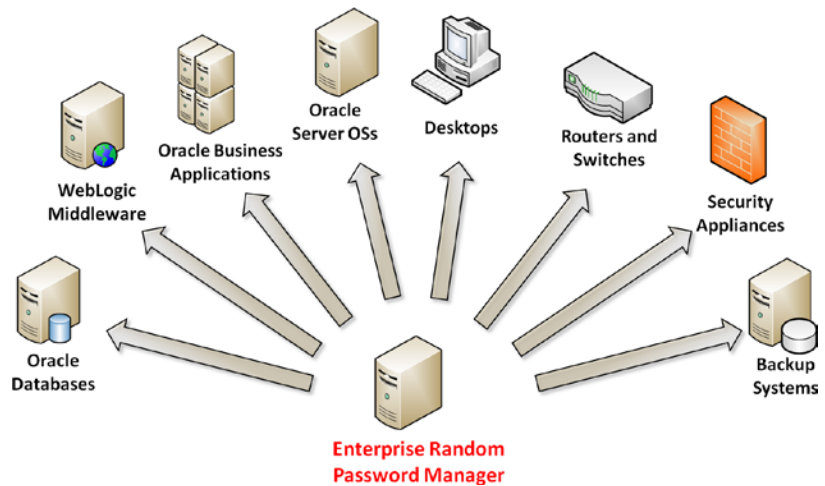


Privileged Identity Management for the Oracle Enterprise

Organizations fail security audits and endure costly data breaches because their privileged identity passwords go unmanaged. Privileged identities are the so-called "super user" accounts that hold elevated permission to access files, run programs, and change configuration settings. They exist on virtually every component in the IT infrastructure. Yet today's identity access management frameworks – including Oracle Access Manager and others – don't manage or control them.

Enterprise Random Password Manager (ERPM) continuously discovers, updates, stores, and enables secure recovery of every privileged account password in the Oracle infrastructure. ERPM detects service account interdependencies and simultaneously deploys changed credentials to avoid disruptions and lockouts. It detects and secures privileged accounts present in:

- ▶ **Oracle Databases** including Oracle 11g, 10g and 9i editions.
- ▶ **Oracle Identity Management** including OIM, Oracle Applications Manager, and Oracle Internet Directory plus other LDAP-compliant directory services.
- ▶ **Oracle WebLogic, Oracle Fusion** and other middleware applications.
- ▶ **Oracle Applications** including Oracle E-Business Suite, PeopleSoft, Siebel, JD Edwards, Hyperion and more.
- ▶ **Oracle-Supported Operating Systems** including Oracle Enterprise Linux and other Oracle-supported Linux platforms, Sun Solaris, HP-UX, HP OpenVMS, IBM AIX, IBM z/OS, Microsoft Windows, Mac OS X Server and more.
- ▶ **Network Devices** including Cisco routers and switches, Juniper, HP Procurve, Riverbed, and others.
- ▶ **Third-Party Software** including multi-platform databases, line-of-business applications and Web services.



Enterprise Random Password Manager Identifies Privileged Accounts and Their Interdependencies in the Oracle Enterprise

Safeguard Your Enterprise in Real Time

ERPM stores privileged account passwords and audit records in an encrypted Oracle database and can be installed on an Oracle Enterprise clustered database for utmost reliability. ERPM integrates out-of-the-box with:

- ▶ Oracle Internet Directory
- ▶ Sun Java System Directory Server
- ▶ RSA SecurID, and
- ▶ Most popular LDAP-compliant authentication providers.

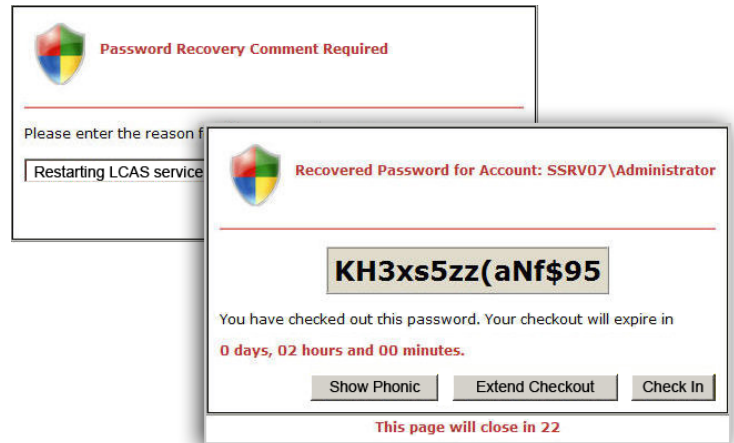


Secure and Scalable

ERPM creates unique, cryptographically complex passwords for each privileged account and changes these credentials as often as your policies require. ERPM installs rapidly, without the need to maintain scripts or deploy agents. It also supports a zone processing architecture that eliminates synchronization errors on networks with DMZ layers and remote, high-latency sites.

Unmatched Oracle Support

ERPM utilizes the Oracle database for secure, encrypted storage of all privileged account passwords. It also discovers and updates Oracle Internet Directory service passwords and accounts present in Oracle databases. ERPM integrates with Oracle Internet Directory and other Role Based Access Control systems.



ERPM Dynamically Discovers Privileged Credentials and Enables Fast, Audited Password Recovery

Managed Computer Platforms

- ▶ Oracle Enterprise Linux, CentOS, FreeBSD, Fedora Core, MAC OSX, Novell SUSE, OpenSUSE, Red Hat, Ubuntu
- ▶ Sun Solaris, HP-UX, IBM AIX, z/OS, SGI Irix
- ▶ IBM AS/400, OS/390
- ▶ Windows Server 2008, 2003, 2000, and NT4 and Windows 7, Vista, XP Professional

Managed Databases

- ▶ Oracle 11g, 10g and 9i, Microsoft SQL Server, MySQL, Sybase ASE, IBM DB2

Managed Applications

- ▶ Microsoft IIS 6 & 7, ASP.NET, SharePoint
- ▶ PeopleSoft, Siebel, BMC Remedy, HP OpenView, IBM Tivoli, SAP, and most Line of Business (LOB) applications.

Managed Network Devices

- ▶ Cisco IOS, Juniper, Riverbed, HP ProCurve, NetApp and others

Back-End Database Platforms

- ▶ Oracle 11g, MS SQL Server

Supported Application Hosts

- ▶ Windows Server 2008, 2003

Supported Authentication

- ▶ Oracle Internet Directory, Sun Java System Directory Server, Active Directory, RSA SecureID, Novell eDirectory, Apache Directory Server, and most other LDAP-compliant directories

