ORACLE

Oracle Key Vault: Frequently Asked Questions

Enterprise, multi-cloud key and secrets management

October, 2025 – Version: 21.12

ORACLE

Table of contents

ORACLE

ORACLE

Overview

Oracle Key Vault securely stores encryption keys, Oracle Wallets, Java KeyStores, SSH key pairs, and other secrets in a scalable, fault-tolerant, and continuously available cluster. Users can deploy Key Vault servers in Oracle Cloud Infrastructure (OCI), Microsoft Azure, Amazon AWS, Google Cloud, and on-premises on dedicated hardware or virtual machines. Key Vault supports the OASIS KMIP standard.

This document answers frequently asked questions about Oracle Key Vault features, use cases, and deployment.

Features

What kind of keys and secrets can I manage using Oracle Key Vault?

Oracle Key Vault lets you centrally manage the following:

- Oracle Advanced Security Transparent Data Encryption (TDE) master encryption keys
- SSH key pairs for remote server access control and centrally managed public key authentication
- Passwords, for example:
    - for unattended maintenance scripts, or
    - database account passwords used by Oracle GoldenGate
- GoldenGate trail file encryption master keys
- ZFS Storage Appliance master encryption keys
- MySQL TDE master encryption keys
- ACFS (ASM Cluster File System) volume encryption keys
- Oracle Wallets
- User Certificates
- Asymmetric Key pairs (RSA 2048 to 4096 key length)
- Symmetric keys (3DES112, 3DES168, AES128, AES192, AES256)
- Java KeyStores (JKS/JCEKS)
- Kerberos keytab files
- Encryption keys for `dbms_crypto`

Can Oracle Key Vault manage Oracle wallets?

Yes. Oracle Database servers and clients use Oracle Wallets to store Oracle Advanced Security Transparent Data Encryption (TDE) master keys, certificates, server passwords, and connection strings. An Oracle Wallet is a standard PKCS#12 file (.p12), encrypted with a password-derived AES256 key. Oracle Key Vault centrally stores and manages the contents of uploaded Oracle Wallets. It allows sharing of wallet contents across endpoints and audits access to wallet contents.

How does Oracle Key Vault facilitate the sharing of keys, wallets, and keystores?

Oracle Key Vault administrators can define access control policies between related server endpoints and a set of keys and secrets. A set of keys and secrets in Oracle Key Vault is called a virtual wallet. Administrators may assign

endpoints to virtual wallets, which allows those endpoints to share the contents of the virtual wallet. This is helpful for databases using Oracle Data Guard, Real Application Clusters (RAC), globally distributed (sharded) databases, and middleware servers requiring Java keystores.

TDE online master encryption key management

What are the benefits of online TDE key management using Oracle Key Vault?

Centralizing TDE keys in Oracle Key Vault makes them easier to administer and better protected from loss or theft, especially when TDE is used across hundreds or thousands of databases. Maintaining encryption keys separate from the servers hosting encrypted data is also essential for many compliance requirements, such as PCI. Centralizing key management in Oracle Key Vault facilitates secure key sharing across RAC instances, globally distributed (sharded), and standby databases. Centralized key management also provides better governance and security, as the key lifecycle can be managed (backed up, revoked, suspended, and recovered). The largest known OKV deployment manages the TDE master keys of well over 44,000 PDBs in Oracle Key Vault.

Which Oracle Databases does Oracle Key Vault support?

Oracle Key Vault provides online master encryption key management for all Oracle databases from version 12.1.0.2 to 23ai, running on Linux, UNIX, Windows, AIX, HP-UX, ARM, and zLinux endpoint platforms. In addition to on-premises Oracle Databases, it works with databases running in virtual machines, compute instances on OCI, and third-party clouds.

Oracle Key Vault is integrated into the database provisioning workflow for:

- Autonomous Database on Dedicated Exadata Infrastructure (ADB-D)
- Autonomous Database Serverless (ADB-S)
- Exadata Database Service on Dedicated Infrastructure (ExaDB-D)

in Oracle OCI, Microsoft Azure, Amazon AWS, and Google Cloud, as well as

- Exadata Database Service on Cloud at Customer (ExaDB-C@C), and
- Autonomous Database on Exadata Cloud@Customer (ADB-C@C)

Please refer to the Oracle Key Vault documentation for information about supported endpoint platforms.

Do I need to maintain Oracle TDE master keys in an Oracle wallet after migrating them to Oracle Key Vault?

No; **only Oracle Key Vault** allows uploading current and retired (pre-migration) keys from the wallet to OKV. You can easily migrate an encrypted database to Oracle Key Vault by running the "`ADMINISTER KEY MANAGEMENT MIGRATE`" SQL*Plus command. Please refer to the Oracle Key Vault documentation for further details.

