Termguardium Portal

Web terminal emulator for enterprise legacy applications

> Termguardium — security and access for green-screen and character-mode enterprise applications.

Generated 2026-10-14 · Confidential — for customer and partner use

Web terminal emulator for enterprise legacy applications

ComFix Software



Executive summary

Termguardium Portal is a **browser-based terminal emulator** and **managed session server** for Telnet, TLS, SSH, VT, TN3270, and TN5250 workloads. It gives users **zero-install access** from a modern web UI while preserving the keyboard, colors, function keys, and layout expectations of classic green-screen applications.

When paired with **Sentinel** (recommended for security deployments), the web terminal emulator routes sessions through the relay so every screen and keystroke can be **recorded, searched, and replayed** for UAM and fraud workflows. Portal authenticates the user and presents **named connection profiles**; Sentinel remains the evidence and policy authority.

The challenge

Organizations struggle to balance **accessibility** and **control** for legacy hosts:

- Shipping desktop terminal emulators to every contractor, partner, and work-from-home user is costly and hard to patch.
- Browser VDI or generic remote-access tools often **break terminal key maps**, multilingual layouts, or IBM session negotiation.

- **Direct Telnet** from the browser to production hosts bypasses central logging and admission policy.

Portal delivers a **faithful web terminal emulator** with an optional **Sentinel path** so security teams keep a single choke point.

What Portal does

Full-featured web terminal emulator

- **Profile-based connections** — Operators pick approved profiles (host, port, emulation, terminal type) from Director-managed catalogs.
- **IBM support** — TN3270 and TN5250 (including TN3270E/TN5250E options), code pages, keyboard layouts, on-screen PF keys, PowerPad buttons, and presentation settings.
- **VT and Telnet** — VT220-class terminal emulator sessions, Telnet and TLS, scrollback and session tools where enabled.
- **Shared decode with Station and Sentinel** — Same terminal engine for escape sequences and IBM orders—forensics matches what users see in the browser emulator.

Session lifecycle

- **Connect / Reconnect / Disconnect** from the Portal UI over a **WebSocket** terminal session.
- **Help, theme, and automation** surfaces integrated in the product shell.

Managed mode (Director-controlled)

With **Termguardium managed access**:

- Users **log in** (local, LDAP, OIDC paths per deployment).
- **Profile catalog is entitlement-filtered** — no anonymous host list; secrets stay server-side.
- **Launch bundles** drive WebSocket connect with server-issued tokens.
- Foundation for **Identity Guard SDP**: catalog hidden until authentication, then only authorized profiles appear.

Sentinel integration

Portal is the **identity and launch client** for the web terminal emulator in the integrated architecture:

Integration	Benefit
Session request to Sentinel	Relay opens; returns listen port and optional **connect token**
Routed profiles	Terminal emulator connects to Sentinel listeners instead of raw host ports
Forensics APIs	List sessions, query evidence, kill live sessions
Zero-trust metadata	MFA proof, group memberships, client IP bound into admission requests

Important: Direct-to-host profiles **do not** traverse Sentinel; forensics and UAM require profiles configured **through Sentinel**.

Key strengths

1. **No client install** — HTTPS + WebSocket **web terminal emulator**; ideal for partners, ops centers, and quick rollout.
2. **Director-aligned administration** — Connection profiles, groups, roles, and SSO configured once in Director, consumed by Portal.
3. **Same decode engine as Sentinel and Station** — Reduces drift between **on-screen emulator** and **forensics replay** when sessions are bridged.
4. **Dual deployment** — Standalone Portal for labs; **Portal + Sentinel** for production UAM and Identity Guard.
5. **Automation and keyboard fidelity** — Layout bindings, PowerPad, IBM PF row, charset mapping for multilingual IBM i and VT hosts.

Typical use cases

- **Operations and support** — Browser **terminal emulator** access to IBM i, z/OS, or Unix without VPN plus fat client.
- **Call centers and BPO** — Standardized profiles; Sentinel captures screens for quality and fraud review.
- **Identity Guard user plane** — Authenticated operators launch only entitled channels through Sentinel admission.
- **Training and demos** — Portal + Sentinel labs with public and private sample hosts.

Deployment snapshot

Item	Typical value
Web terminal emulator UI	HTTPS portal URL (default lab: port 3847)
Director admin	Connections, users, groups via Director surfaces
Sentinel integration	Portal configured with Sentinel service URL for bridged profiles

Portal is **not** a replacement for Sentinel recording or Director identity stores—it is the **primary web terminal emulator** in the Termguardium family.

Related reading (PDF)

- Termguardium Suite Overview (PDF)
- Termguardium Sentinel — UAM & Fraud Detection (PDF)
- Termguardium Director — Administration & Identity Guard (PDF)
- Termguardium Station — Desktop Terminal Emulator (PDF)
- Product site: comfixsoftware.com