

Fischer International Identity
BUILT FOR BUSINESS... YOURS™

PRODUCT OVERVIEW

Fischer Password Manager

The Case for Password Management

Managing passwords is a common challenge that is shared from the smallest organizations to the largest. The problem is how to protect an increasing number of IT assets such as data, systems and applications while reducing costs and enhancing user experience and productivity. Further complicating the picture are factors such as inter-organizational partnerships, additional applications and platforms as well as the need to prove compliance with numerous regulations.

From an end-user perspective, it's not uncommon to have to remember more than a dozen accounts and passwords. That's difficult enough, but end users are also being forced to use longer, more complex passwords, and to change passwords more frequently, which causes frustration and lost productivity, and results in expensive and sometimes embarrassing calls to the Help Desk. Predictably, users try to choose easy or obvious passwords, or resort to writing their passwords, and sometimes even storing their passwords in obvious locations. Not only do these factors increase expenses for the Help Desk and administrators, they reduce employee productivity and increase exposure to unauthorized access. Any solution to this problem must be intuitive and easy to use or end users will find a way to circumvent its use.

From an operational perspective, analysts report that password problems are the primary source of calls to the Help Desk and typically account for more than 30% of the call volume. Reported costs vary widely from under \$10 per call to more than \$50 per call, and as much as \$200 per user per year depending on the industry, geography, organization size, and even the individual organization. Each enterprise, and often each application, has a unique set of security policies that must be managed cost effectively. Without a password management tool, the Help Desk personnel or administrators must be trained to manage their policies using multiple administrative interfaces. Training (and trust of help desk personnel) must be substantial, or some calls will need to be escalated to administrators since improper administration can cause major problems.

Auditors demand proof that security policies are actually enforced and that organizations comply with numerous regulations. While seemingly straightforward, achieving a corporate view of compliance is difficult because password management event logs may be stored in a different database/format than event logs for provisioning and other activities.

Many organizations have attempted to address some of these challenges with technologies like web single sign-on (SSO) or even enterprise SSO. Unfortunately, these technologies are costly, they're typically hard to integrate, and they usually address only some of the systems and applications.

Selecting a Solution

When selecting a password management product, look at provisioning first as most organizations that start with password management later implement provisioning. Fischer Password Manager provides more value and capability than any other password management product because we have the most advanced and robust provisioning solution available. Provisioning products go hand-in-hand with password management, and most organizations should consider one vendor to provide both solutions. However, provisioning is far more complex and has much larger compliance, business efficiency, and cost implications. Since conventional provisioning products are notorious for costing more and delivering less than expected, organizations can be headed for disappointment or even disaster if they don't evaluate the vendor's provisioning product when selecting their password management solution.

Fischer Password Manager Features

Fischer provides a cost-effective and easily-deployed solution to password management challenges. Password Manager improves security, reduces costs, improves productivity, and improves the user experience, and it's fast and easy to implement to meet each organization's particular requirements.

24/7 Password Reset – users can quickly and easily reset forgotten passwords using a choice of interfaces instead of calling the help desk, even when the Help Desk is closed. Users choose to authenticate through challenge-response or by using their credentials for any of their other accounts.

Password Changes – users can periodically change the passwords for all their accounts at once through a single interface. Users are immediately alerted if a chosen password does not comply with policies.

Intuitive Interfaces – users require little or no training to reset or change their passwords through Password Manager.

Faster Password Reset By Help Desk – for users who continue to call for password resets, Help Desk personnel use a single interface to change passwords for all systems and applications instead of learning and repeatedly switching between multiple proprietary interfaces. Help desk personnel no longer require credentials for each system they'll reset and can handle all password resets without escalation. They are also prevented from making changes that would harm the systems and applications.

Security Policy Enforcement – enforces any password policies to meet each organization's requirements. Each connected system can have unique policies or the organization can choose to normalize policies for multiple connected systems to simplify password management. Fischer Password Manager can also enforce unique password policies for multiple groups of users for a single connected system or application. Point & click policies include rules such as the following:

- minimum characters
- maximum characters
- no password reuse
- # of numerals
- # of letters
- dictionary check
- # of special characters
- # failed logon attempts allowed
- # failed password resets allowed

Regulatory Compliance – helps comply with governmental regulations such as Sarbanes-Oxley, HIPAA, the European Privacy Directive, etc. by proving enforcement of security policies.

Password Groups – simplifies the case where password policies of some connected systems are in conflict with each other. Organizations can specify which connected systems will have their passwords changed together as a group. For instance, passwords of all connected systems that require at least 8-character passwords could be changed as one group while passwords of all connected systems that permit a maximum of 7 characters could be changed as another group.

