ABSOLUTE ID

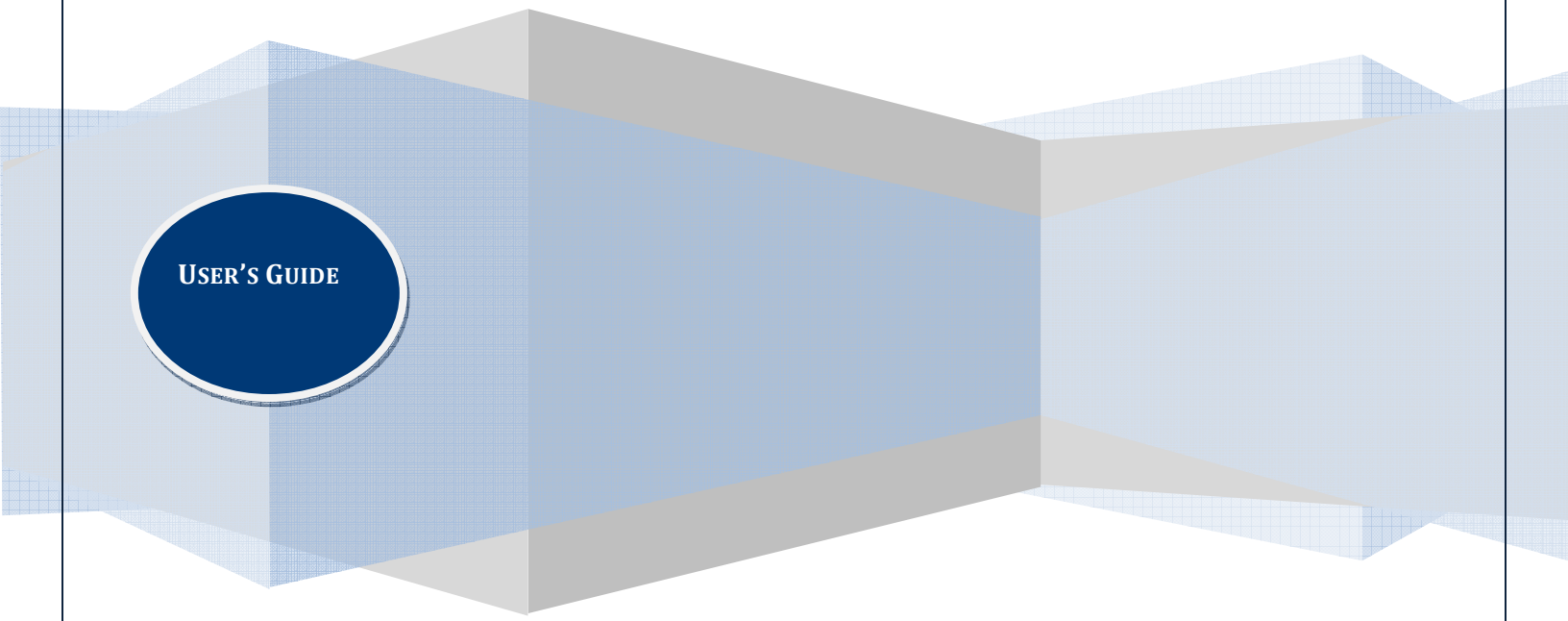
When You Absolutely Need to Know!

KANGURU Solutions™

"Technology on the move!"

RocIT™ Defender User's Guide

ViSoS™ – Virtual System on a Stick



USER'S GUIDE

Table of Contents

1. Introduction 3
    1.1. Minimum System Requirements 3
    1.2. Drive Specifications 4
2. Startup Procedure 4
    2.1. Configure computer BIOS to boot from USB 4
    2.2. Authentication Process 5
    2.3. Changing the Drive Password 7
3. The Preloaded Virtual Machine and Operating System 7
4. ViSoS™ Runtime Environment (VRE) 8
    4.1. VRE Overview 8
    4.2. Virtual Machine Manager (VMM) – Oracle VirtualBox 8
    4.3. Accessing the VRE 9
5. VM Taskbar Menus 10
    5.1. Machine Taskbar Menu 12
    5.2. Devices Taskbar Menu 13
6. Installing a New Guest Operating System 13
    6.1. Creating a New Virtual Machine (VM) 13
    6.2. Installing a New Guest Operating System 17
7. Attaching USB Devices and Printers 17
8. Windows Tuning Tips 18
    8.1. Set Swap File to 200MB 18
    8.2. Set Automatic Updates for Windows to Download and Notify 19
9. Setting up Network Connections 19
    9.1. Setting up Wireless Network 19
10. Windows Activation 21
11. Warranty Information 21
12. Technical Support 21

1. Introduction

Thank you for choosing the Kanguru RocIT Defender USB drive, the world's premier, secure, mobile computing platform.

The technology incorporated into this device provides the ultimate in convenience, portability and security. Utilizing a bootable, hardware encrypted, tamper proof architecture, this drive can be connected to a computer and run completely independent from that system, thereby providing an autonomous and secure solution that will leave no trace on the host system once it is shutdown and disconnected/removed.

The drive comes equipped with a virtualized Windows operating system (demo version) that is integrated within a Virtual Machine Manager. A different operating system may also be installed and activated. Currently 32 bit Windows XP, Vista and Windows 7, as well as Linux are supported. A virtual machine (VM) is a special environment that is created where a guest OS may be run. In other words, the guest operating system is run within a VM.

Since the drive is compatible with multiple OS's running under this Virtual System on a Stick (ViSoS) environment, any applications which are supported by each operating system may be run within the VM, as drive space allows of course. The ViSoS Runtime Environment (or VRE) on the drive provides a secure area within the drive from which multiple Guest operating systems can be installed and managed. The VRE also provides a convenient mechanism for switching among each OS that has been loaded and is running on the drive.

