ForenClarity

for Windows v1.1.0 Commercial

Complete User and Administrator Documentation

Installation | Operation | Network Monitoring | Reports | Uninstall | Troubleshooting

Release status
Commercial Windows documentation baseline for the v1.1.0 package validated on Windows 10 x64 and documented for supported Windows 10/11 x64 environments. This document replaces the previous v1.0.0 / Build17 website PDF.

Release item	Verified value
Product	ForenClarity for Windows
Public version	v1.1.0 Commercial
Supported operating systems	Windows 10 and Windows 11, 64-bit
Installer SHA256	29ED6FCB51CFD185C22CBFC51D2AF52DD3DCF1A2093EF94220E8134DA83F409E
Installer size	4,531,427 bytes
Trial	60-day protected local trial
Documentation purpose	Public website/download documentation

Contents

Important safety statement
A Clean result means that no enabled ForenClarity rule generated a suspicious finding during that scan. It does not prove that the computer is compromise-free and does not replace antivirus, EDR, SIEM, firewall administration, forensic investigation, or incident response.

1. Product purpose and scope

ForenClarity is an evidence-clarity and triage assistant for Windows administrators, security practitioners, small organizations, and technical users. It collects and summarizes endpoint, network, Microsoft Defender, startup, service, process, firewall, and optional local-engine evidence, then presents it in readable dashboards and reports.

Area	What ForenClarity provides
Primary problem	Security evidence is often spread across logs, services, processes, open ports, antivirus events, firewall data, and local IDS engines.
ForenClarity role	Organizes scattered evidence into a readable triage view, highlights review items, and provides practical next steps.
Customer promise	Evidence clarity and administrative guidance without claiming that a machine is guaranteed safe.
Windows commercial scope	A protected Windows v1.1.0 application with dashboard, network monitoring, report export, trial state, startup handling, and optional Snort/Suricata controls.

2. Capabilities, boundaries, and commercial positioning

Capability	Description
Endpoint evidence	Processes, services, startup items, scheduled tasks, Defender/AV status, PowerShell events, and other available Windows security signals.
Network evidence	Listening ports, established connections, remote/external

	connections, firewall-log readiness, packet-capture readiness, passive scan/probing evidence, and historical network evidence.
Readable reports	Full security reports and network-monitor reports in readable formats, with CSV files retained as the detailed technical record.
Advanced sources	Administrator-focused status and controls for Snort, Suricata, Wazuh readiness, pfSense visibility guidance, and future integrations.
Protected trial	A 60-day local trial with protected local state and integrity checks.
Reduced alert fatigue	Popups are limited to high or critical conditions in the accepted configuration, while lower-severity evidence remains available for review.

What the product does not claim

- It is not antivirus, EDR, SIEM, firewall-management, full digital-forensics, or incident-response software.
- It does not guarantee that a system is clean or uncompromised.
- Optional engines remain separate products and may require administrator configuration, interface selection, rules, and permissions.
- Future sources such as Zeek, cloud collection, central dashboards, mobile workflows, and expanded integrations are roadmap items until separately completed and validated.

3. System requirements and dependencies

Requirement	Guidance
Operating system	Windows 10 or Windows 11, 64-bit.
Privileges	Administrator rights are required for installation, uninstall, firewall-log access repair, dependency installation, and local-engine actions.
Processor and memory	A modern x64 Windows computer capable of running Python-based desktop software and local evidence collection. Optional IDS engines increase CPU, memory, and disk use.
Disk space	Allow space for the application, Python runtime, optional dependencies, CSV evidence, logs, and exported reports.
Network	Internet access is useful for dependency acquisition and future updates. Local evidence collection can operate within the installed scope without continuous internet access.
Security provider	Microsoft Defender is the native AV provider verified for this Windows release.

External components

Component	Purpose and uninstall policy
Python	Runtime used by the Windows application package. Remove only when no other software depends on that installation.
Npcap	Packet-capture driver used for capture readiness and related workflows.
Wireshark	Optional packet-analysis tool used for validation and troubleshooting.
Snort	Optional local IDS engine. Started by administrator action and monitored through ForenClarity evidence views.
Suricata	Optional local IDS engine. Started by administrator action and monitored through eve.json and status evidence.
Wazuh / pfSense	Integration-awareness and visibility guidance are shown where detectable; they remain separately administered systems.

