

ORACLE DATABASE SECURITY FOR PRIMAVERA P6 EPPM 8

ENCRYPTION AND PRIVILEGED USER CONTROLS FOR PRIMAVERA P6

KEY FEATURES:

- Encrypt Oracle Primavera data, preventing data access at the operating system layer
- Project data on backup media
- Help protect against threats targeting privileged database accounts

KEY BENEFITS

- High performance, transparent encryption for Oracle Primavera data
- Increased protection for Oracle Primavera data, including project planning, intellectual property, financial, and customer related data

Databases have increasingly become the target of sophisticated threats targeting sensitive information, including project planning, intellectual property, financial, and privacy related data. Oracle Database Security solutions provide a multi-layered, defense-in-depth approach that helps protect Oracle Primavera data from threats both external and internal. Oracle Advanced Security provides a transparent and scalable encryption solution for Oracle Primavera P6 application data. Oracle Database Vault enforces real-time preventive controls inside the database, helping protect against threats from both outside and inside.

Oracle Advanced Security for Primavera P6 EPPM 8

Oracle Advanced Security Transparent Data Encryption (TDE) seamlessly encrypts Oracle Primavera data stored inside the Oracle database, protecting against database bypass attacks that attempt to read data directly from files on the operating system. Data remains encrypted on backup media without any additional configuration steps.

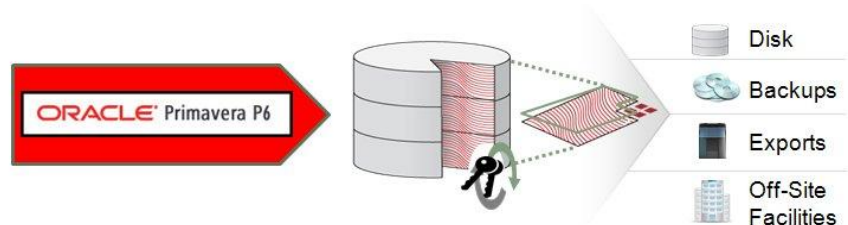


Figure 1. Oracle Advanced Security Transparent Data Encryption

Once encrypted, data remains secure in the event of unauthorized access to files at the operating system level, discarded disk drives and off-site backup media.

Oracle Advanced Security TDE works seamlessly with Oracle Advanced Compression, automatically applying compression and encryption in the correct sequence, enabling Oracle Primavera P6 EPPM 8 customers running on Oracle Database 11g with Oracle compression to increase security and save on storage costs. Oracle Advanced Security is integrated with Oracle DataPump and Oracle RMAN to provide seamless encryption of database exports and backups to disk, providing protection for data exported from the database or transported off-site on backup media.

Oracle Advanced Security TDE tablespace encryption for Oracle Primavera P6 EPPM 8.x encrypts the application data, preventing unauthorized access outside the database with low single digit performance overhead. Oracle Advanced Security TDE tablespace encryption with Oracle Database 11g Release 2 automatically leverages the hardware acceleration available on platforms with Intel® CPUs with AES-NI or Oracle SPARC T4.

Oracle Database Vault Protection for Oracle Primavera P6

Oracle Database Vault enables Oracle Primavera P6 customers to prevent access to application data by privileged database users. Oracle Database Vault certification with Oracle Primavera P6 applications provides preventive controls on privileged user access to application data using Oracle Database Vault realms. This is especially important when a privileged account is targeted from outside or inside the organization. Day to day database administration tasks remain unchanged.

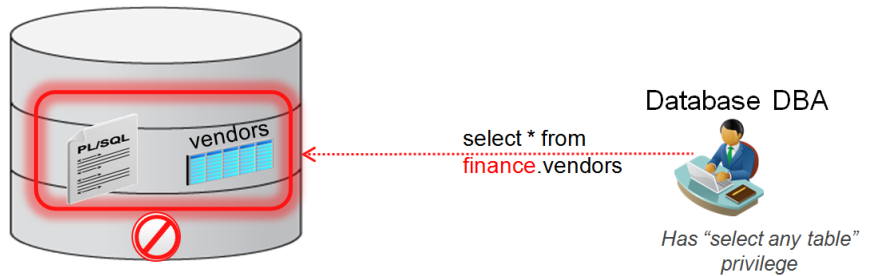


Figure 2. Oracle Database Vault

The Oracle Database Vault security policies and installation guide can be downloaded from the Oracle Database Vault home page on the Oracle Technology Network. Customers can extend the Oracle-supplied Oracle Database Vault security policies to enforce more granular access controls based on factors such as IP address and date/time. A complete list of factors can be found in the Oracle Database Vault administration guide.

Contact Us

For more information about Oracle Advanced Security or Oracle Database Vault, please visit oracle.com/security or call +1.800.ORACLE1 to speak to an Oracle representative.



Copyright © 2012, 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 licensed through X/Open Company, Ltd. 0112

Hardware and Software, Engineered to Work Together