ForenClarity

Parrot OS v1.0.0

Installation, Operations, Validation and Uninstall Guide

Commercial 60-day evaluation release
Validated on Parrot Security 7.3 (Debian 13.5, KDE Plasma X11, x86_64)

Release documentation - July 2026

Contents

1. Product overview

ForenClarity Parrot OS v1.0.0 is a privacy-conscious security evidence and alerting tool designed to reduce analyst fatigue. It collects local evidence, filters repetitive noise, merges related observations, explains the meaning of findings, and guides the operator toward the next action.

- Runs as a systemd service; the graphical control center is optional.
- No forced reboot during installation.
- No cloud upload in this release.
- Uses local-time display in the GUI and reports; UTC remains available in structured data.
- Separates active alerts from historical alerts and applies a 10-minute deduplication/cooldown window.
- Produces HTML, JSON and text evidence reports.

Validated release: The v1.0.0 package completed installation, reboot persistence, launcher, alert, report, trial-continuity and clean-uninstall testing on Parrot Security 7.3.

2. Supported platform and prerequisites

Item	Validated configuration
Operating system	Parrot Security 7.3 (echo), Debian 13.5
Architecture	x86_64 / amd64
Desktop	KDE Plasma, X11
Python	Python 3.13.x
Privileges	sudo/root required for install, service control and uninstall
Network	Internet access required to install repository dependencies and optional OSQuery
Disk	Allow at least 300 MB free for dependencies, logs and reports

The installer detects the active network interface and calculates the local network range for Snort HOME_NET configuration. It also records which packages existed before installation so the uninstaller can protect them.

3. Release package contents

Public ZIP filename:

```
ForenClarity_Parrot_OS_v1.0.0.zip
```

File	Purpose
Install_ForenClarity_Parrot.sh	Interactive installer and dependency manifest creator.
Uninstall_ForenClarity_Parrot.sh	Safe uninstall, dependency removal and purge workflow.
Verify_Build_Integrity.sh	User-facing SHA-256 package integrity verification.
Verify_Release_Integrity.sh	Equivalent release integrity verifier.
Verify_ForenClarity_Parrot.sh	Post-install package, service, dependency and state verification.
forenclarity_1.0.0_all.deb	ForenClarity application, service, CLI and control center package.
FILE_SHA256SUMS.txt	SHA-256 values for release files.
CHECKSUM_INFORMATION.txt	Checksum and verification explanation.
README_FIRST.txt	Quick-start instructions.
VALIDATION_GUIDE.txt	Release validation procedure.
RELEASE_NOTES.txt	Version summary and known limitations.

4. Verify package integrity

Always verify the extracted release before installation. The verifier checks each packaged file against FILE_SHA256SUMS.txt.

```
cd ~/Desktop
unzip ForenClarity_Parrot_OS_v1.0.0.zip
cd ForenClarity_Parrot_OS_v1.0.0
chmod +x Verify_Build_Integrity.sh
./Verify_Build_Integrity.sh
```

Expected final line:

```
PASSED: release file checksums are valid.
```

Stop condition: Do not install if any file reports FAILED, MISSING, or a checksum mismatch. Obtain a clean copy of the release package.

5. Installation procedure

From the extracted release folder, start the installer:

```
sudo ./Install_ForenClarity_Parrot.sh
```

5.1 Installer confirmations

1. Review the detected interface, IP/CIDR, protected baseline packages and dependency plan.
2. Type INSTALL_FORENCLARITY to continue.
3. When offered OSQuery, type INSTALL_OSQUERY to install it, or press another value to skip.
4. At the final service prompt, type START_AND_ENABLE to start the service immediately and enable it at boot.

```
INSTALL_FORENCLARITY
INSTALL_OSQUERY
START_AND_ENABLE
```

5.2 Installation behavior

- Installs only missing repository dependencies.
- Creates an install manifest distinguishing pre-existing packages from packages installed by ForenClarity.
- Creates an Applications menu launcher and an executable Desktop launcher.
- Creates and enables forenclarity.service when START_AND_ENABLE is selected.
- Creates the protected local trial anchor and license state.
- Does not require or force a reboot.

Zeek on Parrot 7.3: Zeek is intentionally skipped because the currently available external Debian package requires an incompatible libc ABI. Installation continues safely without Zeek.