Code-signing notice

Until the Windows installer is code-signed, Windows may show an Unknown Publisher or SmartScreen warning. This is different from an integrity-manifest failure. Do not use a package whose posted SHA256 or internal integrity validation does not match.

4. Installation and first start

1. Download the Windows v1.1.0 installer only from the official ForenClarity website or verified release location.
2. Compare the installer SHA256 with the value published on the download page.
3. Close any existing ForenClarity window before reinstalling or upgrading.
4. Run the installer and approve the Windows UAC prompt.
5. Follow the installer prompts. Do not remove unrelated dependencies and do not force a reboot unless Windows requires one.
6. Start ForenClarity from the desktop shortcut or Start menu.
7. Run Scan Now, open Network Monitor, and confirm that reports are created under the output folder.
8. Restart Windows once and confirm that only one ForenClarity process starts automatically.

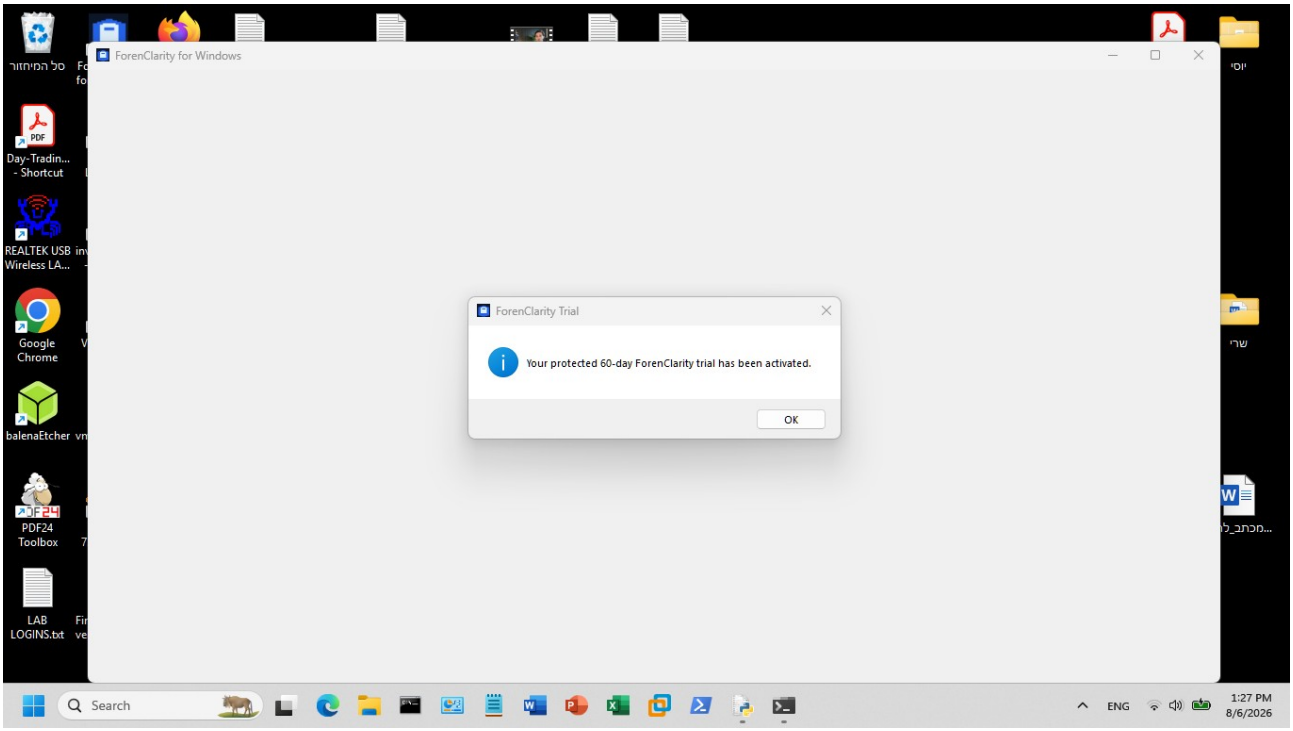

Figure 1. Windows installation/restart validation screen from the accepted v1.1.0 test cycle.

