

ORACLE CRM ON DEMAND DATABASE VAULT



Oracle understands how critical data security is to our customers, and we implement sophisticated technical, administrative and physical controls designed to safeguard the customer data stored in the Oracle CRM On Demand environments. As a supplement to Oracle's standard security practices, Oracle CRM On Demand Database Vault is a premium security service for Oracle CRM On Demand customers. Available to Single-Tenant customers, the Oracle CRM On Demand Database Vault service offering further restricts Oracle CRM On Demand support personnel access to the CRM On Demand customer's data repository.

THE WORLD'S MOST COMPREHENSIVE CRM ON DEMAND SOLUTION

- Easy to use for high user adoption
- Deploys quickly with little IT investment
- Embedded sales, marketing and service best practices
- Powerful and easy to use real-time and historical analytics
- Works online or offline

Oracle CRM On Demand's Standard Security Practices

Oracle CRM On Demand leverages advanced security in the areas of application security, organizational security, infrastructure and operational security. Security controls available to you include full user management, password policies (expiration, minimum strength, and security questions), failed login audit, and the ability to restrict users to approved IP addresses. All communications to and from CRM On Demand require a minimum of 128-bit SSL encryption. Customers can manage visibility to sensitive data via role-based access controls. General application security controls include single sign-on, web application security best practices; as well as third-party application security audits.

Regulatory requirements, business risk, technology shifts and increased concerns over data security have driven requirements for stronger access controls on customer data. Oracle's worldwide data centers have adopted strong physical, network and infrastructure security controls. These include hardened servers - monitored by Oracle Enterprise Manager. Real-time alerts are sent to the Oracle Command Center for processing. Oracle employs Host Intrusion Detection Systems, vulnerability assessment and management, centralized access management solutions, centrally managed Public Key Infrastructure (PKI) services, logging and auditing. Oracle's security controls are described further in the *Oracle SaaS Security Practices* document and service-specific *Supplements for the Oracle SaaS Security Practices* documents.

KEY FEATURES

- Prevent privileged database users from accessing Oracle CRM On Demand customer's data transparently
- Provide stronger access control to CRM On Demand data repository
- Further enforces separation of duty within the Oracle CRM On Demand database environment for security and compliance

Oracle Database Vault Protection for Oracle CRM On Demand

Building on the Oracle SaaS Security Practices, Oracle Database Vault enables Oracle CRM on Demand Cloud Services to deploy transparent, real-time preventive controls that go even further to restrict access to customer data stored in the database.

Deployed only on Oracle On Demand Single-Tenant environments, including production, stage, and Private Customer Test environments, Oracle Database Vault benefits you by:

- Restricting CRM ON Demand DBAs from accessing customer data stored in the CRMOD databases.
- Requiring additional approvals to access the database to conduct maintenance and troubleshooting activities.
- Recording each access request and approval.
- Limits the duration of approved access to the time required to complete the specific activity.

Provide Real Time Rules and Factors

Oracle Database Vault provides command rules and factors that tighten security by limiting who, when, where, and how the data is accessed. Oracle Database Vault will evaluate the rules and determine whether the command should be blocked from a specific user. Hence, even the privileged user is limited in their ability to access your CRM On Demand data.

Prevent Access By Privileged Users

This offering leverages the realms that are provided by Oracle Database Vault. The realms are placed around CRM On Demand application data or a set of tables designed to block access to your data from privileged users. Oracle CRM On Demand Cloud Services database administrators are able to manage, troubleshoot and tune the Oracle database, however they cannot access CRM On Demand application customer data.

Enforce Separation of Duty

Oracle Database Vault provides out-of-the-box controls on database operations, such as creating accounts, granting powerful roles and changing tables' structures. Oracle CRM On Demand Cloud Services leverages the following three distinct separation of duty controls to manage operations as part of the Database Vault Services:

RELATED PRODUCTS

- Oracle CRM On Demand

Oracle Database Role	Separation of Duty Description
Database account management	Manage Oracle database accounts. Oracle Database Vault blocks account creation by existing privileged users.
Database administrator	Traditional database administration tasks such as managing tablespaces. Oracle Database Vault blocks ad-hoc grants of the DBA role.
Oracle Database Vault security administrator	Manage Oracle Database Vault security settings for Oracle CRM On Demand related to Realms and Command Rules.

Figure 1. Oracle Database Vault Separation of Duty with Oracle CRM On Demand

Oracle CRM On Demand Cloud Services has deployed the Oracle Short Term Access Request (STAR) system on Oracle databases on which Oracle Database Vault is deployed. This system provides controls on accessing your CRM On Demand database. Oracle employees must request access to the database using the STAR system to conduct support activities. Access is granted for a limited time and all actions are logged. Oracle Database Vault will create an audit record of potential violations. The logs and violations are retained for the last 24 months and are reviewed through periodic audits.

CONTACT US

For more information on Oracle CRM On Demand and Oracle Database Vault, please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2021, 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.

Oracle is committed to developing practices and products that help protect the environment