Password Aging and Notification – enforces the required frequency of password changes. Users can be notified by email when their passwords are near expiration. Organizations specify how many days notice are given to users, and daily notices are automatically sent until passwords are actually changed. Organizations can easily lock accounts whose passwords have not been changed according to policy.

Audit Log – all successful and failed password resets and password changes are automatically logged to the audit database so they can be reported for regulatory compliance.

Enable Password Changes For Individual Accounts – specify whether Password Manager transparently changes passwords for all accounts or whether the user is permitted to selectively change passwords.

Password Changes for Lotus Notes – in addition to managing Lotus Domino passwords at the server level for the Lotus Notes web client, Password Manager securely manages Notes password files at workstations for the Lotus Notes desktop client. A desktop component is required for workstations needing this level of password management.

No Desktop Changes – other than the component for Lotus Notes desktop clients, no changes (such as GINA replacement) are required, even to reset passwords for workstations authenticated through the LAN.

Realtime Termination – immediately revoke access to all accounts when an end user leaves the organization.

SSO / ESSO Integration - (E)SSO integration takes several forms:

- Password Manager can change / reset a user's password for (E)SSO.
- For organizations that allow users to access applications directly as well as through (E)SSO, users can securely reset their forgotten passwords for specific applications.
- Fischer's user self-service and administrative interfaces can be authenticated through (E)SSO.
- (E)SSO and other authentication systems can incorporate multi-factor access control such as biometrics, tokens, etc.

RSA Token Management – enables users and administrators to manage RSA SecurID tokens:

- Associate a SecurID token with an particular user
- Change User PIN settings
- Enable/Disable a SecurID token associated with a user
- Additional features are available with Fischer Provisioning

Integration with Help Desk Software – automatically opens / updates / closes Help Desk tickets.

No Geographic Boundaries – Password Manager securely works across the Intranet and Extranet with employees, partners, customers, etc. It can easily replace the non-secure facilities commonly used for Extranet password resets that send user passwords via email.

Account Matching – any set of accounts and IDs can be assigned to a user. User IDs don't need to match across systems.

Realtime Changes – unlike password management systems that require nightly updates, changes to Password Manager are effective in realtime.

Secure Password Kiosk – enables users to securely reset their passwords, even when their workstation is authenticated through the LAN and they cannot authenticate to their workstations. When combined with Fischer Provisioning, this interface also enables organizations to securely distribute new accounts to users without exposing passwords to anyone. Selected challenge-response authentication answers can be automatically pre-populated with information from one or more connected systems.

Choice of User Interfaces – Fischer Password Manager offers a choice of several interfaces to meet the needs of each organization. User interfaces can be combined in any combination as required: Web interface, Secure Password Kiosk, Windows Network Login, NetWare Network Login, Integrated Voice Response (IVR) or Fischer iFly (mobile access).

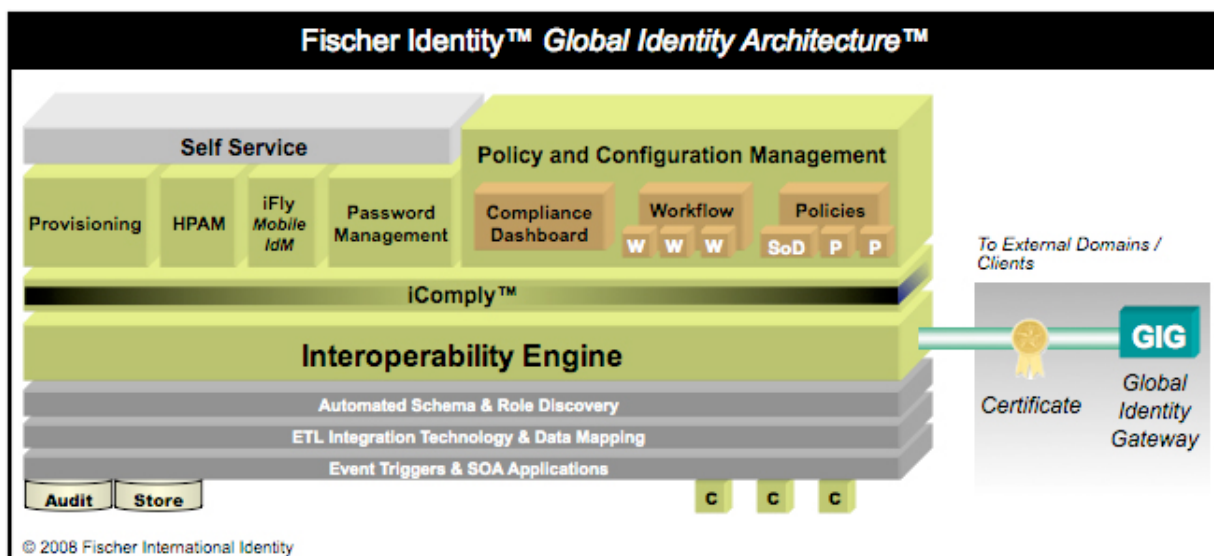
Configurable Challenge-Response Process – a secure process is used to authenticate users who forget their passwords. Organizations specify:

- Number of questions to be answered during the setup phase, including the number of questions that users can create themselves.
- Number of questions that must be answered to reset a password.
- Text of questions.