Expected first-run result

Item	Expected state
Header	ForenClarity for Windows; Windows v1.1.0 shown in the license/version line.
License	Trial active with protected local cache.
Endpoint evidence	Ready after a successful scan.
Network evidence	Available when local network collection and capture readiness are present.
Optional engines	Ready, Review, Source, Detected, or Not detected according to installed components and current state.
Severity	Clean when no enabled rule produces a suspicious finding; otherwise the highest applicable severity.
Reports	Generated under %LOCALAPPDATA% \ForenClarityApp\output.

5. Main dashboard

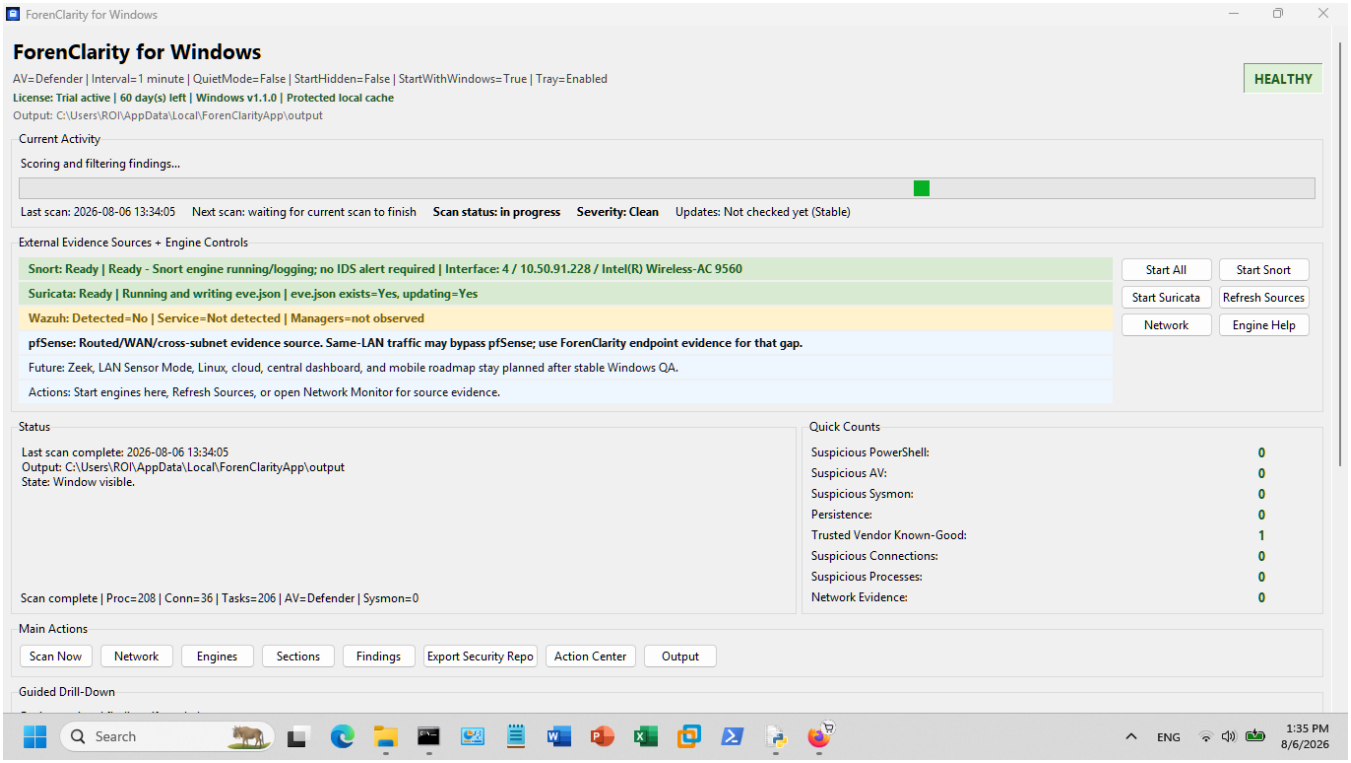

Figure 2. Windows v1.1.0 main dashboard with active trial, healthy state, engine evidence, and scan progress.

