

Gatekeeper_SS_File

Gatekeeper: USB Device Control & Monitoring Framework

1. Project Initialization (Idle State) :

Gatekeeper is launched and running in the terminal. No USB activity is detected yet, showing the system's baseline monitoring state.

```
[root@parrot]--[home/gr0ot/Desktop/gatekeeper]
#python3 main.py
[Gatekeeper] USB Device Control & Monitoring Framework starting...
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-0:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-0:1.0
[Gatekeeper] Monitoring USB events in real-time. Plug/unplug a device ...
```

2. Registered USB Device Detection and Authorization :

A trusted USB device is connected. Gatekeeper identifies the device attributes and applies policy rules, resulting in an ALLOW decision.

```
[root@parrot]--[home/gr0ot/Desktop/gatekeeper]
#python3 main.py
[Gatekeeper] USB Device Control & Monitoring Framework starting...
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-0:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1:1.0
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1
[Baseline] 2026-02-05 00:18:26 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-0:1.0
[Gatekeeper] Monitoring USB events in real-time. Plug/unplug a device ...
[Monitor] 2026-02-05 00:18:58 | add | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
/home/gr0ot/Desktop/gatekeeper/main.py:39: DeprecationWarning: Will be removed in 1.0. Access properties with Device.properties.
  if device_event:
[Identify] 2026-02-05 00:18:58 | 058f:6387 | Serial: 86D89FF7 | Path: /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
[Policy] 2026-02-05 00:18:58 | ALLOW | 058f:6387 | Serial=86D89FF7
[Alert] 2026-02-05 00:18:58 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
[Gatekeeper] Waiting for USB mount...
[Audit] Monitoring file transfers on /media/gr0ot/64 GB for device 86D89FF7
[Gatekeeper] Audit started on /media/gr0ot/64 GB
[Gatekeeper] Final Decision: ALLOW for 058f:6387 Serial=86D89FF7
[Gatekeeper] Report updated: data/logs/gatekeeper_report_2026-02-05.txt
```

3. File Transfer Audit on Authorized Device :

Once mounted, file transfers on the authorized USB are monitored. Audit logs capture file names and SHA256 checksums for integrity verification.

```
[Gatekeeper] Waiting for USB mount...
[Audit] Monitoring file transfers on /media/gr0t/64 GB for device 86D89FF7
[Gatekeeper] Audit started on /media/gr0t/64 GB
[Gatekeeper] Final Decision: ALLOW for 058f:6387 Serial=86D89FF7
[Gatekeeper] Report updated: data/logs/gatekeeper_report_2026-02-05.txt
[Audit] 2026-02-05 00:19:59 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/.Trash-1000/info/rockyou.2.txt.trashinfo | SHA256=e3b0c44298fcl149afb4c8996fb92427ae41e4649b934ca495991b7852b855
[Audit] 2026-02-05 00:19:59 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/.Trash-1000/info/rockyou.2.txt.trashinfo.RZ6MK3 | SHA256=98010557b0f2371110db3dbb9c61d4f6fe72d8f4eeale785fa55084d1a1688f4
[Audit] 2026-02-05 00:19:59 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/.Trash-1000/info/rockyou.2.txt.trashinfo.RZ6MK3 | SHA256=98010557b0f2371110db3dbb9c61d4f6fe72d8f4eeale785fa55084d1a1688f4
[Audit] 2026-02-05 00:21:30 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/untitled folder/new file | SHA256=e3b0c44298fcl149afb4c8996fb92427ae41e4649b934ca495991b7852b855
[Audit] 2026-02-05 00:22:15 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/test1.txt | SHA256=e3b0c44298fcl149afb4c8996fb92427ae41e4649b934ca495991b7852b855
[Audit] 2026-02-05 00:22:15 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0t/64 GB/test1.txt | SHA256=e3b0c44298fcl149afb4c8996fb92427ae41e4649b934ca495991b7852b855
```

4. Device Removal and Report Generation :

The authorized USB device is safely removed. Gatekeeper records the event and generates a daily report summarizing all activity.

```
[Monitor] 2026-02-05 00:22:52 | unbind | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1/1-1:1.0
[Identify] 2026-02-05 00:22:52 | unknown:unknown | Serial: unknown | Path: /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1/1-1:1.0
[Policy] 2026-02-05 00:22:52 | BLOCK (unauthorized) | unknown:unknown | Serial=unknown
[Alert] Ignoring sub-event with unknown fingerprint: /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1/1-1:1.0
[Gatekeeper] Final Decision: BLOCK for unknown:unknown Serial=unknown
[Gatekeeper] Report updated: data/logs/gatekeeper_report_2026-02-05.txt
```