6. First start and post-reboot validation

6.1 Immediate verification

```
systemctl is-active forenclarity.service
systemctl is-enabled forenclarity.service
forenclarity-cli status
```

Expected service responses are active and enabled.

6.2 Reboot persistence

```
sudo reboot
```

After login:

```
systemctl is-active forenclarity.service
systemctl is-enabled forenclarity.service
```

6.3 Launchers

- Open ForenClarity Control Center from the Desktop launcher.
- Open it again from the Applications menu to verify both launch paths.
- On first use, KDE may request “Allow Launching” for the Desktop shortcut.

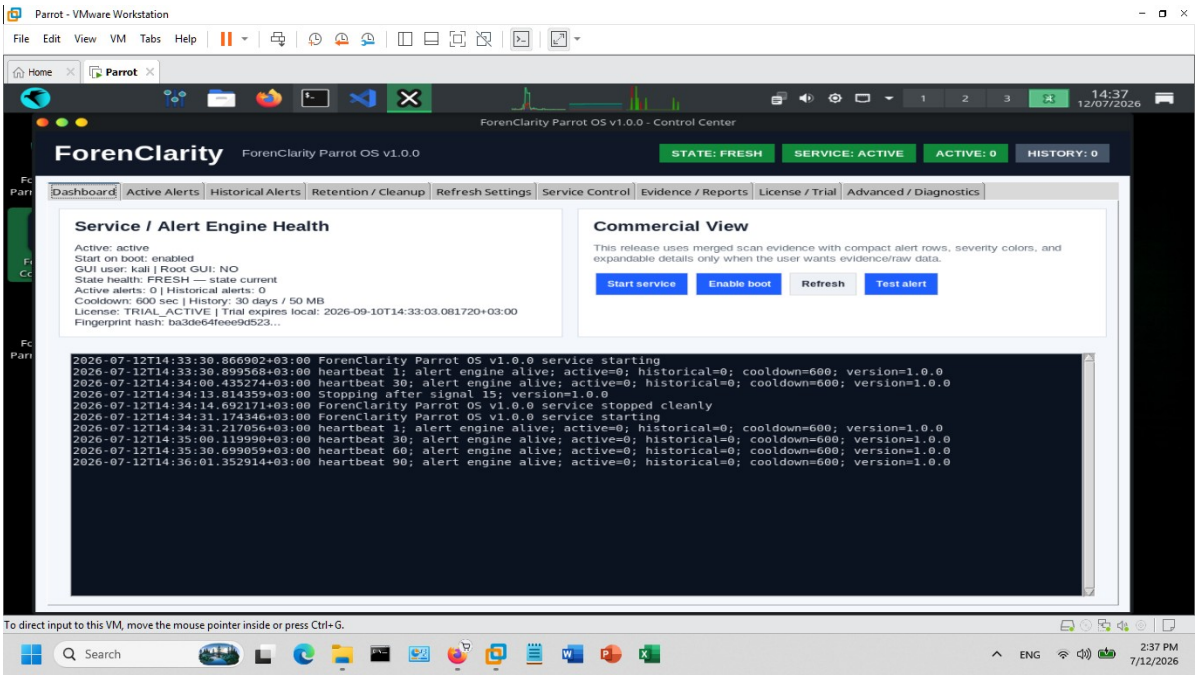

Figure 1. ForenClarity Parrot OS v1.0.0 dashboard with active and enabled service.

7. Control Center overview

Tab	Purpose
Dashboard	Service and alert-engine health, trial state, heartbeat log and quick actions.
Active Alerts	Current actionable alerts with expandable evidence, meaning and recommended action.
Historical Alerts	Previously cleared or aged alerts retained according to policy.
Retention / Cleanup	Retention days, size limits and cleanup controls.
Refresh Settings	Refresh behavior and display update settings.
Service Control	Start, stop, restart and boot-enable controls.
Evidence / Reports	Generate and locate HTML, JSON and text reports.
License / Trial	Trial status, expiry, fingerprint information and privacy note.
Advanced / Diagnostics	Runtime state, logs and detailed diagnostic information.