Dashboard element	Meaning
AV=Defender	Microsoft Defender is detected as the native antivirus evidence provider.
Interval	Configured automatic scan interval.
QuietMode	Whether normal interface notifications are reduced.
PopupThreshold	Minimum severity that triggers a popup; the accepted configuration limits popups to High/Critical.
StartHidden / StartWithWindows / Tray	Current startup and tray behavior.
License and version line	Protected 60-day trial state and Windows v1.1.0 product version.
Current Activity	Current scan phase, last scan time, next scan, scan status, severity, and update state.
External Evidence Sources + Engine Controls	Current Snort, Suricata, Wazuh, pfSense, and future-source status or guidance.
Quick Counts	Counts of suspicious PowerShell, AV, system, persistence, process, connection, and network evidence.
Main Actions	Scan Now, Network, Engines, Sections, Findings, Export Security Report, Action Center, and Output.

6. Network Monitor and visible sections

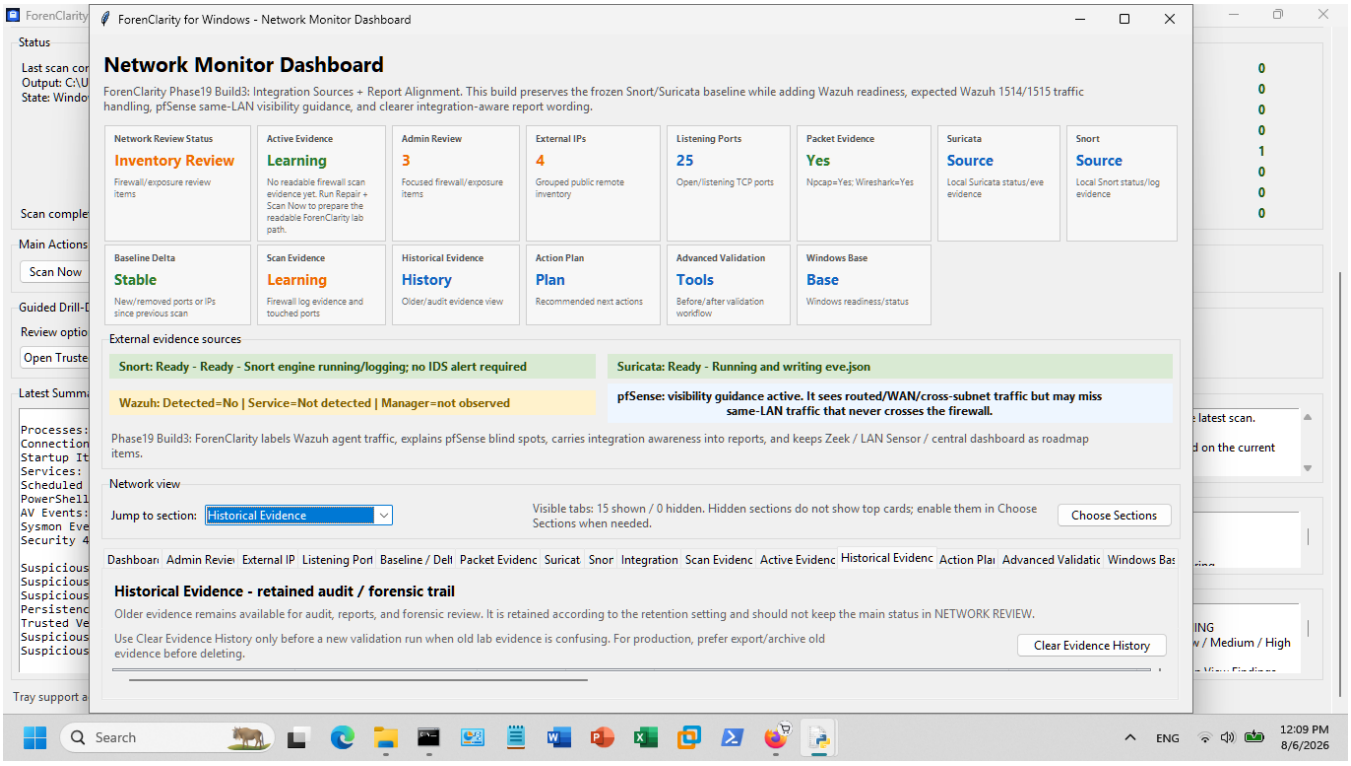

Figure 3. Network Monitor dashboard showing evidence cards, optional sources, section tabs, and historical evidence.

