From Shared Devices to Accountable Operations

How transportation and logistics organizations can improve workforce accountability, access control, and operational visibility.

FIAM Frontline Identity, Access & Management

Is your frontline truly secure?

For too long, companies have relied on basic MDM. But a **managed device is not a fully secure device.** IT teams face two challenges at once: building a real defense against breaches, and consolidating the chaos of too many management tools.

Transportation and logistics organizations rely on shared mobile devices to keep operations moving. Yet many struggle to answer basic questions: Who logged in? Who completed the task? Who accessed sensitive information? Without clear user accountability, organizations face security risks, operational inefficiencies, and audit challenges. **42Gears FIAM** and **DecisionPoint** help create visibility and accountability across frontline workflows while strengthening security and user access controls.

THREE PILLARS, ONE PLATFORM

- Device Trust
- User Identity
- Least-Privilege Access

THE PROBLEM

The Shared-Device Accountability Gap

Traditional IT solutions were designed for desk-bound knowledge workers. Applied to shared frontline devices — the "one device, many hands" model — they create dangerous security and operational gaps. FIAM closes them immediately.

1

One device, many hands

MDM is blind to *user* identity on shared devices, leading to password sharing and audit failure. When incidents occur, supervisors often lack visibility into who performed specific tasks, making investigations and accountability difficult.

SUREMDM + SUREIDP

Layers verified user identity onto every managed device — enabling full audit trails of who accessed what, when.

2

Unworkable authentication

Password + MFA is too slow and impractical — gloves, low input, high turnover — for frontline work. Delayed logins can create bottlenecks during shift changes and reduce workforce productivity.

SUREIDP

Fast, passwordless login via NFC badge tap or QR scan — boosting productivity instantly.

3

Unnecessary Access Exposure

Corporate VPNs grant access to the entire network — far more than the frontline ever needs.

SUREACCESS

Enforces least-privilege access with Per-App VPN micro-tunnels — reducing risk by limiting access to only the applications required for each role.

The business impact of the gap: limited visibility into who accessed devices, performed tasks, or handled operational exceptions. The result can be credential-sharing risks, reduced accountability, longer investigations, compliance challenges, and increased exposure to data loss. Operationally, these gaps can make it difficult to resolve inventory discrepancies, shipment exceptions, and workforce accountability issues.

THE PLATFORM

How Accountability Is Built Into Shared-Device Operations

FIAM unifies three essential capabilities into a single, cohesive platform — replacing complexity with clarity and turning device management into device *security*.

PILLAR 01

Device Trust

SureMDM

Establishes device posture with Kiosk Mode, Threat Defense, and OS/app patching. Ensures frontline devices remain secure, compliant, and ready for use **before** access is granted.

KEY OUTCOME

Extends security beyond device management.

PILLAR 02

User Identity

SureIdP

Confirms user identity with fast, passwordless login — NFC badge tap, QR code, OS-level sign-in — solving password fatigue and seamless shift handovers. Creates accountability by linking device activity to specific users throughout the workday.

KEY OUTCOME

Restores user accountability.

PILLAR 03

Least-Privilege Access

SureAccess

Grants access only to the specific applications needed, using Per-App VPN / DNS micro-tunnels. Reduces operational and security risk by ensuring workers can access only the tools required for their role.

KEY OUTCOME

Limits access to only what each role requires.

CONTINUOUS VERIFICATION

Non-compliant devices are automatically blocked. Access is revoked in real time if risk conditions change.

ZERO TRUST, APPLIED

- → **Never trust, always verify** — user identity + device health, every time.
- → **Least-privileged access** — just enough, exactly when needed.
- → **End-to-end visibility** — every user, device, app and action, logged.

PLATFORM UNIFICATION

From Device Management to Operational Accountability

Stop managing disparate tools. FIAM consolidates your entire tech stack while delivering the most stringent Zero Trust security.

Frontline Devices

Unified Identity, Access & Management on shared devices.

Knowledge Workers

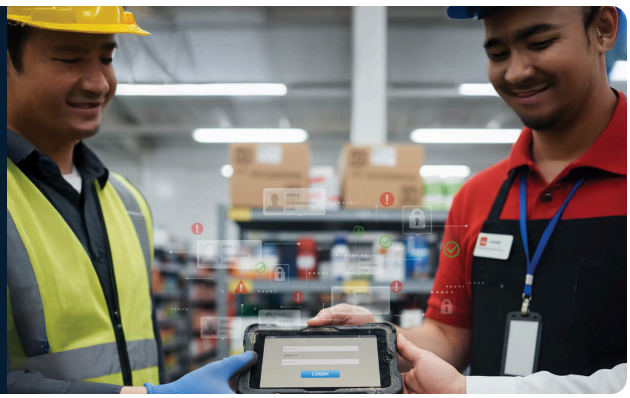
Comprehensive UEM for company phones and laptops.

IoT & Things

Printers, RFID readers and other essential endpoints.

Why DecisionPoint?

Shared-device challenges affect accountability, operational visibility, compliance, and productivity. DecisionPoint helps organizations evaluate workflows, identify gaps, and implement solutions that align security requirements with real-world operational needs.



HOW WE DELIVER IT

01 Assess

- Review device-sharing workflows
- Identify accountability gaps
- Evaluate compliance requirements

02 Design

- Map users, devices, and applications
- Develop role-based access policies

03 Deploy

- Configure and enroll devices at scale
- Validate operational workflows

04 Optimize

- Monitor adoption
- Review access controls
- Improve visibility and reporting

Turn shared devices into accountable operations

Whether you're evaluating new security initiatives or looking to improve existing device management practices, DecisionPoint can help assess your current state and identify opportunities for improvement across your frontline environment.

Schedule a Shared Device Assessment

info@decisionpt.com
decisionpt.com/contact-us

DecisionPoint TECHNOLOGIES | 42GEARS®