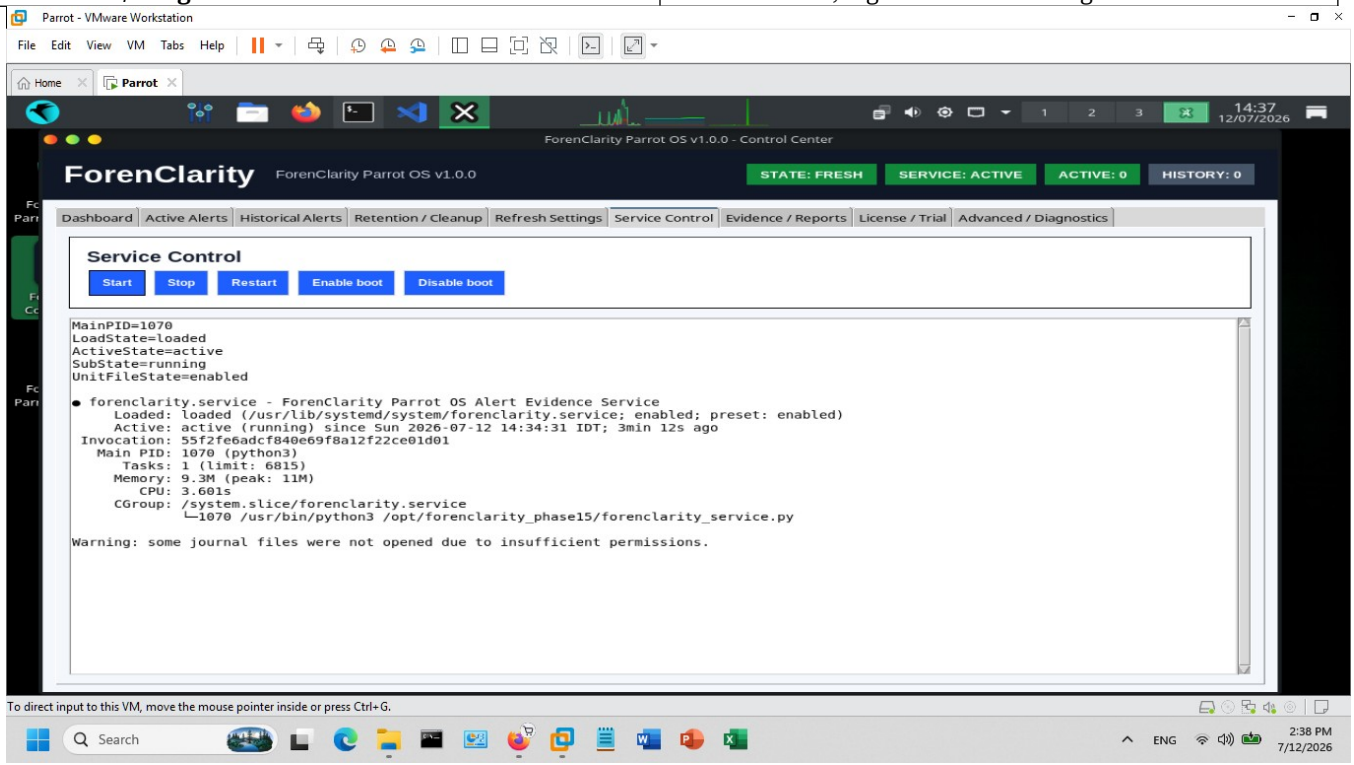

Figure 2. Service Control page showing the active systemd unit and boot-enabled state.

Normal journal warning: A non-root GUI may display “some journal files were not opened due to insufficient permissions.” This does not mean the service failed; use sudo journalctl for full system journal access.

8. Alerts, evidence and reports

8.1 Controlled alert validation

To validate local scan detection on the same host:

```
sudo nmap -sS -T4 127.0.0.1
sleep 5
forenclarity-cli alerts
```

A successful detection should produce one HIGH alert for nmap, capture the target 127.0.0.1, and merge process-table evidence with auditd evidence when both are available. Bare process-only observations without a meaningful target are suppressed to reduce noise.