Network area	Purpose
Network Review Status	Plain-English summary such as Quiet, Inventory Review, or an alert-oriented review state.
Active Evidence	Current readable network evidence and learning state.
Admin Review	Focused administrative items requiring attention.
External IPs	Grouped public remote addresses observed in current evidence.
Listening Ports	Open/listening TCP ports and associated context.
Packet Evidence	Npcap and Wireshark readiness plus packet-capture context.
Suricata / Snort	Local engine status, logs, interface/configuration evidence, and guidance.
Baseline / Delta	New or removed ports/IPs compared with the retained baseline.
Historical Evidence	Older evidence retained for audit, reports, and forensic review.
Action Plan / Advanced Validation / Windows Base	Recommended next actions, before-and-after validation, and Windows readiness/status.

Visible-section selector

The Sections control allows administrators to keep frequently used tabs visible and hide less-used sections without deleting evidence. The final source correction adds a scrollable selector and a fixed button footer so the controls remain reachable on lower-resolution Windows displays.

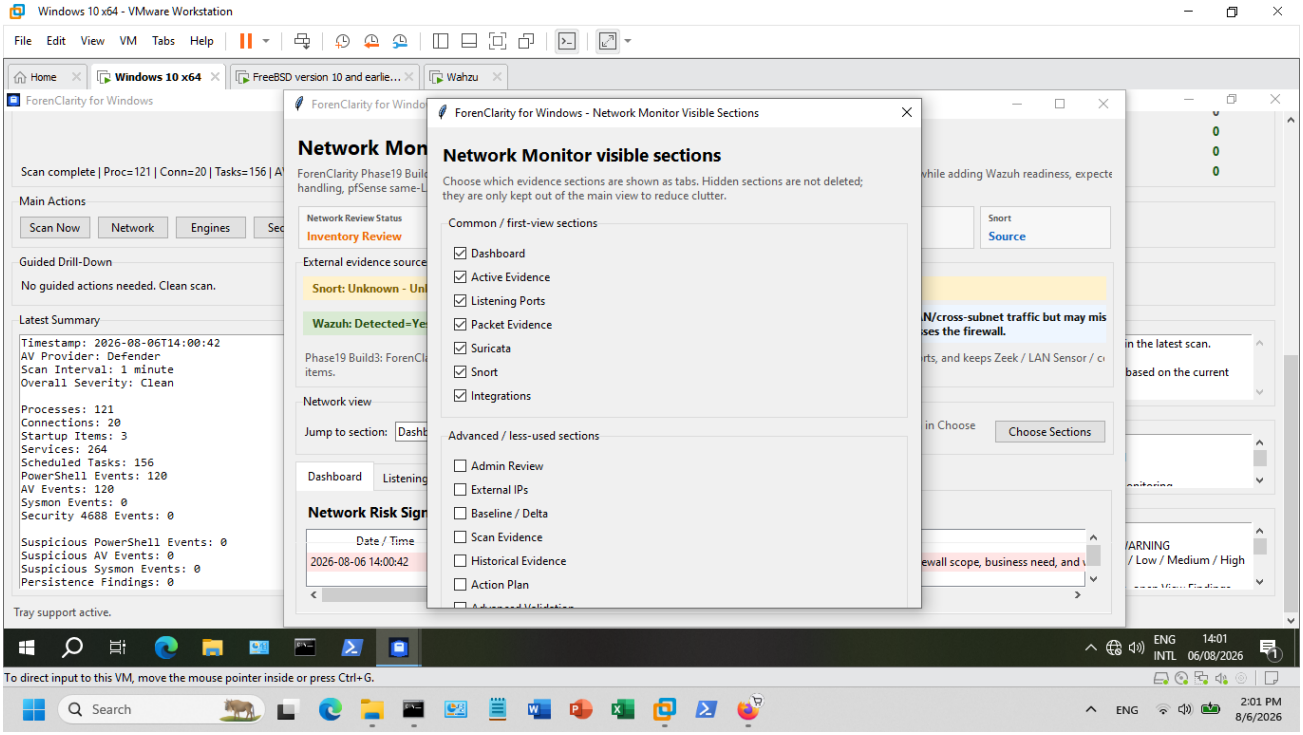

Figure 4. Network Monitor visible-section selector during final Windows validation. The released implementation uses scrolling and a fixed action footer.

7. Optional engines and integrations

Source	How ForenClarity uses it
Snort	Detects installation, maintains a managed configuration location, generates a start launcher, validates interface/configuration details, and summarizes local IDS evidence. Administrator action is required to start the engine.
Suricata	Detects the engine, starts it by administrator action, checks whether eve.json exists and is updating, and summarizes local IDS evidence.
Wazuh	Shows detected/not-detected status and expected service/manager traffic readiness. It does not replace Wazuh administration.
pfSense	Provides visibility guidance. Routed/WAN/cross-subnet traffic may be visible while same-LAN traffic can bypass the firewall; endpoint evidence is used to explain that gap.
Future sources	Zeek, LAN sensor mode, Linux, cloud, central dashboard, and mobile capabilities remain separate roadmap work

	until completed and validated.

Snort and Suricata operating guidance

- Run local-engine actions with administrator rights.
- Confirm the correct capture interface before relying on network evidence.
- Snort uses the managed ForenClarity configuration and log tree under C:\ProgramData\ForenClarity\snort.
- Suricata evidence depends on a valid configuration, correct interface, and an updating eve.json file.
