Defender Bio-Elite30
User Manual

For Models:
- Defender Bio-Elite30

NOTICES AND INFORMATION

Please be aware of the following points before using your Kanguru Defender Bio-Elite30

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 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

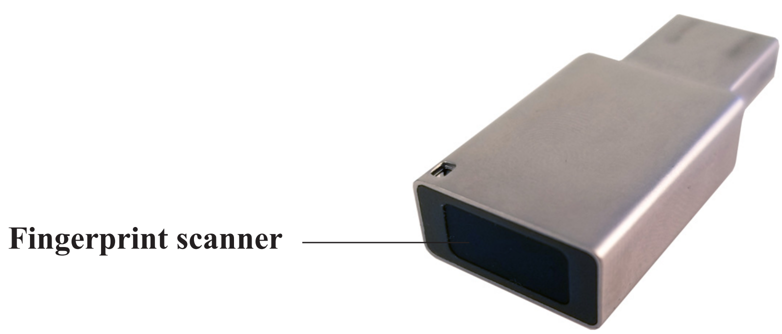
1. Introduction

The Kanguru Defender Bio-Elite30 flash drive is a hardware encrypted, tamper proof USB flash drive with a high-resolution, biometric scanner. The Defender Bio-Elite30 contains two partitions: a virtual DVD-RW partition and a secure, encrypted storage partition. The virtual DVD-RW partition contains the Kanguru Defender Manager Bio application (referred throughout this document as KDMBio) that allows you to configure and manage the device. The secure storage partition is where your data will be encrypted and saved.

The Kanguru Defender Bio-Elite30 flash drive secures your sensitive data using:

- 256-bit AES hardware encryption
- Secure password protection

In addition to secure password authentication, the Defender Bio-Elite30 features a high-resolution biometric scanner located on the rear of the drive that allows you to gain access to device using a registered fingerprint.



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.

- Defender Bio-Elite30 Flash Drive
- 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

2. First Time Setup

While the Defender Bio-Elite30 can be configured for use with any operating system, the initial setup requires running the KDMBio application on a Mac or Windows based computer.

To configure your Defender Bio-Elite 30 for use:

1. Insert your Defender Bio-Elite30 device into an available USB port.

2. Locate and open the Defender Bio-Elite30 DVD-RW drive and then run the **KDMBio application.**

3. The Welcome Screen appears asking you to choose how you want the device to behave:

   ○ **Autoscan Enabled -** When the box is checked, the device will run in Autoscan mode. KDMBio only needs to be run once on a supported Windows PC or Mac to register at least one fingerprint. Afterwards, you will be able to access the secure storage partition using only a fingerprint scan. You will only need to run KDMBio to configure or manage AV, KRMC, SSPM, or fingerprints.

   ○ **Autoscan Disabled -** When the box is unchecked, the device is running in standard mode. You will be required to run KDMBio to access the secure storage partition. Since KDMBio is always needed in this configuration, the drive will only work on a supported Windows PC or Mac. This is typically only recommended for devices managed using KRMC.

Click on the **Next** button to continue setting up your Defender Bio-Elite30.

4. Enter a device name, phone number and primary email address in the appropriate fields and then click on the **Apply button**.

After your contact information has been added to your device you will be able to click on the **Next button** to proceed**.**

5. Enter a security password in the 'Password' field, and then enter it again in the 'Confirm Password' field. Your password must contain at minimum eight characters including at least one uppercase letter and one number.

Note: You can enter your password using KDM's Virtual Keyboard by clicking the **Virtual Keyboard icon** located to the left of the **Save button**.

6. If the passwords entered match and meet the minimum requirements, you will be able to click the **Save button**.

7. Click on the **Next button** to begin enrolling fingerprints.

8. On the fingerprint enrollment screen, click on the circle located over the finger that you are enrolling. A dot will appear within the center of the circle to signal that it is selected.

9. Configure permissions given when logging in with this fingerprint.
   - **Manage fingerprint registration** - When checked, logging in with this fingerprint will allow you to manage other fingerprints registered with this device.
   - **Login with Write Protection -** When checked, logging in with this fingerprint will allow access to the secure storage partition with read-only permissions.

10. Click the **Enroll button** to start scanning your fingerprint.
    Note: You must enroll at least one fingerprint to use the device. You can only enroll one fingerprint at a time.