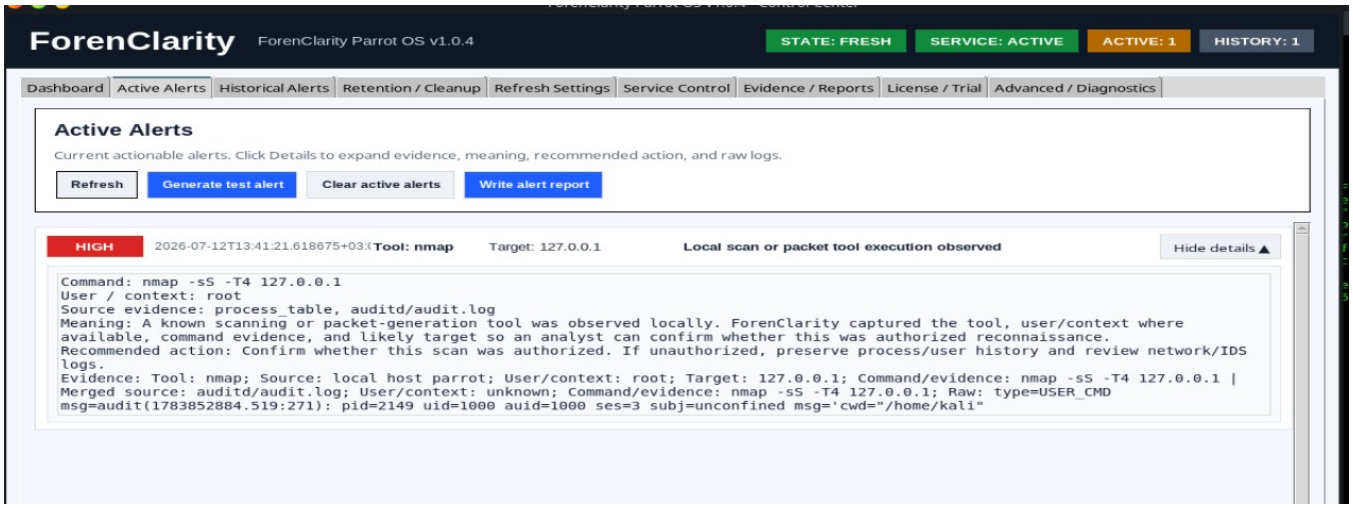

Figure 3. Merged Nmap alert showing tool, target, command, evidence sources, explanation and recommended action.

8.2 Report generation

```
forenclarity-cli report
```

Reports are generated beneath the user output directory, normally:

```
~/forenclarity_output/
```

- HTML - readable analyst report.
- JSON - structured evidence for automation or archival.
- TXT - portable plain-text summary.

9. Trial, privacy and local protection

- The evaluation period is 60 days.
- The local trial anchor survives uninstall/reinstall so reinstalling on the same machine does not reset the trial.
- The fingerprint combines machine-id, hostname, a selected non-loopback MAC address, and OS information, then stores a SHA-256 hash.
- Raw identifiers are not uploaded by this release.
- The protected anchor is retained under /var/lib/forenclarity-trial.
- Local-only licensing can ultimately be bypassed by a privileged administrator; server-side validation is planned for stronger commercial enforcement.

Privacy model: This release performs no cloud upload. Evidence, reports, alert state and licensing data remain on the local machine unless the operator manually exports or transfers them.

9.1 Important paths

```
/var/lib/forenclarity/
/var/lib/forenclarity-trial/
/var/log/forenclarity/
/opt/forenclarity_phase15/
~/forenclarity_output/
```

10. Service and command reference

Command	Use
forenclarity-control-panel	Open the normal-user graphical control center.
forenclarity-cli status	Show service, trial and alert state.
forenclarity-cli alerts	Display recent active alerts.
forenclarity-cli report	Generate evidence reports.
sudo systemctl start forenclarity.service	Start the service.
sudo systemctl stop forenclarity.service	Stop the service.
sudo systemctl restart forenclarity.service	Restart the service.
sudo systemctl enable forenclarity.service	Enable service startup at boot.
sudo systemctl disable forenclarity.service	Disable service startup at boot.
sudo journalctl -u forenclarity.service	Read the complete service journal as root.

