ForenClarity Linux Ubuntu v1.0.4

Commercial Release Documentation Pack

Installation, operation, alert validation, integrity protection, uninstall, troubleshooting, and QA evidence

Generated: 2026-07-01 | Product: ForenClarity | Platform: Ubuntu Linux

Table of Contents

1. Release acceptance summary

Commercial release decision

ForenClarity Linux Ubuntu v1.0.4 is accepted as the Ubuntu commercial release baseline. The tested lifecycle completed: release verification, install, service start/enable, GUI operation, scan detection, auto-refresh, reboot persistence, installed-file integrity, and uninstall of ForenClarity package/service/control-panel paths.

Scope of this document: this manual documents the ForenClarity Linux Ubuntu v1.0.4 package. Windows is documented separately. Parrot and Kali support are planned for later releases.

Area	Result
Release identity	ForenClarity Linux Ubuntu v1.0.4
Package validation	GPG-style release signature/checksum verification passed before installation.
Service	forenclarity.service active and enabled after install and after reboot.
GUI	Control Center title and header show v1.0.4; auto-refresh enabled by default.
Alert detection	Nmap SYN scan, hping3 packet test, and Nmap ping scan detected as expected.
Integrity	Installed-file integrity check: 10 OK, 0 changed, 0 missing.
Uninstall	ForenClarity package/service/control-panel/launcher removed; trial anchor retained by design.
Known limitation	Offline ZIP package is protected by signatures/checksums and installed integrity checks; root/admin can still bypass local-only enforcement. A future license server/signed repository is the stronger commercial option.

2. Package contents and commercial protection

The release ZIP should be distributed as the customer-facing Ubuntu package:

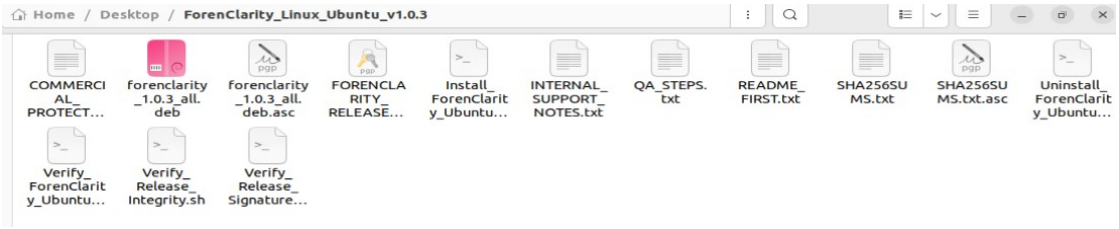
```
ForenClarity_Linux_Ubuntu_v1.0.4.zip
```

2.1 Expected package files

File	Purpose
forenclarity_1.0.4_all.deb	Main Debian package.
Install_ForenClarity_Ubuntu.sh	Installer wrapper with release verification and dependency planning.
Uninstall_ForenClarity_Ubuntu.sh	Uninstaller with SAFE_UNINSTALL, REMOVE_FC_DEPS, and PURGE_EVERYTHING modes.
Verify_ForenClarity_Ubuntu.sh	Post-install verification script.
Verify_Release_Integrity.sh	Release integrity gate: verifies checksums/signatures before install.
Verify_Release_Signature.sh	Signature verification helper.
SHA256SUMS.txt and signature file	Checksums and signature evidence for the release folder.
FORENCLARITY_RELEASE_PUBLIC_KEY.asc	Release verification public key.

README_FIRST.txt	Short first-run instructions.
QA_STEPS.txt	Optional QA validation steps.
COMMERCIAL_PROTECTION_NOTES.txt	Explains current tamper protection and limits.
INTERNAL_SUPPORT_NOTES.txt	Internal support notes; not normally needed by end users.

Screenshot reference - package folder layout:



2.2 What the current commercial protection does

Protection layer	What it does	Limit
Release signatures/checksums	Detects if ZIP contents, .deb, scripts, or notes were changed after packaging.	A user can still edit files, but verification should fail.
Installer verification gate	Installer refuses to continue when expected signature/checksum validation fails.	The .sh file remains readable because shell scripts are text.
Installed-file integrity	forenclarity-cli integrity checks installed product files after installation.	A privileged root/admin user can still modify local files if they intentionally bypass controls.
Root-owned installed files	Installed product paths are owned by root with stricter permissions.	Root can still alter anything locally.
Trial anchor continuity	Uninstall/reinstall on the same machine does not reset the protected local trial anchor.	A local-only trial is not as strong as an online license server.

