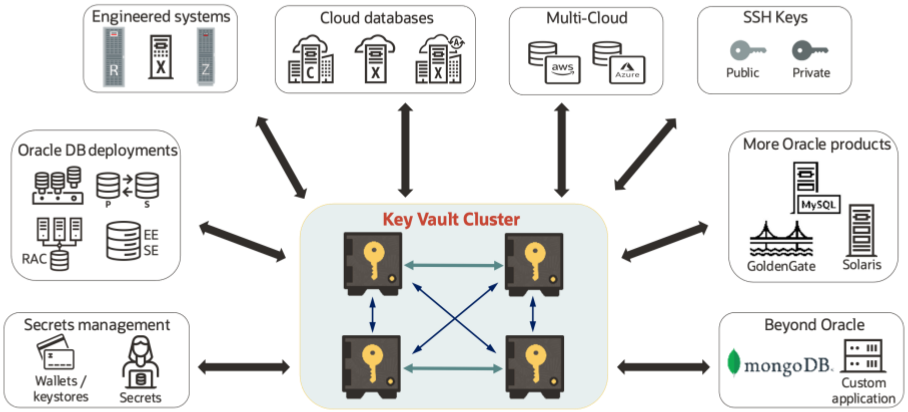
Data Sheet

Oracle Key Vault

Security threats and increased regulations for handling sensitive information drive the use of Transparent Data Encryption (TDE) and other encryption technologies in the data center. As a result, managing encryption keys, wallets, Java keystores, and other secrets is now a vital part of data center operations. Oracle Key Vault simplifies the deployment of TDE and other encryption technologies across the enterprise with scalable, highly available key and secrets management.

Introduction

Oracle Key Vault enables you to deploy encryption and other security solutions by centrally managing Transparent Data Encryption (TDE) database encryption keys, Oracle Wallets, Java Keystores, credential files, and other secrets. Key Vault supports a scalable, fault-tolerant cluster deployment architecture to deliver continuous availability and geographic locality.



Oracle Key Vault delivers secure key management for mission-critical systems across the enterprise.

Manage TDE Master Keys

Many regulations and security best practices require that encryption keys be stored separately from the encrypted data. Key Vault addresses this requirement for TDE users by centrally managing the keys as an alternative to local wallet files, eliminating the operational challenges of wallet file management, such as periodic password rotation, backing up wallet files, recovery from forgotten wallet passwords and inadvertently or maliciously deleted wallets.

Key Vault manages encryption keys for your Oracle databases, including Exadata, Exadata Cloud@Customer, Exadata Database Service on Dedicated Infrastructure,

Use cases

- Key management for Oracle databases using TDE
- Key management for integrated Oracle products and solutions such as GoldenGate and ZDLRA
- Centralized SSH key management
- Wallet, keystore, and credential file management for Oracle Databases and applications
- Secrets management for securing automation scripts
- Centralized key and secrets management for applications that process sensitive information
- Key management for KMIP-compatible endpoints like MySQL or MongoDB