This guide covers the initial configuration of the drive, and details regarding key functions and operations. Please be sure to read this entire guide to ensure you will get the most out of the drive's unique features and important operational processes.

1.1. Minimum System Requirements

The RocIT Defender drive is a self-contained virtual platform that can be connected to a computer and operated independently from that computer's hard drive and operating system. The USB drive will make use of the computer's hardware resources: processor, memory, ports and attached or networked devices. When removed from one computer and then transported and connected into another computer (office/home/etc.), it will then make use of the resources of that computer. As such, the operating system(s) on the RocIT Defender drive will be subject to the limitations of each computer it is connected to, such as variations in the amount of RAM, which may affect the performance of applications installed on the USB drive.

The following are the recommended minimum requirements of the host computer system which the drive runs upon:

- X86-based processor
- 2 GB RAM
- USB 2.0 port
- LAN/WAN Card: 10/100baseT support

1.2. *Drive Specifications*

- **Weight:** 10 grams
- **Power Requirements:** 266 mA
- **Type:** 256-bit AES Hardware encrypted USB drive
  FIPS 140-2 Level 2 Certified
  US DoD DIACAP Certified
  Tamper Resistant
- **Capacity:** 16 GB - 128 GB
- **Certifications:** FIPS 140-2 Level 2 (RocIT Defender Elite model only)

2. *Startup Procedure*

The following steps are required in order to start up and boot a host computer system:

1. Configure computer BIOS to boot from USB drive.
2. Boot the RocIT Defender drive
3. Authenticate to the drive

2.1. *Configure computer BIOS to boot from USB*

The BIOS settings of most computers may need to be configured to boot to the USB drive first. When using the RocIT Defender drive, it will completely bypass the regular computer system (eg. – it will not be accessing the computer's C:\ drive), so it will not be booting into the operating system installed on the computer. **Note:** RocIT Defender drive must be connected to computer prior to boot up.

Refer to the computer's manual for instructions on how to access and configure the computer's BIOS settings. If the computer manual is not available, check with the manufacturer for an online version. If using a corporate computer, permission from the System Administrator may be required to access the computer BIOS settings.

Another way to determine how to access the BIOS area is to watch the initial characters that appear on the screen when the computer is first booted. A couple of lines will usually appear for a brief moment that will tell which key (or sequence of

keys such as <ESC>, <DEL>, or <F1>, <F2>) to press on the keyboard in order to access the BIOS settings. Press the specified key before the computer begins to load its default operating system. If it begins loading the default OS before the BIOS is started, shut down and reboot the computer.

Once in the BIOS area, change the boot order so that the system attempts to boot from a USB drive prior to booting from the system's internal hard drive. To do this, look for the "Boot Priority" settings (or something similar) and change it to move the "Kanguru USB drive" to position # 1 in the boot sequence. Save the changes, exit the BIOS, and reboot if necessary. Additionally, there may be an option to select the boot order. Set the boot order to boot to USB prior to booting to other media such as hard disk, CD / DVD ROM, etc.

A few things to note about BIOS settings:

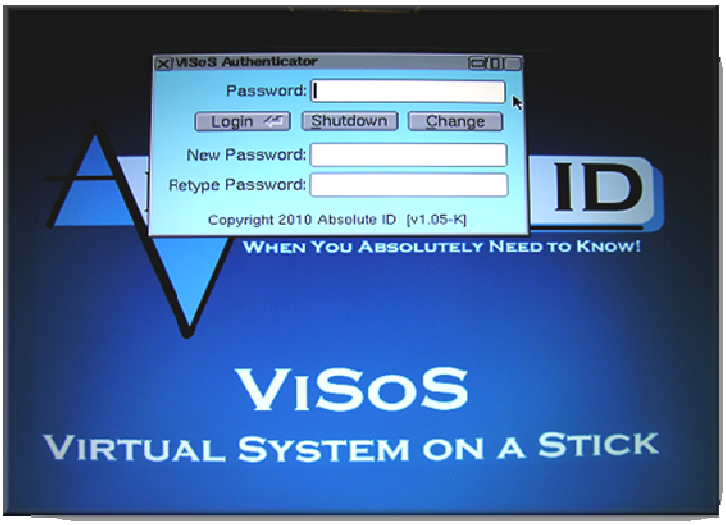
The BIOS may have 2 different areas which need to be changed to boot to the USB drive.

1. Look for a setting area that indicates "Boot Priority".
2. Also look for a setting/option that shows something similar to "Hard Disk Drives". This will show the drives that the BIOS system recognizes and will also need to have the "Kanguru USB drive" or "USB Drive" placed in the # 1 position.

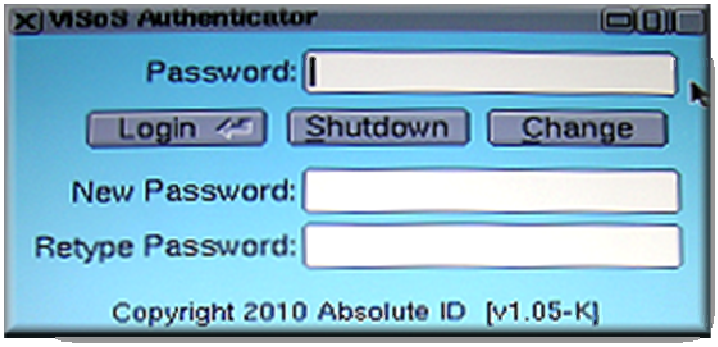
After saving and exiting the BIOS, the system should now boot from the RocIT Drive inserted into the USB port. The settings should have been saved, however it has been found that some computers require that the BIOS is reconfigured for subsequent boots.

2.2. *Authentication Process*

Once the BIOS settings have been properly configured, or if the computer automatically boots directly from the RocIT Defender drive, the ViSoS Authenticator screen will be displayed.



