GETTING STARTED

Setting up and using the CSI Linux Virtual Appliance

This will walk through how to use the CSI Linux within a virtual machine environment inlcuding VirtualBox, VMWare, HyperV, and KVM.

Evidence collection and preservation are essential when doing any investigation or forensic examination. Within the CSI Linux environment, there are several mechanisms in place to provide for the preservation and integrity validation of the evidence while collecting evidence for a case. Using the virtual appliance opens a door for a great method to secure evidence.

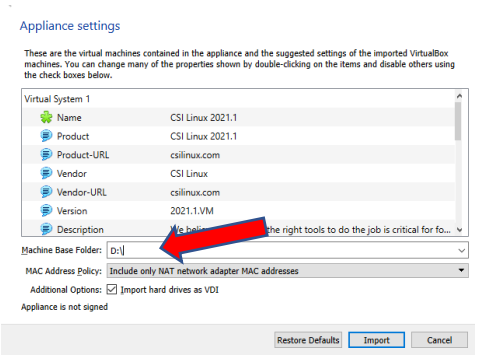
The current version has been built using an Ubuntu 22.04 LTS version for long-term support. There have been many upgrades in the applications, and additional applications have been added. The original CSI Gateway has been retired, and we are not using Whonix. We have also built our own TOR Gateway into the platform (runs like Tails), called the CSI TorVPN. This will encapsulate all your traffic through a Tor "VPN" adapter when it is turned on. We will cover these in a future section.

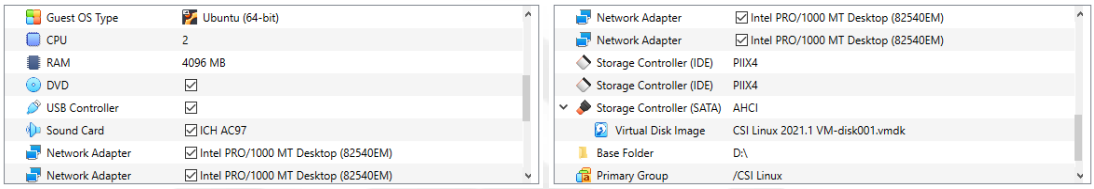
System Requirements

- A system that supports virtualization
- 64 GB free space minimum
  - This is for file downloads and installation.
- 6GB Ram minimum
  - The VM has 4GB preallocated.
- Internet for the internet related tools and updates

Installing the system

1. Download and install VirtualBox. Downloads – Oracle VM VirtualBox
2. Download and install VirtualBox Extension Pack. Downloads – Oracle VM VirtualBox
3. Download the CSI Linux VM.OVA file from the download section.
   a. If you are using the Torrent file or Magnet link, you will need to use BitTorrent software to open those. The BitTorrent file downloads the .OVA file.
   b. After it is downloaded, please consider leaving it in your torrent application to help "seed" the torrent to help others download it.
4. Verify that the .ova file has completed downloading.
5. Once the .ova file has been downloaded, double left click on it, and you should see VirtualBox pop up with setup information on the screen.
6. Make sure you choose a location that has enough disk space. For example, some systems have limited space on the C: drive so that you can install the virtual appliance on your D: drive or external.
7. Scroll down to make sure the settings match your needs. For example, you can increase the RAM if you have a lot available or add more virtual CPUs if your system can handle it. Do not go above what you have physically available to your primary OS.





8. Left click on Import.
9. Left click on Agree.
10. Wait until CSI Linux is installed. This may take a few minutes. Sit back or take a break.
11. You should now see CSI Linux as a system in VirtualBox.
12. Double left click on the CSI Linux VM.

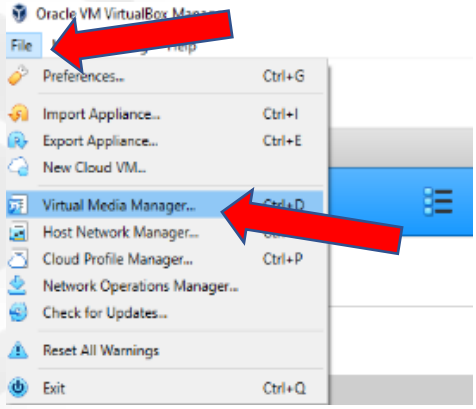
13. The VM should start in a new window. When it gets to the login prompt, enter the username and password.
    a. User: csi
    b. Pass: csi
14. Press or click “Log In”.
15. You should now be in CSI Linux.

