DS

DIGITAL
SAFETY

INDEPENDENT PRIVACY PRACTICES ASSESSMENT

AND NO-LOGS VERIFICATION REPORT

LUX VPN

ASSESSMENT DATE	July 8, 2026
REPORT ISSUED	July 31, 2026
REPORT ID	DS-LUX-2026-01
VERSION	1.0
DISTRIBUTION	Public

Prepared by

Digital Safety
A service of CM Ventures Limited
Van Buren, MO 63965

Curt Majors, Managing Director

1 Document Status and Use

This report presents the results of an independent, point-in-time assessment of the privacy and logging practices implemented by Lux VPN. It is intended for public distribution only in its complete and unaltered form. Individual excerpts should not be presented in a way that changes the meaning or scope of the conclusions.

IMPORTANT SCOPE CLARIFICATION

In this report, the term "no-logs" refers only to the VPN activity data categories specifically examined: traffic contents or destinations, DNS queries, customer source IP addresses, and assigned VPN IP addresses. It does not mean that Lux VPN keeps no business records of any kind. Limited account, billing-reference, and support information is retained as described in Section 7.

2 Executive Summary

Digital Safety performed an independent assessment of Lux VPN on July 8, 2026. Lux VPN provided read-only access to the systems, databases, dashboards, backups, and hosting-provider records relevant to the assessment. The review included 75 Linux-based VPN gateway servers supporting OpenVPN, WireGuard, and L2TP, together with the associated authentication, customer, billing, support, backup, and hosting environments.

Digital Safety examined whether the in-scope environment retained records of customer traffic contents or destinations, DNS queries, customer source IP addresses, or assigned VPN IP addresses. The procedures included configuration and log review, database inspection, review of available administrative and hosting-provider records, and a controlled VPN connection test followed by searches for resulting activity records.

Assessment type	Independent point-in-time privacy practices assessment
Systems reviewed	75 VPN gateways and supporting authentication, customer, billing, support, backup, and hosting systems
Protocols reviewed	OpenVPN, WireGuard, and L2TP
No-logs categories tested	Traffic contents or destinations; DNS queries; customer source IP addresses; assigned VPN IP addresses
Exceptions identified	None
Overall result	Practices observed were consistent with the stated no-logs scope defined in this report

OVERALL CONCLUSION

Based on the procedures performed and the evidence made available on July 8, 2026, Digital Safety did not identify evidence that Lux VPN retained the in-scope VPN activity data categories. No exceptions were identified.

3 Assessment Objective

The objective was to determine whether the Lux VPN systems within scope were configured and operated in a manner consistent with the following defined privacy practice: Lux VPN does not retain traffic contents or destinations, DNS queries, customer source IP addresses, or assigned VPN IP addresses generated through use of the VPN service.

The assessment also documented the limited business records retained for account administration, payment reconciliation, customer support, and backup continuity, so that the no-logs conclusion would not be confused with a claim that no information is retained anywhere in the organization.

4 Scope of Review

Systems and records included

- Seventy-five Linux-based VPN gateway servers.
- OpenVPN, WireGuard, and L2TP service configurations.
- Authentication systems supporting customer access.
- Customer account databases.
- Web and billing servers.
- Customer support systems and ticket records.
- Administrative and billing backups.
- Hosting-provider logs and dashboards made available to Lux VPN.

Data categories tested

- Contents of customer network traffic and destination information.
- DNS queries generated while connected to the VPN service.
- Customer source IP addresses.
- VPN IP addresses assigned to customers.

Access provided

Lux VPN provided Digital Safety with read-only access to the systems, databases, administrative dashboards, backup information, and provider records required for the review. Read-only access allowed the assessor to inspect configurations and records without modifying the production environment.

Protocols and technical environment

Component	Population	Coverage
VPN gateways	75 servers	Linux-based production gateways
VPN protocols	3 protocols	OpenVPN, WireGuard, L2TP
Supporting systems	Multiple systems	Authentication, customer, web, billing, support, backup, and hosting records

5 Assessment Methodology

Digital Safety used a combination of inspection, inquiry, controlled testing, and record searches. The work was designed to evaluate the defined no-logs categories within the environment available on the assessment date. The procedures were not designed as a penetration test or a source-code audit.

Ref.	Procedure	Description
5.1	Access and environment validation	Confirmed that the supplied access was read-only and identified the systems, databases, dashboards, backups, and provider records relevant to the assessment.
5.2	Gateway configuration review	Reviewed logging-related configurations and available records across the 75 Linux VPN gateway servers supporting OpenVPN, WireGuard, and L2TP.
5.3	Authentication and database review	Inspected authentication systems and customer databases for fields, tables, or records that could retain the in-scope customer activity data.
5.4	Web, billing, and support review	Reviewed the web, billing, and support systems to distinguish ordinary business records from VPN activity records.
5.5	Hosting-provider record review	Reviewed provider dashboards and logs made available to Lux VPN for evidence that the hosting layer retained the in-scope activity data.
5.6	Controlled connection test	Created and used a test account, established a VPN connection, generated known activity, disconnected, and searched the available systems and records for resulting entries in the in-scope data categories.
5.7	Backup and retention review	Reviewed the weekly backup cycle and the retention and deletion process for account, billing-reference, and support data.