ViSoS Authenticator screen



At the ViSoS Authenticator screen, enter the drive password in the password field and then click on the **<Login>** button.

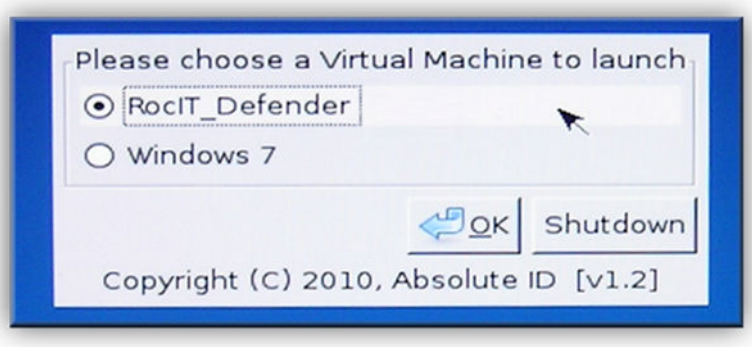
The default password is: **password**

To change the password, refer to section 2.3 on page 7.

If this is the first time logging in through the ViSoS Authenticator, it will prompt you to accept the End User License Agreement (EULA). This will only need to be accepted once and will not appear again during the next login session.

After accepting the license agreement, a "**Booting ViSoS…**" message will appear, and then the Absolute ID splash screen. The RocIT Defender's default virtual machine

and operating system will now be loaded. If more than one virtual machine is loaded on the drive, then a dialog box with a choice of which virtual machine (VM) to load will appear (see image below). Select the VM and click **<OK>** to continue loading the VM (Windows XP).



Congratulations, the RocIT Defender drive is now ready to be used.

2.3. *Changing the Drive Password*

The drive is initially configured with the default password "**password**", or with a password specified by your Systems Administrator. The following procedure provides the steps for changing this password:

1. At the **ViSoS Authenticator** screen (see section 2.2 on page 6), enter the current password into the "Password" field. The default password is: **password**
2. Enter the new password into the "New Password" field, and then confirm it by entering it again in the "Retype Password" field.
3. Click on the "Change" button to set the new password.

Note: After the new password is entered in the "New Password" and "Retype Password" fields, click on the **<Change>** button. Do not press the **<Enter>** button on your keyboard instead of clicking on the **<Change>** button, as this will default to the **Login** action and will not change the drive password.

3. *The Preloaded Virtual Machine and Operating System*

The RocIT Defender drive comes preloaded with a Windows XP operating system within a **RocIT_Defender** virtual machine (VM). This is a demo version/license of Windows XP. Once the drive has been booted and has loaded the operating system, the OS can be customized and additional applications can be installed and run as they normally would within Windows XP.

4. ViSoS™ Runtime Environment (VRE)

4.1. VRE Overview

The VRE (ViSoS™ Runtime Environment) is a hardened environment that has undergone extensive security-enhancing customizations. It is a secure, locked down, Linux-based operating system that has passed thousands of Department of Defense tests to ensure that the environment is protected against most security threats.

When the end-user boots and authenticates to the drive, the VRE is booted from the secure encrypted partition. End-users do *not* have access to the underlying runtime environment or file system. They are *only* provided with the minimum privileges necessary to run the applications that are configured and deployed for the specific customer solution, including Oracle VirtualBox Virtual Machine Manager (VMM). This means that the administrator can configure the drive and limit the end-user's ability to access items within the VRE. The RocIT Defender solution does, however, provide an administrative login capability that enables an administrator, who has the password, access to the underlying VRE and file system and the ability to debug and/or customize a particular drive. **Note:** Performing any *specific drive* customization should not be required, and is not recommended. All configuration and/or application or module changes should be made against a master RocIT image and pushed out to all end-user drives through the centralized RocIT*Safe Update Service.*

When the VRE is first started, it will perform a lookup against the enterprise's (or Absolute ID's) update service to determine if any updates are required. If there are any updates, the VRE update module will automatically download and install the updates onto the specific user's drive.

Additionally, the VRE provides the ability to perform advanced configuration and customizations, including the ability to customize the network interface, drivers, and end-user applications.

4.2. Virtual Machine Manager (VMM) – Oracle VirtualBox

The VRE comes preconfigured with Oracle VirtualBox version 3.2.10 Virtual Machine Manager (VMM) and one or more guest operating systems (Virtual Machines – VM's) within the Bootable version of the application. Refer to http://www.virtualbox.org/ for information on utilizing Oracle VirtualBox. Currently, the only VMM (also known as a hypervisor) supported is Oracle VirtualBox. The VMM within the VRE is configurable and supports the ability to dynamically or statically define rules and settings such as:

- Dynamic attachment and support of external smart card readers (SCR's).

- Dynamic attachment and support of one or more network adapters in bridged or NAT'd (Network Address Translation) mode.
- Ability to specify minimum and maximum memory configurations and settings.
- Dynamically configuring a MAC Address from the drive Serial Number. This enables the ability to control and monitor each drive via the MAC Address regardless of the physical NIC card being utilized in the host computer system.

The VRE provides the ability to support multiple Virtual Machines (VM's) that are configured differently or run within different environments. Each VM can be a pre-loaded image or can be loaded via an automated deployment and build process, which will install end-user Windows applications into the guest operating system.

4.3. *Accessing the VRE*

When the RocIT Drive is first booted, it will either boot directly into the Windows guest operating system, if a single virtual machine (VM) is configured, or it will display a VM Selection dialog to enable the ability to select a VM from those configured on the drive.

