



# **Enterprise Password Management Requirements and Solutions**

[ WHITE PAPER ]

*by*

**e-DMZ Security, LLC**

*June 6, 2007*

: . .9370 | Toll Free: .203.9823 | Fax: .793.4985  
eMail: [par-info@e-dmzsecurity.com](mailto:par-info@e-dmzsecurity.com) | web: <http://www.e-dmzsecurity.com>

## Enterprise Password Management Requirements and Solutions

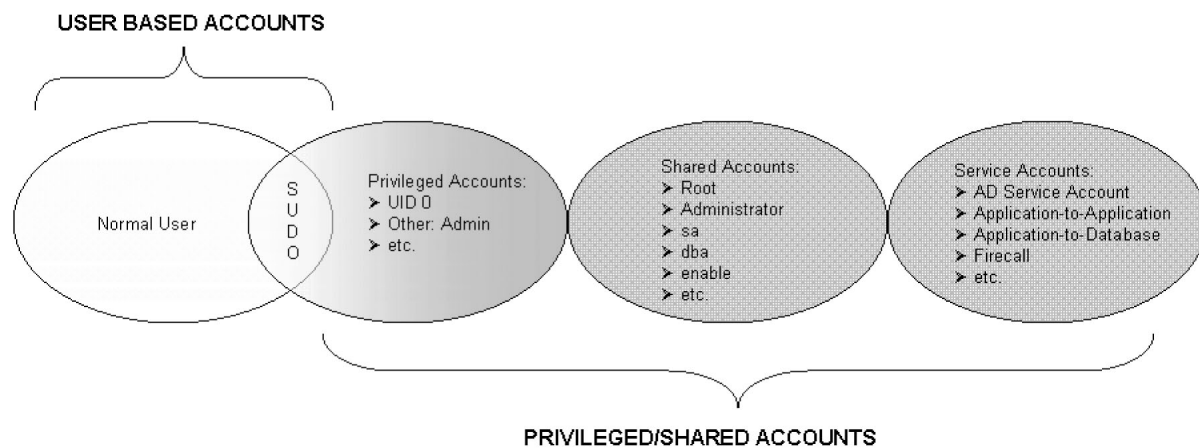
Most all computer systems, network devices and applications will support different account types based on the role/function of the specific user accessing the system. As shown in Diagram 1, these accounts may include:

**User Accounts:** Configured named accounts created for specific user level access.

**Privileged Accounts:** Configured accounts created to provide elevated rights and/or administrative level access.

**Shared System Accounts:** System defined fixed generic account(s) providing 'super user' administrative access.

**Service Accounts:** Defined accounts that will generally have administrative or higher (i.e. LocalSystem) access. Typically used to allow applications and programs to login as a service to perform high level tasks.



**Diagram 1**

The identity and password management issues associated with each account type can differ and today are addressed by various solutions such as:

**Identity Management Solutions (IdM):** IdM solutions such as Sun IDM, CA eTrust provide solutions for the management and control of pervasive user accounts and passwords that can exist across many systems and applications. As shown in Diagram 2, IdM solutions help the enterprise map and control user identities and passwords across many enterprise resources.

**Privileged User Management Solutions (PUM):** PUM solutions such as open source SUDO and Boks by FoxT provide solutions that will manage grant user accounts temporary access to defined privileged or shared accounts. As shown in Diagram 2, PUM solutions help solve the issue of individual accountability to privileged accounts by managing access to generic accounts through defined user accounts.

**Shared/Service Account Password Management (SAPM):** Also known as privileged account password management, SAPM solutions such as e-DMZ Security’s Password Auto Repository (PAR) solve the accountability, storage and management control issues associated with generic shared and service accounts. As depicted in Diagram 2, SAPM solutions like PAR map and control system administrator access to shared privileged accounts. In addition, most SAPM solutions will offer CLI/API access allowing hard-coded script/application/service account passwords to be replaced with password retrieval calls.

