

# TechIDManager PAM

## Privileged Account Management for MSPs

In any cybersecurity framework, it is crucial that each account is uniquely tied to an individual and not shared among multiple users. However, an estimated 99% of Managed Service Providers (MSPs) violate this principle by using a single "Admin" account across multiple networks, tenants, and computers. This practice stems from the logistical challenge of creating and maintaining unique accounts for each technician across multiple systems. Consider the case of a moderately sized MSP with 10 technicians and 100 clients - compliance would necessitate the creation and maintenance of over 1000 unique accounts. For MSPs, the importance of these "Unique identifiers" is particularly relevant when technicians access client networks and systems. This type of security measure serves as a crucial element in ensuring accountability and traceability.

TechIDManager is a Privileged Account Management (PAM) software platform that simplifies this process by automating the creation and management of all such admin accounts. It ensures each technician has a distinct account for every domain, tenant, and machine, facilitating secure and efficient tech access to client's systems.

TechIDManager aids in achieving a robust security posture and facilitates compliance with security frameworks by providing the following features:

- Automated creation of unique accounts for each technician across all client systems, with privileges customized based on role.
- Daily automatic password rotation for all accounts.
- One-click functionality to disable a technician's unique accounts across all client systems, manageable by a supervisor.
- Comprehensive logs to track individual access and activity across all client systems.

Feature	How TechIDManager PAM helps
Creates Unique Accounts	Individual named accounts are the only thing that satisfies cybersecurity frameworks.
Stores Passwords	TechIDManager uses asymmetric encryption to cryptographically guarantee that only the technician that should see their credentials, can see them.
Rotate Passwords	Agent based creation of accounts in Office 365, Azure, on prem domains, local machines and other places, with automatic daily rotation of all passwords.
Disables Accounts	With one button click, the manager can disable a technician's accounts.
Manages Rights	Set appropriate and manage all rights for each technician on all clients' systems with a high degree of control.
Offline Credential Access	Have the option to connect to systems that are not on the internet for whatever reason.
Zero-Visibility Storage	We store credentials in a way that not even we can see them. If we get hacked, your information is not compromised.
Downtime Tolerant	Internet access is not required to see or use credential information.
Self Hosted Option	You can be in complete control of all data electronically and physically. Worldwide and Fedramp hosting available.
Easy Deployment	We do white glove installs that average 45 minutes to get everything working.
Credential injection	Easy injection of credentials into MSP tools

For more information see <https://techidmanager.com> and learn about the complete suite of PAM solutions built for MSPs and IT service providers.

