

Manage Individual and Privileged Accounts with Oracle and Cyber-Ark



Enterprise Password Vault (EPV) secures, manages, automatically changes and logs all activities associated with Privileged Passwords.

As Enterprise Password Vault™ (EPV) is now part of the Oracle® Extended Identity Management Ecosystem, joint Cyber Ark and Oracle customers can benefit from a unified identity management solution for managing and provisioning both personal accounts and shared privileged accounts.

ORACLE

Cyber-Ark®

Cyber-Ark Enterprise Password Vault™ – Part of the Oracle Extended Identity Management Ecosystem

Enterprises must secure, manage and update both individual employee passwords as well as non-personal, administrative and super-user passwords, such as root on a UNIX server, Administrator on a Windows machines, DBA users on databases, and any application account used to connect to a database. However, while 99% of enterprises regularly change passwords for individuals, up to 42% of privileged passwords are never changed. The result? Costly outages, lost business, legal liability and inevitably failed audits. That is why Cyber-Ark chose to partner with Oracle in order to offer a single-source for all enterprise identity management needs.

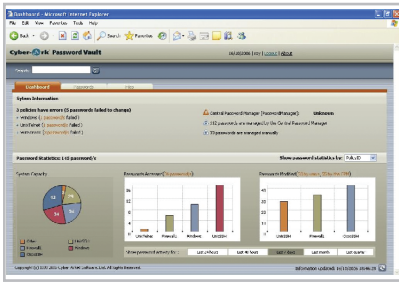
Cyber-Ark's Enterprise Password Vault (EPV) enables organizations to secure, manage, automatically change and log all activities associated with all types of Privileged Passwords by:

- **Protecting Privileged Passwords.** With EPV, you gain a secure Vault in order to store, protect and manage access to Privileged User Passwords at a centralized point. In addition, Cyber-Ark's patented Vaulting Technology™ utilizes a fully integrated model of critical security layers, interwoven to meet the highest security needs.
- **Controlling Privileged Password Access.** The unique access control and audit mechanisms of the Vault control and track any access to privileged accounts.
- **Complying with Audit Regulations.** EPV makes it easy to create audit reports required by Sarbanes-Oxley, PCI and more, to easily track which users have access to privileged accounts, who accessed them, when and for what purposes.
- **Streamlining the Management of Privileged Accounts.** EPV enables the instant and automatic changing of passwords for thousands of servers, network devices, databases and applications, including scripts and parameter files, based on enterprise policies. As changing passwords of such accounts is extremely complicated to be done manually, EPV provides an automated, smooth and robust solution.
- **Integration with Oracle Internet Directory.** Provides EPV with user provisioning and access control management capabilities by synchronizing with OID's LDAP data. This applies to user creation, modification, removal and personal information, as well as permission-groups. Oracle IdM or OID continue to be the enterprise focal point for managing identities and their access rights, while their scope of control is now extended to manage access to privileged and shared accounts.
- **Integration with Oracle Access Manager.** Where IT personnel who need to frequently access all kinds of web applications for monitoring and IT management purposes, by integrating with OAM users are able to authenticate to the EPV web application using the Oracle Single Sign-On capabilities.
- **Integration with Oracle 10g Database.** Cyber-Ark now also offers its patented Vault technology based on an embedded Oracle 10g database.

The Solution: Enterprise Password Vault (EPV)

From streamlining password maintenance to delivering the rock-solid security, EPV offers a robust set of capabilities such as:

- **Leading Solution for Managing Administrative Accounts.** EPV is the choice of hundreds of Global enterprises.
- **Leading Solution for Managing Windows Local Administrators.** EPV was uniquely designed to protect and manage large amounts of Windows administrative accounts found in every enterprise. With its unique auto-detection capabilities, any laptop and desktop joining or leaving the network can be automatically reflected in the Vault environment.
- **Application Password Management.** With EPV, enterprises can overcome one of the greatest security challenges in today's IT environments, omitting all "hard-coded" passwords from applications, scripts and configuration files.
- **Patented Digital Vault Technology.** EPV is a comprehensive system, protecting passwords during transmission as well as at rest. Back-ups are stored in encrypted form instead of clear text.
- **Web Interface to Access Passwords.** EPV offers a flexible and intuitive interface to create personalized views of passwords based on granular access control, providing all the tools to cope with passwords management in an enterprise environment.
- **Built-In Auditing Capabilities.** Audit features include the ability to track time, date, a personalized identity, changes made and logging history. Reports available to auditors in self-service formats including MS Access and Excel.
- **Vast Number of Supported Systems.** EPV supports the widest variety of platforms in the market, including operating systems, databases, firewalls, network devices, routers and key systems such as Active Directory and more. EPV's Central Password Manager is responsible for automating all password updates, and is doing so without installing any software on the managed devices.



EPV delivers one central dashboard console for managing all types of privileged passwords, including the administrative passwords found in routers, servers, databases, workstations as well as those embedded in applications.



About Oracle Identity Management Partner Integration

When Oracle conducts partner integration and testing, the company verifies only that the software integration functions according to the partner's proposed integration plan, and that it makes appropriate use of Oracle components and integration technologies in the environment specified in the published Integration Datasheet. This process applies only to the components providing integration between the partner's software and specified Oracle component; it does not apply to or extend to the partner's software product(s). The integration is performed in a lab environment using standard versions of the Oracle product and the partner's software. The testing is product version specific, hardware specific, database specific, and operating system specific, and is conducted in English, unless explicitly noted otherwise. Similar results may not be able to be duplicated in a production environment, including where the Oracle or partner software is modified or customized upon implementation. Customers are solely responsible for the selection of all third-party software, including any integration software, used in conjunction with Oracle Identity Management and for the result of such use.



Managing Highly-Sensitive Information
©Cyber-Ark Software Ltd. | www.cyber-ark.com | sales@cyber-ark.com