# ForenClarity

## Kali Linux v1.0.0

Installation, Operations, Validation and Uninstall Guide

Commercial 60-day evaluation release
Validated on Kali Linux 2026.2, x86_64

**RELEASE STATUS** ACCEPTED — complete installation, reboot-persistence, launcher, alert, reporting, SAFE_UNINSTALL and PURGE_EVERYTHING validation completed on the clean 13 July 2026 commercial QA baseline.

*Release documentation — 13 July 2026*

# Contents

# 1. Product overview

ForenClarity Kali Linux v1.0.0 is a privacy-conscious security evidence and alerting tool designed to reduce analyst fatigue. It collects local evidence, suppresses 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.
- Does not force a reboot during installation.
- Performs no cloud upload in this release.
- Displays local time in the GUI and reports; UTC remains available in structured data.
- Separates active alerts from historical alerts and applies an approximately 10-minute deduplication/cooldown window.
- Produces HTML, JSON and plain-text evidence reports.
- Includes a protected 60-day local evaluation state with reinstall continuity.

**Commercial release scope** This guide applies to the accepted public Kali Linux v1.0.0 package. Internal build labels and QA-only wording must not appear in the distributed package or user interface.

# 2. Supported platform and prerequisites

| Item | Validated configuration |
|---|---|
| Operating system | Kali Linux 2026.2 |
| Architecture | x86_64 / amd64 |
| Service manager | systemd |
| Privileges | sudo/root required for installation, service administration and uninstall |
| Network | Internet access required for missing repository dependencies and optional OSQuery installation |
| Disk space | Allow at least 300 MB for application files, dependencies, logs and reports |
| Desktop | A graphical desktop session is required only for the optional Control Center and launchers |

The installer detects the active network interface, records the local network context used by supported sensors, and creates a package baseline so that uninstall operations can protect software that existed before ForenClarity was installed.

**Clean-baseline requirement** Commercial acceptance was performed from the clean Kali Linux snapshot dated 13 July 2026. For independent acceptance testing, begin from a known-clean VM snapshot or fully documented endpoint baseline.

# 3. Release package contents

Public ZIP filename:

```
ForenClarity_Kali_Linux_v1.0.0.zip
```

| File | Purpose |
|---|---|
| Install_ForenClarity_Kali.sh | Interactive installer and dependency-manifest creator. |
| Uninstall_ForenClarity_Kali.sh | SAFE_UNINSTALL, dependency-removal and PURGE_EVERYTHING workflow. |
| Verify_Build_Integrity.sh | User-facing SHA-256 release-file verification. |
| Verify_Release_Integrity.sh | Equivalent release integrity verifier. |
| Verify_ForenClarity_Kali.sh | Post-install package, service, dependency and state verification. |
| forenclarity_1.0.0_all.deb | Application, service, CLI and Control Center package. |
| FILE_SHA256SUMS.txt | SHA-256 values for all release files. |
| CHECKSUM_INFORMATION.txt | Checksum and verification explanation. |
| README_FIRST.txt | Concise quick-start instructions. |
| VALIDATION_GUIDE.txt | Release validation procedure. |
| RELEASE_NOTES.txt | Version summary and known limitations. |

**Package cleanliness** The public archive should contain only current release files. Do not include old logs, screenshots from prior operating-system editions, duplicate evidence, temporary build artifacts, or internal QA notes.

# 4. Verify package integrity

Always verify the extracted release before installation. The verifier checks each packaged file against the SHA-256 manifest stored inside the release package.

```
cd ~/Desktop
unzip ForenClarity_Kali_Linux_v1.0.0.zip
cd ForenClarity_Kali_Linux_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. Delete the extracted folder, obtain a clean release ZIP, extract it again, and re-run verification.

# 5. Installation procedure

From the verified release folder, start the installer:

```
sudo ./Install_ForenClarity_Kali.sh
```

### 5.1 Installer confirmations

1. Review the detected operating system, active interface, protected baseline packages and dependency plan.
2. Type INSTALL_FORENCLARITY to authorize installation.
3. When offered OSQuery, type INSTALL_OSQUERY to install it, or select the documented skip option.
4. At the final service prompt, type START_AND_ENABLE to start the service immediately and enable startup at boot.

