

ORACLE DATABASE VAULT

Oracle JD Edwards EnterpriseOne Certification

KEY BENEFITS



- Restrict privileged Oracle Database users from accessing Oracle JD Edwards EnterpriseOne data
- Protect sensitive data such as salary information, credit card numbers, and social security numbers using Oracle Database Vault Realms
- Enable Separation of duty within the Oracle JD Edwards EnterpriseOne database environment
- Available for all Oracle JD Edwards EnterpriseOne application modules starting from version 8.12 and higher

Regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA) require strong internal controls to protect sensitive information such as financial, healthcare, and credit cards records. Outsourcing, application consolidation, and increasing concerns over insider threats have resulted in an almost mandatory requirement for strong controls on access to sensitive application data. Oracle Database Vault enforces real-time preventive controls and separation-of-duty in the Oracle Database to secure the Oracle JD Edwards EnterpriseOne applications.

Oracle Database Vault Protection for Oracle JD Edwards

Oracle Database Vault enables Oracle JD Edwards EnterpriseOne customers to restrict access to application data by privileged database users, enforce separation-of-duty, and provide tighter access control with multi-factor authorization. Oracle Database Vault enforces security controls even when the application is bypassed. Oracle Database Vault certification with JD Edwards EnterpriseOne applications benefits customers by:

- Restricting privileged users' access to sensitive data
- Enforcing separation of duty in the Oracle Database environment
- Providing application specific Database Vault protection realms and command rules

Restricting Privileged Users' Access

Database administrators hold highly trusted positions within the enterprise. With Database Vault Realms, enterprises increase security by preventing unauthorized access to application data even if the request is coming from privileged users. This is especially important when a privileged account is compromised or accessed outside normal business hours or from an untrusted IP address. The ad-hoc tools used by administrators to help manage and tune the Oracle database continue to work as before, but they can no longer access application data.

Enforcing Separation-of-Duty

Oracle Database Vault helps administrators manage operations more securely by providing fine-grain controls on database operations such as creating accounts, granting powerful roles, and changing table structures. Oracle Database Vault default separation-of-duty can be divided into three categories.

RELATED PRODUCTS:

The following products provide additional security to help meet privacy and regulatory requirements:

- Oracle Advanced Security
 - Transparent Data Encryption for Oracle databases at the tablespace or column level
 - 3DES, AES 128, 192, 256
 - Network Encryption, SSL
 - Strong authentication using Kerberos and PKI
- Oracle Label Security
 - Transparent row level access controls using data labels
 - Multi-level security for government and defense organizations
 - Flexible, policy based architecture for commercial organizations
- Oracle Audit Vault
 - Secure and consolidate audit data from Oracle Database 9i, Oracle Database 10g, Oracle Database 11g, Microsoft SQL Server 2000 and 2005, Sybase ASE 12.5-15.0, and IBM DB2 8.2-9.5 databases
 - Built-in reports for compliance and privileged user activity
 - Alert on suspicious activity
 - Central management of audit policies for Oracle databases
- Oracle Data Masking
 - De-identify privacy related application data for non-production environments
 - Automate the masking process with policies and format templates
 - Maintain referential and relational integrity to ensure applications work
 - Sensitive data never leaves the database

Oracle Database Vault Activity	Separation-of-Duty Description
Database account management	Database Vault prevents ad-hoc creation of database accounts unless the administrator is explicitly assigned the Database Vault Account Management administrator role.
Database administration	Traditional database administration tasks such as those associated with managing tablespaces and tuning parameters remain unchanged. Oracle Database Vault blocks ad-hoc grants of the DBA role as well as access to powerful packages such as the DBMS_RLS package.
Database Vault security administration	Only Database Vault administrators can change Database Vault JD Edwards EnterpriseOne security settings related to Realms and Command Rules

Figure 1: Oracle JD Edwards EnterpriseOne with Oracle Database Vault

Protection Realms and Command Rules For JD Edwards EnterpriseOne

This certification provides customers with pre-configured protection realms and command rules designed specifically for JD Edwards EnterpriseOne applications. These protections restrict privileged user access to sensitive application data, prevent application by-pass, and protect the integrity of the application from any user: privileged or non-privileged. The scripts for these protections can be downloaded from the [Oracle Technology Network web site](#)

Extending the Oracle-Supplied Security Settings

Customers can extend the Oracle-supplied security settings by adding additional command rules and realms to accommodate their specific security requirements. For example, the out-of-the-box CONNECT command rule can be customized to restrict database connections to a specific range of IP addresses.

Supported JD Edwards Releases

All Oracle JD Edwards EnterpriseOne application modules and releases version 8.12 and higher are supported with Oracle Database Vault. Oracle Database release 10.2.0.4 and higher, and Oracle Database 11g 11.1.0.7 and higher are supported with this certification.



Copyright © 2009, 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 0109