Important commercial truth

The offline ZIP package is hardened, not impossible to tamper with. The next stronger commercial step is a signed package repository and/or server-side license validation. Do not claim the offline ZIP is 100% tamper-proof.

3. Pre-install checklist

Check	Required action
Ubuntu target	Tested on Ubuntu 22.04-style VM environment. Use a clean baseline for final QA.
Privileges	Installer requires sudo for package installation, service creation, repo additions, and system paths.
DNS/network after VM snapshot revert	After restoring/reverting a VM snapshot, reboot if needed and verify DNS before installing.
External components	Zeek and OSQuery are important product components; installer explains when external sources are needed.
Desktop launcher	Ubuntu/GNOME may require right-click -> Allow Launching once for the desktop icon.
USB transfer	If drag/drop is unreliable, copy the ZIP by USB and

	verify release integrity before install.

```
ping -c 3 google.com
```

4. Clean installation procedure

Use this procedure for a clean installation from the release ZIP. Optional scan tests are intentionally not included in the normal installation command.

```
cd ~/Desktop
unzip -o ForenClarity_Linux_Ubuntu_v1.0.4.zip
cd ForenClarity_Linux_Ubuntu_v1.0.4

{
  echo "===== DNS CHECK ====="
  ping -c 3 google.com

  echo "===== RELEASE INTEGRITY CHECK ====="
  ./Verify_Release_Integrity.sh

  echo "===== INSTALL ALL ====="
  sudo ./Install_ForenClarity_Ubuntu.sh --install-all

  echo "===== START/ENABLE SERVICE ====="
  forenclarity-cli start
  forenclarity-cli enable

  echo "===== STATUS ====="
  forenclarity-cli status

  echo "===== INTEGRITY ====="
  forenclarity-cli integrity
} 2>&1 | tee ~/Desktop/forenclarity_ubuntu_v1_0_4_install_output.txt
```

4.1 Expected installation result

Expected line/result	Meaning
release signature/checksum verification passed	The installer verified the release contents before continuing.
ForenClarity Linux Ubuntu v1.0.4	Installer, package, CLI, service, and GUI identity are aligned.
Active interface detected: ens33	The installer found the active Ubuntu VM interface. Interface names may differ on other machines.
OSQuery and Zeek already installed or installed externally	Required/important components are present.
active / enabled	The service is running and configured for boot.
ForenClarity installed-file integrity check: 10 OK, 0 changed, 0 missing	Installed product files match the integrity manifest.

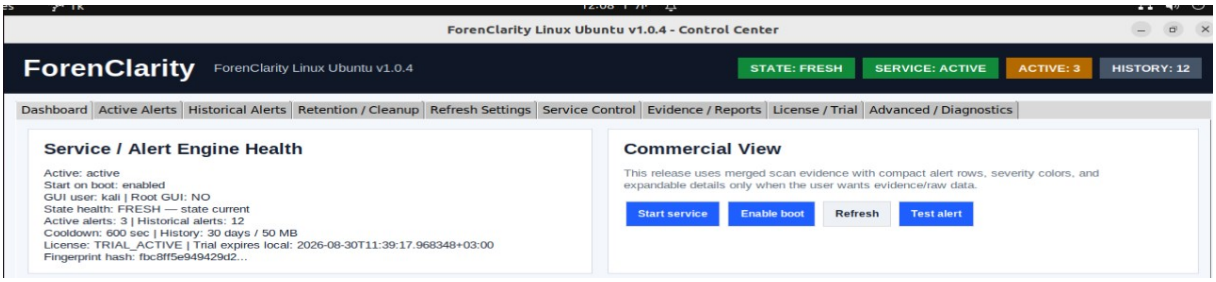
5. Control Center user manual

Launch the GUI as the normal user, not as root:

Desktop launcher note
On Ubuntu/GNOME, the desktop icon may show as untrusted. Right-click it once and choose Allow Launching. This is normal desktop security behavior, not a ForenClarity failure.