11. Using the selected finger, tap the scanner located on the back of the drive repeatedly until you see a green, fingerprint image begin to appear.

12. Once the fingerprint image is fully formed, a message will appear notifying you that fingerprint registration was successful. Click **OK** to continue.

You can enroll up to 6 fingerprints, each with their own permission configuration.

- A hollow circle above a finger indicates that it has not been registered.
- An icon appearing within the circle above a finger indicates that it has been registered. The icon displayed within the circle varies based on the permissions set for that fingerprint:
    -  - Able to manage fingerprints with read/write access for secure storage partition
    -  - Able to manage fingerprints with read-only access for the secure storage partition
    -  - No fingerprint management with read/write access for the secure storage partition.
    -  - No fingerprint management with read-only access for the secure storage partition

As long as there is more than one fingerprint registered, you can delete a registered fingerprint by selecting it and then clicking the **Delete button**.

13. Once you have completed registering your fingerprints, click on the **Finish button** to finalize setting up your Bio-Elite30 drive.

3. Logging In

After you have set a password and registered your fingerprint(s), you will have to either enter your security password or scan a fingerprint in order to access the secure storage partition.

If the device was configured with Autoscan Disabled then you will always be required to login through KDMBio. If your device was configured with Autoscan Enabled, then you only need to login through KDMBio for AV, KRMC, SSPM, or fingerprint management (see Ch.2. First Time Setup on page 5).

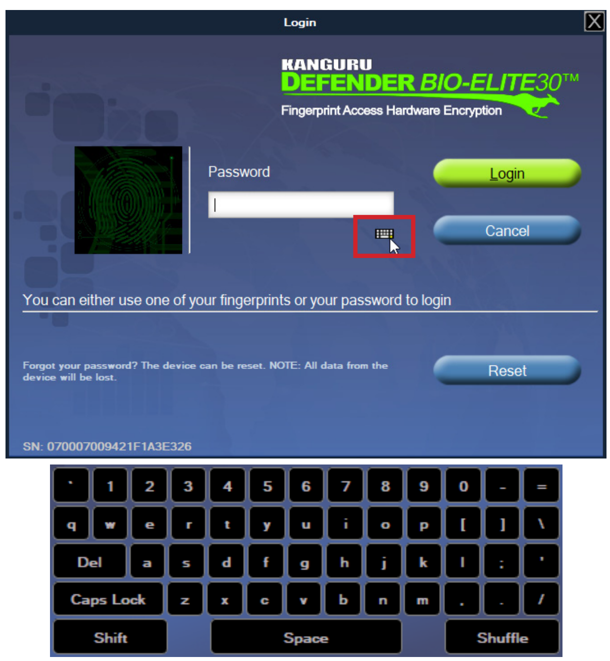
3.1 Login Through KDMBio (Windows and Mac)

1. Insert your Defender Bio-Elite30 device into an available USB port.

2. Locate and open the Defender Bio-Elite30 DVD-RW partition in file explorer and run **KDMBio**.

3. The Login screen appears. You can either scan a registered fingerprint or enter your security password in the 'Password' field.

   Note: To prevent keystroke loggers from potentially spying your security password, you can access a virtual keyboard to enter your password using your mouse. To open the virtual keyboard, click the **Virtual Keyboard icon** located underneath the 'Password' field.



4. If you entered a password, click on the **Login button**. If you scanned a registered fingerprint it will be accepted automatically.

The Command Console launches and the secure storage partition is unlocked.

3.2 Login Using Fingerprint Only

If you only need to access the secure storage partition and your device is set with Autoscan Enabled, then you can unlock the secure storage partition using only a registered fingerprint. Since you are not running the KDMBio application, you can use this method to log in to the device on any operating system.

Note: When logging in using only a fingerprint, you will not have access to AV, KRMC, SSPM, or fingerprint management. Logging in using only a fingerprint is not possible if Autoscan is disabled.

To access the secure storage partition using only your fingerprint:

1. Insert your Defender Bio-Elite30 device into an available USB port.

2. Use one of the fingers that you registered during the first time setup to tap the scanner on the back of the Bio-Elite30 device.

