GFI AppManager™ AI

USE CASE

Secure user & access management

1 The access control problem: the shared credential trap

Many teams fall into the habit of sharing one “admin” login across KerioControl, GFI KerioConnect®, or GFI Archiver AI appliances. It works, until it doesn’t. Shared credentials create:



First Name	Last Name	Email	Status	Role	2FA Status	Account Name	Password Expiry Status	Last Login	Created
[redacted]	[redacted]	[redacted]	Active	Account Admin		Innovative solutions (HQ)	N/A	Nov 12, 2025	Oct 20,2023
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	N/A	Jul 21, 2025	Jan 1, 2025
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	N/A	Dec 24, 2025	Feb 18,2025
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	Apr 6, 2026	Aug 14, 2026	Oct 28,2022
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	N/A	Mar 12, 2026	Nov 12,2024
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	N/A	Mar 15, 2025	Apr 14,2024
[redacted]	[redacted]	[redacted]	Active	Org Admin		Innovative solutions (HQ)	Expired	Mar 25, 2025	Jan 14,2023

- **Zero accountability:** you can’t reliably prove who made which change.
- **Security windows:** when staff depart, you must rotate passwords across the whole fleet; missing one device can leave a long-lived “backdoor.”
- **Delegation gaps:** junior staff get full admin rights because “view-only” access is hard to implement consistently.
- **Compliance exposure:** shared accounts conflict with GDPR/HIPAA/SOC 2 expectations for unique user identification and auditability.

GFI AppManager AI replaces shared logins with centralized invitations, scoped roles, and an at-a-glance user security view, so access is governed, trackable, and easier to manage at scale.

2 The solution: granular, auditable access control

GFI AppManager AI utilizes two primary roles to enforce the principle of least privilege:

2.1 User invitation & identity

Instead of creating local accounts on every appliance, administrators invite users via the GFI AppManager AI portal.

Workflow:

Access is granted. → User receives email → User creates unique password → Admin sends invite

2.2 Role-based access control (RBAC)

GFI AppManager AI utilizes two primary roles to enforce the principle of least privilege:

Role	Responsibilities
Account Admin	View all appliances, modify settings, manage users, and configure alerts.
Org Admin	Access organization level appliance(s) admin interfaces.

2.3 Organization-level isolation

Access is strictly scoped by "Organizations.

User type	Organization strategy	Access Control
Enterprises	One organization per company	Invite staff to single org; roles control permissions
Org Admin	MSP Master Organization + Customer Sub-Orgs	Techs in master org see all customers; customer IT sees only their sub-org

2.4 User management dashboard

Users Section provides at-a-glance portfolio visibility:

View	Purpose
User roster	First/Last name, email, role, account assignment
Security status	2FA enabled/disabled, password expiry state, last login date
Access state	Active (can login) vs Pending (invitation not accepted)
Last login	“Last Login” column highlights inactive/stale accounts
Quick actions	Edit role, manage 2FA, remove access via menu (≡)

2.5 Time-limited access (15-minute access)

- **What it replaces**: long-lived admin access for “just one task”
- **Outcome:** reduces standing privilege; safer third-party and break-glass workflows

2.6 Native identity protections

- **Includes:** passkey protection and 2FA, password policy, account lockout, and centralized auditing
- **Outcome:** hardens the management plane and supports audit readiness

3 Before vs. after workflow

GFI AppManager AI transforms manual access management into a structured, secure process.

User Task	Traditional (Manual/Shared)	With GFI AppManager AI
Staff Onboarding	Create accounts on 20+ appliances or share master password.	One email invitation; instant access to the entire fleet.
Staff Offboarding	Manually delete accounts on every appliance (high risk of oversight).	Click "Remove User" in GFI AppManager AI; access revoked globally in seconds.
Password Recovery	Admin manually resets passwords on individual appliances.	Self-service "Forgot Password" via email verification.
MSP Delegation	No visibility for customers without sharing technician logins.	Invite customer IT as "User" role for 24/7 self-service monitoring.

4 Measured operational impact

Task	Manual (per appliance)	GFI AppManager AI
Provisioning access (10 appliances)	40-60 minutes	3 minutes
Revoking access (Global)	30 minutes	30 seconds
Audit: 'Who has access?"	2+ hours	3 minutes
Password resets	15 minutes (admin work)	1 minute

Copyright © GFI USA, LLC, All rights reserved.