In the default configuration, the VRE Desktop is accessible to all users, but can be locked down as required for delivery to the enterprise. In order to better understand the architecture of the solution, it is important to understand the following aspects:

- The Windows Guest OS (Virtual Machine) runs within the Oracle VirtualBox VMM (Virtual Machine Manager) that is installed on the VRE. In other words, Windows is running within the Linux-based VRE operating system.
- There are three virtual terminals available (VT1, VT7, and VT8), that can be accessed by using the following key combinations (**<Ctrl><Alt><F1>**, **<Ctrl><Alt><F7>**, and **<Ctrl><Alt><F8>**) respectively.
  - **VT1 – Admin Console**: This console provides a command-line terminal console that ONLY the admin user of the VRE can log into.
  - **VT7 – VRE Desktop**: This runs the VRE Desktop GUI interface from which the user can access and modify VRE and/or VM settings.
  - **VT8 – VM Desktop**: The end user virtual machines run within the VT8 Desktop.
- Modification of a VM's configuration can ONLY be performed when the Guest VM is not running.

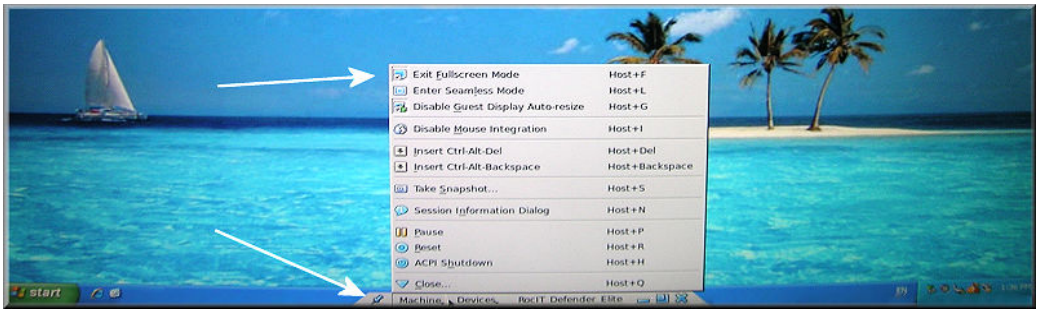
- Shutting down the VM, if only a single VM exists, will shut down the computer, *unless* the VRE admin user is logged into the VT1 terminal.

Thus, if a VM needs to be modified and/or added, it will require that the end-user have the **admin** password and log onto the VT1 terminal with **<Ctrl><Alt><F1>**. After the admin is logged onto the VT1, the user can then switch back to the VT8 window with **<Ctrl><Alt><F8>** and shut down the Windows virtual machine as normal, and the computer will not shut down. The user may then switch to VT7 to access the VRE Desktop to perform system configuration changes, such as running Oracle VirtualBox from the **Applications → System Tools → Oracle VM VirtualBox** menu.

Note: In the current version of RocIT Defender, wireless network access is controlled by accessing VT7 and configuring the network within the VRE. The network will be passed through automatically to the running Guest operating system. *It is NOT required that the Guest OS be shut down to configure or change network settings.*

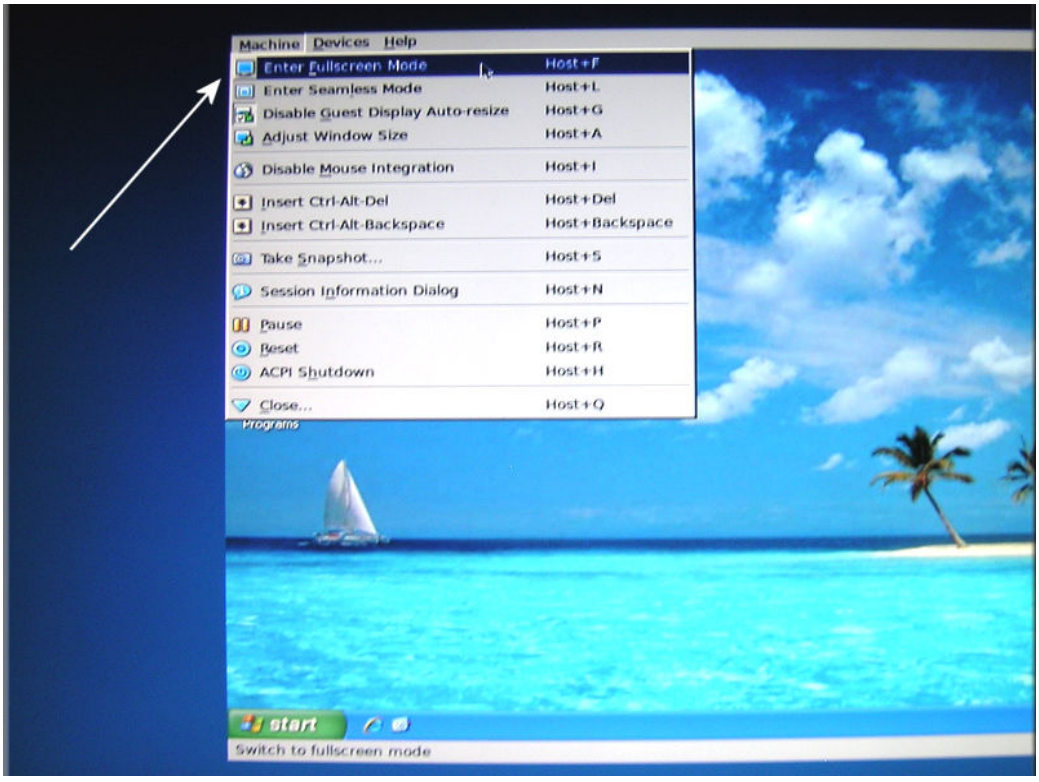
5. VM Taskbar Menus

Because the operating system (OS) of the RocIT Defender drive is running within a virtual machine (VM), a Taskbar Menu is available once the OS is loaded. When the OS is running in **Full Screen Mode** (the default setting), the VRE taskbar menu can be found at the bottom of the screen. The mouse may need to be moved to the bottom of the screen to unhide it and bring it into view. In order to have the menu remain visible, click on the **Pin icon** (left side of the taskbar) to dock the taskbar and have it remain in view when the mouse is moved off the VRE taskbar.