5.1 Dashboard tab

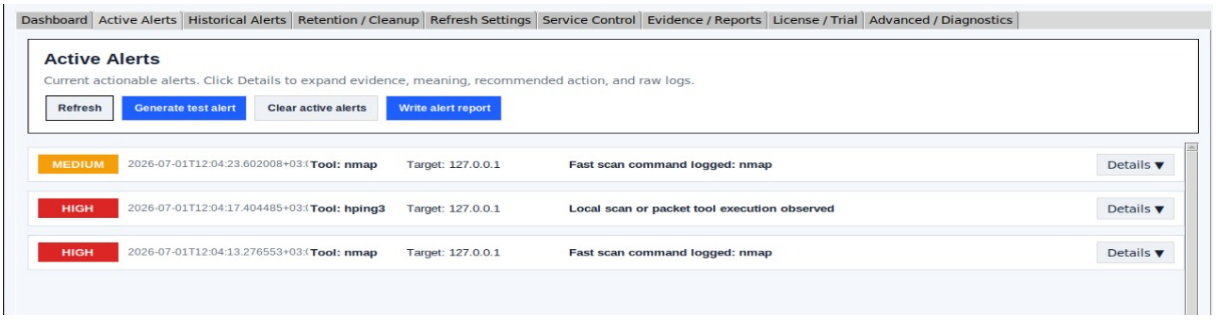
The Dashboard is the operator overview: service health, active count, history count, cooldown, license state, fingerprint hash, and recent service log lines.



Field	Meaning
STATE: FRESH	Runtime state is current.
SERVICE: ACTIVE	Background evidence/alert service is running.
ACTIVE	Number of current actionable alerts.
HISTORY	Number of retained historical alert records.
GUI user / Root GUI	Confirms GUI is running as normal user, not root.
Cooldown	Deduplication/cooldown interval for repeated matching alerts.
License	Local trial/license status.

5.2 Active Alerts tab

Active Alerts contains current actionable findings. Rows are compact by default; use Details to expand evidence, meaning, recommended action, and raw logs.



Column/Action	Meaning
Severity color	High/medium/info visual priority.
Tool	Detected local scan or packet tool, such as nmap or hping3.
Target	Parsed target when available.
Details	Expands full technical evidence and recommended action.
Clear active alerts	Moves/clears current active view according to

	product logic; history remains retained.
Write alert report	Creates a report under the user output folder.

5.3 Historical Alerts tab

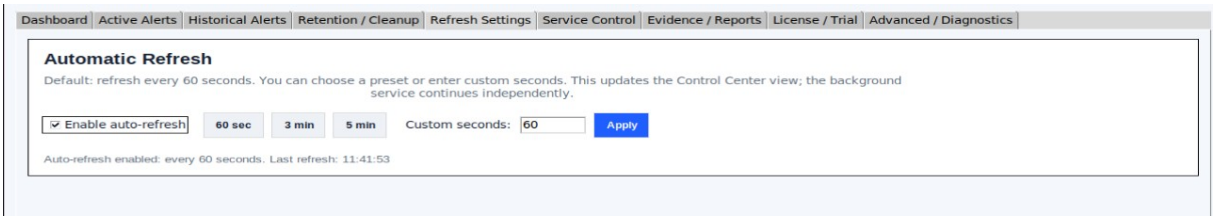
Historical Alerts is the longer-term record. Evidence remains available but is collapsed by default. History can be retained even after active alerts are cleared. After SAFE_UNINSTALL/reinstall, history can remain by design; after PURGE_EVERYTHING, ForenClarity evidence paths are removed except the protected trial anchor.

5.4 Retention / Cleanup tab

Retention controls local alert history limits. Defaults: 10-minute cooldown, 30-day history, 50 MB history cap. Presets adjust the local retention configuration.

