INSTALLATION AND USER INSTRUCTIONS

PhantomDrive

Release 1.0

April 2025
Version 1.0

PhantomDrive

Table of Contents

1 PREFACE 3

1.1 Description of the user 3

1.2 Conventions used in this manual 3

2 Competitive Analysis 4

2.1 How does PhantomDrive Compare? 4

3 PhantomDrive Initial Set-up 5

3.1 Step-by-Step Guide 5

3.2 Virtual Machine Software Installation 9

4 Security Features Of PhantomDrive 10

4.1 Modular Virtual Machines 10

4.2 Lightening Ubuntu OS 10

4.3 Disabling kernel modules 11

4.4 Protecting User Account (Limiting Login Attempts) 11

4.5 Automate Virtual Machines 14

5 Troubleshooting 17

5.1 Common Issues 17

6 Contact and Contributions 18

PREFACE

1.1 Description of The User

The user operates in a high-profile role that requires frequent handling of sensitive or classified documents. Given the dynamic and evolving threat landscape, there is an increasing need to minimize the attack surface and maintain operational security across various environments. The user frequently travels or works in potentially unsecured locations, making them vulnerable to common vectors such as hotel Wi-Fi networks, malicious charging ports or accessories, and physical device theft or tampering. As a result, there is a clear demand for a more portable, hardened operating system that prioritizes security, minimizes digital footprint, and ensures data confidentiality even under adverse conditions.

1.2 Conventions Used in this Manual

Operating Systems

- **Windows 11** is used exclusively for the initial creation of the Live USB environment.
- **Ubuntu 24.04 LTS** serves as the persistent host operating system on the USB, from which all operations and virtual machines are launched.

Virtualization Platform

- **Oracle VirtualBox** is the primary virtualization tool used throughout this manual. Virtual machines are configured with various functional roles and security profiles depending on the intended use case.

Hardware Assumptions

- **USB 3.0** is the preferred medium for storage and transfer due to its improved speed and compatibility. Performance may be limited when using older USB 2.0 hardware.

Command Syntax

- Commands are provided in a Linux terminal format (bash shell). Users running commands in a different environment (e.g., Windows PowerShell or CMD) should adapt syntax accordingly.

PhantomDrive

Competitive Analysis

2.1 How does PhantomDrive compare to existing solutions?

Feature	PhantomDrive	Live USB (Persistent Mode)	Cloud Computing (AWS, Azure, GCP)	Portable VM on External Drive
Real OS Installation	Yes	No (Limited Persistence)	No (Internet Required)	Yes
Storage Included	Yes (ExFAT)	Limited	No	Yes
Cross-Platform	Yes	Limited	Yes	No (Host OS Dependent)
Internet-Free	Yes	Yes	No	Yes
Secure / Isolated	Yes	Limited	No	Yes
Performance	Fast (Native Install)	Slow	Depends on Connection	Varies (VM Overhead)

Conclusion:

- PhantomDrive provides a full OS, unlike persistent Live USBs.
- It works offline, unlike cloud-based workspaces.
- It’s more portable and hardware-independent than external drive VMs.

PhantomDrive Initial Set-up

3.1 Step-by-Step Guide

1. Prepare the USB Drives

   Plug in your 256GB USB drive.

   Open GParted (on Linux) or Disk Management (on Windows).

2.Creating the partitions

- 1GB FAT32 (EFI partition) -> Required for UEFI boot.
- 35GB ext4 partition -> For Ubuntu installation.
- The rest as exFAT -> For storage.

A. Create the EFI Partition (1GB)

Click New.

Set Size: 1000 MB

File System: fat32

Label: EFI

Flag: Right-click -> Manage Flags -> Check boot & esp

Click Add.

B. Create the Ubuntu Partition (35GB)

Click New.

Set Size: 35000 MB

File System: ext4

Label: Ubuntu_24.04

Click Add.

C. Create the Storage Partition (Remaining Space)

Click New.

Set: Use all remaining space.

File System: exFAT (or ext4 if only using Linux).

for exfat, use 'exfatprogs' in gparted

```
sudo apt update
sudo apt install exfatprogs -y
```

Label: Storage

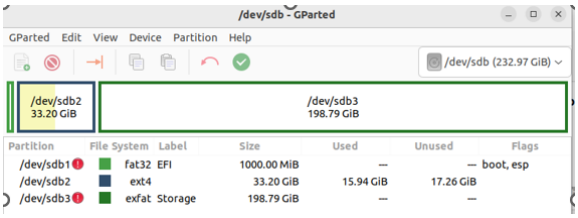
Click Add.