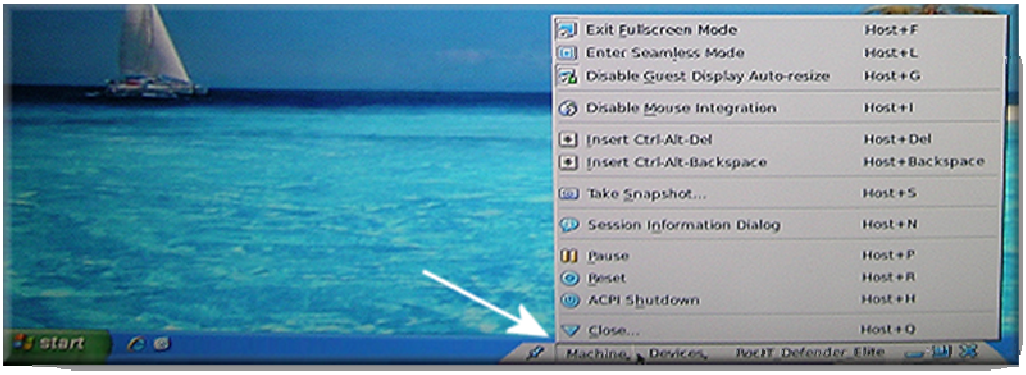
Full Screen Mode: the VRE taskbar is located at the bottom of the screen.

If the OS is running in **Seamless Mode**, the menu will appear as a window within the screen. To set it back to a more useful view, click on the "**Machine**" menu item in the taskbar (top-left of the window) and select <**Enter Fullscreen Mode>**.



Seamless Mode: the VRE taskbar is located at the top-left corner of the screen.

There are three menus in the taskbar menu: **Machines, Devices** and **Help**. The following sections provide details about the Machines and Devices taskbar menus and the options available under each item.

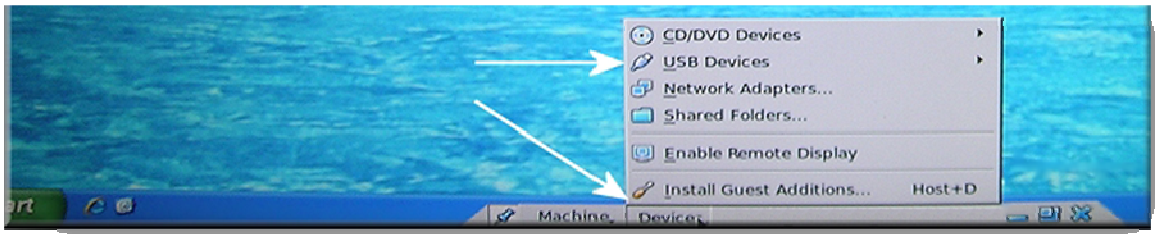


Machine Taskbar Menu

5.1. *Machine Taskbar Menu*

- **Enter/Exit Fullscreen Mode** – Switch between viewing the virtual machine in full screen or Seamless/windowed mode.
- **Enter/Exit Seamless Mode** – Seamless mode allows your host operating system to operate in tandem with a virtual operating system.
- **Enable/Disable Guest Display Auto-resize** – Not applicable to RocIT Defender.
- **Enable/Disable Mouse Integration** – When enabled, the user will be able to control the taskbar menus and the virtual machine using the mouse. When disabled, the user will only be able to control the virtual machine.
- **Insert Ctrl-Alt-Del** – Use this option instead of pressing **<Ctrl><Alt><Del>** to launch Windows' Task Manager.
- **Insert Ctrl-Alt-Backspace** – Use this option instead of pressing **<Ctrl><Alt><Backspace>** to restart a Linux operating system.
- **Take Snapshot** – Not applicable to RocIT Defender.
- **Session Information Dialog** – Displays information regarding the virtual machine's system configuration.
- **Pause/Resume** – Pause or resume the current virtual machine operation.
- **Reset** – Reset the current virtual machine.
- **ACPI Shutdown** – Initiate an ACPI shutdown of the virtual machine.
- **Close** – Shut down the current virtual machine.

Note: The **Host** key referred to in the keyboard shortcuts is the **<Ctrl>** button on the right side of the keyboard. Options can be triggered by using hotkeys. Hotkeys are listed to the right of each option in the "**Machines**" menu. Hotkeys are a combination of pressing the Host key and another key.