5.5 Refresh Settings tab

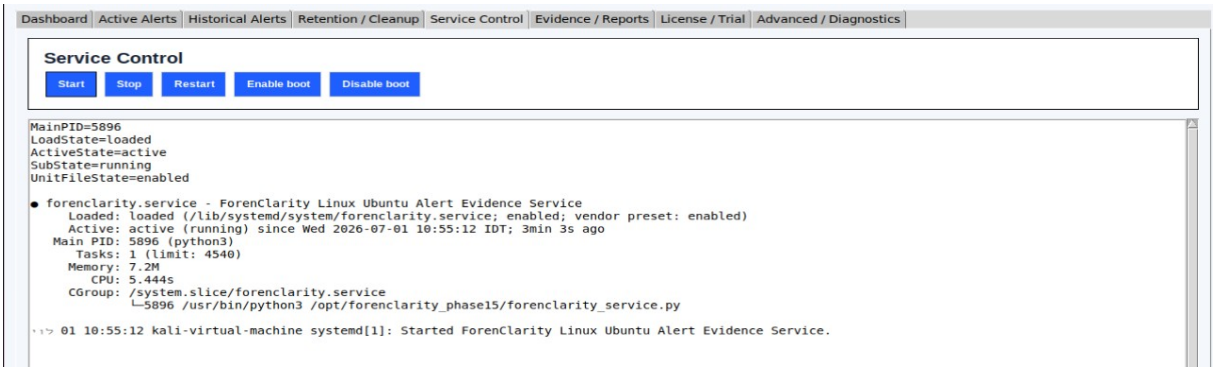
v1.0.4 includes automatic GUI refresh. Default is enabled every 60 seconds. Users can choose 60 seconds, 3 minutes, 5 minutes, or custom seconds. Manual Refresh buttons remain available.



Control	Expected behavior
Enable auto-refresh	Checked by default.
60 sec	Default automatic refresh interval.
3 min / 5 min	Preset slower intervals.
Custom seconds + Apply	Allows the user to set a manual refresh period.
Last refresh	Shows the last time the GUI view updated.

5.6 Service Control tab

Start, Stop, Restart, Enable boot, and Disable boot control the ForenClarity systemd service. The output panel shows systemd state and recent service status.

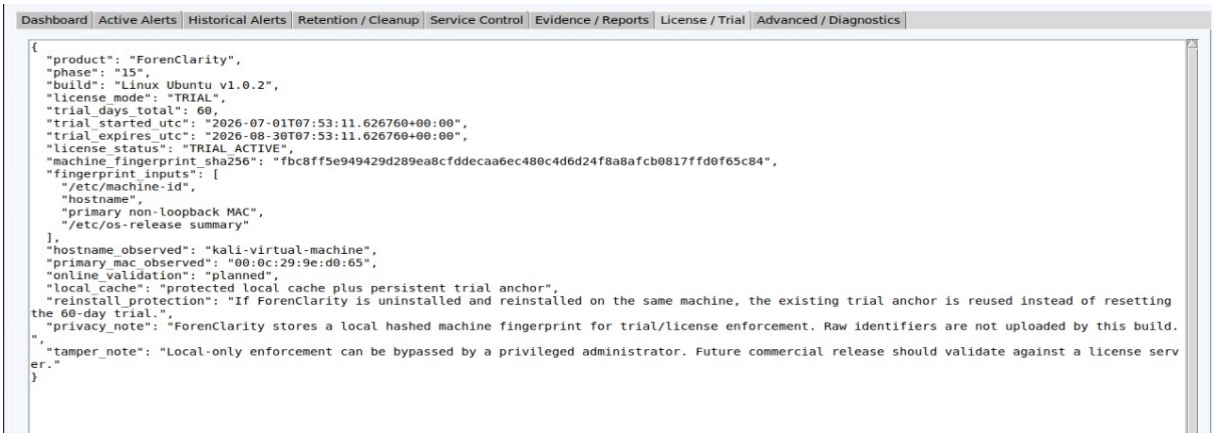


5.7 Evidence / Reports tab

Write full report creates a report under the user output path. Open output folder opens the folder where reports are stored. A blank output panel before running a report is normal.