- A Ready or Source label describes evidence availability; it is not proof that every possible network event is being captured.
- Do not run duplicate engine instances on the same interface without an explicit administrative reason.

Permissions correction
The accepted source includes Windows 10/11 ACL handling for the managed Snort tree so normal application access and elevated Snort operation can coexist. The generated launcher is refreshed when Snort is detected.

8. Findings, reports, and output files

Field or output	Meaning
FindingId / FindingType	Unique identifier and finding category.
Severity	Clean, Info, Review, Low, Medium, High, or Critical according to enabled rules.
Timestamp / DetectedTime / ScanTime	When evidence was captured and processed.
SourceEventTime	Original event time when available.
RepeatCount	Number of grouped occurrences.
Reason	Why the finding appears.
WhatItMeans	Plain-English interpretation.
RecommendedNextSteps	Administrative action guidance.
%LOCALAPPDATA%\ForenClarityApp\output	Primary reports, CSV evidence, summaries, launchers, and engine-related output.
Full Security Report	Readable endpoint/security handoff report.
Network Monitor Report	Readable network-evidence report.
CSV files	Detailed technical evidence used for later review and correlation.

Report-handling guidance

- Export reports before clearing historical evidence or uninstalling the application.
- Treat CSV data as the detailed technical record and the PDF/TXT report as the readable handoff.
- Review timestamps, source availability, interface state, and engine status before drawing conclusions.
- Protect exported reports because they may contain hostnames, usernames, process data, network addresses, and security evidence.

9. Startup, trial, and integrity behavior

Control	Verified behavior
Automatic startup	Registered through the current user Run key using the ForenClarity VBS launcher.
Startup-folder shortcut	Not used in the accepted clean installation.
Process count after restart	One ForenClarity pythonw.exe process.
Trial persistence	License file and protected local/program-data trial markers remain after restart.
Duplicate prevention	The accepted one-shot install/restart test expected and verified no duplicate-instance startup behavior.
Integrity	The installer SHA256 and internal package integrity should be validated before use.

10. Uninstall and dependency review

1. Open Windows Settings > Apps > Installed apps, or Control Panel > Programs and Features.

2. Select ForenClarity and choose Uninstall.

3. Approve UAC when requested.

4. Read the dependency notice carefully. ForenClarity removes its own application components; external tools remain for manual review.

