender flash drive's documentation, click on the **KDM icon** located in the task bar:

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

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

- Click on '**Defender User Manual'** to download a digital copy of the Defender flash drive's User Manual

2.6 About KDM

To see which version of KDM is currently installed on your device, click on the **KDM icon** located in the task bar and then select '**About**'.

Note: Linux users must right-click on the **KDM icon** in the task bar.
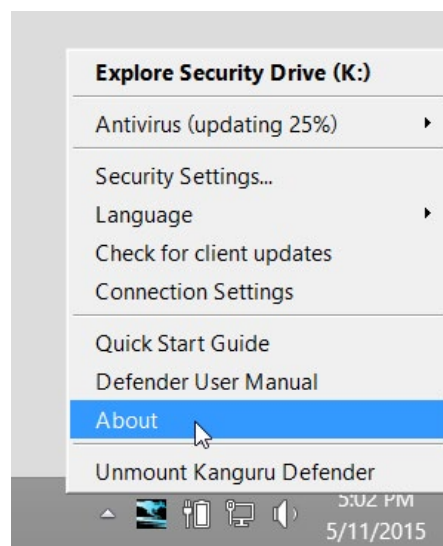
2.7 Unmounting Your Defender

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

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

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

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

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

3.   Updating Your Defender Flash Drive

Updates for your Defender flash drive's client application may be released from time to time. To view the version of the KDM client application currently running on your drive, see section 2.6 About KDM on page 36.

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

3.1 Updating standard edition drives

Standard edition Defender flash drives will automatically check the Kanguru Central Server (KCS) for client updates. Once you have successfully logged into your Defender flash drive's secure partition, KDM will check KCS for any available client updates. If an update is available, you will receive a pop-up notification with instructions for downloading the updater file. If you refuse the update, you will not be prompted to update again until the next version updater is released.

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

To manually check if there is a KDM update available for your device, click on the **KDM icon** located in the task bar and then click on **Check for Client Updates**.
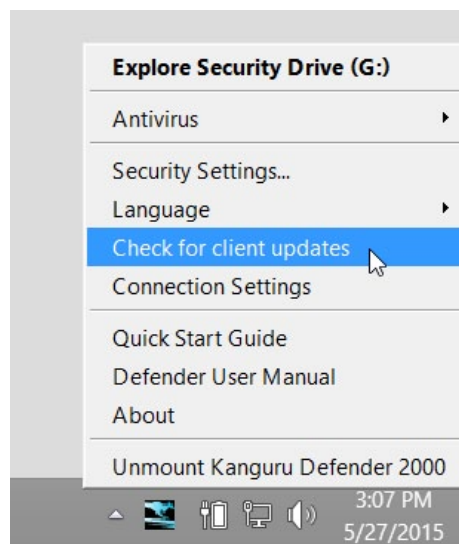
If a newer client version is available for your device, follow the on-screen instructions to download and apply the update.

Standard edition Defender flash drive users can also manually search and download available client updaters from the Kanguru Support site. Defender flash drive 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 flash drives are managed by the Kanguru Remote Management Console (KRMC). Updaters for enterprise edition Defender flash 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).

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

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

3.3 Verifying the download checksum

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

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

To view and verify your download's checksum:
1. Download the SHA256 Checksum tool from the Kanguru Solutions' support site.
2. Save the SHA256 Checksum tool to the same directory that KDM 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 KDM 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 Defender Flash Drive

Before unplugging the Defender flash drive from the USB port, you should always make sure that you have unmounted the secured partition (see section 2.7 Unmounting Your Defender on page 37). 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 2.7 Unmounting Your Defender on page 37.

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

To safely remove your Defender flash drive:
1. Click on the **Safely Remove Hardware icon** located in the task bar.

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

If a message saying "The device cannot be stopped right now" appears, please make sure that any windows or applications accessing the Defender flash drive 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 2.7 Unmounting Your Defender on page 37.

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

Alternatively, you can right-click on the **KDM icon** from the desktop and then select 'Eject' from the pop-up menu, or you can eject it through the Finder window.

Once the KDM icon no longer appears on your desktop then it is safe to disconnect your Defender flash drive.

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 2.7 Unmounting Your Defender on page 37.

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

5. Technical Specifications

5.1 Defender 2000

General Specifications

Model	KDM2000
Interface	USB 2.0 (USB 1.1 compatible)
Encryption Features	Hardware based 256-bit AES encryption
Security Certifications	FIPS 140-2 Certified Level 3 Common Criteria EAL 2+ Certified
OS Compatibility	Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 Max OS X 10.5 and above (Intel based only) Red Hat Enterprise Linux 5, Ubuntu 9/10, OpenSUSE 11.1 Linux Kernel 2.6.02 - 2.6.34 32 and 64 bit compatible
Memory Type	MLC NAND Flash
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
TAA Compliant	Yes

4GB - 16GB Defender 2000 Specifications

Data Transfer Rate	Max Read: 30 MB/s Max Write: 20 MB/s
Weight	35g
Dimensions	72.6mm x 19.5mm x 9mm
Power	Max Read: 5 VDC @ 122mA Max Write: 5 VDC @ 182mA

32GB - 128GB Defender 2000 Specifications

Data Transfer Rate	Max Read: 30 MB/s Max Write: 20 MB/s
Weight	51g
Dimensions	77.3mm x 26.6mm x 9mm
Power	Max Read: 5 VDC @ 150mA Max Write: 5 VDC @ 266mA

