**Oracle® Key Vault**

Release Notes

Release 18.1

E99979-06

July 2019

# Release Notes

These release notes list the new features for this release of Oracle Key Vault, how to download the latest product software and documentation, and how to address known issues in Oracle Key Vault.



## Changes in This Release for Oracle Key Vault

Oracle Key Vault release 18.1 introduces several new features that enhance the use of Oracle Key Vault in a large enterprise.



### Multi-Master Cluster

Oracle Key Vault release 18.1 introduces the multi-master cluster capability. This feature provides an active-active high availability solution that you can extend across data centers and geographic regions to provide disaster recovery and high availability for both read and write key management operations. Also, the multi-master cluster capability provides zero-downtime from the database endpoint perspective.

## Support for FIPS Mode

Oracle Key Vault is currently in the process of obtaining FIPS validations for its cryptographic modules. You can install Oracle Key Vault so that it operates in FIPS 140-2 compliant mode (FIPS mode), which provides increased security. If you do not install Oracle Key Vault so that it uses FIPS mode, then a user with the System Administrator role can enable or disable it from the Oracle Key Vault management console.

## Enhancements to RESTful API

The Oracle Key Vault RESTful services utility enables you to automate Oracle Key Vault administration tasks such as endpoint enrollment and virtual wallet management for a large distributed deployment. With Oracle Key Vault 18.1, customers can also automate key management tasks such as key creation, deactivation, and key deletion for the endpoints.

## Terminology Changes

Beginning in Oracle Key Vault release 18.1, the configuration previously known as high availability is now called primary-standby.

# Downloading the Oracle Key Vault Software and the Documentation

At any time, you can download the latest version of the Oracle Key Vault software and documentation.

- Downloading the Oracle Key Vault Installation Software
- Downloading the Oracle Key Vault Documentation

## Downloading the Oracle Key Vault Installation Software

For a fresh installation, you can download the Oracle Key Vault software from the Software Delivery Cloud. You cannot use this package to upgrade Oracle Key Vault. For an upgrade from an existing Oracle Key Vault 12.2 deployment, you can download the Oracle Key Vault upgrade software from the My Oracle Support website.

1. Use a web browser to access the Oracle Software Delivery Cloud portal:

   https://edelivery.oracle.com

2. Click **Sign In**, and if prompted, enter your **User ID** and **Password**.
3. In the **All Categories** menu, select **Release**. In the next field, enter **Oracle Key Vault** and then click **Search**.
4. From the list that is displayed, select **Oracle Key Vault 18.1.0.0.0** or click the **+Add to Cart** button next to the **Oracle Key Vault 18.1.0.0.0**.

The download is added to your cart. (To check the cart contents, click **View Cart** in the upper right of the screen.)

5. Click **Checkout**.
6. On the next page, verify the details of the installation package, and then click **Continue**.
7. In the **Oracle Standard Terms and Restrictions** page, after you have read the terms and restrictions and agree with them, select **I have reviewed and accept the terms of the Commercial License, Special Programs License, and/or Trial License**, and click **Continue**.

   The download page appears, which lists the following Oracle Key Vault ISO files:

   - V*part_number*.iso (Oracle Key Vault 18.1.0.0.0 - Disc 1)
   - V*part_number*.iso (Oracle Key Vault 18.1.0.0.0 - Disc 2)
8. To the right of the **Print** button, click **View Digest Details**.

   The listing for the two ISO files expands to display the SHA-1 and SHA-256 checksum reference numbers for each ISO file.
9. Copy the SHA-256 checksum reference numbers and store them for later reference.
10. Click **Download** and select a location to save the ISO files.

    You can save each file individually by clicking its name and then specifying a location for the download.
11. Click **Save**.