Evidence standard

The conclusions in this report are based on the configurations, records, systems, and representations available to Digital Safety on July 8, 2026. Where a record was expected to be generated by a controlled test, Digital Safety searched the relevant systems after the test to determine whether the data was retained.

6 Detailed Findings

ID	Area	Result	Observation
F-01	Traffic contents and destinations	**No evidence identified**	The reviewed systems and records did not show retained content of customer network traffic or destination information within the defined assessment scope.
F-02	DNS queries	**No evidence identified**	The reviewed gateway, supporting, and provider records did not show retained customer DNS query history within the defined assessment scope.
F-03	Customer source IP addresses	**No evidence identified**	The reviewed systems and records did not show retained customer source IP addresses associated with VPN activity within the defined assessment scope.
F-04	Assigned VPN IP addresses	**No evidence identified**	The reviewed systems and records did not show retained mappings between customers and assigned VPN IP addresses within the defined assessment scope.
F-05	Controlled connection test	**Passed**	After the test account connected, generated known activity, and disconnected, searches of the available systems did not identify retained records in the four in-scope activity categories.
F-06	Business data separation	**Confirmed**	Account, payment-reference, and support records were identifiable as business records and were not presented as VPN activity logs.
F-07	Exceptions	**None**	No exceptions or corrective-action items were identified during the assessment.

FINDING INTERPRETATION

"No evidence identified" means that the procedures performed did not reveal retained records in the stated category. It is not a guarantee against every possible undiscovered condition, and it does not extend beyond the systems, date, and data categories defined in this report.

7 Account, Billing, and Support Data

Lux VPN retains limited information required to create and administer customer accounts, reconcile charges, issue receipts, and respond to support requests. This information is separate from the VPN activity categories evaluated in Section 6 and is stored in Lux VPN administrative systems hosted in Iceland.

Data element	Purpose	Handling observed
Name and email address	Account administration, receipts, and support correspondence	Stored with the customer account.
Credit card transaction ID	Reference and reconciliation of a payment	Stored as a reference to the charge, not as the customer card number.
Billing address and full payment details	Payment processing	Sent directly to the payment processor and not stored in Lux VPN systems.
Support ticket details	Customer support and follow-up history	Stored with the customer name and email address.

Retention period

Account data consisting of name, email address, credit card transaction ID, and support ticket history is retained while the account remains active and for 180 days after cancellation. At the end of that 180-day period, the account record is purged from active systems.

Backup cycle

Lux VPN creates full billing and administrative backups weekly and maintains a rolling four-week backup set. Each weekly backup replaces the backup from four weeks earlier. As a result, a record removed from active systems can remain recoverable in a backup for up to four additional weeks, after which it rolls out of the backup cycle.

Active account	Account, payment-reference, and support data retained.
After cancellation	Data retained in active systems for 180 days.
Active-system purge	Account record removed after the 180-day window.
Residual backup period	Purged data may remain in a weekly backup for up to four additional weeks.
Backup rotation	Four rolling weekly backups; oldest backup replaced each week.

8 Conclusion

Based on the procedures performed and the evidence made available on July 8, 2026, Digital Safety concludes that the Lux VPN systems within the defined scope were operating in a manner consistent with the following no-logs practice: Lux VPN did not retain traffic contents or destinations, DNS queries, customer source IP addresses, or assigned VPN IP addresses.

No exceptions were identified. Lux VPN did retain limited account, payment-reference, and support information for legitimate administrative purposes, subject to the retention and backup schedule described in Section 7. Those business records do not alter the conclusion regarding the four VPN activity data categories assessed.

> **INDEPENDENT ASSESSMENT OPINION**
>
> In Digital Safety's opinion, the controls and practices observed on July 8, 2026 were consistent, in all material respects within the defined scope, with Lux VPN's stated practice of not retaining the VPN activity data categories evaluated in this report.

9 Limitations

- This was a point-in-time assessment of conditions observed on July 8, 2026. Configurations and practices may change after that date.
- The assessment was limited to the systems, records, and access made available to Digital Safety and the four VPN activity data categories expressly listed in this report.
- The work did not constitute a penetration test, vulnerability assessment, source-code review, legal compliance opinion, SOC examination, ISO certification, or audit performed under AICPA, ISAE, or governmental auditing standards.
- No assessment can provide absolute assurance that all conditions have been discovered. The conclusion should be read together with the scope and methodology sections.
- This report should be published only in full and without alteration.

10 Assessor Attestation

Digital Safety conducted this assessment as an independent third-party assessor. Lux VPN remained responsible for the operation of its systems, the completeness of access provided, and the accuracy of management representations.

Curt Majors
Managing Director
Digital Safety