5. Choose whether to remove ForenClarity reports/settings. Preserve them when evidence must be retained.

6. Choose whether to remove the local trial/license cache.

7. Read the final result panel and verify that the application process, install folder, shortcuts, and startup registration were removed.

8. Review Python, Npcap, Wireshark, Snort, and Suricata separately before removing any of them.

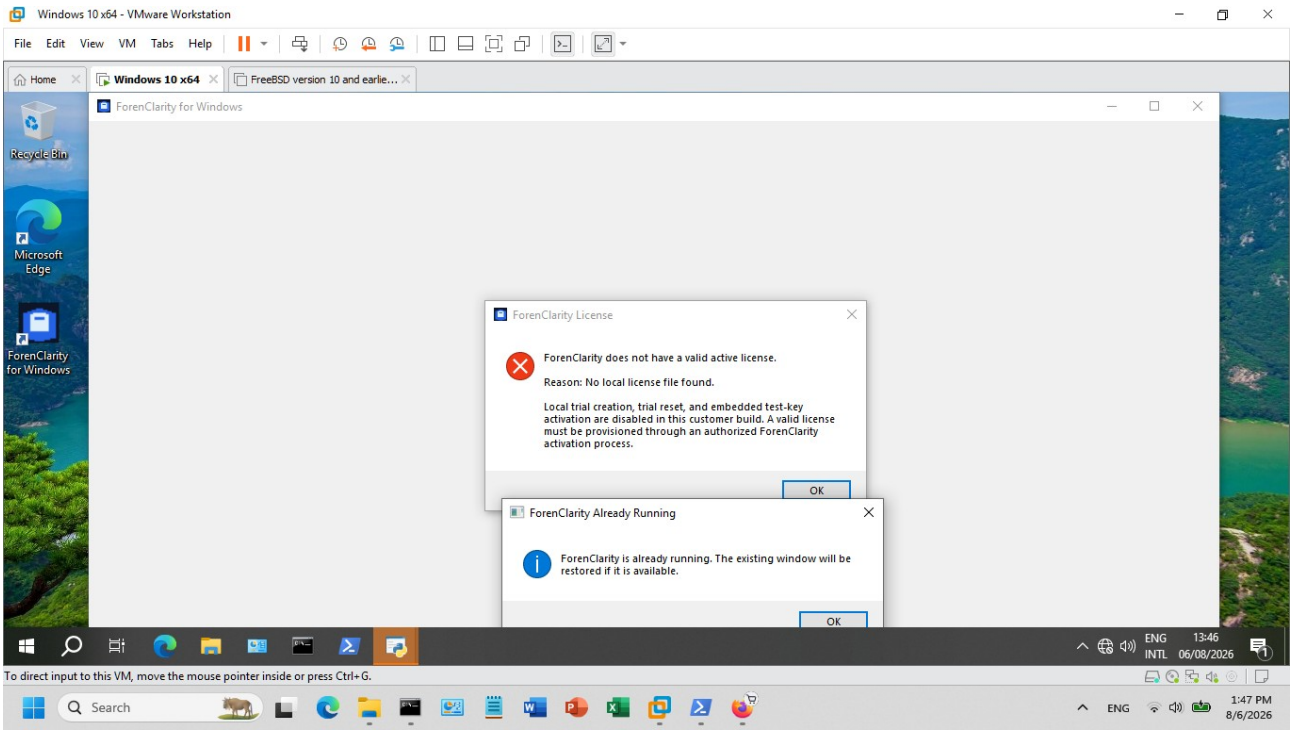

Figure 5. Final uninstall validation screen from the Windows v1.1.0 test cycle.

Manual dependency review

Dependency	Remove only when...
Python	No other local tool depends on that Python installation.
Npcap	No packet-capture or network-analysis tool requires it.
Wireshark	Packet inspection is no longer needed.
Snort	The machine does not use Snort as an independent IDS engine.
Suricata	The machine does not use Suricata as an independent IDS engine.
Firewall logs	Windows Firewall logging no longer points to the folder and evidence retention is not required.

