Warranty Information

This product carries a 1-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 of receipt of merchandise.

Specifications

Weight: 10 grams
Power Requirements: 266 mA
Type: 256-bit AES Hardware encrypted USB drive

- FIPS 140-2 Level 3 Certified (Pending)
- Common Criteria EAL 2+ (Pending)
- US DoD DIACAP Certified (Pending)
- Tamper Resistant

Contact Information

Sales:	1-888-526-4878
Headquarters:	1-508-376-4245
Fax:	1-508-376-4462
Technical Support:	(800) 603-3589
Support:	**techsupport@absolute-id.com**

VIRTUAL DEFENDER
QUICK START GUIDE

Package Contents

- Virtual Defender Flash Drive
- Quick Start Guide
- Registration Form

Minimum System Requirements

- x86-compatible processor
  - Recommend 1.6 GHz dual-core or better
- 1 GB memory
- 1 USB 2.0 port
- Network support (either wired or wireless)

Introduction

Introduction

Thank you for choosing the Virtual Defender Secure Mobile USB drive, the world's premium, secure, mobile-computing platform, providing advanced solutions for the top security threats faced by the Financial-services industry.

This device provides the ultimate in convenience, portability and security. Utilizing a FIPS-certified, bootable, hardware-encrypted, and tamper-proof architecture, your new drive can be connected to a host computer and run completely independent from that system, thereby providing an autonomous and secure solution that will leave no trace on the host system.

1 Setup System BIOS to Boot from USB

The host computer must be configured to boot from a USB storage device in order to run the Virtual Defender drive. Follow these steps to configure your BIOS:

1. Turn on the host computer system.
2. Watch the screen and follow the instructions to enter the system BIOS settings. Press the Pause key if it goes by too fast to read. You can also check the computer's manual for BIOS details and access information.
3. Press the designated key to enter the BIOS (usually **ESC**, **DEL**, or a function key such as **F1** or **F2**).
4. Set the computer to enable booting from USB drives or ports.
5. Set the boot order to boot from USB prior to booting from the Hard Drive.
6. Save and exit the system BIOS and reboot.

2 Boot Virtual Defender Drive

Once your BIOS has been configured follow these steps to boot your Virtual Defender:

1. Turn off the host computer system.
2. Insert the Virtual Defender into an available USB 2.0 slot. USB 3.0 ports are not supported.
3. Power the system on.
4. A dialog titled **Virtual Defender Authenticator** will be displayed. Enter the drive password, and press the <**Enter**> key or click the [**Login**] button.
   *Note: the default password is "**password**".*
5. The first time you access your drive, the End User Licensing Agreement (EULA) will be presented. Click the [**Accept**] button to accept the EULA.
6. A dialog will be displayed with a boot message and the system will start.
7. The Virtual Defender Runtime Environment will then boot from the secure, encrypted partition.

The runtime environment comes preconfigured with the following components and services:

- **Google Chrome Browser:** An Internet browser, pre-configured to run in incognito mode. The browser comes pre-configured with the following browser extensions: Google Virtual Keyboard and Applet2Object.
- **Google Virtual Keyboard:** This extension provides the ability to enter confidential information, such as user IDs and passwords, by clicking on the image of a keyboard. This eliminates the ability for hardware key loggers to record user key strokes, and protects the end user's information.
- **Adobe Reader:** This allows the viewing of local PDF files.
- **Remmina Remote Desktop Client:** Remmina Client version 0.7.4. Kanguru does not provide this service but can direct you to third party who does- http://remmina.sourceforge.net/
- **Gnome Network Manager:** Gnome Network Manager is version 8.4 with Network Manager PPTP Version 8.1. Kanguru does not provide this service but can direct you to third party who does- http://projects.gnome.org/NetworkManager/

3 Changing the Drive's User Password

Follow these steps to change the user's password on the Virtual Defender Drive:

1. At the Virtual Defender Authenticator screen, select the System → Change Password menu option.
2. Fill in the Change User Password dialog and press the <**Enter**> key or click the [**Change**] button.

4 Connecting to the Network

The drive is preconfigured to connect to wired network. For wireless networks, a warning dialog will be presented if an access point hasn't been selected. Perform the following to set up a wireless network:

1. In order to select and configure a wireless network, or other network configuration, locate and press the left mouse key on the Network icon in the upper bar of the Desktop.
2. Select and click on an available wireless network to set up the network configuration settings and connect to the network. The network icon in the top panel will change when you have connected to a network.
3. Once you have a network connection, click the [**Retry**] button in the Virtual Defender Warning Message box. The box will disappear. Pressing the **Shutdown** button will power down the system.
   Note: If no networks are displayed, ensure the wireless network adaptor is enabled on the host system. To do this, right click the network icon to see if wireless is enabled. On some systems there is physical switch that can be used to turn on and off the wireless radio. Make sure this switch is turned to the "on" position.

5 Using the Secure Browser

The Virtual Defender includes a secure Google Chrome browser that is run in Incognito mode, so that no data is stored between sessions. To launch the browser, click the browser icon in the top left corner or on the desktop. Once the browser is launched, the user may change the home page by selecting the wrench icon in the top right corner of the browser and then select Preferences. A dialog box will appear which will allow customization of the browser. Regularly accessed web sites may be bookmarked by clicking the star icon and fill in Bookmark dialog box.

6 Shutting Down the System

In order to shut down the system, press the **Shutdown** button in the top right panel of the screen. This will turn off the entire computer.