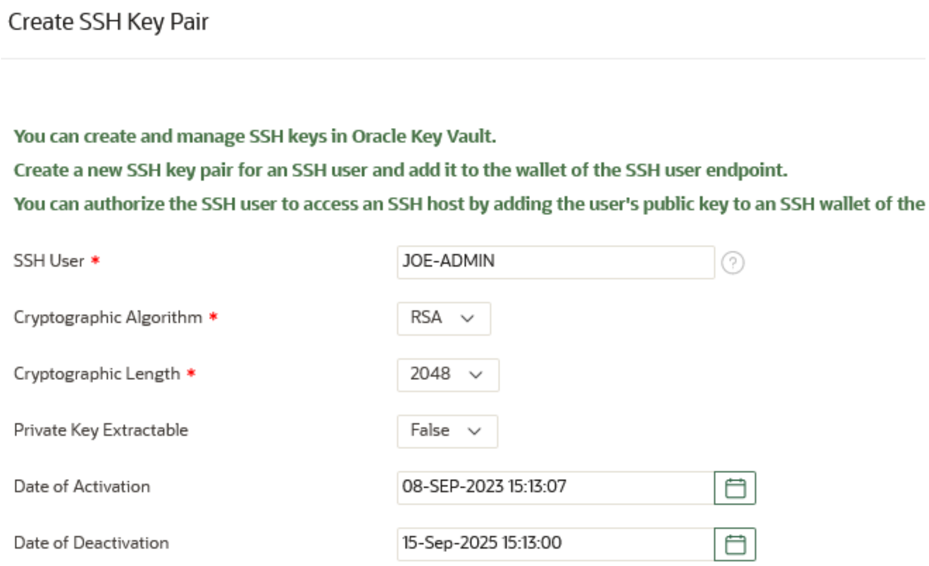
Key Features

MySQL, Oracle databases running on Oracle Cloud Infrastructure (OCI) compute, in Amazon AWS EC2, and Microsoft Azure.

If you are not already using Key Vault, you can easily migrate the existing master keys of your TDE-enabled databases from Oracle Wallets to Key Vault.

Manage SSH Keys and Control Access to Remote Servers

System administrators use public key authentication to access remote servers on-premises and in-cloud compute instances. Administrators are typically responsible for their private keys, and store those keys in files on their workstations. Owners of the remote servers must somehow keep track of the private keys used to authenticate and grant access to their machines. Local management of these keys on multiple clients and servers makes SSH key governance nearly impossible. Key Vault provides a solution for SSH key governance and access control through centralized key management. Key Vault can create and maintain private/public key pairs, which require no key footprint on any workstation:



Create SSH Key Pair

You can create and manage SSH keys in Oracle Key Vault.
Create a new SSH key pair for an SSH user and add it to the wallet of the SSH user endpoint.
You can authorize the SSH user to access an SSH host by adding the user's public key to an SSH wallet of the

SSH User *	JOE-ADMIN
Cryptographic Algorithm *	RSA
Cryptographic Length *	2048
Private Key Extractable	False
Date of Activation	08-SEP-2023 15:13:07
Date of Deactivation	15-Sep-2025 15:13:00

Administrators who need access to a remote machine are granted usage rights on a private key that does not leave Key Vault. Owners of the remote servers can control the administrator's access to their systems by granting access to their corresponding public key in Key Vault. Activities such as key rotations are entirely transparent to all participating entities. Also, owners can temporarily revoke access to any or all remote servers in case of an ongoing security incident with a push of a button.

Secure Oracle Wallets, Java Keystores, and Other Secrets

Administrators often manually copy Oracle wallets and Java keystores across servers and server clusters. Key Vault is purpose-built to simplify the controlled sharing of encryption keys between Oracle Real Application Clusters (RAC) instances, Oracle Data Guard, Oracle GoldenGate, and sharded databases. Secure sharing of encryption keys also streamlines the cloning or relocating of encrypted pluggable databases (PDBs) across container databases.

SSH keys and system passwords are widely distributed in many enterprises without appropriate protective mechanisms. Key Vault securely stores these files, audits access,

- Manages TDE master keys, Oracle Wallets, Java Keystores, and credential files
- Replaces local key stores with online TDE master key management
- Provisions into an OCI tenancy from the Oracle Cloud Marketplace in minutes
- Supports 16 read/write nodes for continuous availability
- Endpoints automatically select available nodes and transparently failover in the event of any outage
- Complete set of RESTful services to automate key lifecycle management, endpoint enrollment, and Oracle Key Vault administration
- Deploy across on-premises data centers, in Oracle Cloud Infrastructure (OCI), Amazon AWS, and Microsoft Azure.
- In-memory and persistent cache options keep encrypted systems running even when network connections are down
- Integrates with Hardware Security Modules (HSMs) as root of trust