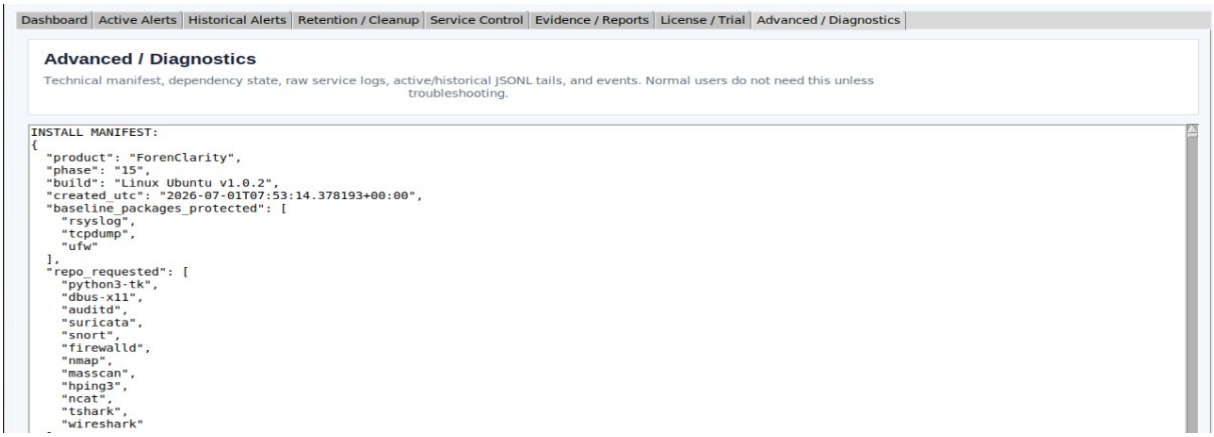
5.8 License / Trial tab

Shows the 60-day local trial placeholder, trial start/expiry, hashed machine fingerprint, and privacy/tamper notes. Raw identifiers are not uploaded.



5.9 Advanced / Diagnostics tab

For support and troubleshooting only. It can show install manifest data, dependency state, raw service logs, active/historical JSONL tails, and events. Normal users do not need this tab unless support asks for it.



6. Optional QA scan validation

Not normal customer operation

The scan validation commands intentionally run sudo-based tools such as nmap and hping3. These prompts are expected in QA. Normal customer use does not require running these tests.

```
{
  echo "===== CLEAR ACTIVE ====="
  forenclarity-cli clear-active

  echo "===== BASELINE ====="
  forenclarity-cli status
  forenclarity-cli alerts

  echo "===== NMAP SYN SCAN ====="
  sudo nmap -sS -T4 127.0.0.1
  sleep 4
```

```
  echo "===== HPING3 TEST ====="
  sudo hping3 -S -c 3 -p 80 127.0.0.1
  sleep 4

  echo "===== NMAP PING SCAN ====="
  sudo nmap -sn 127.0.0.1
  sleep 70

  echo "===== STATUS AFTER AUTO-REFRESH WAIT ====="
  forenclarity-cli status

  echo "===== ALERTS ====="
  forenclarity-cli alerts

  echo "===== INTEGRITY ====="
  forenclarity-cli integrity
} 2>&1 | tee ~/Desktop/forenclarity_ubuntu_v1_0_4_auto_refresh_scan_output.txt
```

Expected result	Details
Baseline active alerts: 0	After clear-active, there should be no current actionable alerts.
After scans active alerts: 3	Nmap SYN, hping3, and Nmap ping scan are detected.
Auto-refresh shows Active: 3	Do not press Refresh; wait about 60-70 seconds and the GUI should update itself.
All alert product/version fields show v1.0.4	No v1.0.2/v1.0.3 mismatch.
Integrity 10 OK, 0 changed, 0 missing	Scan activity did not alter product files.

7. Reboot validation

```
sudo reboot
```

```
{
  systemctl status forenclarity.service --no-pager
  systemctl is-enabled forenclarity.service
  forenclarity-cli status
  forenclarity-cli alerts
  forenclarity-cli integrity
} 2>&1 | tee ~/Desktop/forenclarity_ubuntu_v1_0_4_reboot_output.txt
```

Expected result	Meaning
forenclarity.service active (running)	Service survived reboot.
enabled	Service will start on boot.
status says v1.0.4	Version identity is consistent after reboot.
integrity 10 OK, 0 changed, 0 missing	Installed product files remain valid.