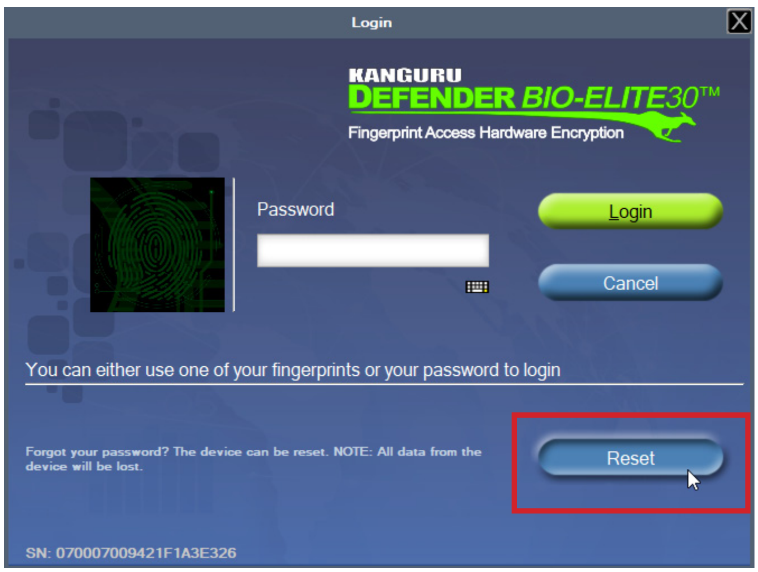
The secure storage partition unlocks and you are now able to access it as normal.

3.3 Resetting the Device

Resetting the device will permanently delete all personal data stored within, erase your security password, erase all registered fingerprints and reset the device back to it's factory-setting state. Resetting should only be performed if you have forgotten your security password or if the device is not functioning correctly.

To delete all personal data and reset your device back to the factory state:

1. Locate and open the Defender Bio-Elite30 DVD-RW partition in file explorer and run **KDMBio**.
2. The Login screen appears. Click the **Reset button.**
3. Confirm the reset by selecting **Yes** when asked if you are sure you want to reset the device.



4. The Command Console

If you used KDMBio to log into your Defender Bio-Elite30 device, the Command Console appears.

If the Command Console doesn't automatically appear, you can launch it by clicking the Kanguru icon located in the taskbar area on Windows or the menu bar area on Macs.

Note: Command Console will only launch if you used KDMBio to login to your device.

4.1 View Encrypted Files

A key feature of the Defender Bio-Elite30 drive is drag & drop encryption; allowing you to simply drag files that you want encrypt directly onto the drive. The device automatically encrypts these files as they are transferred to the secure storage partition, ensuring that your data stays safe and private.

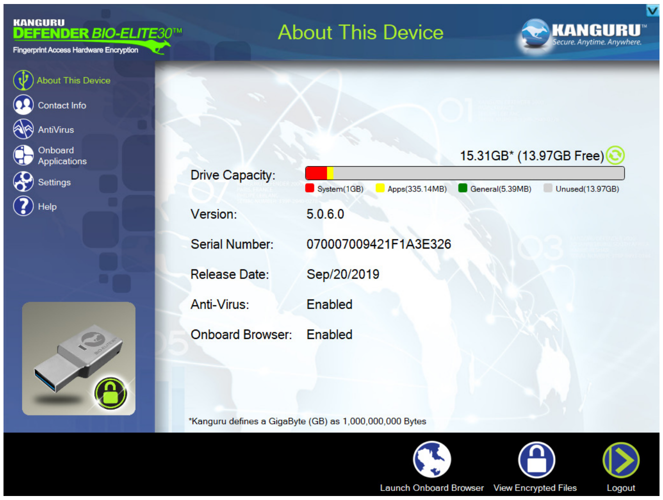
To open the secure partition, click on **View Encrypted Files** from the menu bar at the bottom of the Command Console.

The secure storage partition opens in a new file explorer 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 to the secure storage partition is only accessible after you have successfully logged into the device.

4.2 About This Device

Click on **About This Device** from the menu bar on the left of the Command Console to view basic information about your drive including: details about used/remaining/total storage capacity, firmware version, serial number, release date and whether Antivirus and/or Onboard Browser are enabled.



4.3 Contact Info

Click on **Contact Info** from the menu bar on the left of the Command Console to view the contact information saved to this device.

You can edit the contact information here by updating any of the fields and then clicking the **Save button.**

4.4 Antivirus

Click on **AntiVirus** from the menu bar on the left of the Command Console to access the Defender Bio-Elite30's onboard, antivirus service. The onboard antivirus is a subscription based service and requires a license key. If you do not have a license key you can click on the **Get AV button** to purchase an antivirus license from Kanguru, or to apply a license that you have already purchased from Kanguru.

