Termguardium Director

Administration, identity, and zero-trust access for legacy applications

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

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

Administration, identity, and zero-trust access for legacy applications

ComFix Software



Executive summary

Termguardium Director is the **control plane** for the Termguardium suite. It centralizes **users, groups, roles, connection profiles, channels, and SSO**—the configuration that **Portal (web terminal emulator)** and **Station (desktop terminal emulator)** consume at login time. Director does not terminate terminal traffic; it **defines who may launch what** and how those launches map to **Sentinel listeners** for recording and enforcement.

For zero-trust initiatives on **3270, 5250, and VT-class systems**, Director combines with Portal and Sentinel to deliver **Identity Guard**: legacy **ZTNA** scoped to green-screen applications—not a generic SaaS VPN replacement.

The challenge

Legacy terminal environments often suffer from **fragmented administration**:

- Connection definitions live on each desktop or ad hoc spreadsheet.
- Host firewall rules grant **network reachability** without **user-level entitlement**.
- IAM teams manage SSO for web apps while **IBM i and mainframe** still rely on shared service accounts and flat Telnet listeners.

- Security projects stall because “ZTNA” vendors do not speak **5250 menus** or **3270 maps**.

Director provides **one administration model** for profiles and identity, while Sentinel enforces **per-user, per-channel admission** when Identity Guard is enabled.

What Director does

Identity and access administration

- **Users, groups, and roles** — Local directory and admin CRUD; import/export for migration.
- **Connection profiles** — Named targets for web and desktop **terminal emulators** (emulation, host, port, terminal options, presentation, PowerPad, scripts) without exposing secrets in the browser catalog where managed mode applies.
- **Profile access rules** — Group-based visibility of which profiles a user may see or launch.
- **Channels alignment** — Profiles that route through Sentinel reference channel names that match Sentinel listener configuration.
- **SSO** — OIDC/SAML/LDAP integration paths per deployment.

Administration surfaces

Director ships as the **management layer of Portal** (web admin UI) and optional **Director service** for scale-out and HA-oriented store backends (connections document with revision control, identity stores, session stores).

Operators use Director to:

- Onboard a user and assign **operators** vs **viewers** groups.
- Publish an IBM i profile that points at **Sentinel**, not direct host Telnet.
- Map **Identity Guard channel assignments** on Sentinel to the same user/group model.

Identity Guard — ZTNA for legacy (cross-product)

Identity Guard is implemented **across Director, Portal, and Sentinel**:

Layer	Responsibility
Director	Users, groups, profiles, channel mapping, SSO configuration
Portal	Web terminal emulator: authenticates user; SDP-style catalog; session request to Sentinel with MFA metadata
Sentinel	ACL, connect token, TCP admission, session limits, evidence with **admitted user id**, step-up, SOC kill

What Identity Guard covers

- TN3270, TN5250, VT-class sessions **through Sentinel**
- Least privilege via channel assignments
- Single-use connect tokens, optional **listen mTLS**
- **MFA at admission**, idle/max session duration
- Fail-closed denials with audit and SIEM hooks

What it does not claim

- Generic ZTNA for all SaaS and web apps
- Device posture (Intune, EDR) as shipped today
- Replacement for enterprise IdP—Portal remains the policy enforcement point for login; Sentinel enforces admission

Honest positioning: *Zero trust access for green-screen and character-mode hosts—identity-bound admission and session control through Termguardium.*

Key strengths

1. **Single profile source of truth** — Web and desktop **terminal emulators** pull the same entitled catalog.
2. **Security-aligned routing** — **Via Sentinel** profiles so UAM and fraud workflows inherit Sentinel evidence automatically.
3. **Identity Guard without a fourth product** — Same suite deployment; configuration activates ZT behavior.
4. **Software-defined perimeter for terminals** — No host list before login in managed mode; profiles appear only after authentication and ACL filtering.
5. **Enterprise scale-out** — Externalized connections and identity stores for multi-replica Director.

Typical use cases

- **Central IT** — Onboard hundreds of operators with approved IBM i or mainframe **terminal emulator** profiles; revoke access by disabling the user in Director.
- **Compliance** — Demonstrate that only **finance** group sees payment-related profiles.
- **Zero-trust pilot** — Pair Director assignments with Sentinel admission; deny unassigned users with auditable denials.
- **Managed desktop** — Station **desktop terminal emulator** users receive launch bundles from Director with keyboard, colors, and PowerPad standardized.

Deployment snapshot

Item	Notes
Primary UI	Portal-hosted administrator (connections, users, groups)
Director service	Optional HA/control-plane deployment
Sentinel alignment	Channel definitions and zero-trust settings must match Director assignments

Director **must not** duplicate Sentinel forensics or terminal parsing—it **governs** who launches which profile toward which Sentinel channel.

Related reading (PDF)

- Termguardium Suite Overview (PDF)
- Termguardium Sentinel — UAM & Fraud Detection (PDF)
- Termguardium Portal — Web Terminal Emulator (PDF)
- Termguardium Station — Desktop Terminal Emulator (PDF)
- Product site: comfixsoftware.com/product-overview.html