MK Mahwete

Setting and Configuring USB Guard (usbguard)

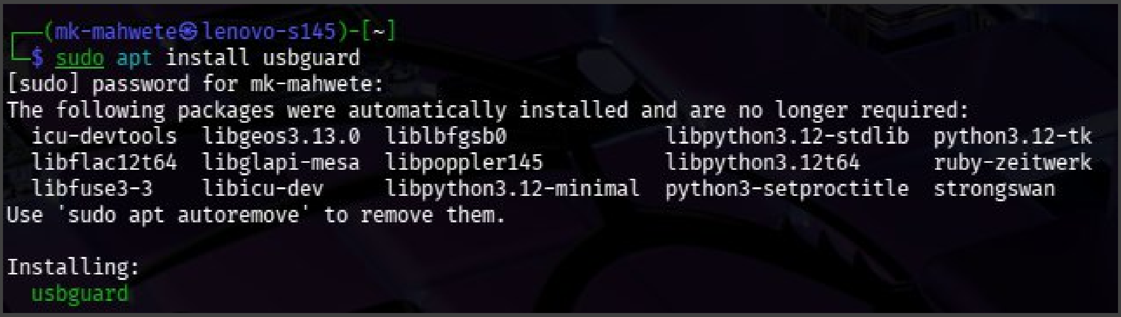
In order to use the script, I recommend that you install usbguard (a Linux tool that can control what USB devices are allowed to talk to your system. It blocks unknown USB devices before the system mounts them). This tool will allow you to add, remove, deny or allow certain trusted devices to be auto mounted to the system.

Step 1: Install usbguard

Update the system by running this command in your terminal:

```
sudo apt update
sudo apt install usbguard
```

- This command will update your repository and install usbguard



```
┌──(mk-mahwete㉿lenovo-s145)-[~]
└─$ sudo apt install usbguard
[sudo] password for mk-mahwete:
The following packages were automatically installed and are no longer required:
  icu-devtools  libgeos3.13.0  liblbfgsb0            libpython3.12-stdlib  python3.12-tk
  libflac12t64  libglapi-mesa  libpoppler145         libpython3.12t64      ruby-zeitwerk
  libfuse3-3    libicu-dev     libpython3.12-minimal python3-setproctitle  strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
  usbguard
```

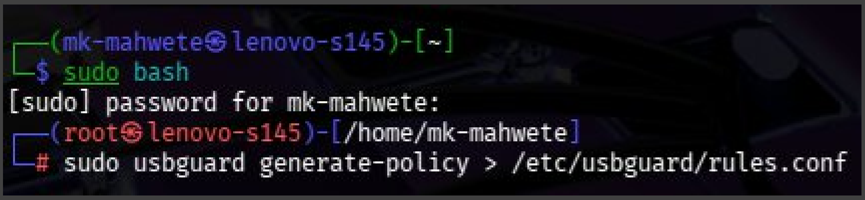
>> $————————————————————————————————[29 April 2025]

Step 2: Generate Your Device Rules (Trusted List)

Plug in your trusted USB thumb drive (and any other trusted devices you want, like keyboard, mouse, etc). Make sure everything you want to KEEP working is plugged in right now.

run this command to generate the list and store it:

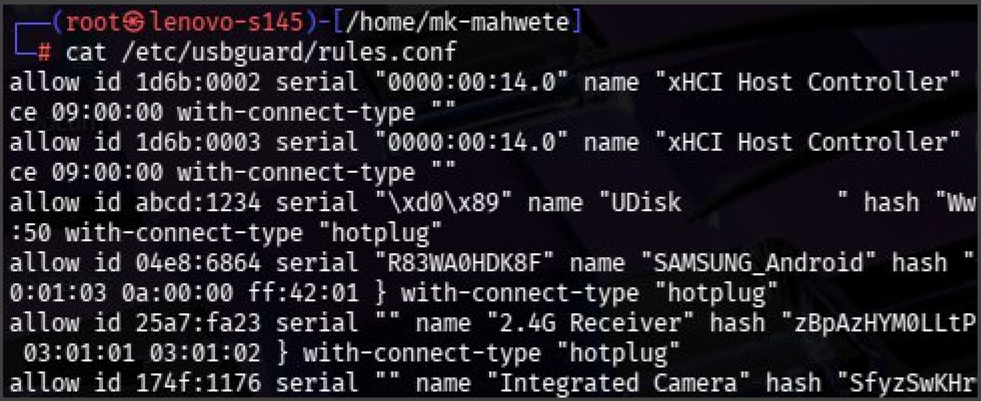
```
sudo bash
sudo usbguard generate-policy > /etc/usbguard/rules.conf
```



```
┌──(mk-mahwete㉿lenovo-s145)-[~]
└─$ sudo bash
[sudo] password for mk-mahwete:
┌──(root㉿lenovo-s145)-[/home/mk-mahwete]
└─# sudo usbguard generate-policy > /etc/usbguard/rules.conf
```

Run this command to see which devices are allowed:

```
cat /etc/usbgard/rules.conf
```



```
┌──(root㉿lenovo-s145)-[/home/mk-mahwete]
└─# cat /etc/usbguard/rules.conf
allow id 1d6b:0002 serial "0000:00:14.0" name "xHCI Host Controller"
ce 09:00:00 with-connect-type ""
allow id 1d6b:0003 serial "0000:00:14.0" name "xHCI Host Controller"
ce 09:00:00 with-connect-type ""
allow id abcd:1234 serial "\xd0\x89" name "UDisk           " hash "Ww
:50 with-connect-type "hotplug"
allow id 04e8:6864 serial "R83WA0HDK8F" name "SAMSUNG_Android" hash "
0:01:03 0a:00:00 ff:42:01 } with-connect-type "hotplug"
allow id 25a7:fa23 serial "" name "2.4G Receiver" hash "zBpAzHYM0LLtP
 03:01:01 03:01:02 } with-connect-type "hotplug"
allow id 174f:1176 serial "" name "Integrated Camera" hash "SfyzSwKHr
```

- A USB stick is allowed
- A Samsung android device is allowed
- A wireless mouse is allowed
- My webcam is allowed

If a new, unknown USB is plugged in later, it will be blocked.

>> $————————————————————————————————[29 April 2025]

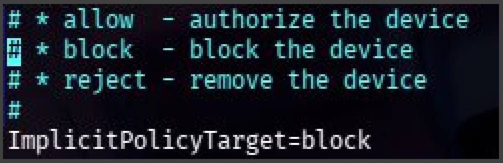
Step 3: Set USBGuard to Enforce Mode

Right now, usbguard is passive and we must tell it to "BLOCK everything not on the trusted list!"

Open the usbguard configuration file and cahnge some few settings:

```
sudo vim /etc/usbguard/usbguard-daemon.conf
```

Inside the file, look for this line and type block if allowed:



```
# * allow  - authorize the device
# * block  - block the device
# * reject - remove the device
#
ImplicitPolicyTarget=block
```

- This means if a USB device is NOT in my rules.conf file ➔ BLOCK it immediately.

Now lets enable usbguard at boot and start it:

```
sudo systemctl start usbguard
sudo systemctl enable usbguard
```

This means No auto-mount, no communication, nothing.

>> $————————————————————————————————[29 April 2025]

Run this command to see which new devices are connect:

```
sudo usbguard list-devices
```

Wanna add a new device, no problem. Run this command to add a new trusted device to the list:

```
sudo usbguard allow-device <device-id>
```

- Reload rules without reboot with this command: sudo **systemctl reload usbguard**