Once you have received an AntiVirus license key from Kanguru, copy the license key into the 'New License Key' field and then click the **Apply button**.

Once your on-board antivirus license has been activated, antivirus functionality and real-time virus scanning is automatically enabled. All files copied to the secure storage partition will be scanned for viruses and malware.

Note: Real-time scanning is enabled only once all virus definitions have been downloaded. 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.

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

Caution! Do not delete the virus definition files stored in the 'System' folder in the secure storage 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.

4.5 Onboard Applications

Click on **Onboard Applications** from the menu bar on the left of the Command Console to access the applications that can be run securely from the Defender Bio-Elite30.

Each Onboard Application has two buttons:

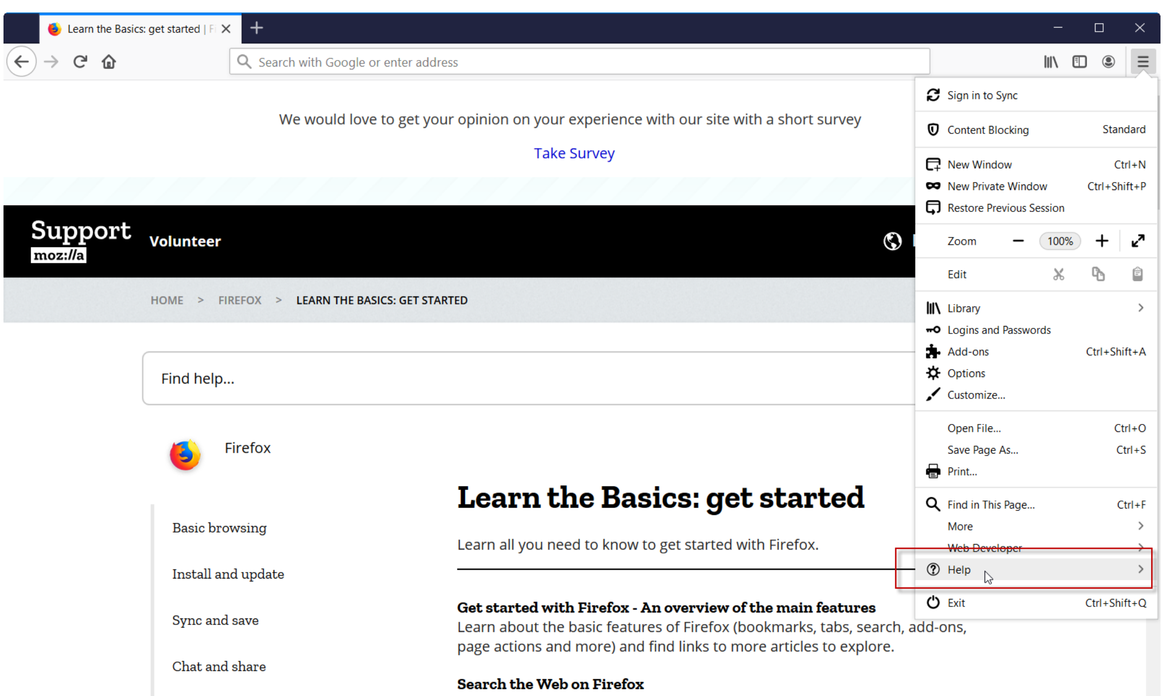
- **Start** - Launch the application
- **Manage** - Allows you to:
  - **Reinstall Now** - Reinstall the application in case it is not functioning properly
  - **Update Now** - Update the application if a new version of the application is available

4.5.1 Onboard Browser

One of the main features of the Defender Bio-Elite30 is the secure, onboard web browser. The onboard web browser runs Mozilla FireFox completely self-contained within the Defender Bio-Elite30 device. Browsing history, bookmarks, stored passwords and any information saved within the onboard browser is only accessible by first logging into KDMBio.

Click on the **Start button**, or the **Onboard Browser icon**, or **Launch Onboard Browser** to start the onboard browser.

The onboard browser to opens in a new window. It functions the same as a normal FireFox web browser. For more information about using FireFox, visit the Mozilla website or refer to the browser's help file:



4.6 Settings

Click on **Settings** from the menu bar on the left of the Command Console to manage passwords, fingerprints, KRMC and other settings.