Apply the Changes

Click the Checkmark "Apply" button.

Wait for the operation to complete.

Done!



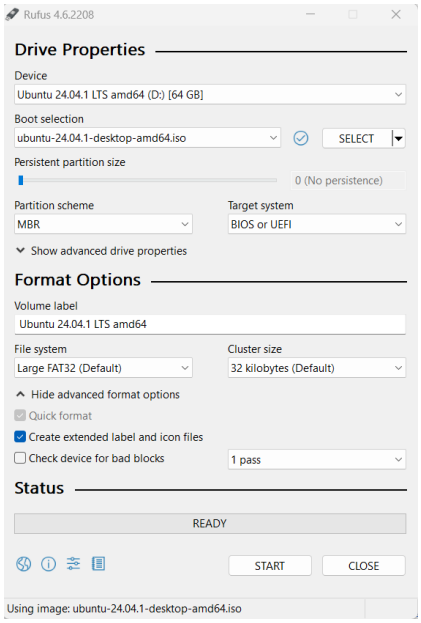
Now your USB is partitioned correctly and ready for Ubuntu installation.

3. Create a Live USB

A. Download Ubuntu 24.04 ISO from the official site.

B. Insert second USB (recommended: 16GB or greater)

C. Use Rufus (Windows) or Balena Etcher (Linux/Mac) to flash the ISO onto a second USB.

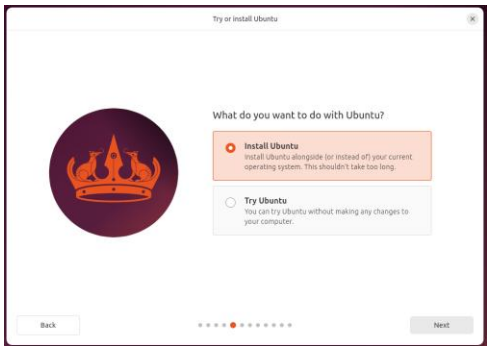


D. Restart to boot from the Live USB.

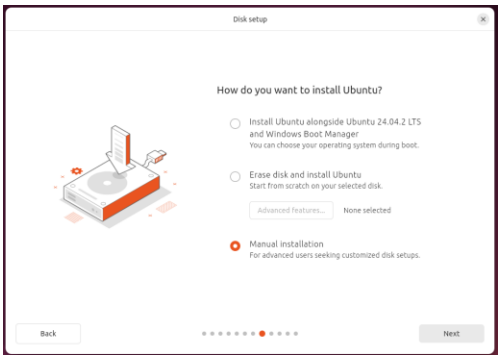
Note: Machines differ and may require the user to enter the boot menu (option key – MacOS. Return, then f12 on Windows)

4. Install Ubuntu 256GB USB

A. Install Ubuntu onto 35GB Partition



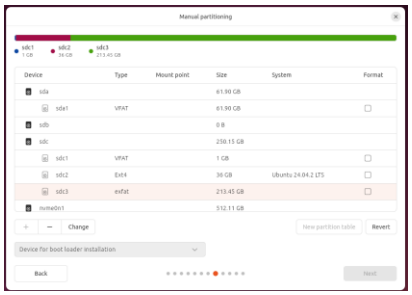
- Select "Manual installation" in the partitioning step.



B. Find your 35GB ext4 partition (carefully avoid selecting your main drive).

Set it as:

- Mount point: /
- Use as: Ext4



C. Install the bootloader on the USB drive itself (e.g., /dev/sdc1, not /dev/sda).

D. Proceed with the installation.

Reboot computer and enter boot menu, choose Ubuntu.

3.2 Virtual Machine Software installation

Installing Oracle Virtual Box on Ubuntu 24.04 LTS

A. To install the current version of Oracle Virtual Box, in the Ubuntu terminal (ctrl-alt-t) type:

```
sudo apt update
sudo apt install virtualbox-7.1.6
```

B. The Virtual box extension pack is also required:

```
Wget https://download.virtualbox.org/virtualbox/7.1.6/
Oracle_VirtualBox_Extension_Pack-7.1.6.vbox-extpack
```

```
sudo vboxmanage extpack install
Oracle_VirtualBox_Extension_Pack-7.1.6.vbox-extpack
```