```
INSTALL_FORENCLARITY
INSTALL_OSQUERY
START_AND_ENABLE
```

### 5.2 Installation behavior

- Installs only missing repository dependencies.
- Creates an install manifest that distinguishes pre-existing packages from packages installed by ForenClarity.
- Creates Applications-menu and Desktop launchers for the Control Center.
- 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.

**Do not patch an installed release** When a release defect is confirmed, rebuild and reinstall a clean package. Do not modify files in place and then treat the endpoint as a validated commercial baseline.

## 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. The CLI should report the v1.0.0 application state, active trial status, and current alert counts.

### 6.2 Reboot persistence

```
sudo reboot
```

After login, repeat:

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

### 6.3 Launchers

5. Open ForenClarity Control Center from the Desktop launcher.
6. Open it again from the Applications menu to verify both launch paths.
7. If the desktop environment requests trust confirmation, select Allow Launching.

# 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 | Historical retention period, size limit 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, machine fingerprint information and privacy notice. |
| Advanced / Diagnostics | Runtime state, logs and detailed diagnostic information. |

**Normal journal warning** A normal-user GUI may report that some journal files could not be opened because of insufficient permissions. This does not indicate service failure. Use sudo journalctl for complete 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 test should produce one enriched HIGH alert for nmap, capture target 127.0.0.1, and merge useful process and audit evidence when available. Bare observations without a meaningful target should be suppressed to reduce noise.

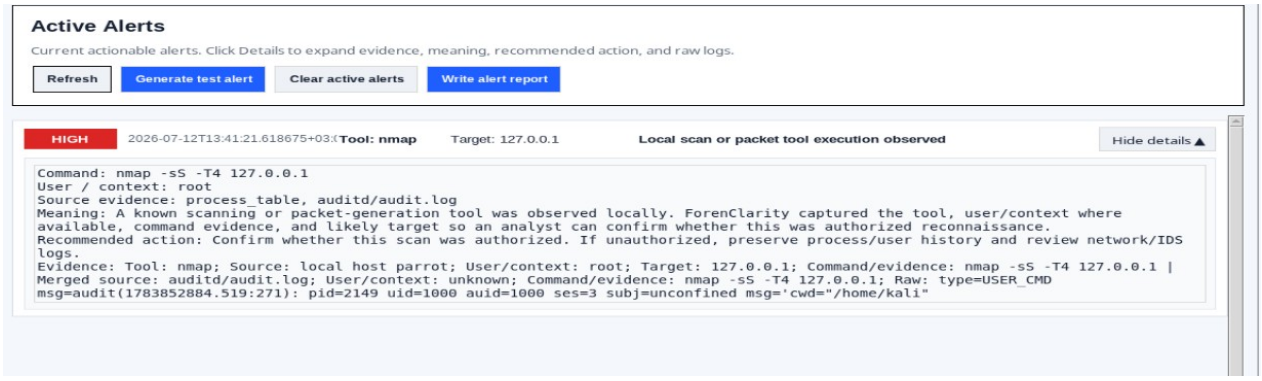


*Figure 1. Representative Active Alerts detail view. The screenshot is cropped to focus on the validated evidence presentation.*

### 8.2 Report generation

```
forenclarity-cli report
```

Reports are normally generated beneath:

```
~/forenclarity_output/
```

| Format | Use |
|---|---|
| HTML | Readable analyst report for review and case documentation. |
| JSON | Structured evidence for automation, archival or downstream processing. |
| TXT | Portable plain-text summary for simple transfer or terminal review. |

## 9. Trial, privacy and local protection

- The evaluation period is 60 days.
- The protected local trial anchor survives uninstall/reinstall so reinstalling on the same machine does not reset the trial.
- The fingerprint combines multiple machine and operating-system signals and stores a derived hash rather than a user-facing raw identifier.
- This release does not upload licensing or evidence data to a cloud service.
- The protected anchor remains under /var/lib/forenclarity-trial after SAFE_UNINSTALL and PURGE_EVERYTHING.
- Server-side activation, license validation and blacklist support are planned for stronger commercial enforcement.

**Security boundary** A privileged local administrator can ultimately alter or delete local protection data. This is a known limitation of local-only license enforcement, not a claim of tamper-proof protection.

### 9.1 Important paths

| Path | Purpose |
|---|---|
| /var/lib/forenclarity/ | Runtime state and application data. |
| /var/lib/forenclarity-trial/ | Protected trial-continuity anchor. |
| /var/log/forenclarity/ | Installation, service and event logs. |
| /opt/forenclarity_phase15/ | Installed application implementation path. |
| ~/forenclarity_output/ | User-generated evidence and report 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 startup at boot. |
| sudo systemctl disable forenclarity.service | Disable 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 uninstaller closes open or hidden Control Center processes automatically.

