

# Oracle Privileged Account Manager 11g R2 PS3



Oracle Privileged Account Manager (OPAM) is a secure password management solution designed to generate, provision, and manage access to passwords for privileged accounts like Linux/Unix “root” or Oracle database “sys” accounts. It enables auditing and establishes accountability for users including those who share privileged account credentials. Additionally OPAM provides Session Management and Recording. OPAM is an integral service of the Oracle Identity Governance Suite and provides central governance for both, regular and privileged users. It further enables complete auditing, reporting and certification of a user’s regular or shared accounts, and account lifecycle management from request, approval, to certification and usage tracking. OPAM greatly enhances security and significantly improves compliance.

## KEY FEATURES

- Secure password vault for privileged accounts
- User Session Management and Recording
- Extensible Java based framework to build custom solutions
- Easy to use user interface for OPAM administrators and users
- Auditing and reporting of privileged account activities
- RESTful and command line interface provides standardized access to OPAM functionality and allows custom integrations
- Rich set of target connectors for Databases, UNIX/Linux and Directories, Network Devices and Hypervisors
- Integrated service of the Oracle Identity Governance Suite
- Complements existing Oracle solutions: DB Vault, DB Enterprise User Security and Authentication Services for Operating Systems

## Oracle Privileged Account Manager

OPAM manages privileged account passwords (either human accessible or application service accounts) for a broad range of target systems. Privileged account credentials are centrally managed and the OPAM administrators define policies governing who (user, role or group) can access specific privileged account credentials.

When a user needs to access a target system using the privileged account, the user must authenticate to OPAM and be authorized to retrieve (checkout) the credential. Access to a (shared or exclusive) privileged account credential is audited, and granted for specific time periods.

For SSH based target systems for instance UNIX, Network Devices or Hypervisors OPAM’s user session management enables individual accountability through searchable session transcripts (using keystroke logging) and enforces command restrictions through “white lists” which contain commands a user can execute. On Windows based systems user activities can be recorded into MPEG4 videos.

Users and OPAM administrators interact with OPAM through the same web-based console. The web console supports role-based access to determine if it is a user retrieving a password or session, or an OPAM administrator who needs to manage OPAM’s services. Users check-out/check-in privileged accounts passwords or sessions, and OPAM administrators manage targets, accounts, grantees, usage and password policies. OPAM console access can be secured by Oracle Access Manager and Oracle Adaptive Access Manager for strong two factor authentication and single sign-on (SSO).

All OPAM user interactions or application/service access through OPAM’s RESTful API

**KEY BENEFITS**

- Monitoring and recording of user sessions enables individual accountability through session transcripts or session videos recordings
- Enforce internal security policies and eliminate potential security threats from privileged users
- Cost-effectively enforce and attest to regulatory requirements
- Reduce IT costs through efficient self service and common security infrastructure
- Centralized auditing and customizable audit reports through BI Publisher
- Enables custom built solutions, for example Ticketing System integration, through Java plug-ins

are audited and stored in a central audit database potential forensic analysis. At any given time the OPAM administrator can see which accounts are checked out.

OPAM leverages Oracle's standard Integrated Connector Framework (ICF) to provide connectors that link OPAM with target systems such as user directories, database servers, operating systems, Network Devices and Hypervisors. The OPAM server exposes a RESTful API used by OPAM client applications including the OPAM console and the OPAM command-line. Customers can build custom integrations using OPAM's public RESTful API or the flexible Java based plug-in framework. Privileged accounts can be auto discovered and identified through connectors. Passwords managed by OPAM are persisted in an Oracle DB credential store. When passwords are stored in an Oracle database, customers can leverage Oracle Database Vault and Transparent Data Encryption (TDE) for additional security.

## Oracle Identity Governance Suite

OPAM can be used as a standalone component, although, a key benefit is its integration with the Oracle Identity Governance Suite. Oracle Identity Governance provides a complete governance solution which supports lifecycle management of both regular and privileged accounts, as well as the support of exclusive and shared accounts to meet enterprise compliance requirements. Integration includes, user provisioning into the OPAM identity store using policy and role-based provisioning, and delegating access to privileged accounts through self-service delegation functionality. Administrators can request privileged account access via the Access Request catalog, or make "break-the-glass" (emergency) requests, to access accounts they are not normally entitled to. Privileged access can also be certified by Oracle Identity Governance and revoked if access is no longer required.

## OPAM Complements Oracle Solutions

Oracle Database Vault enables fine-grained authorization and separation of duties to prevent DBAs from unauthorized access to application data stored in the database. Database Enterprise User Security enables centralized management of database users (except privileged DB accounts like "sys") and enterprise roles in a directory. Oracle Authentication Services for Operating Systems (OAS4OS) enables enterprises to centralize the management of Unix and Linux account. OPAM complements these solutions through management of privileged database, directory and operating system accounts and users to ensure individual user accountability, auditing, enhanced security and compliance.

## Summary

Oracle Privileged Account Manager (OPAM) provides a versatile and integrated solution that allows organizations to manage their privileged account passwords and audit privileged activities. OPAM's user Session Management Recording enables individual accountability through session transcripts and video recordings. OPAM can operate as a standalone solution, but delivers more value when used as an integral part of the Oracle Identity Governance Suite. The Oracle Identity Governance Suite provides a complete governance solution supporting lifecycle management of both regular and privileged accounts and users' individual and shared accounts to meet enterprise compliance requirements.

**CONTACT US**

For more information about Oracle Privileged Account Manager, visit [oracle.com](http://oracle.com) or call +1.800.ORACLE1 to speak to an Oracle representative.

**CONNECT WITH US**

-  [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

**Hardware and Software, Engineered to Work Together**

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0515