    The combined size of both ISO files exceeds 4 GB, and will take time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.
12. After the ISO files are downloaded to the specified location, verify the SHA-256 checksums of the downloaded files:

    a. From a Linux or Unix machine, generate a SHA256 checksum for the first V*part_number*.iso:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in step 9.

    b. Generate a SHA-256 checksum for the second V*part_number*.iso:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in step 9.
13. Optionally, burn each of the two V*part_number*.iso files to a DVD-ROM disc and then label the discs:

    - OKV 18.1 Disc 1

- `OKV 18.1 Disc 2`

You can now install Oracle Key Vault on a server machine.

## Downloading the Oracle Key Vault Documentation

1. Access the Oracle documentation site.

   `https://docs.oracle.com/en/database/`
2. Select **Related Products**.
3. In the Database Security section, search for and download the most current version of the Oracle Key Vault 18.1 documentation, including these release notes.

# Known Issues

At the time of this release, there are issues with Oracle Key Vault that could occur in rare circumstances. For each issue, a workaround is provided.

- Multi-Master Cluster Issues
- General Issues

## Multi-Master Cluster Issues

This section describes Oracle Key Vault issues specific to a multi-master cluster configuration.

- Replication May Fail to Resume After Multiple System Failures in OKV Cluster
- System Settings Changed on an OKV System After Conversion to a Candidate Node Do Not Reflect On The Controller Node
- OKV 18.1: Aborting the Addition of a Node Takes an Hour When the Controller Node Can't Contact the Candidate Node
- OKV 18.1: Clicking Candidate Node on the Cluster Management Page of a Non Controller Node Redirect to a Wrong Page
- Create Cluster Between OKV Servers Fails With HSM
- Reverse Migrate From HSM Using Same Passphrase Gives Error ORA-20101: Failed To Change Recovery Passphrase
- Errors During Pairing Are Not Propagated to the Oracle Key Vault Management Console
- Retry OKV Server Certificate Creation

### Replication May Fail to Resume After Multiple System Failures in OKV Cluster

**Issue:** Due to GoldenGate Bug 29624366, after multiple system failures in an Oracle Key Vault cluster, replication from some nodes may fail to resume. Specifically, Gold-

enGate replicats will terminate and not be able to process new change logs in the GoldenGate trail file when it happens.

**Workaround:** Manually reposition such replicats to skip erroneous records in the trail file or forcefully delete the troubled Oracle Key Vault nodes from the cluster and add new nodes to replace them.

**Bug Number:** 29700647

### System Settings Changed on an OKV System After Conversion to a Candidate Node Do Not Reflect On The Controller Node

**Issue:** If system settings are changed on an Oracle Key Vault system after it has been converted to a candidate node, and after the controller node's initial attempt to verify the candidate node's settings has failed, the updated settings do not reflect on the controller node. The pairing process must be aborted and the candidate node re-installed.

**Workaround:** None. Verify that the Oracle Key Vault system's settings match with those of the cluster before attempting to convert it into a candidate node and induct it into a cluster.

**Bug Number:** 29430349

### OKV 18.1: Aborting the Addition of a Node Takes an Hour When the Controller Node Can't Contact the Candidate Node

**Issue:** When attempting to add a node to a multi-master cluster, if the controller node fails to make contact with the candidate node, aborting the addition of the node can take an excessively long time. This is due to the controller node's repeated attempts to make contact with the candidate node before ultimately failing and letting the abort proceed.

**Workaround:** No workaround to abort faster.

**Bug Number:** 29688831

### OKV 18.1: Clicking Candidate Node on the Cluster Management Page of a Non Controller Node Redirect to a Wrong Page

**Issue:** When you add a node to a multi-master cluster, on the **Cluster Management** page, in the **Cluster Details** table, if you click the name of the candidate node on any node other than the controller node, you will be redirected to the **Add Node to Cluster** page instead of to the candidate node.

**Workaround:** Directly navigate to the candidate node using its URL instead of clicking the name of the candidate node in the **Cluster Details** table.

**Bug Number:** 29669752

### Create Cluster Between OKV Servers Fails With HSM

**Issue:** Recovery passphrases over 16 characters caused the node induction process to fail when both the controller and candidate node are HSM-enabled.

