



Fischer International Identity

Built for Business... *Yours*™

High Privilege Account Management (HPAM): Solution Overview

Introduction

High privilege accounts are commonly shared and are a growing security concern, particularly for organizations that must adhere to corporate governance and compliance regulations. Generally, they are the Administrative, Super User, Root, and Fire-Call accounts which provide the nearly-unlimited access to system resources that is essential for everyday and emergency IT operations.

A consequence of this broad, uncontrolled access is that organizations are left wide open for compliance violations, privacy breaches, and fraud. For organizations to have a closed security and compliance loop, part of the overall strategy must include a process for monitoring and managing high privileged accounts. The bottom line is that without an automated privileged account management (PAM) solution, an organization does not have security or compliance.

Privileged Account Management Challenges

The following are high-privilege account challenges.

- **Insufficient oversight and audit:** Most organizations lack appropriate controls to regulate the privileges and usage of high-privilege accounts. Yet regulations such as Sarbanes-Oxley, HIPAA, J-Sox and GLBA, dictate that organizations be able to prove who had access to which data and resources, when, why, and who approved their access and entitlements.
- **Common access to account IDs and passwords (shared accounts):** Many organizations create a small pool of high-privilege accounts that are shared among several people. The typical problem with "shared accounts" is that everyone uses the same ID and password. This creates compliance challenges as it is impossible to determine who has access to the accounts and who actually performed a specific function.
- **Inappropriate Segregation of Duties:** The IT Resource Staff that use and maintain high privilege accounts are typically the largest holders of informational access in any organization. Certain high-privilege accounts, especially those designed for emergency operations and incident handling, can allow misuse to go virtually undetected or not be traced to any individual. This forces organizations to choose between compliance and the ability to quickly recover or troubleshoot issues.
- **Self-enforcement of "The Principle of Least Privilege:"** Some administrative-level users choose to use a high-privilege account for everyday activities instead of their general user account, as it eliminates the time and interruption to acquire the high-privilege account, continually re-enter passwords, etc. This practice unnecessarily increases an organization's level of exposure in the event the high-privilege account is compromised or errors are inadvertently committed.
- **Hard-coded IDs and Passwords:** Administrative IDs and passwords are sometimes embedded in programs or scripts for automated processes or kept in configuration files without being changed according to policy. This increases the likelihood of hackers finding passwords since the scripts and configuration files are usually not completely secured.
- **Stand-alone PAM Products Undermine Efficiency and Compliance.** Privileged account management is best when it is part of the overall Identity solution rather than a standalone product. Standalone PAM products that are not part of the provisioning architecture do not possess core functionality (account creation, entitlements/privileges management, etc.) required for a closed-loop solution, and introduce an additional infrastructure (connectors, policies, workflows, approvals, audit data base, etc.) to implement and maintain. Only PAM solutions that are part of a user provisioning product should be considered as they provide all the functionality required to create and manage high-privilege accounts and can leverage the existing provisioning infrastructure, making implementation, administration, and audit activities much faster, easier, more reliable, and less expensive.

Solution Overview

Fischer's **High Privilege Account Management™ (HPAM)** solves the problem of managing high privileged accounts. Fischer HPAM provides the control, auditing, and compliance required for securing and managing access to administrative and other highly-privileged accounts, including temporary and single-use administrative accounts. HPAM is part of Fischer's Global Identity Architecture and takes full advantage of Fischer Identity's core capabilities (provisioning, password management, self-service, approvals, etc.) and infrastructure components (policies, workflows connectors, etc.) to provide better control and security with less overhead. For example, HPAM:

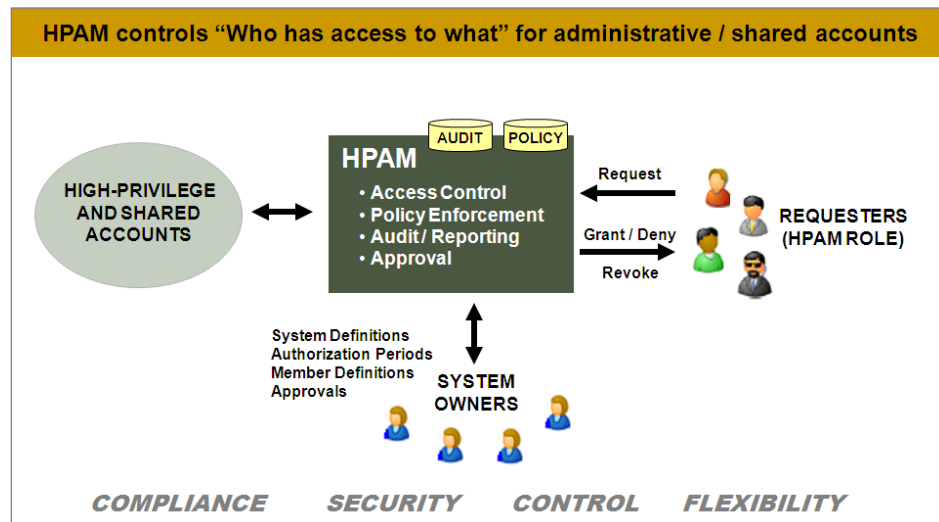
- **Provides accountability and avoids material weaknesses:** control and track privileges across multiple shared accounts. Track account usage back to a specific user.
- **Prevents casual use of privileged accounts:** all account access is recorded and subject to approval/review of managers and system owners, discouraging use of privileged accounts for routine operations
- **Accelerates and simplifies audits:** PAM data is stored in Fischer's single audit database and is easily incorporated into compliance reports
- **Never embed passwords within scripts:** HPAM eliminates the need to hardcode administrative IDs and passwords within scripts and programs
- **Self-documenting internal controls:** automatically documents the compliance process detailing: who can perform administrative tasks, when and who approved their access, and the rationale and approval history for the accounts.