```
cd /path/to/ForenClarity_Kali_Linux_v1.0.0
sudo ./Uninstall_ForenClarity_Kali.sh
```

## 11.1 Available modes

| Mode | Effect |
|---|---|
| SAFE_UNINSTALL | Remove the ForenClarity package, service, CLI and launchers while preserving evidence, logs, dependencies and the protected trial anchor. |
| REMOVE_FC_DEPS | Remove ForenClarity and only packages recorded by the install manifest as newly installed by ForenClarity and still present. |
| PURGE_EVERYTHING | Remove ForenClarity, manifest-recorded dependencies, evidence, logs, runtime license state and application paths. The protected trial anchor remains intentionally. |

## 11.2 Full commercial purge

```
PURGE_EVERYTHING
REMOVE_CONFIRMED
CLEAN_INSTALLER_FILES
```

- The package, CLI, service and launchers are removed.
- The Control Center closes automatically.
- User output, application runtime state and installer files are removed when cleanup is confirmed.
- Dependencies installed by ForenClarity are removed only when the manifest proves they were not pre-existing.
- Protected baseline packages, including rsyslog and tcpdump in the accepted QA, remain installed.
- The protected trial anchor remains intentionally for evaluation continuity.

**Validated purge result** The accepted Kali v1.0.0 purge left no application package, service, process, CLI command, launcher, runtime path, installer folder or matching installer ZIP. Protected baseline packages remained

installed, and only the trial-continuity anchor remained intentionally.

# 12. Troubleshooting

| Symptom | Action |
|---|---|
| Service is inactive after installation | 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 Center closes to background | The close action may hide the GUI while the service continues. Reopen it from a launcher or run forenclarity-control-panel. |
| CLI appears cached after uninstall | Run hash -r and test the command again. |
| Complete journal is not visible in GUI | Run sudo journalctl -u forenclarity.service. |
| Integrity verifier reports a failure | Delete the extracted folder, obtain a clean ZIP, extract again, and do not install until every check passes. |
| Matching installer ZIP is not found during cleanup | The uninstaller removes the current extracted folder and reports the missing ZIP. Remove any separately moved ZIP manually after confirming its exact filename. |
| A protected package appears scheduled for removal | Stop the uninstall, preserve the transcript, and do not continue. Revalidate the package baseline and use a rebuilt release rather than patching the installed system. |

# 13. Known limitations

- The 60-day evaluation uses local enforcement. A root administrator can modify or delete local protection data.
- The release is currently unsigned; customers should verify the internal SHA-256 manifest and any separately published outer-ZIP checksum.
- No cloud upload, remote management, central console or centralized licensing is included in v1.0.0.
- The normal-user GUI cannot display every privileged journal entry without sudo.
- Dependency availability may vary as Kali Linux repositories evolve; integrity and installation validation should be repeated for each republished package.
- Enterprise multi-endpoint management, team roles, a central database, update orchestration and cloud licensing belong to later roadmap phases.

# 14. Release acceptance checklist

☐ Public ZIP name is ForenClarity_Kali_Linux_v1.0.0.zip.

☐ Verify_Build_Integrity.sh reports PASSED.

☐ Installer uses public wording and INSTALL_FORENCLARITY.

☐ Package and user interface display version 1.0.0 with no internal build labels.

☐ Service installs, starts and is enabled.

☐ Service remains active and enabled after reboot.

☐ Desktop and Applications launchers open the Control Center.

☐ 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.

☐ SAFE_UNINSTALL removes the product while preserving designed evidence/dependencies and trial anchor.

☐ PURGE_EVERYTHING closes the open Control Center.

☐ Manifest removal protects pre-existing packages, including rsyslog and tcpdump.

☐ 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 after full purge.

**Release status** ACCEPTED — ForenClarity Kali Linux v1.0.0. This guide reflects the validated 13 July 2026 release procedure and is intended for distribution with the public Kali Linux download.

# Appendix A. Quick-start card

| Step | Command / action |
|---|---|
| 1. Extract | unzip ForenClarity_Kali_Linux_v1.0.0.zip |
| 2. Enter folder | cd ForenClarity_Kali_Linux_v1.0.0 |
| 3. Verify | chmod +x Verify_Build_Integrity.sh && ./Verify_Build_Integrity.sh |
| 4. Install | sudo ./Install_ForenClarity_Kali.sh |
| 5. Confirm | INSTALL_FORENCLARITY; optional INSTALL_OSQUERY; START_AND_ENABLE |
| 6. Check | systemctl is-active forenclarity.service && systemctl is-enabled forenclarity.service |
| 7. Open GUI | forenclarity-control-panel |
| 8. Generate report | forenclarity-cli report |
| 9. Uninstall | sudo ./Uninstall_ForenClarity_Kali.sh |

**Operational rule** Save long terminal output with tee when performing formal QA, for example: command 2>&1 | tee ~/Desktop/ForenClarity_Kali_QA.txt.

# Appendix B. Administrator validation record

| Field | Record |
|---|---|
| Endpoint / VM | |
| Kali version | |
| Snapshot or baseline date | |
| Release ZIP SHA-256 | |
| Integrity verification result | |
| Installation date/time and timezone | |
| Service active/enabled after reboot | |
| Control Center launchers validated | |
| Controlled alert test result | |
| Report formats validated | |
| Uninstall mode tested | |
| Protected packages verified | |
| Trial anchor verified | |
| Administrator name / approval | |