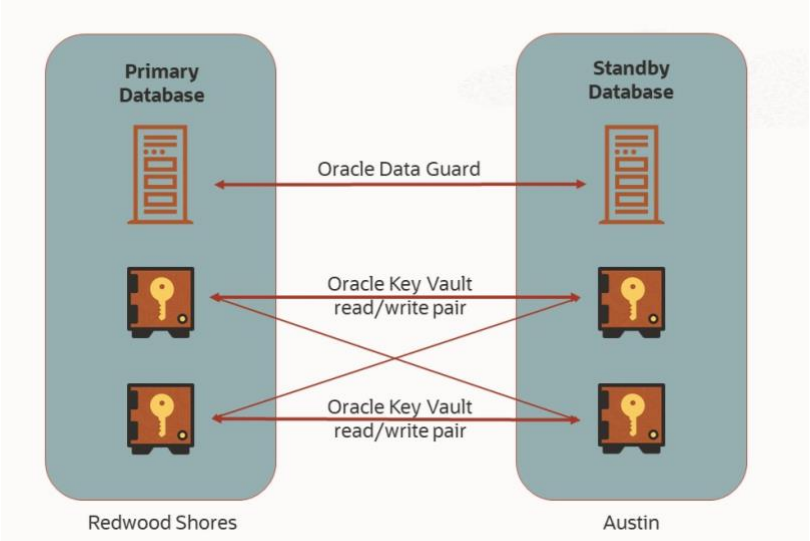
Key Business Benefits

- Provides separation between the key and encrypted data required for compliance shares them across trusted endpoints and backs them up for long-term retention and recovery.

Continuously Available and Scalable Cluster Architecture

Key Vault deploys in a cluster configuration to provide continuous availability and geographic coverage. Key Vault supports up to 16 nodes in a cluster, automatically synchronizing any changes made at one node across the entire cluster.

Each database endpoint transparently maintains a list of available nodes and is continuously aware of changes to the cluster. If the current node becomes unavailable, the endpoint transparently fails over to another nearby node. To further increase resilience for network outages, Key Vault allows the optional creation of a cache on the database servers so databases remain fully functional should network connectivity to all nodes be down.



Database endpoints transparently fail over to a nearby node when the preferred node becomes unavailable.

Key Vault's unique cluster deployment architecture is highly scalable. You can deploy pairs of read-write nodes across data centers to help ensure endpoints have access to a local node for both read and write operations. Finally, each Key Vault server deploys on commodity hardware platforms that can be sized to meet the most demanding service loads. The result is a key service that can support thousands of databases deployed worldwide, with extreme availability and high service levels.

