Termguardium Station

Desktop terminal emulator — standalone power and Director-managed enterprise mode

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

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

Desktop terminal emulator — standalone power and Director-managed enterprise mode

ComFix Software



Executive summary

Termguardium Station is the **native Windows desktop terminal emulator** for Termguardium. It targets power users, branch offices, and automation teams that need **full keyboard performance**, **multi-session workflows**, and **deep host integration** beyond what a **web terminal emulator** alone provides.

Station is also the **modernization anchor** for legacy operations: keep proven green-screen applications while centralizing profiles, scripts, and presentation through **Director**, and optional **Sentinel** recording for UAM and fraud investigation.

Station operates in two modes:

1. **Standalone** — Classic **desktop terminal emulator**: local profiles, direct or Sentinel-routed connections, HLLAPI, PowerPad, and scripting.
2. **Director-managed** — Users authenticate to Director/Portal; Station receives a **launch bundle** with entitled profiles, terminal emulator settings, PowerPad, colors, and automation—ideal for **standardized corporate desktops** and **Identity Guard** paths.

In both modes, routing **terminal emulator** sessions **through Sentinel** preserves **UAM, fraud investigation, and admission controls** on the same evidence pipeline as Portal.

The challenge

Enterprises still standardize on **Windows desktops** for IBM i, z/OS, and Unix character applications:

- **Web terminal emulators** excel at reach; **Station** excels at **speed, HLLAPI/RPA continuity, and operator-grade desktop emulation**.
- Unmanaged terminal emulators scatter profiles and macros across machines—no central entitlement, revocation, or script governance.
- Fraud and audit teams need **the same screen evidence** whether the user chose browser or desktop **terminal emulator**.
- **Modernization** pressure demands better security and administration **without** rewriting host applications.

Station closes the gap: **one desktop terminal emulator on Windows**, optional **Director control**, optional **Sentinel in the path**, and an automation story that bridges legacy hosts and contemporary integration teams.

Global languages and terminal emulator fidelity

Station is built for **real-world host languages**, not a single keyboard locale:

Capability	What operators get
Left-to-right (LTR)	Latin, Nordic, and English operator layouts; VT and IBM sessions with standard code pages
Right-to-left (RTL)	Hebrew, Arabic, and other RTL host presentations with keyboard and host charset mapping
Double-byte / DBCS	East Asian and other multi-byte host character sets where configured—aligned with Portal web terminal emulator and Sentinel forensics
IBM 3270 / 5250	Display and printer session kinds, PF keys, PowerPad, and presentation profiles per connection
VT / Telnet / TLS / SSH	Character-mode hosts with scrollback, session tools, and tunnel options

Shared terminal engine — Station, Portal, and Sentinel use the same decode core so the **desktop terminal emulator** shows the same grid that Sentinel captures for replay.



Scripting, automation, and modernization

Station is the suite's **automation hub** for teams modernizing around—not replacing—legacy applications.

HLLAPI — integrate in your language

- **Industry-standard HLLAPI** (32- and 64-bit) lets RPA tools, test harnesses, and custom apps drive the **terminal emulator** from **C#, Java, Python, VB, and other ecosystems** that speak HLLAPI.
- Screen scraping and workflow automation stay on the **same semantic surface** operators use—ideal for gradual modernization while host programs remain unchanged.

PowerPad and operator macros

- **Configurable PowerPad** toolbars (per layout and emulation) bind function keys, Enter, Clear, and **script actions** for one-click host workflows.
- Director can push **PowerPad and keyboard** settings in managed launch bundles so branch offices share identical operator UX.

C# scripting

- **In-client C# scripts** automate multi-step host interactions, validations, and messaging—power users and admins reduce repetitive keystrokes without a separate toolchain.
- Managed mode can deliver **approved scripts** from Director in the launch bundle (client-executed; governed by your rollout policy).

TypeScript automation in the suite

- **Director and Portal** expose **TypeScript-oriented automation and remote API contracts** for catalog migration, profile tooling, and integration paths—Station participates in the same **managed profile and channel** model those tools configure.
- Together: **HLLAPI for external stacks**, **C# scripts for power users**, **PowerPad for the floor**, **Director for centralized policy**—a practical modernization ladder.