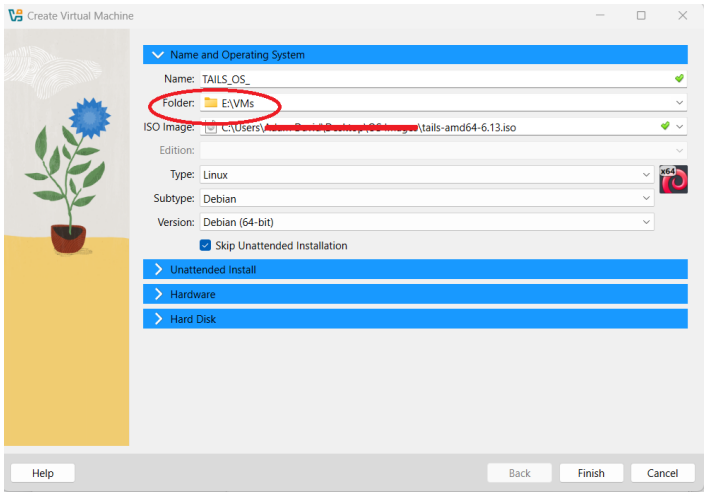
C. Before using VirtualBox, add your user account to the "*vboxusers*" group

```
sudo usermod -aG vboxusers $USER
```

Security Features of PhantomDrive

4.1 Modular Virtual Machines

- Create a destination folder in the Storage directory (E:) to store VMs



4.2 Lighten the Ubuntu operating system by removing unnecessary programs.

- In the Ubuntu terminal (ctrl-alt-t) type:

```
sudo apt-get remove --purge thunderbird rhythmbox
libreoffice* gimp evolution rhythmbox* thunderbird* --
auto-remove && sudo apt-get clean
```

Note: This command removes thunderbird email, rhythmbox music player, libre office productivity suite, evolution calendar/contacts manager and gimp graphics editor. This action reduces the attack surface, requires few software upgrades, decreases dependencies and frees resources for the operating system to function more efficiently. Hence providing a secure and quick environment to run customized Virtual machines.

4.3 Disable Kernel Modules

To further lighten the OS and reduce the attack surface, disabling kernel modules can be beneficial. Kernel modules act like plug-ins that add functionality to the operating system. By disabling these plug-ins, the system can be further secured.

- To check kernel modules running

```
lsmod
```

- From this list, select modules that may not be needed. For example, Bluetooth, webcam, & audio features. Add them to the ‘blacklist.conf’ file.

```
echo "blacklist bluetooth" | sudo tee –a /etc/modprobe.d/blacklist.conf
```

4.4 Protect user account by limiting log in attempts.

- **Note**: This script causes the Ubuntu host operating system to be deleted upon 3 incorrect password attempts. This is irreversible, please take caution to remember passwords.

- Create script to count unsuccessful logins in the root folder.

```
sudo nano auth_fail_handler.sh
```

```
#!/bin/bash

# Config
MAX_FAILS=3
FAIL_FILE="/var/log/auth_fail_count"
WIPE_SCRIPT="/root/wipe_drive.sh"

# Ensure file exists
touch "$FAIL_FILE"
chmod 600 "$FAIL_FILE"

# Read fail count
fails=$(cat "$FAIL_FILE")

# Increment
fails=$((fails + 1))
echo "$fails" > "$FAIL_FILE"

# Check threshold
if [[ $fails -ge $MAX_FAILS ]]; then
    logger "AUTH FAILURE: Reached $fails attempts.
Initiating drive wipe."
    bash "$WIPE_SCRIPT"
fi
```

- Create script named “wipe_drive.sh” in the root folder

```
sudo nano wipe_drive.sh
```

```
#!/bin/bash

DRIVE="/dev/sdc2"   # replace with ubuntu drive
LOGFILE="/var/log/wipe_triggered.log"

echo "$(date): WIPING DRIVE $DRIVE" >> "$LOGFILE"
shred -v -n 3 -z "$DRIVE"

sync
poweroff
```

- Modify the permissions to run scripts

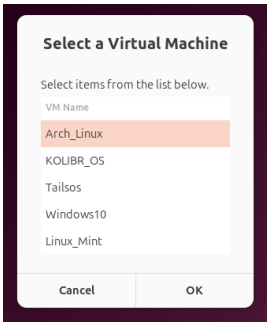
```
chmod 700 /root/wipe_drive.sh
/root/auth_fail_handler.sh

chown root:root /root/wipe_drive.sh
/root/auth_fail_handler.sh
```

- Authorize pam exec module to run script during login by adding “auth required pam_exec.so seteuid /root/auth_fail_handler.sh” at top of the following file:

```
sudo nano /etc/pam.d/common-auth
```

4.5 Automate Virtual Machines

This script monitors the virtual machine folder for new additions and allows the user to launch current virtual machines from a dialog box, seen below.