Will Oracle Key Vault impact TDE encryption performance?

TDE master keys are accessed from Oracle Key Vault and used to decrypt the data encryption keys. Since the data encryption keys are obfuscated and cached in the database, using Oracle Key Vault does not impact TDE performance.

ORACLE

SSH Key Management

What are the advantages of using Oracle Key Vault to store and manage SSH keys?

Administrators use SSH keys to access remote servers and IT systems, and that use has exploded with the rise of cloud computing. Unmanaged SSH key pairs used for public key authentication are a security and management challenge. Oracle Key Vault helps organizations better manage their SSH keys in two ways:

1. **Centralized access control** – Administering users' public keys for SSH hosts in Oracle Key Vault makes provisioning and revocation of access to systems by administrators easy to manage. Administrators can provide a user with access to a remote server by uploading the user's public key into an SSH server wallet in Oracle Key Vault. To deny access to the remote servers, SSH administrators only need to remove the user's public keys from the SSH Server wallets. Centralizing the management of SSH public keys allows administrators to track and report on failed or successful access attempts in real-time.
2. **Improved SSH key governance** – Centralizing private and public keys in a fault-tolerant, scalable, and continuously available key management system allows for enhanced key governance. With centralized key management, organizations can enforce corporate security policies such as required key length and algorithm, periodic key rotations, and key usage reporting and auditing. Furthermore, administrators can quickly restrict all remote access in case of an ongoing security incident. Enhance the security of SSH keys by generating a private/public SSH key pair on-board Key Vault, making the private key non-extractable, so it cannot leave Key Vault's cluster boundary. Copying the user's public key into the SSH Server wallet in Key Vault provides the user with server access. The end-user who attempts to access a remote server can do so as long as

   a) the public key is in the remote server's SSH wallet and

   b) the user has access to the matching private key in Key Vault.

   Managing keys in Key Vault mitigates risks associated with disk-based private keys, including key theft, unauthorized copying and sharing of keys, and key loss.

   With non-extractable private keys, the signing is performed inside OKV; with extractable private keys, signing happens locally in the PKCS#11 library.

Visit our new LiveLab to experience remote server access controls and private key governance for SSH public key authentication with Oracle Key Vault.

How does SSH user management work with Oracle Key Vault?

]

For SSH user keys without a password: OpenSSH version 7.2p1 (Oracle Linux 7 and later); with a password, OpenSSH version 8.1p1 (Oracle Linux 9 and later).

How does SSH access management work with Oracle Key Vault?

Oracle Key Vault administrators can create SSH wallets in Oracle Key Vault for each SSH host user. The one-time installation of the endpoint software and configuration of the SSH daemon on the SSH host enables these hosts to access their virtual wallets dynamically on Oracle Key Vault at the time of an SSH connection request. An administrator can allow an SSH user to access a remote host by adding their public key to the host's virtual wallet. Managing SSH users' public keys in a virtual wallet in Oracle Key Vault enables centralized provisioning/de-provisioning/suspending users' access to SSH hosts and enhanced access and activity reporting capabilities.

ORACLE

Managing private and public keys in Oracle Key Vault allows key administrators to rotate SSH keys without SSH user or client re-configuration.

Scale

How many keys can Oracle Key Vault store and manage?

Oracle Key Vault can store and manage hundreds of thousands of keys. Oracle Key Vault clusters can have up to 8 read/write pairs, providing vertical (bigger servers) and horizontal (more OKV cluster nodes) scalability.

How many server endpoints can Oracle Key Vault manage?

Most endpoints connect intermittently to the Oracle Key Vault appliance, so an Oracle Key Vault cluster can support thousands of endpoints. Users can deploy additional Key Vault servers to an existing cluster to scale to more endpoints and provide high levels of availability and locality.

For more information about Oracle Key Vault sizing, visit chapter “Oracle Key Vault Installation Requirements” in the OKV Installation and Upgrade Guide.

Key availability and backup

How does Oracle Key Vault provide continuous key availability?

Users can deploy up to 16 Oracle Key Vault instances to form a key management cluster, potentially encompassing geographically distributed on-premises and cloud data centers. Keys are shared across all nodes in the cluster, and endpoints may access any available node to access their keys.

How does Oracle Key Vault mitigate the potential for lost keys?

Each Oracle Key Vault cluster has at least one synchronous read/write pair of Key Vault nodes. When an endpoint writes a new key to one of the nodes in the pair, the update operation is not complete until it is updated on the node's synchronous partner node. Distributing these synchronous pairs across regions or data centers helps ensure that key updates are recorded even if hardware or a facility fails.

How do I back up the Oracle Key Vault appliance?