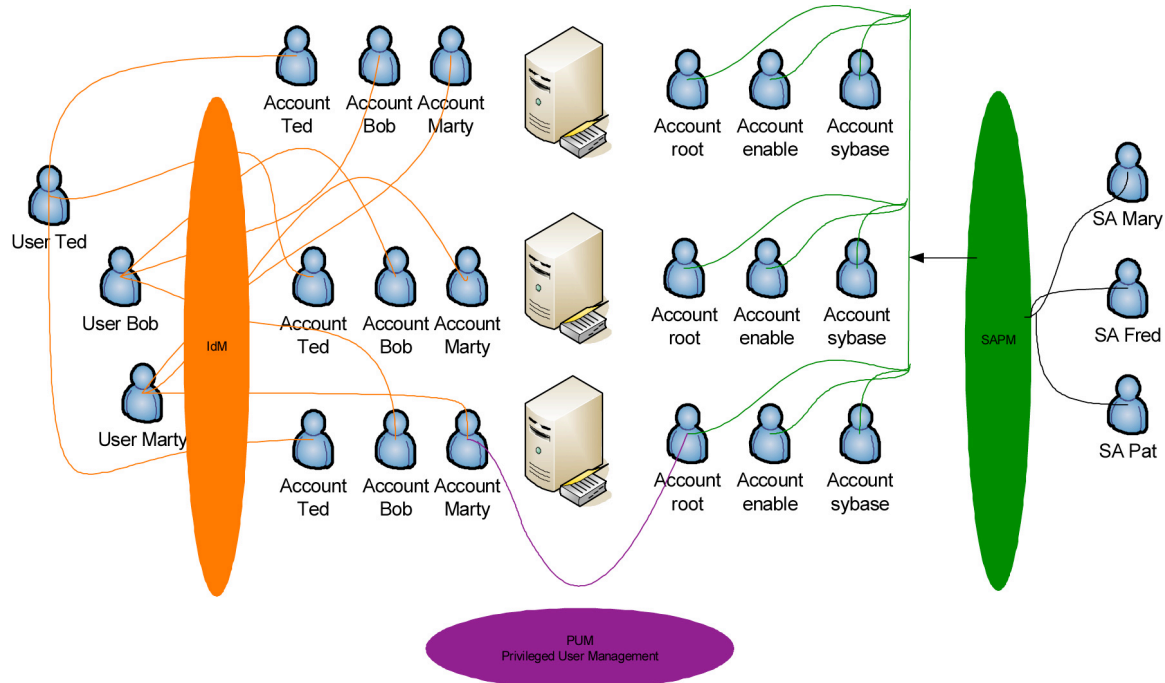


Diagram 2

Increasing security and compliance demands are bringing additional focus and attention to how an enterprise manages and controls privileged account, shared account and service account passwords. The level of privilege associated with these accounts along with their inherent generic nature open them to potential internal abuse and audit. A recent Secret Service/Carnegie Mellon University study found that **86% of internal abuse was from people holding IT level positions and 90% of those held privileged access.**

Secure and compliant management of these accounts requires many features, functions and capabilities not found in standard IdM and/or PUM solutions. As is shown in Table 1 below, while IdM and PUM solutions can together deliver a degree of individual accountability for generic accounts, they are not able to provide many of the core features required to effectively manage the life cycle storage, release and change control requirements of privileged account, shared account and/or service account password management.

e-DMZ Security’s PAR was designed as a standalone purpose built appliance that can easily integrate into your existing workflow and provide the feature rich set of capabilities demanded to meet today’s growing security and compliance requirements for SAPM. Deployed in 4 of the Forbes top 10 ranked companies PAR is delivering SAPM to tens of thousands of systems world-wide.

Account Password Management Comparison			
Feature/Function	SAPM (PAR)	IdM	PUM
User Account Management		√	
User Password Management	√	√	
User Elevated Rights Management			√
Privileged Password Management	√	√	
Shared Account Password Management	√		
Service Account Password Management	√		
Secure Password Storage	√		
Dual (or more) Release Controls	√		
Individual Accountability (generic accounts)	√		√
Supports High Availability	√	√	
Time Based Password Change	√	√	
One time use passwords	√		
Console Access/Password Management	√		
Available CLI/API	√	√	√
Password Change for Services, Tasks, Com+	√		

Table 1

Designed specifically to address the unique set of security and compliance requirements for privileged account, shared account, service account and hard-coded/embedded password management and control, PAR delivers a feature-rich set of capabilities not available in user focused account management and password management solutions.

- One-time-use passwords
- Delivers assured individual accountability for generic accounts
- Secure storage of passwords
- Automated password synchronization
- Supports both networked and non-networked (i.e. direct console) workflow
- Configurable dual (or more) release controls
- Clientless deployment
- CLI/API for enterprise integration and embedded password support
- Extensive platform/OS/application support