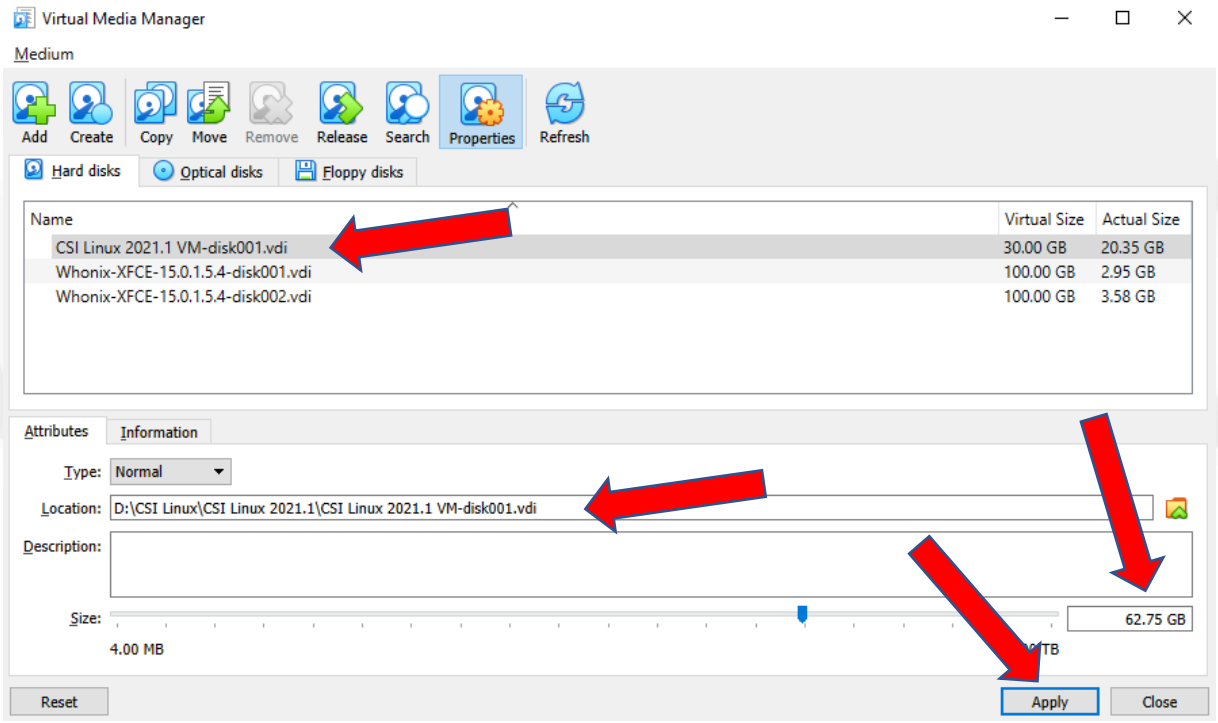
Optional - Changing Disk Size

If you want more space within CSI Linux, you can increase it to meet your needs.

Step 1

1. Make sure the CSI Linux Virtual Appliance is turned off.
2. Left click on “File”.
3. Left click on “Virtual Media Manager”.
4. You should now see a new window pop up. Left click the CSI Linux VM drive.
   Left click on “Properties”.
5. Towards the bottom, you can either slide the scale or type in the exact size you want the drive to grow.
6. Then left click “Apply”.

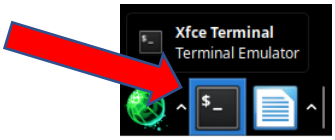


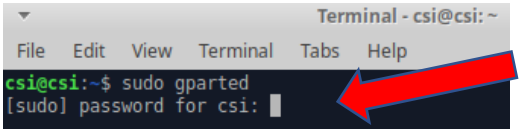


Step 2.

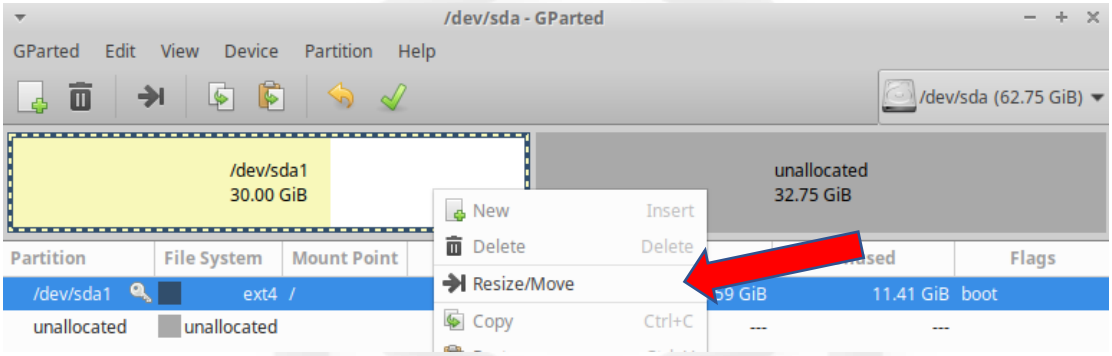
1. When the virtual media window closes, start the CSI Linux VM.
2. Log into CSI Linux
3. Open a terminal window by left clicking on the terminal icon.
4. Type in the following and press enter.

