

Application Identity Manager™



Cyber-Ark® offers a comprehensive suite of software and services to securely manage application and script accounts, and to eliminate the use of hard coded credentials.



With AIM hard-coded credentials can be eliminated from scripts, jobs and applications, and replaced by a simple function call. AIM can also be utilized to push updated credentials to 3rd party applications where code changes are not feasible.

THE CHALLENGE

In today's complex IT environments, multiple scripts, processes and applications, need to access multi-platform resources, to retrieve and store sensitive information. Such applications are granted use of dedicated accounts, usually allowing unlimited access to sensitive information stored in corporate databases, and these accounts are usually embedded inside the application code, data sources or .configuration files.

Securing, managing and sharing these service accounts impose significant challenges and a major overhead to IT departments. As a result, up to 42% of enterprises report that they never change hard-coded and embedded passwords for application IDs, testing scripts and batch jobs.

Mismanaged App2App passwords impose great risks to organizations including:

- **Failed Audits.** Hard coded and embedded passwords pose serious auditing challenges to organizations. The PCI Data Security Standard, for instance, specifically instructs enterprises to develop and maintain secure systems and applications, remove any custom usernames and passwords from applications, including the enforcement of strong access control and authentication mechanisms on systems accessing cardholders' data.
- **Lack of Accountability.** Application passwords may be required for use by IT personnel or developers for troubleshooting and emergency cases. Existing solutions provide very limited auditing and control for such scenarios.
- **Security Risks.** App2App passwords are

almost never changed and often stored in clear text and known by a wide variety of IT personnel, developers and regular end-users as well as many ex-employees or external sub-contractors. Any attempt to change hard coded passwords involves code changes and changes in production systems, resulting in continuous downtime to critical business applications.

- **Elevated Damage Threat.** Application accounts are powerful accounts with almost unlimited access to backend systems. Compromising the application account may lead to uncontrolled access to highly-sensitive business information and to severe damages.

THE SOLUTION

Application Identity Manager™ (AIM), part of Cyber-Ark's Privileged Identity Management (PIM) Suite, is the only solution to fully address the challenges of App2App identities by:

Eliminating Hard-Coded Passwords. AIM eliminates the need to store App2App passwords and encryption keys found in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed with Cyber-Ark's patented Vaulting Technology®.

Complying with Audit Regulations. Using AIM, organizations can comply with internal and regulatory requirements for regularly replacing passwords and securely monitoring privileged access across all systems, databases and applications.

Assuring Business Continuity. AIM fully addresses the need to assure the highest availability for applications running the

SPECIFICATIONS

Encryption Algorithms:

- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

Access and Workflow Management:

- LDAP directories
- Identity and Access Management
- Ticketing and workflow systems

Authentication Methods:

- Username and Password
- RSA SecurID
- Web SSO
- RADIUS
- PKI and smartcards
- LDAP
- Windows-based Authentication

High Availability:

- Operating System: Windows, Linux/UNIX, OS390, AS400, OVMS, HP Tandem, MAC OS

Monitoring:

- SIEM integration
- SNMP traps
- Email notifications

Application Platforms:

- Windows
- Linux/UNIX
- AIX
- Solaris
- HP-UX

Application Platforms:

- .net
- Java
- CLI
- COM
- C/C++
- Application Servers: Websphere, WebLogic, JBOSS, Tomcat

enterprise business, independent of network availability and with the highest performance.

Supporting Broad Platforms. To address the needs of large enterprises, AIM supports a variety of systems, applications, Application Servers, scripts, jobs and more.

FEATURES & BENEFITS

AIM utilizes Cyber-Ark's patented Digital Vault Technology™, which is ICSA certified, and designed to meet the highest security requirements for managing privileged and App2App accounts. The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection.

AIM delivers a complete infrastructure to centralize the management of credentials to resources along with a comprehensive set of abilities for managing these service accounts, including:

- **Eliminate Hard-Coded Passwords.** Using the AIM variety of password SDKs, enterprises can remove passwords from all scripts, application code and configuration files, making them invisible to developers and support staff.
- **Automatic Password Synchronization.** To comply with audit regulations, AIM offers the ability to change passwords on demand and according to the enterprise policy without any interruption to production or need for development/testing and IT support. AIM can also be utilized to “push” passwords to different locations within 3rd party applications, where code changes are not feasible.
- **Application Authentication.** AIM utilizes advanced means to authenticate applications requesting credentials ensuring only allowed applications can access them. This includes enforcing limitations like machine IP, OS user, application path and run-time signature.
- **High Availability, Redundancy and Business Continuity.** AIM is designed to meet high-end enterprise requirements for availability and business continuity for the most critical business applications, even within complex and distributed network environments. With its secure caching capabilities, enterprises can rest assure their mission critical applications will always have access to their service accounts, independent of network performance and availability. The caching

agents require zero management while providing the highest levels of resiliency and performance to calling applications.

- **Unique Solution for Application Server Data-Source Credentials.** AIM provides the only solution for securing and automatically managing credentials required by mission critical applications and stored within Application Server Data Sources. The patent pending solution is implemented without code changes and zero downtime or restarts are required during password changes.
- **Web Based UI for Managing Applications.** Flexible views allow enterprises to audit, track and securely manage all their App2App communication.
- **Encryption.** All passwords are encrypted while at rest in the Vault or in a secure local cache and while in transit to the requesting application.
- **Access Control.** Using the Vault's access control security layer, “right to use” the passwords can be managed down to the application level.
- **Accountability.** Each Vault transaction is logged providing auditing and accountability for every password request.
- **Enterprise Readiness.** Easily integrates with the enterprise infrastructure. This includes LDAP and IAM integration for user management and automatic account provisioning; use of Windows domain, RADIUS, PKI, SSO or RSA SecurID for authentication; monitoring and SEIM integration using SNMP, Syslog and SMTP; integration with ticketing and workflow systems; robust SDK, built-in HA/DR and much more!

THE POWER OF PIM

AIM solution is part of the market leading PIM Suite, a full lifecycle solution for centrally managing privileged and shared identities. Policy based definitions allow easily enforced access control and auditing to sensitive network resources, session monitoring, privileged SSO, as well as ensuring compliance with regulatory requirements. The PIM suite provides out of the box support for over 50 types of managed devices, including all common enterprise databases, network devices, operating systems, applications and more, allowing full scale implementation across the IT infrastructure. ■