Fischer's Global Identity Architecture

Fischer Password Manager is part of Fischer Identity, a suite that shares the same architecture and was designed with a single vision, which enables rapid implementation and benefits with minimal ongoing support requirements. All components in the suite are quickly and easily installed together during a standard installation process, but organizations license and configure only the components they require.

Fischer's Global Identity Architecture (GIA) is a patent-pending, out-of-the-box capability that quickly, easily and securely extends all facets of Identity Management across domains, including password management, user provisioning, workflows, policy management, approvals, self service, connectivity and compliance. Fischer Identity is the only suite that provides the ability to cross enterprises, domains and firewalls without adding significant additional components or possibly even duplicating the entire solution. It minimizes complexity and cost without the risk of opening potential security holes, which is important since most organizations operate across multiple domains.



Operating Environment

Since Password Manager is a Java application, it will run on any Java platform. Fischer supports Password Manager on a variety of commercial and open systems including Linux, Solaris, Windows, PostgreSQL, SQL-Server, Oracle DB, Sun Java System Directory, Active Directory, WebSphere, WebLogic, IIS or Apache / Tomcat.

Connectivity

An “agentless” approach simplifies connectivity. For legacy systems that don’t natively support TLS/SSL, connectors can optionally be placed on the connected system servers to provide the needed security.

Fischer iFly (mobile access)

iFly allows mobile workers to manage their passwords using PDAs, including the ability for a user to change a password and have it synchronized to all his/her accounts across the enterprise. Resetting passwords is accomplished through a challenge and response facility that is similar to the one in the web-based interface. iFly also enables other functions such as provisioning approvals and directory search.

Security

Fischer’s long heritage of creating enterprise-class security products attests to the high quality standards and practices utilized in Fischer Identity. Communications sessions and data are secured with Web Services-Security (WSS), TLS / SSL, HTTPS and / or Java Secure Socket Extension (JSSE). Fischer uses WSS to secure communication channels between the various components as well as between Fischer Identity and 3rd-party SOAP or .NET clients.

Fischer Identity **never releases sensitive information** such as administrative IDs and passwords for the connected systems. Of course, sensitive data such as passwords and answers to security questions are hashed using SHA-1; other information can be encrypted as well. That means that no passwords or other sensitive data are ever exposed, including file exports for backups and other purposes.

Administration

Administrators handle all aspects of the product through a web-based UI. They can configure connectivity to participating systems as well as specifying policy-based security to enforce which features are available to end users, the Help Desk and others.

Audit

Records of all password change / reset activities are automatically stored in a standard database for audit and compliance. Audit information includes the date, time, status and identity of who initiated the last password change / reset for each account, which helps detect if an intruder has attempted to gain access.

High Privilege Account Management (HPAM)

In addition to managing end user passwords through Password Manager, Fischer Identity manages access and passwords for high privilege and shared accounts through the HPAM component of Fischer Provisioning. HPAM enables authorized users to access needed resources while tracking exactly who has permission to access each resource at any given moment. Also, HPAM's programmatic checkout ability eliminates the need to embed administrative passwords in scripts.

Benefits

Fischer Password Manager provides many benefits while setting the standard for rapid time to value and low total cost of ownership.

- Improved security and audit procedures help organizations comply with government regulations such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and the European Privacy Directive.
- Password policy enforcement strengthens security. Since users can be permitted to access all resources with a single password, they can be required to choose stronger passwords without the need to write them anywhere. Standardized authentication for password resets can eliminate "social engineering" by intruders.
- Costs are reduced by virtually eliminating most password reset calls to the help desk. Calls that do reach the help desk can be handled more rapidly through a single interface.
- Managing password resets and synchronization across the enterprise cost-effectively improves productivity: users who forget their passwords return to work faster by securely resetting their own passwords.

Fischer International Identity
3073 Horseshoe Drive South
Naples, Florida 34104
+1 239-643-1500
www.FischerInternational.com



Built for Business... *Yours*™

Document MCB-08-110A: May, 2008

©2008 Fischer International Identity, LLC. All rights reserved.

Fischer International, Fischer International Identity, Managed Identity Services, Identity as a Service, IaaS, the Fischer International Logo, Global Identity Architecture, DataForum, Fischer Global Provisioner, Built for Business...Yours, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International. All other company, product, or trade names are the property of their respective owners.