**Workaround:** Contact Oracle Support for information on patch 29792398.

**Bug Number:** 29792398

## Reverse Migrate From HSM Using Same Passphrase Gives Error ORA-20101: Failed To Change Recovery Passphrase

**Issue:** Using the same recovery passphrase for the old and new recovery passphrase inputs when reverse-migrating from HSM when not in a cluster raises an inappropriate error.

**Workaround:** Contact Oracle Support for information on patch 29792398.

**Bug Number:** 29799098

## Errors During Pairing Are Not Propagated to the Oracle Key Vault Management Console

**Issue:** Errors during pairing are not propagated to the Oracle Key Vault management console.

**Workaround:** If pairing is taking an excessively long time on one step without progress, you may want to check if pairing has failed. This will require SSH being enabled on both the controller and candidate node before beginning pairing. Log on to each node with these steps:

1. Use SSH to connect to the Oracle Key Vault server as the `support` user.

   ```
   ssh support@Oracle_Key_Vault_IP_address
   ```

2. Switch user to the `root` user.

   ```
   su - root
   ```

3. Display the contents of the status file and look for error messages to determine if the pairing has failed.
   - If you are on the candidate node, display the contents of the `new_node_status.txt` file.

     ```
     cat /var/okv/log/mmha/new_node_status.txt
     ```

   - If you are on the controller node, display the contents of the `welcome_node_status.txt` file.

     ```
     cat /var/okv/log/mmha/welcome_node_status.txt
     ```

## Retry OKV Server Certificate Creation

**Issue:** Attempting to induct a new node into an Oracle Key Vault 18.1 multi-master cluster may intermittently fail with `okv_enroll_cert: Error creating cert` errors seen in the log files of the candidate node.

**Workaround:** Abort the pairing. Apply patch 22993467 on the controller node. Re-install Oracle Key Vault 18.1 on the candidate node, or use another freshly-installed Oracle Key Vault 18.1 system as the candidate node. Apply patch 22993467 on the candidate node as well, and then try to add it to the cluster again.

**Bug Number:** 29968244

**Patch Number:** 22993467

## General Issues

This section describes general Oracle Key Vault issues.



### Unable to Open the Database When a DNS Server Is Configured to Access HSM

**Issue:** Users can configure DNS servers by using the management console. However, if access to HSM depends on a DNS server, the database fails to open when HSM starts.

**Workaround:** Add the DNS server entries to `/etc/resolv.conf`. Add the same DNS servers using the management console: **System** tab > **System Settings** page > **DNS** section. Alternatively, you can provide the IP address of the HSM.

**Bug Number:** 24478865

### On HP-UX System, SELECT FROM V$ENCRYPTION_KEYS May Return ORA-28407 Occasionally

**Issue:** On HP-UX operating system, a Transparent Data Encryption (TDE) query such as the following that is executed in a long-running database process or session may occasionally result in an `ORA-28407 Hardware Security Module error detected` error:

```
SELECT * FROM V$ENCRYPTION_KEYS;
```

This is because the system could not create another thread-specific data key because the process had reached or exceeded the system-imposed limit on the total number of

keys per process, which is controlled by the `PTHREAD_KEYS_MAX` setting. `PTHREAD_KEYS_MAX` is typically set to `128`.

**Workaround:** Switch the database sessions and execute the TDE query again. If it is not convenient to switch the sessions, then set `PTHREAD_USER_KEYS_MAX` to `16384` before starting the database and the listener.

**Bug Number:** 28270280

### OKV 12.2 BP1: User Gets Locked and Expired with Multiple Failed Logins

**Issue:** The current password policy locks the user account for a day if the user has incorrectly entered the password more than three consecutive times. Therefore, the user will be able to log in only after the 24-hour lockout period expires.

