Oracle Key Vault: Frequently Asked Questions

Enterprise, multi-cloud key and secrets management

February, 2026 – Version: 21.14

Public

Table of contents

Overview & Introduction

What is Oracle Key Vault?

Oracle Key Vault (OKV) is a secure, centralized system for storing and managing encryption keys, certificates, passwords, Oracle wallets, SSH keys, and other secrets. OKV helps organizations safely store, retrieve, and share sensitive cryptographic materials across servers and multiple cloud platforms.

Why do organizations need centralized key management?

Modern IT systems rely on many encryption keys and secrets to protect data and enable secure operations. Spreading these across servers creates risk and complicates compliance. OKV enables strong protection and compliance by providing central governance, simple retrieval, and secure sharing for all keys and secrets.

Key Features & Benefits

What types of keys and secrets can OKV manage?

- **Database encryption keys:** For Oracle TDE, MySQL, ACFS volume encryption keys, GoldenGate encrypted trail files, `dbms_crypto`, and other supported platforms.
- **SSH key pairs:** Secure remote server access control and private key governance.
- **API & application keys:** Including JSON service account private keys.
- **Passwords & credentials:** For automation, storage, and user access.
- **Digital certificates & keystores:** Such as Java KeyStores and Oracle Wallets
- **Secret files:** Including Kerberos keytabs.

How does OKV improve security and operations?

- **Central control:** One secure, unified repository for all keys and secrets
- **Secure sharing:** Easily manage which servers and users get access.
- **Regulatory compliance:** Simplifies demonstrating key separation and backup practices
- **Audit & reporting:** Tracks all key and secret usage.
- **Key lifecycle management:** Rotate, suspend, or retire keys as needed.
- **Automated key & certificate monitoring:**
  OKV can monitor and alert about TDE keys that haven't been rotated in time, helping to enforce internal security policies. It also monitors and sends alerts about certificates that are nearing expiry, have become too short, or use outdated algorithms—ensuring compliance with up-to-date security standards for certificate length and algorithms. (Reference: NIST SP 800-57, Key Management , NIST SP 800-131A, Algorithm and Key Length Guidance)

Can OKV help manage SSH keys?

Yes! SSH keys are widely used for public key authentication to remote servers—a need that exploded with the rise of cloud computing. With OKV, **public keys are centrally stored and**

managed, giving organizations strong, centralized, remote server access control. OKV can also generate and store **private SSH keys as non-extractable assets**, removing them from the custody of server administrators. This provides enhanced **governance, compliance, and auditability**: private keys never leave OKV, enabling detailed control, monitoring, and reporting of remote access, and enforcing organizational security policies.

Deployment & Scalability

Where can I deploy Oracle Key Vault?

- **On-premises:** Dedicated servers, virtual machines, **Oracle Database Appliance (ODA)**, and **Compute Cloud@Customer (C3)**
- **Cloud:** Oracle Cloud Infrastructure (OCI), Microsoft Azure, Amazon AWS, Google Cloud
- **Hybrid/multi-cloud:** Manage keys and secrets for workloads across cloud and on-premises datacenters.

How well does OKV scale and stay available?

- OKV achieves **continuous availability** with clustering of up to **16 nodes (8 read/write pairs)**. If a node is unavailable, others in the cluster take over, ensuring uninterrupted access to keys and secrets.
- Supports **thousands of servers/endpoints** and **hundreds of thousands of keys**.

What are the hardware requirements?

- x86-64 server, minimum: 16 CPU cores, 16 GB RAM, and 2 TB disk; higher specs are recommended for larger deployments.

Security & Compliance

How does OKV protect keys and secrets?

- **Encryption at rest:** All data is encrypted.
- **Access control:** Strict, role-based policies limit access.
- **Audit trails:** Logs all access and changes for review and compliance.
- **Secure communication:** All network traffic is protected with strong mutual TLS encryption.

What makes OKV a uniquely strong fit for regulated environments?

OKV is the **only key manager** that enables truly secure migration from legacy TDE wallets: You can upload both current and retired TDE master keys to OKV, then **delete the old TDE wallet** from the database server after migration.

Does OKV meet other major compliance standards?

- Supports **FIPS 140-2 mode** for U.S. government and regulated industry use cases.

- Integrates with Hardware Security Modules (HSM) for higher assurance and root-of-trust.

Administration & Integration

How is OKV managed?

- **Web-based Management Console:** Modern, intuitive dashboard for administration
- **Command-Line & REST APIs:** Support automation, cloud, and large-scale deployments
- **Role-based access:** Admin, operator, and auditor roles align with enterprise best practices.
- **Directory integration:** Works with Active Directory and Single Sign-On (SAML) for centralized user management

How does endpoint integration and onboarding work?

- **Automated onboarding** into OKV has been added to the OCI control plane for Exadata Database Service on Cloud@Customer (ExaDB-C@C), Autonomous Database on Cloud@Customer (ADB-C@C), as well as Exadata Database Service on Dedicated Infrastructure (ExaDB-D) and Autonomous Database on Dedicated Exadata Infrastructure (ADB-D), deployed in OCI and all other third-party clouds.
- This functionality requires a simple, one-time registration of the OKV cluster with OCI, after which new databases are automatically enrolled in OKV with no manual effort.
- Lightweight, secure software agents are easily installed with no downtime for onboarding.
- Integration is smooth for Oracle Databases, applications, cloud, and hybrid environments.

Backup & resilience:

- OKV supports automated and manual backups.
- Clustering ensures that keys and services remain available even if a node fails.

Getting Started & More Resources

See Oracle Key Vault in action:

- Migrate encrypted databases to OKV
- SSH access control and private key governance

Product details & documentation:

- Oracle Key Vault official site
- Official documentation

Contact Oracle:

- North America: 1.800.ORACLE1
- Worldwide: oracle.com/contact

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

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