4.6.1 Change Password

Click on the **Change Password tab** within the Settings menu to manage the password that you use to login to KDMBio.

To change your KDMBio login password:

1. Enter the current login password into the 'Old Password' field.

2. Enter a new password in the 'New Password' field, and then enter it again in the 'Confirm New Password' field.

3. When your entered passwords match and meet the minimum requirements, you will be able to click the **Save button**.

   Note: You can enter your password using the Virtual Keyboard by clicking the **Virtual Keyboard icon** located to the left of the **Save button**.

Your KDMBio login password has successfully been changed.

4.6.2 KRMC

Click on the **KRMC tab** within the Settings menu to register your device with a KRMC Cloud account.

Note: If the KRMC tab is not visible within the Settings menu then the device is already registered with a KRMC Cloud account.

To register your device with a KRMC Cloud account:

1. Click on the **Enable KRMC icon** to enable KRMC management on the device. The device can now be registered and managed with a KRMC Cloud account.

2. Enter the Cloud ID for the KRMC Cloud account that will be managing the device into the corresponding field and then click on the **Verify button**.

The device is now registered with the KRMC Cloud account and the KRMC tab will no longer be visible in the Settings menu.

4.6.3 General

Click on the **General tab** within the Settings menu to configure the following settings for your device:

- **Minimum Password Length** - Number of characters a KDMBio login password must contain in order to be valid.
- **Application Language -** The language that KDMBio text and menus will be displayed in.

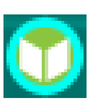
- **Proxy Settings -** If your device connects to the internet through a proxy (e.g. to download antivirus definitions or to communicate with KRMC), enter the proxy server information in the appropriate fields and then click the **Save Proxy button**.

4.6.4 Fingerprints

Click on the **Fingerprints tab** within the Settings menu to manage fingerprints registered with your device or to enroll new fingerprints.

You can have up to 6 fingerprints registered at any time, each fingerprint with their own permissions configuration. A hollow circle appears above each finger that is free to be enrolled.

An icon appears within the circle above each finger that has a registered fingerprint. The icon indicates the permissions configuration for that fingerprint:

-  - Able to manage fingerprints with full read/write access to secure storage partition
-  - Able to manage fingerprints with read-only access to the secure storage partition
-  - No fingerprint management with full read/write access to the secure storage partition.
-  - No fingerprint management with read-only access to the secure storage partition

To manage fingerprints, click on the circle located over a finger to select a fingerprint to manage. A dot will appear within the center of the circle to signal that it is selected.

If you are enrolling a new fingerprint:

1. Configure the permissions granted when logging in with this fingerprint.
   - **Manage fingerprint registration** - When checked, logging in with this fingerprint will allow you to manage fingerprints registered with the device.
   - **Login with Write Protection -** When checked, logging in with this fingerprint will allow access to the secure storage partition with read-only permissions. .

2. Click the **Enroll button** to start scanning your fingerprint.

3. Use the selected finger to tap the scanner located on the back of the drive repeatedly until you see a green, fingerprint image start to appear.

4. Once the fingerprint image is fully formed, a window will appear notifying you that fingerprint registration was successful. Click **OK** to continue.

If there is more than one fingerprint currently registered, you can delete a registered fingerprint by selecting the circle above the registered finger and then clicking the **Delete button**.

5. Logout and Removing the Device

You should always safely unmount the secure storage partition before disconnecting the Bio-Elite30 from the computer. Do not attempt to remove the device while an application is accessing data on the secure storage partition. Doing so may result in the partition becoming corrupted and potential data loss.

The process for removing your device safely will be different, depending on whether or not you ran KDMBio to access the secure storage partition.

Logging out and unmounting through KDMBio

If you logged in through KDMBio, you can safely logout and unmount the secure storage partition by clicking the **Logout button** located at the bottom right of the Command Console window. Once the Command Console window closes, you can safely disconnect the Bio-Elite30 drive from the computer.

Unmounting through the Operating System

If you only used a fingerprint to access the secure storage partition, without running KDMBio, you should follow the operating system's instructions for safely removing a USB storage device to unmount the secure storage partition before disconnecting the Bio-Elite30 drive from the computer.

6. Warranty Information

All Defender Bio-Elite30 flash drives 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 Bio-Elite30 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

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