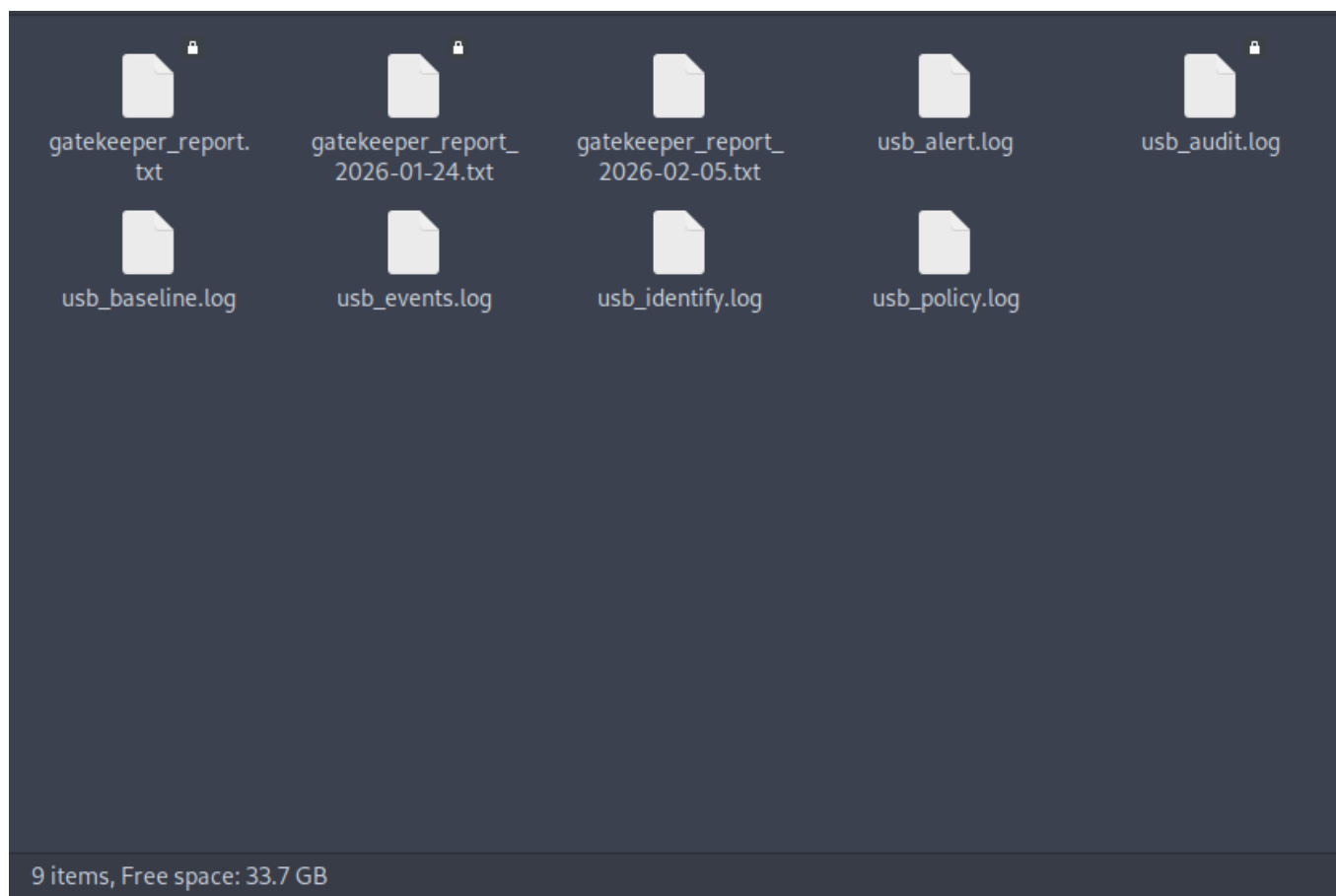
5. Unregistered USB Device Blocked :

