

Fischer Identity as a Service™ Solutions

Remotely-hosted, secure Managed Identity Services® without the cost or risk of traditional deployments



Privileged Account Access Service

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’s Privileged Account Access Service 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.

The Privileged Account Access Service 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.

Additionally, this managed service lets you avoid the cost and distraction to license, deploy, and maintain identity software. Fischer’s Identity as a Service™ (IaaS™) solutions let you “pay as you go” for just the services you need and for only the people you need.



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 sharing (or 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

- Privileged accounts provide unlimited access to system resources but are often not controlled
- Not possible to report who performed a specific function or to enforce Separation of Duties on shared accounts
- Insufficient controls cost TJ Maxx and other organizations hundreds of millions of dollars and their reputations
- Accounts used for fire-call purposes need to be readily available for emergencies, but current access control methods often leave the highest-privileged accounts dangerously vulnerable to attack or misuse

➤ Compliance & Audit

- Auditors demand proof of controls for these accounts, yet most organizations cannot comply

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 as a Service™ Solutions

Remotely-hosted, secure Managed Identity Services® without the cost or risk of traditional deployments

CONTROLLED, AUDITED ACCESS EXACTLY AS YOU NEED

The Privileged Account Access Service provides you with a flexible framework for enabling audited and rapid access to privileged accounts. Access requirements may be defined for each account or groups of accounts: *e.g.*, who may request access, if a reason must be provided, what is the maximum duration, if the account password must be reset upon check-out, when an approval is required, how to process approvals 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 the Automated Role & Account Management Service to create a closed-loop solution including account creation, entitlements/privileges management, etc.**
- **Roll-out identity services in days, not months**
- **Rightsize your solution as your business requirements change**
- **Stay focused on your business: avoid diverting time and attention to non-core activities**



Discover the Family of Fischer Identity as a Service™ Solutions

Fischer's IaaS™ solutions include "turnkey" packages that can be deployed in a fraction of the time and cost of a traditional, fully-customized identity management project. These packages rapidly deliver low-cost, high-value identity services to organizations in a matter of days and provide an extremely low total cost of ownership (TCO).



Fischer: Trusted Data Security for More Than 25 Years



Built for Business...Yours™

Fischer International Identity

3073 Horseshoe Drive South
Naples, Florida 34104
+1 239-643-1500

www.FischerInternational.com

Please contact us to learn more.