   sudo gparted

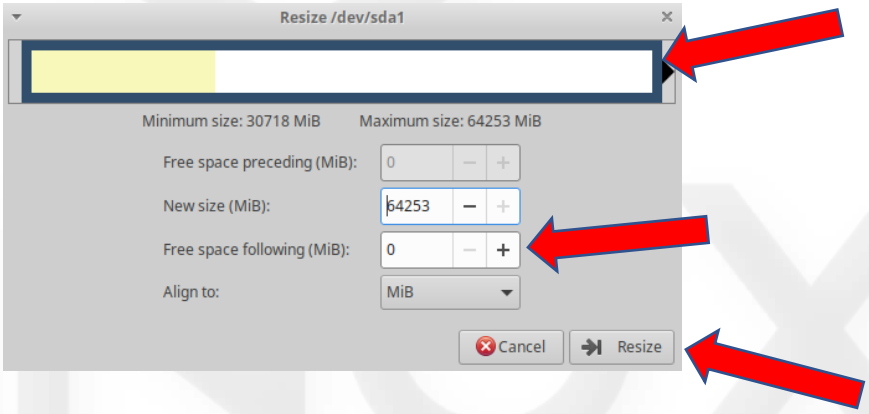




5. Use the password “csi”.
6. Right click on the CSI Linux drive (example: 30.00 GB). Then left click on “Resize/Move”.



7. Slide the slider bar to the far right or type in “0” for the “Free space following (MiB)” and press enter. This should now fit the new size you created in step 1.



8. Left click “Resize” and then left click the check icon.

9. Left click “Apply”. When it is done, left click “Ok”, then close Gparted.

You can now start using your investigation environment with more disk space.

Methods of using the CSI Linux Virtual Appliance

There are two ways to use the CSI Linux virtual appliance for your cyber investigations. The most common method is to use one instance of CSI Linux for multiple cases. The case management system separates the cases into their folders, makes an MD5 hash of all the files in the case, and compresses them into the archive folder when you are done with your tools.

The second method is to use one CSI Linux instance for one case. This is a popular method for Law Enforcement and other organizations that need to ensure Confidentiality, Integrity, and Availability of the evidence. When the case is done, an archive that instance and save that as your evidence container. This way, the environment is only used for one case, and there is no possibility of accidental cross-contamination if you enter the wrong case information. When a case is closed, you can move it to a "Closed Cases" group within VirtualBox. When you need to clear up space or officially archive the cases, you can create an OVA appliance of the CSI_Linux_CaseName virtual machine, copy it to two different locations (backup redundancy), and remove the CSI Linux instance from VirtualBox.

We are going to walk through both methods.

1. CSI Linux for multiple cases
2. CSI Linux for one case (Sandboxed)

You need to download and install VirtualBox and VirtualBox extensions from virtualbox.org/wiki/Downloads. Then you need to download the.OVA file for CSI Linux from csilinux.com/download

CSI Linux for multiple cases

Step 1

1. Double left click on the CSI Linux .ova file
2. Go through the setup wizard
3. Wait for it to install.

***Note**: You should see a CSI Linux instance in VirtualBox. Start the virtual machine, and you are good to go.*

CSI Linux for one case (Sandboxed)

Step 1

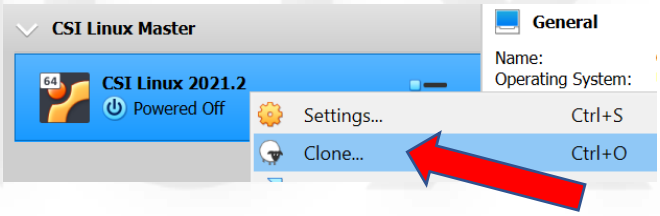
1. Double left click on the CSI Linux .ova file
2. Go through the setup wizard
3. Wait for it to install. You should then see a CSI Linux instance in VirtualBox.
4. Right click on the virtual machine group "CSI Linux."
5. "Rename Group" to CSI Linux Master. This will act as your "golden image." Keep the original.OVA file and archive it in case there is a reason you need to backdate your CSI Linux Master.