Devices Taskbar Menu

5.2. Devices Taskbar Menu

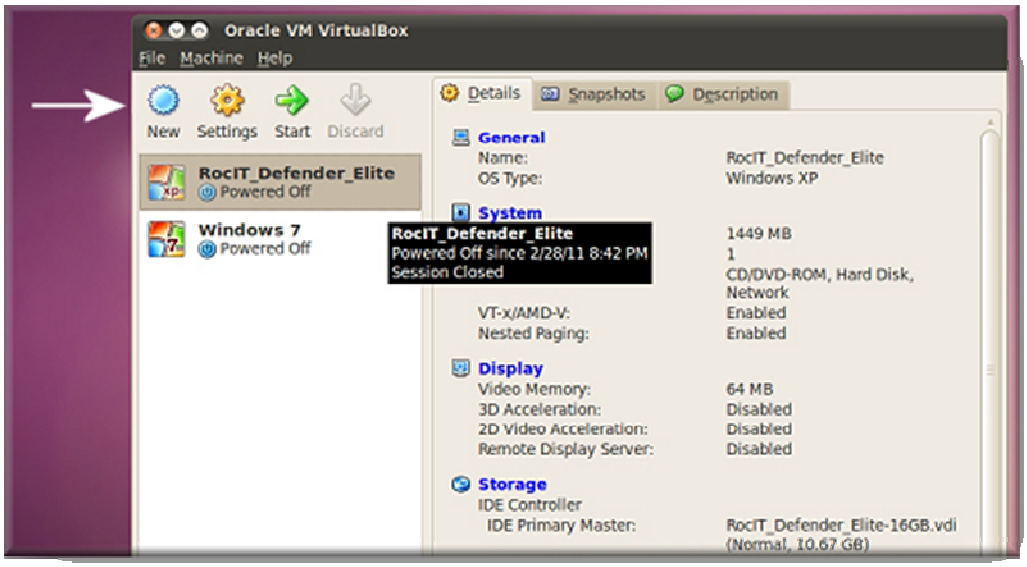
- **USB Devices** – Mouse over the "**USB Devices**" option and a list of USB connected devices will be displayed. Devices that have a checkmark next to them are currently connected to the virtual machine. Devices that do not have a checkmark next to them are not in use by the virtual machine. ***CAUTION!*** *Do not try to select the Kanguru Defender drive. Selecting the Kanguru Defender drive in USB Devices will cause the virtual machine to crash.*
- **Network Adapter**s – Select the Network Adapters option to configure a network adapter for connecting the virtual machine to the internet.
- **Shared Folders** – Not applicable to RocIT Defender.
- **Enable/Disable Remote Display** – There is a built-in server for remote desktop protocol, which allows the user to see the output of a virtual machine's window remotely on any other computer and control the virtual machine from there, as if the virtual machine was running locally.
- **Install Guest Additions** – Guest additions add some extra features that improve the performance between the guest operating system and the host operating system. This option must be run after a new operating system is installed on the RocIT Defender drive.

6. Installing a New Guest Operating System

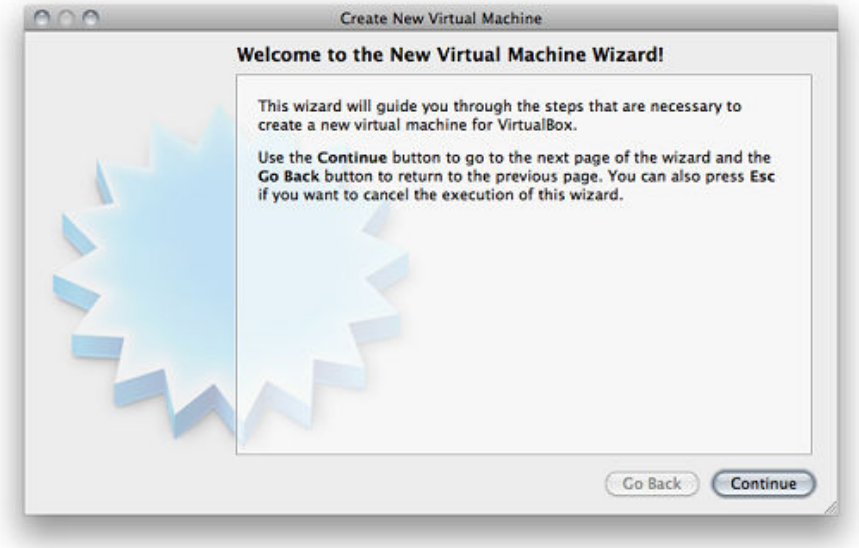
The RocIT Defender drive comes preloaded with a demo version of Windows XP. However, it is easy to install other operating systems on the RocIT Defender drive. Each new OS that is added becomes another Virtual Machine (VM) that is managed within the ViSoS Runtime Environment (see Section 4 on page 8 for VRE details).

6.1. Creating a New Virtual Machine (VM)

Before installing a new OS, the first step is to create a new Virtual Machine (VM) within the VRE (see Section 4.3 page 9 for details on how to access the VRE). A VM is the container into which the new OS will be installed. In the VRE, select menu option **Applications --> System Tools --> Oracle VM VirtualBox**. This will launch the Oracle VirtualBox graphical interface application. A list of VM's that are available upon the drive will be presented in the left panel of the application. At this point, there will only be the RocIT Defender in the list. The panel on the right provides details of each Virtual Machine selected on the left.

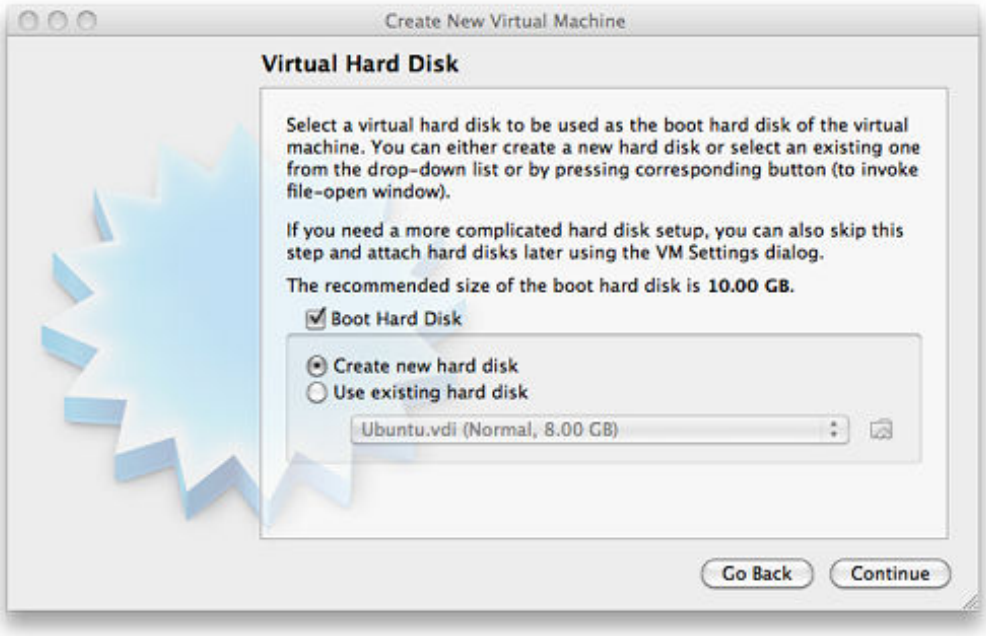


To create a new VM, click on the **<New>** button at the top of the VirtualBox Manager window. A **New VM Wizard** will pop up to guide the user through setting up a new virtual machine.