Verification commands

tasklist | findstr /i "python pythonw foren"

dir "%LOCALAPPDATA%\Programs\ForenClarity" /s /b

dir "%LOCALAPPDATA%" /b | findstr /i "Foren"

11. Troubleshooting

Issue	Action
Unknown Publisher or SmartScreen warning	Expected until code signing is added. Confirm the official

	download source and published SHA256 before proceeding.
Integrity manifest or package check fails	Do not use the package. Download a fresh official copy and compare its SHA256.
Application does not start	Run from the desktop/Start menu, check Windows security prompts, verify the installation folder, and review application output/logs.
More than one instance appears	Close all instances, inspect startup registrations, and confirm that only the HKCU Run launcher is active.
Firewall-log access issue	Use the Repair Firewall Log Access action as administrator, then rerun the scan.
Snort does not start or log	Verify installation, interface number, managed configuration, ACLs, launcher output, and C:\ProgramData\ForenClarity\snort\logs.
Suricata evidence is stale	Verify the selected interface, configuration, running process, and whether eve.json is updating.
No suspicious findings	This means no enabled rule fired during that scan; it does not prove the machine is safe.
Dependency remains after uninstall	Expected. Remove only after confirming that no other software needs it.
Buttons do not fit at low resolution	Use the final v1.1.0 build. The visible-section selector is scrollable and uses a fixed action footer.

12. Verified Windows v1.1.0 release acceptance

Acceptance item	Verified result
Installer identity	Windows v1.1.0 one-shot installer; size 4,531,427 bytes; SHA256 matches all recorded copies.
Build and package	Build completed successfully with protected payload, native guard, integrity manifest, and installer output.
Clean reinstall	Previous application, data, license markers, and startup remnants were removed before installation; reinstall succeeded.
Restart behavior	Automatic restart performed; exactly one ForenClarity process was present after restart.
Startup registration	Current-user Run entry present; Startup-folder shortcut absent.
Trial state	License file and protected local/program-data markers present after restart.
UI validation	Responsive dashboard/network-monitor work completed; final selector correction adds scrolling and fixed buttons.
Snort correction	Managed-tree ACL and launcher-generation source fixes validated for syntax.

Uninstall lifecycle	Application process, install folder, shortcuts/startup, settings, and license state can be removed according to administrator choices; external dependencies remain for manual review.
Commercial documentation	This v1.1.0 document replaces the v1.0.0 / Build17 website documentation.

Release integrity value
Installer SHA256: 29ED6FCB51CFD185C22CBFC51D2AF52DD3DCF1A2093EF94220E8134DA83F409E

13. Website download and publishing notes

Public download package

- Publish the Windows v1.1.0 installer and this documentation PDF together.
- Use a clean public filename without internal Build, Test, timestamp, user, or workstation wording.
- Publish the exact installer size and SHA256 beside the download button.
- State clearly that the current installer may show Unknown Publisher until code signing is implemented.
- Do not publish internal source paths, usernames, VM names, build scripts, test logs, or private QA artifacts.
- Keep the previous documentation archived privately, but replace the website copy with this v1.1.0 document.

Recommended website wording

Product summary
ForenClarity for Windows v1.1.0 turns endpoint, network, Defender, firewall, process, startup, service, and optional local-engine evidence into readable triage views and reports. It helps administrators understand what requires attention and what to check next, without pretending to replace antivirus, EDR, SIEM, or professional incident response.

Download-page checklist

Item	Required website state
Version	Windows v1.1.0 Commercial
Primary download	Final Windows installer
Documentation	ForenClarity Windows v1.1.0 Final Website Documentation.pdf
Integrity	SHA256 displayed in copyable text
System requirements	Windows 10/11 x64 and administrator rights

Trial	60-day protected local trial
Publisher warning	Honest notice that code signing is not yet present
Dependencies	Python/Npcap/Wireshark/Snort/Suricata may remain after uninstall and require manual review
Support	A working support/contact route and clear issue-reporting instructions
Analytics	Track page visits, download clicks, completed downloads, and support/feedback events without misleading users.

Final customer notice

ForenClarity provides evidence clarity and administrative triage guidance. Security decisions should consider the complete environment, source availability, timestamps, endpoint context, network architecture, and the limitations of optional engines. Preserve evidence before making destructive changes, and escalate serious or uncertain findings to a qualified security professional.