Multi-session and connectivity

- **Multi-session workflows** (session tabs / letters) for operators who jump between host applications in one **desktop terminal emulator** shell.
- **TLS and SSH** upstream options, SSH tunnel patterns for IBM paths, and file-transfer options where enabled—meet security architecture without abandoning terminal workflows.

Modernization outcomes (why customers choose Station)

1. **No rip-and-replace** — Keep IBM i, mainframe, and Unix apps; add Sentinel UAM and Director governance on the path you choose.
2. **Automation continuity** — Preserve HLLAPI investments while **web terminal emulator** and managed clients roll out in parallel.
3. **Central rollout** — Director-managed Station images with profiles, scripts, and PowerPad—fewer “snowflake” desktops.
4. **Evidence-ready** — Sentinel-routed **terminal emulator** sessions give fraud and audit teams **replay-grade** history for desktop users, same as Portal.

What Station does

Standalone desktop terminal emulator

- **Windows desktop application** with connection profiles, session tabs, and terminal rendering.
- **Protocol coverage** — Telnet, TLS, SSH, VT families, TN3270, TN5250 (including printer/session-kind paths where enabled).
- **Windows packaging** — Installer/MSI-oriented release path for corporate deployment.

Users may connect **direct to host** or **via Sentinel listen ports** depending on profile design—security teams should standardize on Sentinel-routed profiles for UAM.

Director-managed mode

- **Managed access** for high-assurance deployments—login to Director/Portal; fetch entitled profiles; launch with server-issued credentials/tokens.
- **Launch bundle** applies **terminal emulator** keyboard, colors, PowerPad, and automation scripts from the server—users cannot point at arbitrary hosts outside catalog.
- **Identity Guard journeys** — Desktop **terminal emulator** participates in Station → Director → Sentinel admission paths.

Managed mode is the **desktop equivalent** of Portal managed login: same identity, same entitlements, different **terminal emulator** shell.

Semantic export and policy (integration)

Where enabled, Station exports **screen semantics** (fields, meanings, fidelity metadata) toward Sentinel for **field-aware policy and DLP**—complementing Sentinel's in-path parse.

Sentinel may respond with **policy actions** (including block) that Station honors on the session.

Key strengths

1. **Global language support** — LTR, RTL, and double-byte host presentations with keyboard and charset mapping in a full **desktop terminal emulator**.
2. **Automation depth** — HLLAPI (any language), PowerPad, C# scripts, and Director-delivered automation in managed mode.
3. **Modernization without migration** — Desktop **terminal emulator** access, centralized policy, and optional Sentinel evidence alongside the **web terminal emulator**.
4. **Two deployment models** — Standalone for dev/power users; managed for **locked-down enterprise** desktops.
5. **Suite consistency** — Same profiles and channels as Portal when Director is authoritative.
6. **Evidence parity** — Sentinel-routed sessions produce the same **forensics replay** as the web terminal emulator.
7. **Zero-trust desktop path** — Managed + Identity Guard + Sentinel admission without forcing browser-only access.

Typical use cases

- **Branch banking or retail back-office** — Managed **desktop terminal emulator** images with approved IBM i or mainframe profiles and shared PowerPad macros.
- **RPA and test automation** — HLLAPI-driven flows against 5250/3270/VT **terminal emulator** sessions through Sentinel for recorded evidence.
- **Global operations** — RTL and DBCS host languages with consistent Director-managed presentation.
- **Developer or admin standalone** — Full local control with optional Sentinel relay for audit.
- **Incident response** — Replay in Sentinel whether the session originated from **Station or Portal terminal emulator**.

Deployment snapshot

Item	Notes
Platform	Windows desktop **terminal emulator**
Managed access	Director/Portal login and launch bundles
Evidence	Requires Sentinel-routed profiles for Sentinel forensics
Learn more	comfixsoftware.com

Station is **not** the administration server and **not** the session relay—it is the **premium desktop terminal emulator and automation endpoint** in the Termguardium family.

Related reading (PDF)

- Termguardium Suite Overview (PDF)
- Termguardium Director — Administration & Identity Guard (PDF)
- Termguardium Sentinel — UAM & Fraud Detection (PDF)
- Termguardium Portal — Web Terminal Emulator (PDF)
- Modernization narrative: comfixsoftware.com/modernization.html