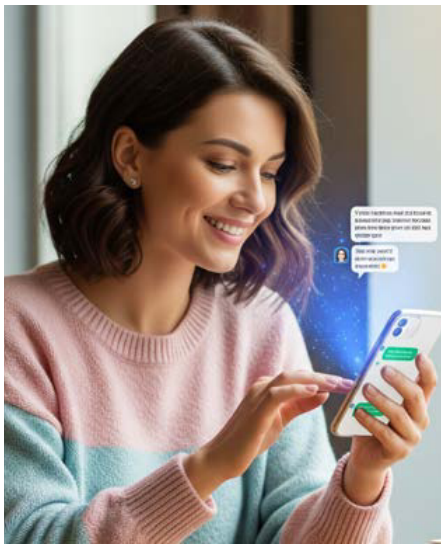
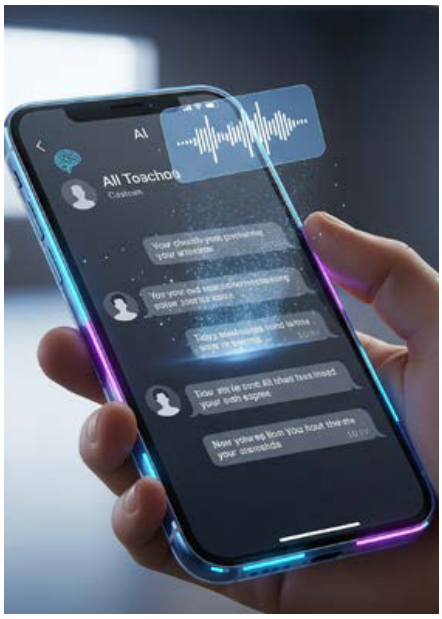
TACACS+ SERVER

One Platform, Every Device, Full Command Control

DATASHEET





Carrier-Grade Device Administration

Our TACACS+ platform handles authentication, authorization, and accounting for every router, switch, and firewall on your network, from one place. It's built for speed, with a low-latency core that keeps commands fast even under heavy load.

We built it on RFC 8907 with AES-256-GCM credential encryption, and hardened it against the NIST SP 800-53 control map, so security is never an afterthought.

2,000	<10ms	NIST 800-53
TPS per Node	Latency	Controls Mapped

KEY CAPABILITIES

- **High-Performance Core:** validated at up to 2,000 TPS per node with latency under 10ms, on just 4 CPU cores
- **Third-Party Identity:** Okta SSO for the console, plus RADIUS and LDAP external authentication with automatic failover
- **Fast, Flexible Deployment:** containerized deployment that scales horizontally as you grow
- **NIST-Aligned Hardening:** TOTP MFA, automatic lockout, and a tamper-evident, hash-chained audit trail
- **AI-Powered Operations:** Smart Problem Detection surfaces the root cause of access issues in seconds, not hours
- **Modern Web GUI & REST API:** configure users, devices, and policies from a modern web console — no CLI required

STANDARDS & DEPLOYMENT

- RFC 8907 protocol
- Database agnostic
- Containerized deployment
- Minimal hardware footprint: a single lightweight node handles up to 2,000 TPS, so even large deployments run on modest, low-cost infrastructure, reducing capital outlay and per-node cloud spend.

ARCHITECTURE

- Horizontal scaling
- Multi-tenant isolation service

AUTHENTICATION & ACCESS CONTROL

- TOTP MFA for console and TACACS+ device logins
- Configurable password policy: legacy rotation or NIST 800-63B modern mode
- Automatic account lockout after repeated failed logins
- User / device / global enable-password hierarchy
- Command-level authorization via policy engine

ACCOUNTING & OBSERVABILITY

- Structured EDR events for every AAA action
- Tamper-evident, hash-chained audit trail with off-box SIEM forwarding
- Prometheus metrics with Grafana KPI dashboards

IDENTITY & INTEGRATION

- LDAP/LDAPS/STARTTLS with group & privilege mapping
- RADIUS external authentication with automatic failover
- Okta OAuth2 SSO for web console admins
- Local-only, local-first, or external-only auth modes
- REST API & interactive docs via Scalar UI
- CSV bulk import/export with validation & reporting

SUPPORTED USE CASES

- Operator read-only access (show commands only)
- Time-of-day change windows
- Source-IP / network restricted device access

BUSINESS BENEFITS

Alepo TACACS+ Platform: Centralized Control, Simplified Audits

OPERATIONAL EXCELLENCE

Stop managing local passwords on every device. Our centralized console handles device administration from one place, so your team spends less time on device-by-device changes.

ENHANCED SECURITY & COMPLIANCE

Our NIST SP 800-53 control map, covering Access Control, Identification & Authentication, and Audit & Accountability, is ready to hand to your compliance team, backed by multi-factor authentication, automatic lockout, and a tamper-evident audit trail.

FASTER TIME-TO-VALUE

Go from pilot to production in days. Containerized deployment and a modern web console mean your team is never blocked waiting on a CLI expert.

SIMPLIFIED OPERATIONS

Prometheus and Grafana plug into the monitoring your team already runs, and a database-agnostic design means IT never has to stand up a new database just for us.

AI-POWERED INNOVATION

Agent Assist: pull up an instant snapshot of a device or user's auth history and active sessions.

Session & Auth Analytics: flags brute-force login attempts and privilege-escalation anomalies as they happen.

AI Agents & Report Intelligence: ask plain-English questions and get compliance-ready audit summaries on demand.

ALEPO

CONTACT US
sales@alepo.com

LEARN MORE
www.alepo.com

STAY CONNECTED
linkedin.com/company/alepo