***Note**: We do this because we are going to use the CSI Linux Master as the baseline image to lone new cases from. When you update the CSI Linux Master, the new cases will also contain the updates.*

Step 2

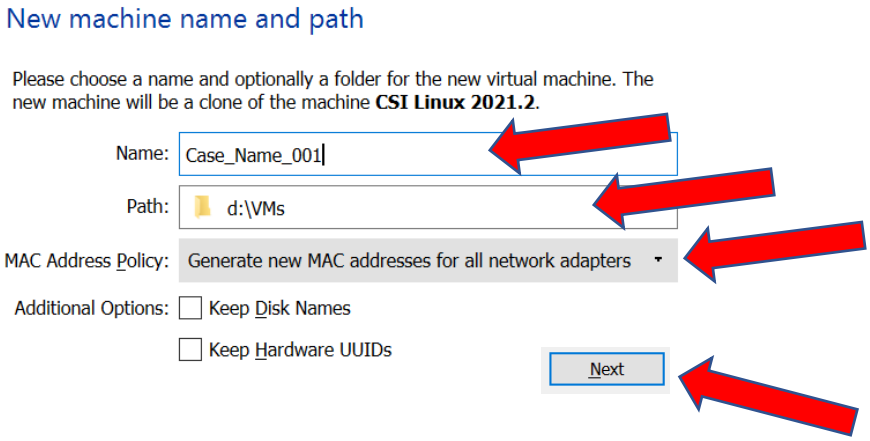
Now, for our first case.

1. right in the CSI Linux VM (in this instance, it is CSI Linux 2021.2)
2. left click on "**Clone**".



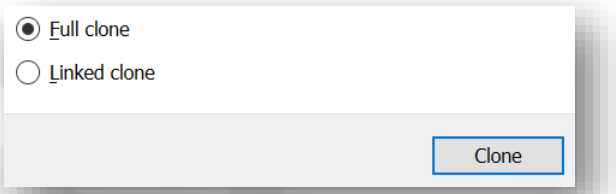
Change the following to meet your environment needs:

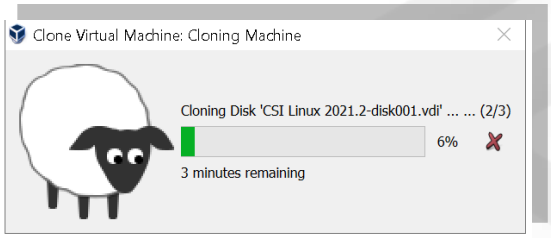
- **Name**: *Needs to be a unique case name*
- **Path**: *Point to a disk that is large enough to store your cases.*
- **MAC Address Policy**: *Switch to "Generate new MAC addresses for all network adapters."*