Oracle Key Vault can be backed up manually or automatically on a configurable schedule. The backup process executes the internal backup script, encrypts the backup file, and then automatically moves the encrypted backup file to a remote destination (any external filesystem that can be reached by scp or sftp, for example Oracle ZFS Storage Appliance) over a secure connection. Optionally, Oracle Key Vault allows to define the retention period of backups by automatically deleting them after a defined number of days, or a defined number of backups. Refer to the Oracle Key Vault documentation for further details.

Administration

How do I administer and manage Oracle Key Vault?

A browser-based management console makes it easy to administer Oracle Key Vault, provision server endpoints, securely manage key groups, and report on access to keys. Key Vault also contains a command line interface to perform administrative functions such as upgrades and patching. Additionally, endpoint enrollment and provisioning can be automated using RESTful interfaces for mass deployment on-premises or in the cloud.

ORACLE

How does Oracle Key Vault support centralized users?

The Oracle Key Vault console users can be managed locally or centrally through integration with Microsoft Active Directory. The console also supports user authentication using SAML tokens to provide a seamless single sign-on experience for users authenticated to federated identity providers, such as Azure Active Directory (AD) or Active Directory Federation Services (ADFS).

How does Key Vault provide administrative separation of duties?

Key Vault administrator roles can be divided into key, system, and audit management functions to separate duties. Additional users with operational responsibilities for server endpoints can be granted access to their keys and wallets for ease of management.

- **System Administrator** role provides privileges for creating and managing users, creating and managing endpoints, configuring system settings and alerts, and generally administering Oracle Key Vault. This is the most powerful role.
- **Key Administrator** role provides privileges for managing the key life cycle and controlling access to all security objects in Oracle Key Vault.
- **Audit Manager** role provides privileges for managing the audit life cycle and audit policies.

Security

How does Oracle Key Vault secure its stored keys and secrets?

Oracle Key Vault uses various Oracle Database security technologies to secure its stored keys and secrets. These include Oracle Advanced Security Transparent Data Encryption to encrypt the keys and secrets and keep them private, Database Vault to prevent sensitive data exposure to privileged users, and Virtual Private Database for user-level access control. Oracle Key Vault audits all access to the stored keys and secrets and can forward audit logs to Oracle Audit Vault and Database Firewall for analysis and consolidation. Audit information can be forwarded to Oracle Audit Vault for deeper analysis and correlation with enterprise-wide audit events; once the audit records are committed to Audit Vault, they can be deleted in OKV.

How are keys transported between Oracle Key Vault and the endpoints?

Endpoints such as database and middleware servers communicate with the Oracle Key Vault server using OASIS KMIP (Key Management Interoperability Protocol) over a mutually authenticated secure mTLS 1.2 transport over fixed port 5696. The Oracle Key Vault browser-based management console uses HTTPS (fixed port 443). Browser-based management console supports third-party certificates.

Can I enable FIPS mode in Oracle Key Vault?

Yes, Oracle Key Vault supports installation in FIPS 140–2 mode. Selecting the option to install with FIPS 140–2 mode performs all required changes during the installation. FIPS 140-2 mode can also be enabled after the installation.

Can I integrate Oracle Key Vault with my corporate HSM?

Yes. When a Hardware Security Module (HSM) is deployed with Oracle Key Vault, the Root of Trust (RoT) remains in the HSM. The HSM RoT protects the wallet password, which protects the TDE master key, which in turn protects all the encryption keys, certificates, and other security artifacts managed by the Oracle Key Vault server. This three-tier hierarchy mitigates the risk of administrators potentially extracting keys and credentials from systems they can

physically access. In this RoT usage scenario, the HSM does not store customer encryption keys. Customer keys are stored and managed directly by the Oracle Key Vault server. For more information on certifying HSMs for Oracle Key Vault Root of Trust, see chapter "Vendor Instructions for Integrating an HSM as the Root of Trust for Oracle Key Vault" in the "Root of Trust HSM Configuration Guide".

Installation and hardware requirements

How is Oracle Key Vault delivered?

Oracle Key Vault is packaged as a software appliance containing everything needed to install the product on dedicated hardware or as a virtual machine, including the operating system. During installation, the Key Vault installer partitions and formats the disks and installs the base OS (Oracle Linux 8), user-space libraries, Oracle Database 19c, and Oracle Key Vault software. It configures all software components (OS, networking, database) automatically and with minimal user involvement. It hardens the operating system, network configuration, and database according to hardening best practices. It removes unnecessary packages and software and turns off unused services and ports.

What are the recommended hardware specifications for Oracle Key Vault on dedicated hardware?

The minimum hardware requirements for deploying the Oracle Key Vault software appliance are:

- CPU: Minimum: x86-64 16 cores. Recommended: 24-48 cores with cryptographic acceleration support (Intel AESNI).
- Memory: Minimum 16 GB of RAM. Recommended: 32–64 GB.
- Disk: Minimum 2 TB. Recommended: 6 TB.