A. Install dependencies. Zenity and inotify assist in monitoring and displaying folder changes

```
sudo apt install inotify-tools zenity
```

B. Create the vms_monitor script

```
nano vms_monitor.sh
```

```
#!/bin/bash


# Set the correct VirtualBox VM directory
# Define the mount point for the USB drive
USB_MOUNT_POINT="/media/$USER/Storage"  # Change to your actual USB
name
VM_DIR="/media/$USER/Storage/VMs"  # Adjust this path if needed

# Function to wait until the VM directory exists
wait_for_vm_dir() {
    echo "Waiting for VM directory to be available..."
    while [[ ! -d "$VM_DIR" ]]; do
        notify-send "Waiting for Storage" "VirtualBox VMs directory
not found. Retrying..."
        sleep 3  # Retry every 3 seconds
    done
    notify-send "VM Storage Ready" "VirtualBox VMs directory is now
available."
}


# Function to list VM folders
list_vm_folders() {
    find "$VM_DIR" -mindepth 1 -maxdepth 1 -type d -printf "%f\n"
}

# Function to start a selected VM
start_vm() {
    local vm_folder="$1"
    local vbox_file

    # Find the .vbox file inside the selected folder
    vbox_file=$(find "$VM_DIR/$vm_folder" -maxdepth 1 -name "*.vbox"
| head -n 1)

    if [[ -n "$vbox_file" ]]; then
        vm_name=$(basename "$vbox_file" .vbox)

      # Check if VM is already registered
        if ! VBoxManage list vms | grep -q "\"$vm_name\""; then
            notify-send "Registering VM" "Adding $vm_name to
VirtualBox..."
            VBoxManage registervm "$vbox_file"
        fi

      VBoxManage startvm "$vm_name"
        notify-send "Starting VM" "Launching $vm_name in GUI mode..."
    else
        notify-send "Error" "No .vbox file found in $vm_folder."
    fi
}

#Continued below
```

```
# Function to prompt user to pick a VM folder
prompt_user() {
    export DISPLAY=:1
    export XAUTHORITY="$HOME/.Xauthority"


    local selected_folder
    selected_folder=$(list_vm_folders | zenity --list --title="Select
a Virtual Machine" --column="VM Name" --width=400 --height=300
2>/dev/null)

    if [[ -n "$selected_folder" ]]; then
        start_vm "$selected_folder"
    fi
}

# Wait until the VM directory is available
wait_for_vm_dir

# Run on startup to check for VMs and prompt
prompt_user &

# Monitor the VM directory for new VM folders
inotifywait -m -e create --format "%f" "$VM_DIR" 2>/dev/null | while
read NEW_FOLDER; do
    if [[ -d "$VM_DIR/$NEW_FOLDER" ]]; then
        notify-send "New VM Folder Detected" "New VM $NEW_FOLDER
added. Prompting to open..."
        prompt_user
    fi
done
```

- Modify the permissions to run script

```
chmod a+x vms_monitor.sh
```

Open ‘gnome-session-properties’ in terminal. Add the line “/bin/bash /home/$USER/vms_monitor.sh”

Troubleshooting

5.1 Common Issues

PhantomDrive is designed to boot seamlessly across diverse hardware platforms, including Windows-based PCs and Mac systems. However, certain hardware-specific or firmware-specific troubleshooting may be required:

A) Secure Boot Compatibility: On many modern Windows and Mac systems, secure boot may need to be temporarily disabled or modified in UEFI/BIOS settings to permit PhantomDrive booting. This can be done by entering the firmware settings and toggling secure boot to "off" or selecting an option such as "Allow Booting from External Media."

B) Boot Order Configuration: Ensure the USB device is prioritized in the boot order settings of the BIOS/UEFI firmware.

C) Compatibility Mode Boot: Older systems might require enabling legacy or compatibility boot modes in their firmware settings.

D) GRUB Issues: Occasionally, incorrect GRUB installations or updates may require using recovery methods, including Boot Repair utilities or manual GRUB reinstallation via a chroot environment.

E) Partition Recognition Issues: Verify that the EFI partition flags (esp, boot) are correctly set if the drive fails to boot initially.

F) Meet system requirements (As per Ubuntu 24.04 LTS download page)
   - 2 GHz dual-core processor or better
   - 4 GB system memory
   - 25 GB of free hard drive space
   - Either a USB port or a DVD drive for the installer media
   - Internet access is helpful

G) USB 3.0 will achieve best operating speeds.

6 Contact and Contributions

For questions, comments and concerns contact:

PhantomDrive@PROTON.ME

For contributions and further troubleshooting resources visit:

Github.com/8BitCommit/PhantomDrive