LogVeil — Frequently Asked Questions

v1.1 · 5 September 2026 · PUBLIC

> **Change note — v1.0 → v1.1 (5 September 2026).** The table in question 3 is now generated from LogVeil's formats register at the moment this document is produced, instead of being copied into it by hand, so the two can never disagree. No question, answer or status has changed.

LogVeil, from Zindagi Technologies, is a bundle sanitisation system: it takes an OEM diagnostic bundle in and gives back the same bundle with every sensitive value rewritten consistently under your own policy, plus a signed Sanitisation Attestation of what was done, what was checked and what is not asserted. These are the questions we are asked most, answered the way we would answer them in the room.

What it does

1. What does LogVeil actually do?

When a firewall, an identity server or a network controller breaks, the vendor's technical assistance centre asks for its diagnostic bundle. LogVeil reads that bundle — every nested archive, every member, every filename and header — finds the sensitive values in it, rewrites them consistently under a policy you wrote and a key you hold, re-checks its own output with independent scanners, and hands you back a bundle the vendor can still work with, together with a signed statement of exactly what it did and did not do. It runs inside your own network, on your own virtual machines, with no connection to the outside.

2. What is in a diagnostic bundle that is worth protecting?

More than most teams expect. Management and data addresses and the subnet structure behind them; hostnames that encode sites; serial numbers and asset tags; SNMP community strings and RADIUS or TACACS secrets; certificates and private keys — a single firewall-management bundle can carry hundreds; usernames, e-mail addresses and phone numbers; engineers' names in filenames; and the timestamps, paths and archive headers that give away the rest. The vendor is honest, but it is in another jurisdiction, under no duty to protect your topology, and it may keep the bundle indefinitely.

3. Which vendors' bundles does it understand?

The table below is LogVeil's public roadmap and carries three statuses only. Supported in early access means within the scope of the early-access programme; in development means being built now; planned means committed but not yet started. Nothing here says "supported" without its qualifier.

VENDOR	BUNDLE FAMILY	STATUS
Cisco	Secure Firewall Management Center (FMC) troubleshoot bundle	supported in early access
Cisco	Secure Firewall Threat Defense (FTD) troubleshoot bundle, including high-availability pairs	supported in early access

VENDOR	BUNDLE FAMILY	STATUS
Cisco	Identity Services Engine (ISE) support bundle	supported in early access
Cisco	Catalyst Center (formerly DNA Center) RCA and support bundles	supported in early access
Check Point	Gaia cpinfo	in development
Cisco	IOS-XE show tech-support and binary trace (btrace) archives	in development
Radware	Alteon ADC and vADC techdata	in development
Radware	DefensePro / NIPS support bundle	in development
Cisco	Catalyst 9800 wireless LAN controller debug bundle	planned
Fortinet	FortiGate TAC report and console log	planned
Infoblox	NIOS support bundle	planned
Juniper	Junos request support information (RSI)	planned
Palo Alto Networks	PAN-OS tech support file (TSF)	planned
Any	Packet captures (pcap, pcapng) — standalone or inside a bundle	planned
Any	Generic text archive (unknown bundle types)	planned

Register as at 5 September 2026.

A vendor or product not on this list is added by writing a profile — a declarative description of the bundle family — not by changing the engine (question 17).

4. Will the output still be useful to the vendor's engineer?

That is the point of doing it properly rather than with search-and-replace. Addresses are rewritten by a prefix-preserving, key-derived transform, so two addresses that shared a subnet before still share one after and the topology remains legible. The same original always gets the same replacement, across every member of the bundle and across every bundle you send under the same key, so a case that spans several uploads stays coherent. Structured members — JSON, XML, YAML, configuration grammars, object dumps — are rewritten in place by transformers that understand the format, and a set of utility checks runs on the output: a structural diff of member counts and sizes, well-formedness of structured files after rewriting, referential integrity (every masked value appears exactly where the original did), and a check that harmless look-alikes such as version strings survived untouched.

5. Do the vendors accept a sanitised bundle?

We have not put the question to the OEMs. Some support processes ask for a bundle unmodified, and we would rather tell you that than pretend otherwise. LogVeil's value does not depend on the answer: it is also how you satisfy your own release policy before anything leaves your network — what may go out, under whose rules, with what record — and that decision is yours whatever a vendor's process says.

6. Does the attestation mean the output contains nothing sensitive?

No. LogVeil does not promise that nothing sensitive remains. It states, in a signed attestation, what was rewritten, what was dropped, what was passed through, which scanners checked the output and what they found, and what is explicitly not asserted. In the vocabulary the attestation itself uses: policy-conformant sanitisation, verified by independent scanners, with declared non-assertions. For arbitrary input that is the only honest statement a tool can make, and it is a more useful one than a promise, because it tells your security cell exactly where to look.

7. What is a "non-assertion"?

A line in the attestation that says what LogVeil is not claiming about this output: sensitivity classes your policy did not cover; encodings outside the enumerated list it searches; binary members it passed through unread, by name; structural information it did not rewrite — subnet sizes, host counts, timing; member formats it did not recognise; and anything a reviewer chose to override. Non-assertions are mandatory. An attestation without them would be a marketing document, not a record.

Your policy, your key

8. Who writes the policy, and who holds the key?

You do, on both counts. The policy is a signed, versioned document owned by your policy author: which subnets pin to which, which site names become which tokens, which keywords to replace, what to preserve, what to drop. The master key is generated and held inside your deployment; it is never exported in plaintext and Zindagi never sees it. There is no universal policy shipped as "safe for everyone" — every policy is yours and is signed by you.