The New VM Wizard will ask for the bare minimum of information that is needed to create a VM, in particular:

1. The "**VM name**" will later be shown in the VM list of the VirtualBox Manager window, and it will be used for the VM's files on disk. Even though any name could be used, keep in mind that once a few VMs are created, they will be easier to manage if they were given informative names; "My VM" would thus be less useful than "Windows XP SP2 with OpenOffice".
2. For "**Operating System Type**", select the operating system that will be installed into the VM. The supported operating systems are available within a pick list. In order to install an OS that is not listed, select **"Other"**. Depending on the selection, VirtualBox will enable or disable certain VM settings that the guest operating system may require. It is therefore recommended to always set it to the correct value.
3. Next, the user will be prompted to select the memory (RAM) that VirtualBox should allocate every time the virtual machine is started. Skip this step, since the RAM will be dynamically controlled by the VRE.
4. Next, a virtual hard disk for the VM must be created. The wizard displays the following window:



   a) Check the **"Boot Hard Disk"** option and the **"Create new hard disk"** option, and click on the **<Continue>** button.

   b) This brings up another window, the "**Create New Virtual Disk Wizard**", which helps to create a new disk image file in the new virtual machine's

folder. Select the "**Dynamically Expanding File"** option. This will create a virtual hard disk (VDI file) that will grow as data is stored within it.

Selecting a "**fixed-size file**" will pre-allocate a VDI file of the specified file, and will take a fairly long time on a flash drive.

c) Specify the size in megabytes for the VM. Please refer to the following sizing parameters on different capacity drives. Note that this is the total space available upon the drives, after storage of VRE subsystem and ViSoS utilities. Thus if the drive has multiple VDI's, the drive space must be allocated accordingly.

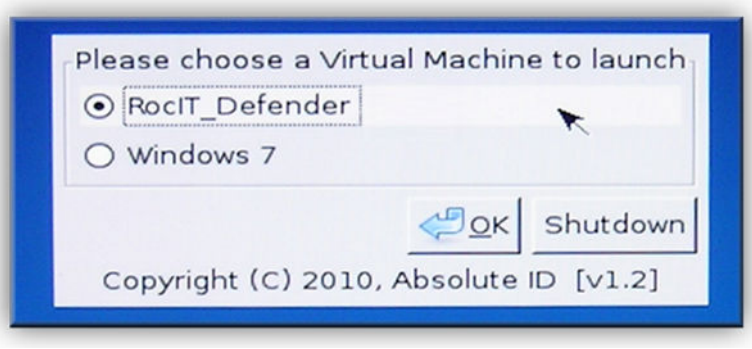
Drive Capacity	Recommended VDI Size per OS
16GB	10.5 GB
32GB	24 GB

5. After having selected or created the VDI image file, again click on **<Next>** to go to the next step.
6. After clicking on **<Finish>**, the new virtual machine will be created. The new VM will be displayed within the VM list on the left side of the VM Virtualbox Manager window, with the name that was entered.

6.2. *Installing a New Guest Operating System*

With the new Virtual Machine container created, the next step will be to install the new Guest operating system into the VM. To install a new operating system on the RocIT Defender:

1. Boot the computer into the ViSoS Authenticator and login. The VRE will load and will present the user with a VM Selection dialog box to choose which VM to launch. In the sample below, it shows the RocIT Defender and a Windows 7 VM which is ready to have its OS installed.



Insert the operating system installation disc into the disc drive and wait for it to spin up, and then click on the new VM option (eg. - **Windows 7** in the image above) and then click on <**OK>**.

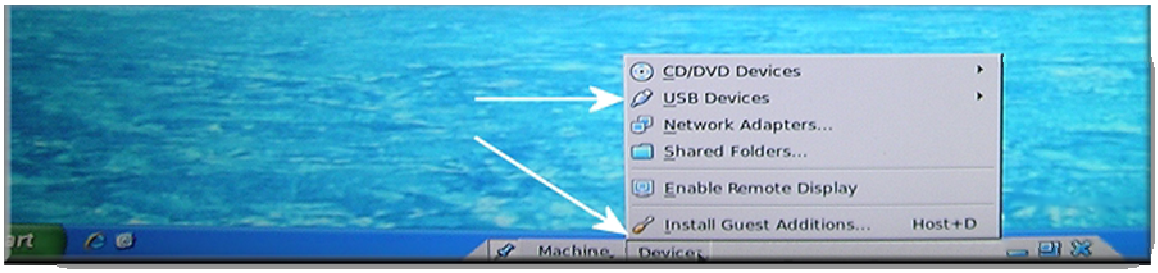
The system will then boot to the operating system installation disc. In this example, the next screen would then show the message "Windows is loading files". Follow the usual prompts and setup instructions (eg. - read and agree to the EULA, choose setup options and installation type, etc.), and proceed with completing the installation and activation of the new operating system.

Once the installation is complete, the new OS will operate and function as normal. It can then be customized and run through configuration options, and have applications installed within it. With multiple OS's on the RocIT Defender drive, when closing or shutting down the new OS, the user will have the option to launch the OS, or shut down the drive and power off the computer completely.

