

ORACLE DATABASE VAULT

CERTIFICATION WITH ORACLE E-BUSINESS SUITE

KEY BENEFITS



- Restrict privileged database user access to E-Business Suite application data
- Enforce real-time preventive controls on access to E-Business Suite application data
- Enable Separation of duty within the E-Business Suite database environment
- Extend seeded security policy with command rules and multi-factor authorization
- Available for E-Business Suite 11.5.10 and 12.0.4 running with Oracle Database Vault 10.2.0.3

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 enforces separation-of-duty in the Oracle Database supporting the Oracle E-Business Suite application.

Oracle Database Vault Protection for E-Business Suite

Oracle Database Vault enables Oracle E-Business Suite customers to restrict access to application data by highly privileged 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 Oracle E-Business Suite benefits customers by:

- Providing E-Business Suite-specific Database Vault realms
- Restricting named database accounts access to sensitive application data
- Enforcing separation-of-duty in the database

Restricting Privileged Users

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 un-trusted 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, changing table structures and using security related packages related to Virtual Private Database and Label Security. 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 9i and later databases, SQL Server 2000 and 2005 databases
 - Built-in reports for compliance and privileged user activity
 - Raise alerts on suspicious activity
 - Centrally manage audit policies for Oracle databases

- Oracle Data Masking
 - De-identify privacy related application data for development and test environments
 - Create masking policies for easy management

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.
E-Business Suite Database Vault security administration	Only Database Vault administrators can change Database Vault E-Business suite security settings related to Realm and Command Rules

Table 1 Oracle Database Vault E-Business Suite Separation-of-Duty

Extending the Oracle Supplied Database Vault Settings

Customers can extend the Oracle-supplied security settings for Oracle E-Business Suite to accommodate their specific security requirements. Customized realms and command rules can be combined with numerous built-in Database Vault factors to strengthen security even further. For example, customers can setup a CONNECT command rule to restrict connections to the database to a specific range of IP addresses, creating a trusted-path to the Oracle Database and helping prevent the application bypass security problem. Please refer to Oracle Metalink for additional information on how to extend the Oracle-supplied security settings.

E-Business Supported Releases

E-Business Suite release 11.5.10 and 12.0.4 are certified with Oracle Database Vault release 10.2.0.3. All Oracle Database Vault 10.2.0.3 released platforms are supported with this certification. Oracle Metalink provides best practices on common E-Business Suite specific maintenance tasks in the Oracle Database Vault environment. For more information on using Oracle Database Vault with Oracle E-Business suite releases 11.5.10 and 12.0.4, please refer to Oracle Metalink notes 428503.1 and 566841.1 respectively.

Copyright 2008, Oracle. 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 is it 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.