

Fischer Identity™

Turn Identity Management into a Strategic Advantage



Privileged Access Management

Control and audit access to high-privilege accounts

TAKE BACK THE KEYS TO THE KINGDOM

When your records show that "Administrator" created an account, do you know who actually created it? Administrative, Super User, Root, and other privileged and shared accounts provide unlimited access to system resources, yet access is typically loosely controlled and not auditable. Fischer **Privileged Access Management** enables you to recapture the "keys to the kingdom" by providing a simple and efficient method for acquiring and auditing the use of high-privilege accounts.

Privileged Access Management protects you from security breaches, fraud, and compliance violations, as well as providing proof of which users could access an account at any point in time. The bottom line: without automated control of privileged accounts, you don't have security or compliance.



Solve These Business Issues Within Days

Privileged accounts such as Administrative, Super User, Root, and Fire-Call provide the nearly-unlimited access to system resources that is essential for everyday and emergency IT operations. However, these accounts are typically shared, resulting in multiple persons knowing the credentials for a single account on a system or application.

Thus, it's often impossible to determine which individual actually performed an activity such as creating a new account or changing permissions for an account. Auditors have reported material deficiencies as this violates regulations such as Sarbanes-Oxley and HIPAA.

↳ Data Security Problems

- Unable to protect the keys to the kingdom: cannot control or trace who uses privileged accounts due to shared credentials
- Increased risk: TJ Maxx and other organizations lost hundreds of millions of dollars as well as their reputations
- Fire-call accounts are dangerously vulnerable to attack or misuse: highly-privileged accounts must be readily available for emergencies

↳ Compliance & Audit

- Inability to prove compliance for shared accounts: not possible to report who performed a specific function
- Insufficient controls: cannot enforce Separation of Duties on shared accounts

Strategic Advantages

Safeguard access to sensitive corporate and personal data such as protected health information

Mitigate risk of inappropriate access to trade secrets, financial data, and other resources

Prove that the control of privileged accounts complies with regulations

Document who had access to a privileged account at any point in time

Quickly and accurately respond to audits

Fischer Identity™

Turn Identity Management into a Strategic Advantage

CONTROLLED, AUDITED ACCESS EXACTLY AS YOU NEED

Privileged Access Management provides you with a flexible framework for enabling audited and rapid access to privileged accounts. Access requirements may be defined for each account or for groups of accounts: *e.g.*, who may request access, whether a reason must be provided, what is the maximum duration, whether the account password is reset upon check-out, when an approval is required, how to process requests that expire without action, and so on.

- **Authorize users to request access to tightly-controlled accounts**
- **Track account access to individual users of shared accounts**
- **Granular control of access requirements: requesters, approvals, expiration, etc.**
- **Control, audit, and secure resources to comply with regulations like Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, Family Educational Rights and Privacy Act (FERPA), etc.**
- **Provide authorized persons with immediate access to fire-call accounts**
- **Enable system owners to periodically revalidate longer-term accounts**
- **Secure protected accounts by preventing system owners and administrators from viewing account passwords**
- **Combine with Automated Role & Account Management to create a closed-loop solution including account creation, entitlements/privileges management, etc.**
- **Roll-out privileged account access in days, not months**



Finally, Identity Management for any-sized organization and any procurement model

- **Traditional on-premise**
- **SaaS**
- **Hosted**
- **Remotely Managed**



Fischer: Trusted Data Security for More Than 25 Years



For more information

Fischer Identity removes the complexity of identity management to enable organizations to focus on automating and managing business processes instead of technology. Ask your Fischer Representative for additional information or visit www.FischerInternational.com.

USA: +1 239-643-1500
info@fischerinternational.com