7. *Attaching USB Devices and Printers*

When attaching USB devices, such as a printer, Windows will not necessarily recognize the new device right away. Within a guest operating system, USB devices need to first be activated with a VRE USB controller. To accomplish this, use the VRE taskbar menu at the bottom of the screen. Click on "**Devices"** menu, then hover over

the "**USB Devices**" option and a list of USB items connected to the computer will appear. Select the USB device that is required from the items presented in the menu.



Once attached, a check mark will appear beside the device in the list to indicate it has been recognized by the OS. Recognizing that new hardware has been attached, Windows may then require drivers for the USB device. The next step will be to either download the device drivers from a network, or use the installation drivers from the CD/DVD that came with the device.

CAUTION! *Do not attempt to attach the* ***Kanguru Defender drive****. This will crash the system.*

8. Windows Tuning Tips

When installing a new operating system on the RocIT Drive, it is important to understand that it is running the OS on flash media. Flash media is not as fast at writing data as spinning hard drives, so it is important to tune the installed operating system accordingly. Below are several tips for tuning the operating system to get the best performance:

8.1. Set Swap File to 200MB

On regular hard disk drives, the writing mechanism to a drive is fairly quick. The writing speed on flash media, however, is not as quick and using a large Swap Space can slow down writing speeds significantly. To set the Swap File Size on Windows XP, perform the following:

1. Right click on **My Computer** and select **Properties** to open **System Properties.**
2. Select **Advanced Tab → Performance → Settings** option within **System Properties** dialog.
3. Select **Advanced Tab → Virtual Memory → Change** option within **Performance Settings** dialog.

4. Check **Custom Size** radio button, and set both **Initial Size** and **Maximum Size** to 200MB.
5. Click on the **<OK>** button to save the new settings on all dialogs and exit.

8.2. Set Automatic Updates for Windows to Download and Notify

If Windows is set to allow Automatic Updates, it can reduce system performance when the updates happen in the background. This may be inconvenient when the user is busy working on an important document. Therefore, it is recommended that Windows Updates be set to Notification mode. Windows will then notify the user when updates are available, and the user can then download and install the updates later at their convenience.

1. To change the setting, select **Start --> Control Panel**.
2. Select "**Automatic Updates".**
3. Select "**Notify me but don't automatically download or install them**."
4. Click on the **<OK>** button to save and exit.

9. Setting up Network Connections

Network connectivity is configured and controlled by the ViSoS Runtime Environment (VRE) in which the Windows VM is run. By default, network connectivity utilizes NAT'd (Network Address Translation) networking, where the physical IP address of the drive is determined by the DHCP gateway and the network that the host computer is plugged into. The VM is launched within a VMM, which then creates a unique address for the guest operating system. Thus the VM is *not* using the IP address of the host computer directly, but is routed through the NAT gateway.

The RocIT Drive is pre-configured to support wired network connectivity automatically, so booting the drive off of any computer that is physically connected to the network through a wired connection will automatically provide network access within the guest OS and virtual machine.

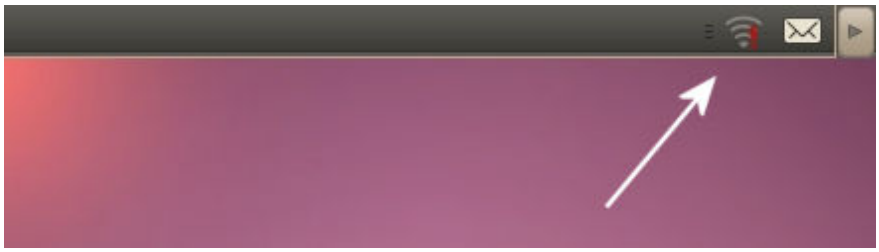
9.1. Setting up Wireless Network

To set up and configure Network settings, the user will need to first access the VRE Desktop in VT7 (see Section 4.3 on page 9). The VRE controls network connections and proxies them into the VM's that hold the installed OS's.

1. If the drive is not locked down by an enterprise Admin, then after booting the drive and logging into the ViSoS Authenticator screen, the user will see the VM Selection dialog box. From here the user would normally launch into a VM OS.

Instead, press <**Ctrl**><**Alt**><**F7**> to enter the VRE desktop area. When finished setting up network connections, press <**Ctrl**><**Alt**><**F8**> to return to the VM Selector dialog to choose the OS to launch with enabled network connections.

2. In the VRE (ViSoS Runtime Environment) desktop, there is a top panel Menu Bar. On the right of the bar there is a **connections icon** that looks like several bars.



3. Hovering over the applet will display a list of available wireless networks. Right-clicking the mouse on the icon will allow the ability to edit the system's connections.

4. The system's wireless network will show up here. Click on it and it will prompt to enter the WPA code or equivalent for the wireless network. Enter the code, and it should connect to the network.

   Note: The network settings may also be saved, which will auto-connect in the future, so that the user will not have to press **<Ctrl><Alt><F7>** to access the VRE again the next time the drive is booted.

5. Once the network is connected, press **<Ctrl><Alt><F8>**. The system will now switch to the Windows Virtual Machine (or the Virtual Machine Selector dialog screen if multiple OS's are installed, from which the user can choose which OS to launch). When the VM is launched, it will now have network access.

Note: *The network can be changed within the VRE Desktop while the VM is running. i.e. The user does not have to shut down the VM to change the network settings.*

10. Windows Activation

The Windows XP license that is preloaded on the drive is a demo version. If the hardware on the computer changes significantly it will require reactivation. Please follow the on screen directions for Windows reactivation.

11. 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.

12. Technical Support

If you experience any problems using your Kanguru RocIT Defender, or have any technical questions regarding this product, please contact Absolute ID's technical support department at: **techsupport@absolute-id.com.**