An unknown USB device is connected. Policy rules enforce a DENY decision, and Gatekeeper logs the alert to prevent unauthorized access.

```
[root@parrot]~[/home/gr0t/Desktop/gatekeeper]
#python3 main.py
[Gatekeeper] USB Device Control & Monitoring Framework starting...
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-0:1.0
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.0
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-1
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.0
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1/2-2.1:1.1
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-2/2-2.1:1.0
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1
[Baseline] 2026-02-05 00:25:25 | baseline | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-0:1.0
[Gatekeeper] Monitoring USB events in real-time. Plug/unplug a device ...
[Monitor] 2026-02-05 00:25:34 | add | usb | /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
/home/gr0t/Desktop/gatekeeper/main.py:39: DeprecationWarning: Will be removed in 1.0. Access properties with Device.properties.
  if device_event:
[Identify] 2026-02-05 00:25:34 | cb25:125f | Serial: FA5055A1 | Path: /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
[Policy] 2026-02-05 00:25:34 | BLOCK (unauthorized) | cb25:125f | Serial=FA5055A1
[Alert] 2026-02-05 00:25:34 | BLOCKED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
Error looking up object for device /devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
[Gatekeeper] Final Decision: BLOCK for cb25:125f Serial=FA5055A1
[Gatekeeper] Report updated: data/logs/gatekeeper_report_2026-02-05.txt
```

6. Log Files Overview :

A consolidated view of monitor, alert, and audit logs. These files provide detailed records of device events, policy decisions, and file transfers.



7. Daily Report Snapshots :

Examples of generated daily reports (gatekeeper_report_YYYY-MM-DD.txt). Each report aggregates device events, alerts, and audit logs into a single summary.

```
=== Gatekeeper Report ===
Generated: 2026-02-05 00:25:34

>> Device Events (Monitor)
No monitor events recorded.

>> Policy Decisions (Alert)
2026-01-23 04:07:38 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 04:07:38 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 18:24:25 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 18:24:25 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 18:53:46 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 18:53:46 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 18:58:44 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 19:01:18 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 19:02:18 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 19:05:06 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
```

```
2026-01-23 22:22:08 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 22:24:35 | BLOCKED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-23 23:59:07 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-24 00:30:27 | BLOCKED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-24 00:31:40 | ALLOWED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-24 00:36:01 | ALLOWED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-01-24 00:36:55 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-02-05 00:15:44 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-02-05 00:18:58 | ALLOWED | 058f:6387 | Serial=86D89FF7 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
2026-02-05 00:25:34 | BLOCKED | cb25:125f | Serial=FA5055A1 | Path=/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1
```

```
>> File Transfers (Audit)
2026-01-23 19:54:40 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/.Trash-1000/info/OWASP_WSTG_Checklist.4.xlsx.trashinfo |
SHA256=e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

2026-01-23 19:54:40 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/.Trash-1000/info/OWASP_WSTG_Checklist.4.xlsx.trashinfo.WUHIJ3 |
SHA256=b3e22bcc52cac5847917a129648b462ab8f3fef71ab88f8b779387e301c57f19

2026-01-23 19:54:40 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/.Trash-1000/info/OWASP_WSTG_Checklist.4.xlsx.trashinfo.WUHIJ3 |
SHA256=b3e22bcc52cac5847917a129648b462ab8f3fef71ab88f8b779387e301c57f19

2026-01-23 19:54:51 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/OWASP Web Application Security Testing Checklist.docx |
SHA256=76ad30e8e4a753329eac5702fc0b09e349d5d01a79c17c34bf791958d0a3647e

2026-01-23 19:54:51 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/OWASP Web Application Security Testing Checklist.docx |
SHA256=76ad30e8e4a753329eac5702fc0b09e349d5d01a79c17c34bf791958d0a3647e

2026-01-23 19:54:51 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/OWASP Web Application Security Testing Checklist.docx |
SHA256=76ad30e8e4a753329eac5702fc0b09e349d5d01a79c17c34bf791958d0a3647e

2026-01-23 20:09:51 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/.Trash-1000/info/OWASP Web Application Security Testing Checklist.3.docx.trashinfo |
SHA256=e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

2026-01-23 20:09:51 | TRANSFER | 058f:6387 | Serial=86D89FF7 | File=/media/gr0ot/64 GB/.Trash-1000/info/OWASP Web Application Security Testing Checklist.3.docx.trashinfo.YYUYJ3 |
SHA256=d7431aa2143072e91708497ea76097d3eb7521f5d5f3765bb67952e1f486246
```