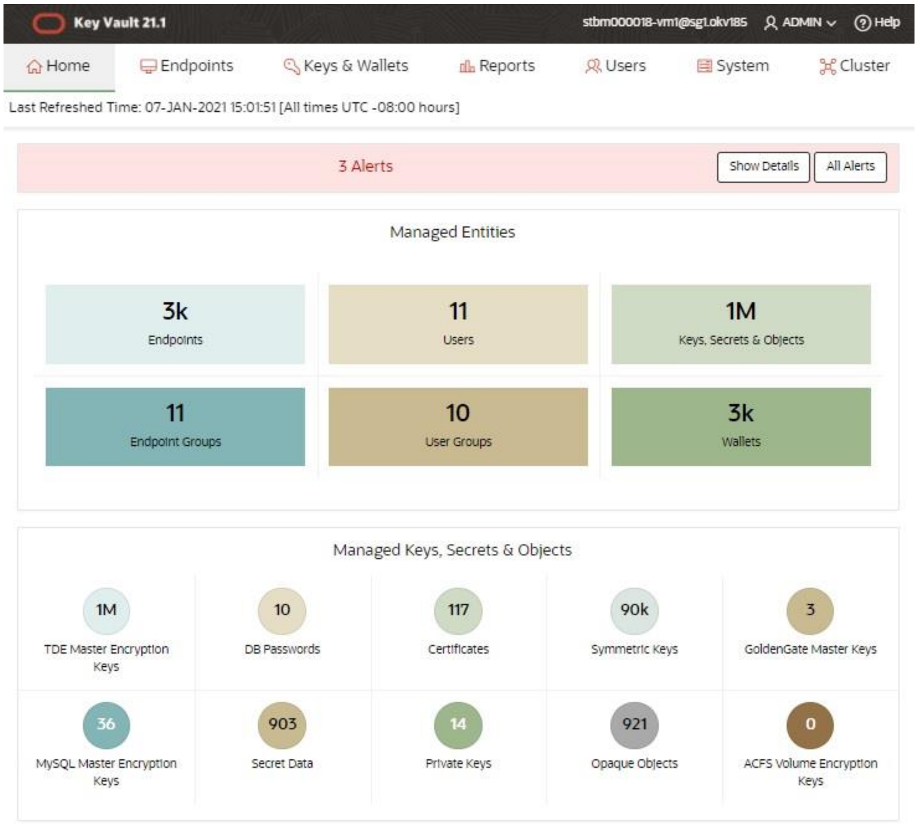
Easy Administration

A browser-based management console makes it easy to administer Key Vault servers, manage clusters, provision server endpoints, securely manage key groups, and report on access to keys. Administrators receive email alerts for important status updates and system activities such as upcoming password and key expirations. Endpoint enrollment and provisioning can be automated using protected RESTful interfaces for mass deployment to databases.

- Reduces risk and cost by consolidating key stores
- Protects keys and secrets from accidental loss or theft
- Ensures continuous key and secret availability when software, hardware, or network fails
- Scales to thousands of databases
- Lowers hardware cost with no idle nodes
- Full accountability of key management life cycle with auditing

Related products

Oracle Key Vault is an important database security control. Related Oracle Database Security products include:



Key Vault management console allows users to understand at a glance the various security objects under management.

Secure Software Appliance

Security is a critical requirement for enterprise-scale deployment. Key Vault addresses security at multiple layers, including infrastructure, administration, and operations. Key Vault is delivered as an ISO image and installs as a pre-configured and secured software appliance that can be installed on dedicated hardware or VM guests on-premises or in OCI, Azure, and AWS. It uses various Oracle Database security technologies to protect keys and secrets stored inside Key Vault. For example, Key Vault uses Transparent Data Encryption to encrypt keys stored in the embedded Oracle Database. It also uses Database Vault to restrict unauthorized privileged user access.

Administrator roles can be divided into key, system, and audit management functions for the separation of security duties. Key Vault audits all critical operations, including key access and key life cycle changes. The audit data can be forwarded to Oracle Audit Vault and Database Firewall (AVDF) or to a syslog server for record retention and reporting. Oracle Key Vault supports SNMP v3 for remote monitoring.

Key Vault can integrate with hardware security modules (HSMs) to provide additional security for keys, certificates, and other security artifacts during patching and upgrades. In this case, the HSM serves as a root of trust, protecting 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 Key Vault server.

Deploys on-premises and in the Oracle Cloud

- Oracle Advanced Security
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting
- Oracle Audit Vault and Database Firewall
- Oracle Data Safe cloud service

Key Vault is easy to install and can be deployed on compatible x86-64 hardware of users' choice. It is also available from the Oracle Cloud Marketplace. It can be deployed in an OCI tenancy within minutes, providing fault-tolerant, continuous key management services to on-premises, hybrid, or multi-cloud database deployments. Key Vault supports endpoints on common enterprise platforms, including Oracle Linux, Red Hat Linux, SUSE Linux Enterprise Server, Solaris SPARC, Solaris x86, IBM AIX, HP-UX (IA), and Microsoft Windows.

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