5.2 Defender 3000

General Specifications

Model	KDM3000
Interface	USB 3.0 (USB 2.0 compatible)
Encryption Features	Hardware based 256-bit AES encryption
Security Certifications	FIPS 140-2 Certified, Level 3 Common Criteria Evaluated
OS Compatibility	Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 Max OS X 10.5 and above (Intel based only) Linux Kernel 2.6.02 and above 32 and 64 bit compatible
Data Transfer Rate	Max Read: 230 MB/s Max Write: 85 MB/s
Memory Type	MLC NAND Flash
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
Weight	38 g
Dimensions	7.3 x 1.9 x 0.9 cm
TAA Compliant	Yes

5.3 Defender Elite30

General Specifications

Model	KDFE30 series
Interface	USB 3.0 (USB 2.0 compatible)
Encryption Features	Hardware based 256-bit AES encryption (XTS mode)
Security Certifications	N/A
OS Compatibility	Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 Max OS X 10.5 and above (Intel based only) 32 and 64 bit compatible
Data Transfer Rates	Max Read: 230 MB/s Max Write: 85 MB/s
Memory Type	Solid State NAND flash
Write Cycles	10,000 write cycles / block
Data Retention	10 years or more
Operating Temperature	0°C to 70°C
Storage Temperature	-25C to 85°C
Humidity Range	20% - 90%
Shock Resistance	1000G Max
Vibration	15G Peak to Peak Max
Weight	14g
Dimensions	7.7 x 2 x 0.9 cm
Power	Max Read: 5 VDC @ 122mA Max Write: 5 VDC @ 182mA
TAA Compliant	Yes

5.4 Defender Elite200

General Specifications

Model	KDFE30
Interface	USB 2.0 (USB 1.1 compatible)
Encryption Features	Hardware based 256-bit AES encryption
Security Certification	FIPS 140-2 Certified, Level 2 Common Criteria EAL 2+ Certified
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
Memory Type	Dual Channel MLC NAND Flash
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
TAA Compliant	Yes

* 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

Data Transfer Rate	Max Read: 33 MB/s Max Write: 16 MB/s
Weight	12g
Dimensions	64mm x 18.5mm x 9mm
Power	Max Read: 5 VDC @ 105mA Max Write: 5 VDC @ 100mA

32GB - 128GB Defender Elite200 Specifications

Data Transfer Rate	Max Read: 33 MB/s Max Write: 22 MB/s
Weight	22g
Dimensions	71mm x 27mm x 9mm
Power	Max Read: 5 VDC @ 150mA Max Write: 5 VDC @ 266mA

5.5 Defender Elite300

General Specifications

Model	KDFE300 series
Interface	USB 3.0 (USB 2.0 compatible)
Encryption Features	Hardware based 256-bit AES encryption (XTS mode)
Security Certifications	FIPS 140-2 Certified Level 2 Common Criteria Evaluated
OS Compatibility	Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 Max OS X 10.5 and above (Intel based only) Linux Kernel 2.6.02 and above 32 and 64 bit compatible
Data Transfer Rates	Max Read: 8GB = up to 150 MB/s 16GB - 128GB = up to 230 MB/s Max Write: 8GB - 16GB = up to 20MB/s 32GB = 45 MB/s 64GB - 128GB = up to 85 MB/s
Memory Type	Solid State NAND flash
Write Cycles	10,000 write cycles / block
Data Retention	10 years or more
Operating Temperature	0°C to 70°C
Storage Temperature	-25C to 85°C
Humidity Range	20% - 90%
Shock Resistance	1000G Max
Vibration	15G Peak to Peak Max
Dimensions	7.7 x 2 x 0.9 cm
Power	Max Read: 5 VDC @ 122mA Max Write: 5 VDC @ 182mA

6. Warranty Information

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

7. Tech Support

If you experience any problems using your Kanguru Defender flash drive 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 2000** with the following specifications has been certified by Common Criteria:
  - Client software version : **1.2.1.8**
  - Firmware version : **02.03.10**

- **Defender Elite200** with the following specifications has been certified by Common Criteria:
  - Client software version : **2.0.0.0**
  - Firmware version : **02.03.10**

Important! Defenders 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'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 in any way.

Updates to the Kanguru Defender Manager 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 Defenders. For more information about updating your Defender's client software version, please see Chapter 3. Updating Your Defender Flash Drive on page 38.

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 KDM.

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

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

- If KDM is able to determine your proxy server's address and no authentication is required then KDM will read this information and connect to the internet as normal.

- If KDM is able to determine your proxy server's address but the proxy requires authentication then you will need to enter your credentials in the window that appears.

- If KDM is unable to determine your proxy server's address then you will need to enter the proxy server address, proxy type and credentials:
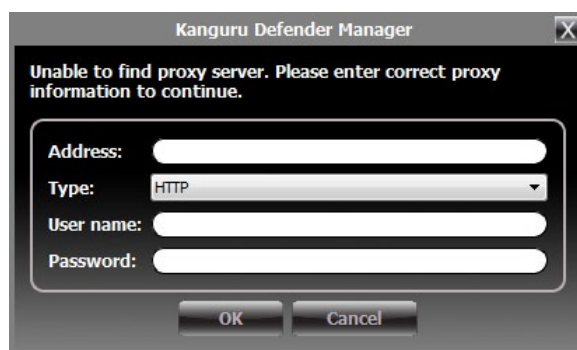
Enter the proxy address and the port to connect to in the address field (e.g. 192.168.0.193:8080 or proxycomp:8080). Select your proxy type and then enter your credentials. If KDM is able to connect to the proxy server using those credentials then the authentication information is saved in an encrypted proxy settings file on the host computer.

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