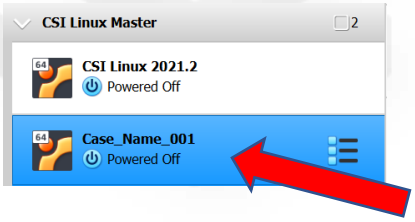
3. Left click **Next**

4. Make sure "**Full clone**" is chosen
5. Left click **Clone**
6. Now wait

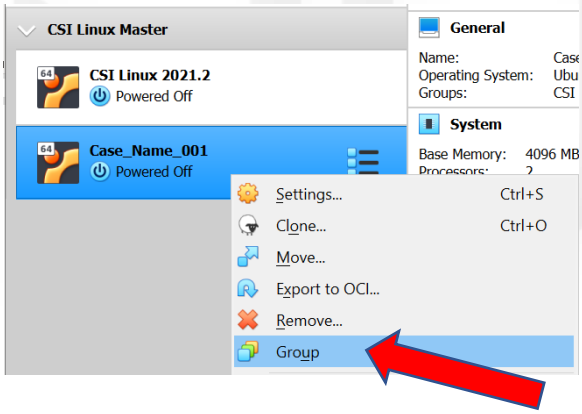




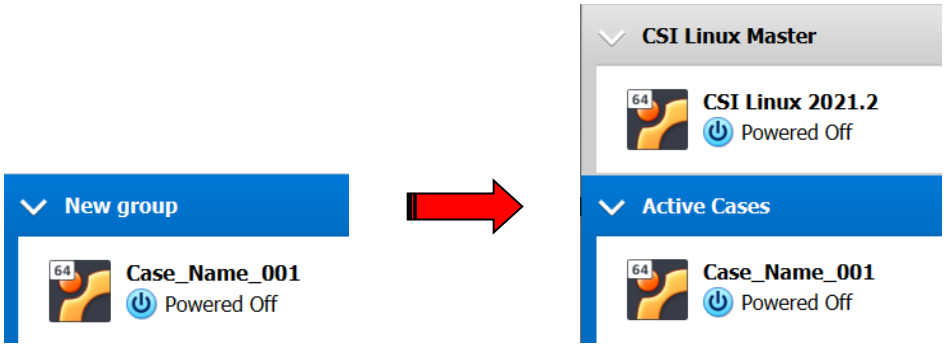
7. Once it is done, you should have a second CSI Linux instance.



8. Right click on the new case instance and left click on "**Group.**"



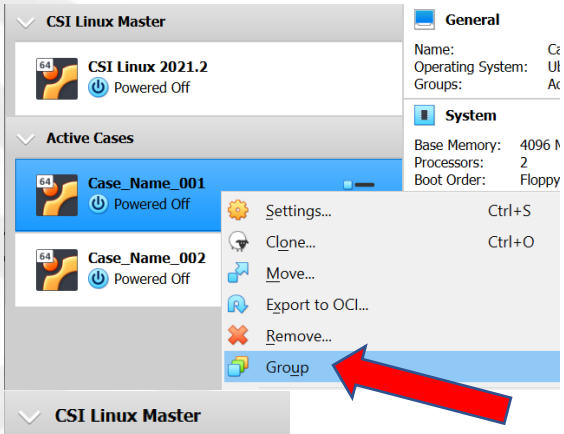
9. Right click on the new group and rename the group to "**Active Cases**".



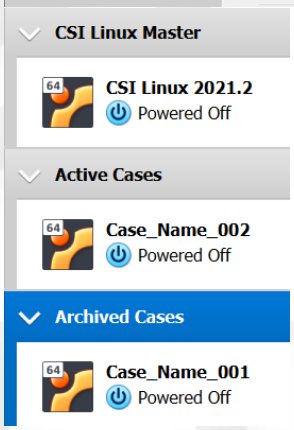
10. Drag the new case instances into the Active Cases group and not onto another VM instance. If you do, it will create a new subgroup. Rinse and repeat.

Step 3

Archiving the cases is very similar. If this is the first time you are archiving a case, right click on the VM instance you want to archive from the Active Cases and left click on "**Group**".



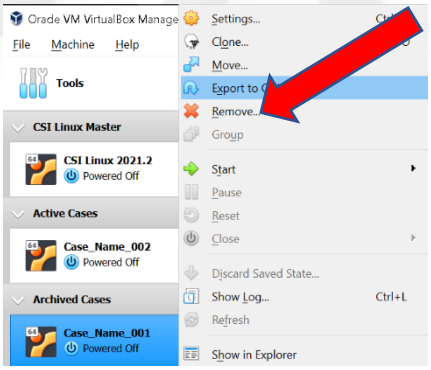
1. Right click on the new group
2. Rename the group to "**Active Cases**". You can also rename it "Closed Cases" if that makes more sense or makes it more visually different to minimize potential miss grouping.



3. Drag the new case instances to archive into the Archived Cases group and not onto another VM instance. If you do, it will create a new subgroup. Rinse and repeat.

Step 4

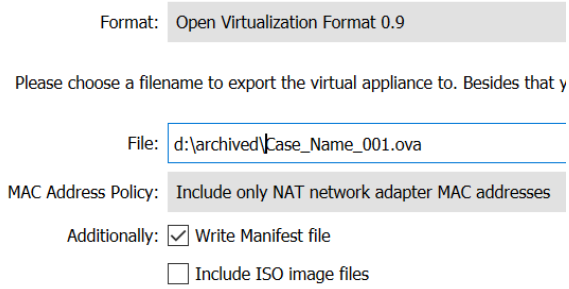
You export the VM instance to move the cases off the investigation system for offline storage. To do this:



1. Right click on the VM instance
2. Left click on "**Export to OCI**".

Change the following to meet your environment needs:

- **Format**: *Open Virt Format 0.9*
- **File**: *Point to a disk that is large enough.*
- **MAC Address Policy**: *Leave the default*
- **Additional**: *Check Write Manifest file*



3. Left click "**Next**"
4. Left click "**Export**"