Fischer HPAM offers a simple and cost effective way for organizations to improve security and automate privileged compliance.

How HPAM Works

HPAM enables organizations to conveniently maintain small pools of high-privilege accounts instead of having to create and manage a large number of user-specific accounts. When an authorized user needs access to a high-privilege account, he/she simply opens the HPAM web interface and requests the type of account required, for which period of time, and why the account is needed. Depending on the organization's rules and the requester's attributes, the requester can receive access immediately, upon approval by the System Owner through Dual Control, or after a specified period of time. Automated approval can be desirable when, for example, an emergency situation occurs in the middle of the night and no approver is available. Pre-assigned persons can automatically receive the access they need for a limited period of time. Requests can also be automatically rejected if not approved within the specified period of time or can be automatically escalated to another approver. In any case, the System Owner retains full control and can easily revoke access that has been granted to accounts. Refer to Figure 1.

Figure 1:
Fischer HPAM Solution
Overview



HPAM includes a complete audit record of **exactly** who can perform administrative and other high-privilege functions, for which periods of time, why the functions were needed, who approved the privileges, and why the requests were approved. Administrators can specify that account passwords are changed every X minutes / hours for ultimate security and control. All events are audited (more than 90 different events) whether they occur at an end-user interface, at a connected system or on the Fischer Identity Suite™ server. This incorporates all actions taken by requesters and approvers including comments regarding why accounts were needed and why approvers took specific actions. Auditors can quickly see the full scope of compliance including comments by administrators overriding policies. HPAM simplifies the auditing process by proving that most high-privilege accounts were inactive for long periods of time. HPAM also enables periodic re-approval or “attestation” of accounts including permanent administrative and other high-privilege accounts. HPAM users and System Owners can automatically receive email notifications regarding accounts that have been approved, relinquished, rejected, are about to expire, are automatically expired, etc.

HPAM is always secure. System Owners specify which requesters can view / request / relinquish specific resources. System Owners can approve / revoke / reject the use of any high-privilege accounts. By utilizing these high-privilege accounts with appropriate permissions, there's typically no need to divulge the root password of a controlled system, yet the administrative function is quickly available if it's ever required. HPAM also never stores user passwords and IT operations personnel no longer need to handle passwords or allocate accounts. When Fischer Provisioning™ creates a new account, it's assigned appropriate privileges and protected by a randomly-generated password that no one knows. Once a high-privilege account has been approved, HPAM enables the requester to securely change the password to a value that complies with the organization's password policies for the system, including minimum and maximum length, dictionary check, and password composition such as the number of alpha characters, numerals, special characters, etc. When a high-privilege account is revoked or relinquished, HPAM can again automatically change the password by Account Type so that no one can use the account without approval, not even super user administrators. All communication with connected systems and applications are protected by WS-Security and/or TLS/SSL.

HPAM uses out-of-the-box connectors to securely provide administrative credentials to programs and scripts instead of using embedded credentials. For Application Servers on either UNIX or Windows, HPAM can periodically rewrite the file containing the credentials, or it can periodically invoke an existing script that is used for this purpose.

Exclusive Benefits

HPAM eliminates the risk of compliance violations, privacy breaches, and fraud due to shared accounts or excessive privileges. Unlike other products, only HPAM can leverage the power of Fischer's Global Identity Architecture™ to provide the following exclusive benefits:

- Manage both local and remotely-connected systems using the same procedures.
- Easily manage individual access to high-privilege accounts to eliminate shared accounts.
- Maintain identity-related compliance without delaying access to accounts.
- Enforce the Least Privilege principle by enabling access to high-privilege accounts only when needed.
- Automatically audit all high-privilege accounts to enable reporting.
- Manage Administrative, Super User, Root, and Fire-Call accounts within the same identity framework as the rest of the enterprise.
- Eliminate requirements for coding, scripting, or proprietary hardware.
- Control virtually any systems and applications via agentless plug & play connectors.
- Access HPAM via web browsers without any client software.
- Provide flexible access control approval with full oversight.
- Tightly control processes for requesting and approving high-privilege accounts.
- Enforce password policies and provide automated password randomization.
- Securely generate passwords on demand rather than storing passwords as a target for hackers.

-
- Never reveal passwords to anyone except intended users, not even to super user administrators.
 - Prevent problems possible with other solutions, such as inadvertently rendering an account unusable when changing a password
 - Eliminates the requirement to embed credentials in your scripts and applications.
 - Automatically change passwords in configuration files to meet your password policies.

Fischer International Identity

Built for Business... *Yours*™

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

Document MCB-07-250G: October, 2007

©2007 Fischer International Identity, LLC. All rights reserved.
Fischer International, Fischer International Identity, Managed Identity Services, Managed Identity Services Technology, Identity as a Service, IaaS, the Fischer International Logo, Global Identity Architecture, Built for Business...Yours, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International Identity.



Built for Business... *Yours*™