**Workaround:** Make a note of the password and keep it accessible and secure.

**Bug Number:** 23300720

### OKV Alerts Still Show in the List After Fixing the Problem

**Issue:** User password expiration alerts are still showing even after the user changes their password.

**Workaround:** In the Oracle Key Vault management console, select **Reports** and then **Configure Reports**. Then uncheck the **User Password Expiration** option. Alternatively, ignore the alert.

**Bug Number:** 27620622

### Private Keys Are Not Overwritten When a Java Keystore Is Uploaded Using the -o Option of the okvutil Utility

**Issue:** When you upload a Java keystore (JKS) or Java Cryptography Extension keystore (JCEKS) to the Oracle Key Vault server using the `-o` option of the `okvutil upload` command, user-defined keys are not overwritten.

**Workaround:** Remove the private key from the wallet and then upload the keystore again.

**Bug Number:** 26887060

### Upgrade to OKV 18.1 Fails With Any One of the Following Errors

**Issue:** Upgrade to OKV 18.1 fails with any one of the following errors in the log files:

```
ORA-02437: cannot validate KEYVAULT.ACCESS_MAPPING_PK) - primary key violated
```

or

```
Populate KEYVAULT.AO_OBJGRP_CREATOR
...more output...
ORA-01403: no data found
```

**Workaround:** Restore the system to its original state from backup. Apply patch 22975725 on the system per the instructions and retry the upgrade.

**Bug Number:** 29912855

# Oracle Key Vault Considerations

Below are details and changes of behavior of Oracle Key Vault 18.1.

- Oracle TDE and Oracle Key Vault Integration
- Reports are Affected by Audit Replication in a Multi-Master Cluster
- Updates in a Multi-Master Cluster are Slower Than in a Single Instance

## Oracle TDE and Oracle Key Vault Integration

Depending on the Oracle Database version used and on the feature of TDE used, there might be a need to patch the Oracle database for smooth operations.

Refer to the MOS-NOTE with Doc ID 2535751.1 to ascertain if your deployment needs a database patch.

The MOS-NOTE lists known issues with Oracle Database Transparent Data Encryption (TDE) feature when it is configured to use Oracle Key Vault as the keystore. The document also lists the fixes that resolve the issues enabling smoother integration between Oracle Database TDE and Oracle Key Vault. The issues could be defects, reducing the user burden with simplified operations, or improving the integration between TDE and OKV. The document is for Database Administrators and others tasked with managing the TDE Master Keys with Oracle Key Vault.

## Reports are Affected by Audit Replication in a Multi-Master Cluster

Oracle Key Vault reports and details in the home page are generated from Oracle Key Vault audit records. Each node will show reports of the operations specifically done on that node if audit replication is turned off. Each node will show reports of the operations done on all nodes in the cluster if audit replication is turned on.

The recommendation is to turn off audit replication and use a security information and event management (SIEM) solution like Oracle Audit Vault and Database Firewall (AVDF) to collect audit records from all nodes.

## Updates in a Multi-Master Cluster are Slower Than in a Single Instance

An update in a multi-master cluster might check for an object's existence, which may result in a scan of all nodes in the cluster slowing down the update operation. The time

will increase proportional to the number of nodes in the cluster. The update could take several minutes to complete.

Setting and rotating the TDE master encryption key are examples of update operations.

## Supported Database Versions

The following versions of Oracle Database are supported with Oracle Key Vault 18.1:

- Oracle DB 11.2 with the compatible parameter set to 11.2
- Oracle DB 12.1 with the compatible parameter set to 11.2
- Oracle DB 12.2
- Oracle DB 18c
- Oracle DB 19c

## Critical Patch Updates Included in Release 18.1.0.0.0

Oracle Key Vault release 18.1 updated the underlying infrastructure to incorporate the April 2019 Release Update for Oracle Database 18 (18.6 DB RU) - April Release Update. Please sign in for full details.

https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

Oracle Key Vault release 18.1 also includes security and stability fixes for Java and Oracle Linux (OL) operating system.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

## Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Key Vault Release Notes, Release 18.1
E99979-06

Copyright © 2013, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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 of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.