9. Can a masked value be reversed? By whom?

Yes, deliberately, and under control. When the vendor's engineer writes back about a masked address, one of your people with the Reverser role submits that single value with a written justification; a second person approves; the original is returned; and the whole exchange is written to an append-only, hash-chained audit log. Reversal is one value at a time. Exporting the map in bulk is not a function of the product. The map itself is stored encrypted, with envelope keys, and the key-encryption key is never at rest in plaintext.

10. Is the same value masked the same way next time?

Yes. Under the same key, the same original value produces the same replacement, in every member, in every bundle, for as long as you keep the key. That is what keeps a long-running support case coherent. Two runs of the same bundle under the same policy version and key produce byte-identical output and an identical attestation body, so a result can be reproduced and checked.

Size, binaries, captures

11. Is there a file-size limit?

No. LogVeil processes a bundle member by member with bounded memory, so a multi-gigabyte member is handled the same way as a small one. For scale, measured on real bundles in our lab: a single Cisco FMC troubleshoot bundle held 11,412 files nested seven levels deep; an FTD high-availability troubleshoot, 40,821 files nine deep; a third bundle, 11,529 files eleven deep; an ISE support bundle carried one member of 4.98 GB; a Catalyst Center RCA bundle expanded fifteen-fold on extraction. Those figures describe the vendors' formats, not any customer.

12. What happens to binaries, packet captures, databases and certificates?

Each is handled by a rule and declared in the attestation. Certificate bodies and private keys are dropped and marked, and the names inside certificates are rewritten like any other hostname. Database exports, core files, compiled traces and other binaries are dropped or passed through according to your policy, and every passed-through binary is listed by name as a non-assertion. Packet captures are recognised, inventoried and declared today — passed through or dropped as your policy says — and rewriting of capture contents is planned. Nothing is passed through silently.

13. Does it use AI?

Not for the result. The engine that finds and rewrites values is deterministic, and it alone produces the map and the attestation. AI is optional and off by default. If an administrator enables it, anything that has not yet been verified may be shown only to a local model on the same host with its network egress blocked; an external service, if you choose to enable one, receives only verified output or synthetic data — enforced in code, not configuration. What AI can do is open review items for a person to resolve and explain a finished attestation in plain language. It cannot change a map or an attestation, and we do not describe LogVeil as AI-driven, because it is not.

Where it runs

14. Where does it run, and does it connect to the internet?

Inside your network, on your own virtual machines, delivered as an offline kit: signed container images, a pinned compose file, an installer, a software bill of materials per image and signed checksums. A smoke test in the installer runs a full job with the outbound network blocked and confirms that nothing tried to connect. There is no telemetry, no update check, no external font or script. Nothing phones home, because there is nothing to phone.

15. What does the deployment need?

Docker Compose on Ubuntu 24.04 LTS or RHEL/Rocky 9, on amd64 or arm64, with local scratch storage sized for the bundles you expect to process — a large bundle can expand many times over on extraction. Hypervisor images (OVA, qcow2, VHDX) are planned. Exact sizing is agreed during early access against your own bundle sizes.

16. Is there a cloud version?

No. A hosted instance exists only as a demonstrator on synthetic data. LogVeil is designed for the air gap, and a real bundle never leaves your network to be processed.

17. How is a new vendor, product or format added?

By a profile — a declarative description of the bundle family — and, only where a member format has a grammar nobody has seen before, a content transformer for it. The engine has five kinds of plug-in (container handlers, content transformers, recogniser packs, transform packs and bundle profiles), each with a versioned interface and a conformance harness that tests every pack on recall and over-masking before it is accepted. Adding a vendor never touches the core.

18. Who can do what inside LogVeil?

Seven roles, enforced by the server on every request: a platform administrator (users, tenants, keys, plug-ins — who cannot reverse a value), a policy author, an operator who runs jobs, a reviewer who resolves review items and approves a release, a reverser, an auditor with read-only access to everything, and a plug-in publisher. Directory integration, single sign-on and multi-factor authentication are planned for the full product.

About us, and next steps

19. Who is Zindagi Technologies?

A systems-engineering organisation building sovereign, large-scale, mission-critical infrastructure for government and defence, predominantly as the technical delivery partner to system integrators. Founded 2017; bootstrapped. ISO 9001:2015 and ISO 27001:2022 certified; DPIIT-recognised Startup; Udyam MSME (Small); incubated inside DSCI. Engineering team in-house — no outsourcing, no freelancers. Our flagship product is CriticalRange™ (criticalrange.com), a sovereign cyber range platform; LogVeil comes from the same engineering team.

20. What is the status, and what happens next?

LogVeil is in development. An early-access programme opens after our first field trial. Early access is a free, guided proof-of-concept on your own bundles inside your own network: you choose the bundles, you write the policy with our help, and you keep the key; we hand over the offline kit, run the first jobs with your engineers, and leave you with the attestations. After that comes the kit for your own operation and, on the roadmap, an appliance with a local GPU. To talk to us: **sales@zindagi.tech** or **+91 97739 73971**.

Zindagi Technologies Private Limited · 301, 3rd Floor, Bakshi House, Nehru Place, New Delhi 110019 · sales@zindagi.tech · +91 97739 73971 · Document 2026-09-05_Z26-050_LogVeil-FAQ_v1.1 · PUBLIC