SignLogger

Enterprise Log Management, Signed Log Archiving and Network Access Control Platform

Law 5651 logging · Hotspot / Captive Portal · NAC (RADIUS) · Router Mode

One platform, one panel, one licence

signlogger.com · Sysnet Yazılım · Version 7 Platform · September 2026

What Is SignLogger?

SignLogger collects records from firewalls, switches, wireless controllers, servers and other network components over syslog, API, SSH and the Windows agent, normalizes them, indexes them for fast search and turns them into signed archives for long-term retention. With the guest network (Hotspot / Captive Portal) and NAC (RADIUS) modules it verifies the identity of every user and device that joins the network — so the question "who produced this log record?" is answered with certainty. With Router Mode the device becomes the network gateway: zone-based security policy, NAT, SD-WAN and DHCP / DNS are managed from one panel, and Law 5651 records are generated first-hand without relying on an intermediate device.

Organisations today are forced to run separately licensed, separately managed products for log collection, reporting, guest-network management and network access control. SignLogger unifies all of it in a single interface, a single data model and a single licence structure — cutting both total cost of ownership and operational load significantly.

Why SignLogger?

- **One platform, one panel** — Log collection, reporting, guest network and network access control in the same product; no separate products, training or licences.
- **Compliance-driven design** — Signed log archives, day-based retention policies and an independent verification tool keep you audit-ready at all times.
- **Vendor independence** — FortiGate, Sophos, SonicWall, WatchGuard, Zyxel, Palo Alto, Cisco and Ricon from one panel; reporting in one format.
- **Provable integrity** — Every archive is signed; upload the archive file and prove within seconds that the logs were not altered.
- **Capacity forecasting** — Log Analytics calculates daily volume, compression ratio and 1-2 years of disk need — no surprise full disks.
- **Enterprise governance** — Multi-domain architecture, role-based authorisation, audit log and trusted administrator addresses.
- **Self-managing system** — Automatic updates, disk cleanup, backups, service monitoring and notifications keep the management burden minimal.

Architecture and Technical Features

- **Web-based integrated architecture**
  All modules on one server; no extra components
- **syslog / API / SSH integration**
  Log collection from multi-vendor devices
- **FTP / SMB archive transfer**
  Secondary signed copy off-site
- **Certificates, roles and audit log**
  Management access under control
- **Index-based search engine**
  Fast queries over large data volumes
- **RADIUS, LDAP and 2FA**
  Authentication with your existing directory
- **SMTP and SMS notifications**
  Alert, report and verification channels
- **Automatic updates and backups**
  Version history, one-click restore

15+	1000+	100M+	500+
Years of Experience	Enterprise Customers	Daily Log Records	Successful Projects

What's in One Platform?

Each module delivers value on its own; used together they give end-to-end visibility of the organisation's network.

Central Log Collection and Search

System, Windows, Hotspot and Firewall logs in one search experience. Index-based infrastructure; results in seconds across millions of records.

Signed Log Archiving

Automatic daily / weekly / monthly signing and compression. Off-site secondary copy to FTP or SMB targets.

Log Verification

Upload the signed archive file; the integrity of the records is reported independently.

Hotspot and Captive Portal

Branded portal design, multiple languages, several verification methods led by SMS, session monitoring from one screen.

NAC (RADIUS) and 2FA

Access policies with a rule wizard, LDAP / Active Directory integration, two-factor authentication, MAC anomaly monitoring.

Router Mode and Firewall Management

The device becomes the gateway: zone-based rules, NAT / port forwarding, SD-WAN, DHCP / DNS and captive portal in one panel; first-hand Law 5651 records.

Reporting and Automatic Reports

Device- and category-based firewall reports; scheduled reports delivered to stakeholders automatically.

Log Analytics and Capacity Forecasting

Daily log volume, compression ratio and 1-2 years of disk need are calculated; configuration recommendations generated.

Real-Time Monitoring

System health, service status, device connections, disk projection and signing results on one dashboard.

Multi-Domain Structure and Authorisation

Branch / customer isolation with multi-domain architecture; role-based permission profiles and a detailed audit log.

System Management

Device, service, licence, update, disk, backup and certificate management in the same panel; fast rollout with the setup wizard.

Agent Management (Windows Agent)

Collects Windows event logs and enforces 2FA at logon. Zero-touch rollout via GPO / SCCM with a signed MSI + EnrollToken; the fleet is managed and licensed from one center.

Easy Rollout and Management

The setup wizard walks through basic network, time, domain and licence configuration step by step; log flow starts shortly after devices are added to the panel. Ready-made virtual machine packages are provided for Hyper-V and VMware; average installation time is 30 minutes. Updates are applied with one click from the panel, and backup management keeps configuration and data safe. A single system administrator can comfortably run a large infrastructure.

SignLogger turns log management from an obligation into a visibility and security capability for the organisation.

Regulatory Compliance and Audit Readiness

Law 5651 and related regulations expect access records to be retained unaltered for a set period, their integrity secured by signature, and produced on request. SignLogger meets these requirements with automatic signing, configurable retention policies, an independent verification tool, user identity established by Hotspot / NAC, server and client event records collected by the Windows agent, and traffic records generated first-hand by Router Mode.

In practice: when an audit or legal request arrives, the relevant records are found within minutes, presented as a signed archive and technically proven unaltered.

Who Is It For?

Public sector & municipalities	Legal retention and audit-ready archives
Universities, schools, dorms	Heavy guest traffic, identity verification
Hospitals & healthcare	Access control and traceability on sensitive networks
Hotels, malls, cafés & chains	Branded captive portal, SMS-verified Wi-Fi
Multi-branch retail & finance	Central log management across dispersed sites
Factories & industrial zones	Per-device visibility on OT/IT networks
MSPs & system integrators	Multi-customer management with multi-domain

Supported Vendors

FortiGate · Sophos · SonicWall · WatchGuard · Zyxel · Palo Alto Networks · Cisco · Ricon

Also works vendor-independently with every brand that supports syslog, RADIUS and an external captive portal (Mikrotik, UniFi, Aruba, Ruckus, TP-Link Omada, Huawei and others).

See SignLogger up close

For a free demo, technical evaluation and pricing:

signlogger.com · signlogger.com/en/contact