11. Uninstall options and clean removal

Run the uninstaller from the extracted release folder. The control center may remain open; the uninstaller closes open or hidden control-panel processes automatically.

```
cd /path/to/ForenClarity_Parrot_OS_v1.0.0
sudo ./Uninstall_ForenClarity_Parrot.sh
```

11.1 Available modes

Mode	Effect
SAFE_UNINSTALL	Remove ForenClarity package, service and control panel; keep dependencies and evidence.
REMOVE_FC_DEPS	Remove ForenClarity and only currently installed packages recorded by the manifest as installed by ForenClarity.
PURGE_EVERYTHING	Remove ForenClarity, manifest-recorded dependencies, evidence, logs, license runtime state and application paths. The protected trial anchor remains.

11.2 Full clean uninstall

```
PURGE_EVERYTHING
REMOVE_CONFIRMED
CLEAN_INSTALLER_FILES
```

CLEAN_INSTALLER_FILES removes the extracted installer folder from its actual current location and removes the matching ZIP when it can be safely identified in the same parent directory. If the ZIP is not found, the user receives a clear message; the uninstaller does not perform a broad unsafe search.

- Pre-existing packages such as ufw and tcpdump remain protected.
- The open dashboard closes automatically.
- The Applications and Desktop launchers are removed.
- The CLI and control-panel command wrappers are removed.
- The uninstall transcript is retained on the user Desktop.
- /var/lib/forenclarity-trial remains intentionally for trial continuity.

Validated result: The release uninstall test left no package, service, process, command, launcher, runtime path, installer folder or installer ZIP. Only the protected trial anchor remained.

12. Troubleshooting

Symptom	Action
Service is inactive after install	The final installer prompt may not have received START_AND_ENABLE. Run: sudo systemctl enable --now forenclarity.service.
Desktop launcher is untrusted	Right-click the launcher and choose Allow Launching, or use the Applications menu.
Control panel closes to background	The close button hides the control center while the service continues. Reopen it from the launcher or run forenclarity-control-panel.
CLI appears after uninstall but file is gone	The shell may have cached the command path. Run hash -r and check again.
Full journal is not visible in GUI	Use sudo journalctl -u forenclarity.service.
Zeek is not installed	Expected on Parrot 7.3 due to external package libc incompatibility.
Integrity verifier reports failure	Delete the extracted folder, obtain a clean ZIP, extract again and do not install until all checks pass.
Matching installer ZIP cannot be found during cleanup	The uninstaller removes the current extracted folder and reports the missing ZIP. Remove a separately moved ZIP manually after confirming its filename.

13. Known limitations

- Zeek is unavailable in this Parrot 7.3 release because the available external Debian package targets an incompatible libc ABI.
- The 60-day evaluation uses local enforcement. A root administrator can alter or delete local protection data; online license validation is planned.
- The release is currently unsigned. Customers should verify the bundled SHA-256 manifest and the published outer ZIP checksum.
- ForenClarity does not upload data to a cloud service in this version. Remote management and centralized licensing are not included.
- The GUI is optional and runs as the normal desktop user; privileged journal entries require sudo access outside the GUI.

14. Release acceptance checklist

- ☐ Public ZIP name is ForenClarity_Parrot_OS_v1.0.0.zip.
- ☐ Verify_Build_Integrity.sh reports PASSED.
- ☐ Installer uses public wording and INSTALL_FORENCLARITY.
- ☐ Package version is 1.0.0.
- ☐ Service installs, starts and is enabled.
- ☐ Service remains active and enabled after reboot.
- ☐ Desktop and Applications launchers open the control center.
- ☐ Dashboard displays v1.0.0 and no internal build/final/QA wording.
- ☐ Trial displays active state and local expiry.
- ☐ Controlled Nmap test produces one enriched alert without a bare duplicate.
- ☐ Reports generate in HTML, JSON and TXT formats.
- ☐ PURGE_EVERYTHING closes the open dashboard.
- ☐ Manifest removal protects pre-existing packages.
- ☐ CLI, service, launchers, runtime paths and dependencies installed by ForenClarity are removed.
- ☐ CLEAN_INSTALLER_FILES removes the extracted folder and matching ZIP.
- ☐ Only /var/lib/forenclarity-trial remains intentionally.

Release status: ACCEPTED - ForenClarity Parrot OS v1.0.0

This guide reflects the validated July 12, 2026 release procedure and should be distributed with the public Parrot OS download.