  Oracle Key Vault supports both BIOS and UEFI boot modes. For a system with a disk size greater than 2 TB, Oracle Key Vault supports booting in UEFI mode only.

  Note: Oracle Key Vault does not support fiber channel storage with multipath for the boot disk.

Refer to the Oracle Key Vault documentation for a complete list of requirements.

Can I deploy Oracle Key Vault on OCI?

Yes, you can deploy Oracle Key Vault in your Oracle Cloud infrastructure from the Oracle Cloud Marketplace.

Can I deploy Oracle Key Vault on third-party clouds?

Yes, customers running Oracle databases in 3rd party clouds can minimize network latency by deploying one or more Oracle Key Vault nodes alongside their databases. You can deploy Key Vault on compute nodes in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, delivering the same fault-tolerant, highly scalable, and continuously available key and secret management solution. Up to 16 Key Vault nodes can operate as part of a single cluster and can be deployed in OCI, 3rd-party clouds, on-premises data centers, or a combination based on customer requirements.

Where can I download the software for Oracle Key Vault?

Download Oracle Key Vault from the Oracle Software Delivery Cloud: Go to https://edelivery.oracle.com; Search for "Oracle Key Vault." Click Continue and select Oracle Key Vault, Platform Linux x86-64.

ORACLE

What features are available to support the deployment of Oracle Key Vault on virtual machines?

Oracle Key Vault can be installed in VMware, VirtualBox, KVM, and Hyper-V. Oracle Key Vault supports cloned templates. This capability allows users to add more Oracle Key Vault nodes for high availability or local access for databases spread across multiple data centers. Users can clone an Oracle Key Vault template and then use a few REST commands to add nodes to an Oracle Key Vault cluster in minutes. They can also automate cluster creation, node additions, and node removals.

Integration with target endpoints

How is the endpoint software downloaded and deployed?

Database servers, middleware servers, and systems that wish their keys and secrets to be managed are called endpoints. The Oracle Key Vault management console provides links to download and provision required endpoint software. The endpoint software package contains all necessary binaries, configuration files, and TLS 1.2 certificates for establishing a mutually authenticated secure connection between the endpoint and Oracle Key Vault. When Key Vault system administrators register endpoints, Oracle Key Vault automatically generates a one-time enrollment token. The endpoint administrators then download endpoint software using this enrollment token.

How much downtime should I plan for configuring and provisioning my endpoints?

Endpoints that upload Oracle Wallets or Java Keystores to Oracle Key Vault are not required to have any downtime. Oracle Databases migrating TDE master keys from Oracle Wallet to Oracle Key Vault require no downtime.

Feature compatibility

Which Oracle database and middleware versions are supported by Oracle Key Vault?

Oracle Key Vault supports online TDE key management as well as wallet upload and download for Oracle Database 12.1.0.2 to 23ai on Oracle Linux, Red Hat Linux, SuSE Linux Enterprise Server, Solaris Sparc, Solaris x64, AIX, HP-UX, ARM, zLinux, and Windows.

What types of key storage files does Oracle Key Vault support?

Oracle Key Vault supports Oracle Wallet and Java Keystore (JKS and JCEKS) key storage files. Oracle Key Vault has been tested with Java keystores using Oracle JDK 8 and 11.

Commented [A1]: Please check with Sarma on this

Commented [A2R1]: done

What types of credential files can Oracle Key Vault store?

Oracle Key Vault stores any credential files, such as Kerberos keytabs and files containing SSH keys. A credential file can be any file you want to manage centrally. Each credential file size must be under the 128 KB limit to be uploaded into Oracle Key Vault.

Can Oracle Key Vault encrypt sensitive data?

Oracle Key Vault manages keys and secrets for the endpoints that encrypt data. It can encrypt and decrypt TDE data encryption keys with non-extractable TDE master keys. While Oracle Key Vault encrypts managed data encryption

keys and secrets, the data encryption responsibilities are left to the endpoints. Oracle Key Vault can also perform sign and verify operations.

Can Oracle Key Vault manage DBMS_CRYPTO keys?

Yes. Starting with Oracle Key Vault 21.10, you can download an "Integration Accelerator" which allows you to customize a pre-created program for your specific environment to provide key management for DBMS_CRYPTO in all supported database versions (12.1.0.2 to 23ai).

More information

Where can I find more information on Oracle Key Vault?

There are two LiveLabs for you to experience Oracle Key Vault for free:

1. Migrate an encrypted database from a local TDE wallet to centralized key management with Oracle Key Vault.
2. Remote server access control and private key governance with Oracle Key Vault for SSH public key authentication.

For more information, see the Oracle Key Vault page on Oracle.com. The page has links to helpful information, including the data sheet, white paper, customer references, and product documentation.

ORACLE

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