8. Uninstall and cleanup procedure

Mode	What it removes	When to use
SAFE_UNINSTALL	ForenClarity package/service/control panel only. Keeps dependencies,	Use before upgrading/reinstalling without re-downloading dependencies.

	evidence, and trial anchor.	
REMOVE_FC_DEPS	ForenClarity plus manifest-recorded packages installed by ForenClarity, while protecting pre-existing packages.	Use when removing product and its installed dependencies, but not evidence/trial paths.
PURGE_EVERYTHING	ForenClarity, manifest dependencies where applicable, evidence/log/license/runtime paths. Keeps protected trial anchor by design.	Final QA cleanup or customer full removal.

```
cd ~/Desktop/ForenClarity_Linux_Ubuntu_v1.0.4
sudo ./Uninstall_ForenClarity_Ubuntu.sh 2>&1 | tee
~/Desktop/forenclarity_ubuntu_v1_0_4_purge_uninstall_output.txt
```

For final cleanup choose PURGE_EVERYTHING, confirm with REMOVE_CONFIRMED, and choose KEEP for installer ZIP/folder unless you intentionally want to delete the transferred package files.

Dependency protection behavior
v1.0.4 was validated after a SAFE_UNINSTALL from v1.0.3. Because dependencies already existed, v1.0.4 correctly protected them during its purge. Full dependency purge was already proven in v1.0.2 from clean-zero install. This is correct customer-protection behavior, not a v1.0.4 failure.

9. Troubleshooting and operational notes

Symptom	Cause	Action
DNS fails after snapshot revert	VM networking/DNS may not fully recover after revert.	Reboot VM, then run ping -c 3 google.com before install.
Desktop icon asks to Allow Launching	Ubuntu/GNOME desktop launcher trust behavior.	Right-click -> Allow Launching once.
GUI did not immediately show alerts	Manual refresh disabled or waiting for interval.	v1.0.4 auto-refresh defaults to 60 sec; wait or press Refresh.
Historical alerts are nonzero after reinstall	SAFE_UNINSTALL keeps evidence/history.	Expected. Use PURGE_EVERYTHING for evidence cleanup.
Bottom dashboard log shows old version after SAFE_UNINSTALL upgrade	Retained service/runtime logs from previous installations.	Expected in upgrade test path. Clean purge install should not retain old logs.
Nmap appears to hang briefly	Terminal waits for command completion/sleep in test script.	Expected if the command is still running; wait for prompt.
Integrity reports changed/missing files	Product files modified, wrong package, or damaged installation.	Do not accept release; reinstall signed v1.0.4 and rerun integrity.
Uninstall does not remove dependencies	Dependencies existed before current install or were protected by manifest.	Expected protection. Avoid removing customer-owned packages silently.

10. Evidence summary and acceptance decision

Evidence file	Result summary
forenclarity_ubuntu_v1_0_4_install_output.txt	Release verification passed; install succeeded; service

	active/enabled; integrity 10 OK.
forenclarity_ubuntu_v1_0_4_auto_refresh_scan_output.txt	Baseline 0 active; scan test produced 3 active alerts; all alert product/version fields show v1.0.4; integrity 10 OK.
forenclarity_ubuntu_v1_0_4_reboot_output.txt	Service active after reboot; enabled; status v1.0.4; integrity 10 OK.
forenclarity_ubuntu_v1_0_4_purge_uninstall_output.txt	ForenClarity package/service/commands removed; trial anchor retained; dependencies protected because they pre-existed current install.

Final Ubuntu release decision

ForenClarity Linux Ubuntu v1.0.4 is the accepted Ubuntu commercial release. Keep v1.0.4 as the published Ubuntu package and documentation baseline. as rejected/superseded.

Appendix A. Command reference

A.1 Quick status

```
forenclarity-cli status
forenclarity-cli integrity
forenclarity-cli alerts
```

A.2 Service control

```
forenclarity-cli start
forenclarity-cli stop
forenclarity-cli restart
forenclarity-cli enable
forenclarity-cli disable
```

A.3 Reports

```
forenclarity-cli report
find ~/forenclarity_output /var/log/forenclarity -type f | sort
```

A.4 Release integrity before install

```
cd ~/Desktop/ForenClarity_Linux_Ubuntu_v1.0.4
./Verify_Release_Integrity.sh
```

A.5 Normal GUI launch

```
forenclarity-control-panel
```

Appendix B. Screenshot reference

The screenshots in this documentation are cropped to focus on the product UI and avoid retaining old diagnostic log text from upgrade test paths. The final accepted GUI identity is v1.0.4.