

## ORACLE KEY MANAGER 3

SIMPLE, SECURE, SCALABLE  
ENCRYPTION KEY MANAGEMENT

### KEY BENEFITS

- Get up and running quickly—a day or two for most companies—and manage keys easily with user-defined policies.
- Protect encryption keys for full data lifecycle throughout distributed and heterogeneous storage environments.
- Grow without worry since you can manage thousands of storage devices and millions of encryption keys.

*Compliance with legal, financial, and regulatory requirements is dependent on data security. If you lose sensitive data and it's not encrypted, your business is exposed to sanctions, penalties, and loss of brand equity. Designed to meet stringent enterprise requirements, Oracle Key Manager 3 makes it easy to implement and scale storage-based encryption—for operational and archive data—without unnecessary cost and complexity.*



### Complex Environments—Simple Solution

Distributed and heterogeneous storage infrastructures are a given, so Oracle Key Manager 3 provides a comprehensive, application- and operating system-agnostic platform for tape key management from a single pane of glass. Oracle Key Manager 3 is composed of the following elements:

- Key management appliance (KMA). Two or more KMAs are connected to form a cluster for high availability of keys and optimized performance. The KMAs create, provision, and manage encryption keys based on policies and actions.
- Oracle Key Manager GUI and CLI. A graphical user interface (GUI) or two command line interfaces (CLIs) communicate with the Oracle Key Manager cluster from a workstation over an IP network to manage the system.
- The optional Sun Crypto Accelerator 6000 PCIe Card provides FIPS 140-2 Level 3 compliance to Oracle Key Manager 3.

Simple, Secure, Scalable The Oracle Key Manager 3 is designed with an emphasis on simplicity, security, and scalability so you can realize the following benefits:

- **Security.** Oracle Key Manager 3 is a hardened solution that provides FIPS 140-2 Level 3 compliance (with Sun Crypto Accelerator 6000 PCIe Card) and secure key protection throughout key lifecycle, with a dedicated key management and delivery network.
- **Interoperability.** Open standards-based architecture supports diverse storage devices—mainframe to open systems—under a single storage key management system.
- **Availability.** Ensures high availability with active n-node clustering, dynamic load balancing, and automated failover.
- **Manageability.** User-defined, policy-based automatic key management with a secure client GUI makes it easy to administer the solution in one site or worldwide.

- **Scalability.** On a single clustered Oracle Key Manager appliance pair, you can manage thousands of storage devices and millions of encryption keys. Scale your solution easily and nondisruptively.

### Supported Encryption Endpoints

- Java applications
- Oracle Database 12c and 11g
- Oracle Solaris 11 (ZFS)
- Tape drives and libraries

Oracle Key Manager 3 Supported Tape Drives and Libraries					
Drive Types	Oracle's StorageTek SL24 Tape Autoloader and SL48 Tape Library	Oracle's StorageTek SL500/SL150 Modular Tape Library	Oracle's StorageTek SL3000 Modular Library System	Oracle's StorageTek SL8500 Modular Library System	StorageTek Powderhorn 9310
HP LTO 4	Yes	Yes/No	Yes	Yes	No
HP LTO 5	Yes	Yes	Yes	Yes	No
IBM LTO 4	No	Yes/No	Yes	Yes	No
IBM LTO 5	No	Yes/No	Yes	Yes	No
HP LTO 6	No	Yes	Yes	Yes	No
IBM LTO 6	No	No	Yes	Yes	No
StorageTek T10000A	No	No	Yes	Yes	Yes
StorageTek T10000B	No	No	Yes	Yes	No
StorageTek T10000C	No	No	Yes	Yes	No
StorageTek T10000D	No	No	Yes	Yes	No
StorageTek T9840D	No	No	Yes	Yes	Yes

### Robust Key Management Capabilities

- **FIPS-certified cryptography.** Uses FIPS 140-2 certified cryptography to provide AES-256 bit encryption keys for stored data.
- **Role-based access control.** Supports NIST SP800-60 operational roles to segregate operational functions.
- **Active clustering and failover.** Provides high availability through active n-node clustering of KMAs with fully automated failover.
- **Near-synchronous replication.** Provides near-synchronous, secure replication of transaction data among KMAs within the cluster.
- **Granular role segregation.** Provides operational segregation through six role definitions—Security Officer, Compliance Officer, Operator, Backup Operator, Auditor, and Quorum Member. Each role is access controlled and functionally

restricted, although users can have multiple roles.

- **Quorum.** Quorum is required to activate and to perform other sensitive operations, such as restoring Oracle Key Manager data backups. Quorum parameters are fully configurable.
- **Centralized policy management.** Data encryption policies are managed centrally through the Compliance Officer role. Policies are automatically replicated for disaster recovery purposes.
- **Audit logging.** Maintains audit logs for all operational and key material events and transactions.
- **Open standards.** Developed on open standards including X.509v3 certificates, Simple Object Access Protocol (SOAP), and Transport Layer Security (TLS).
- **Secure management client.** Provides a rich cross-platform compatible client for local and remote management via secure client GUI.
- **Multivendor device support.** Capable of providing encryption key management support to Oracle's most popular tape drives including the StorageTek T10000 A/B/C, StorageTek T9840D, and LTO 4/5/6 tape drives.
- **Enhanced serviceability.** Offers automated support service process by using fault event telemetry from the Oracle Key Manager appliance to initiate a service request.

## Contact Us

For more information about Oracle Key Manager 3, visit [oracle.com](http://oracle.com) or call +1.800.ORACLE1 to speak to an Oracle representative.



Copyright © 2013, 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.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. 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. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1213

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