
Oracle Key Vault: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-000318-001
Revision	D
Release Date	9 April 2021

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Certified Platforms.....	4
Certified platforms for Luna HSM	4
Certified platforms for Luna Cloud HSM	5
Prerequisites	5
Configure Luna HSM	5
Configure Luna Cloud HSM service	7
Set up Oracle Key Vault	10
Configuring Oracle Key Vault to use Thales Luna HSM.....	10
Backing up and restoring Oracle Key Vault in HSM Mode	12
Contacting customer support	16
Customer support portal	16
Telephone support.....	16
Email support.....	16

Overview

This document guides security administrators through the steps for integrating Oracle Key Vault with a Luna HSM or Luna Cloud HSM. You can use Luna HSMs to secure the Root of Trust (RoT) for Oracle Key Vault. The Luna 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 Oracle Key Vault. The Luna HSM does not store any customer encryption keys. The customer keys are stored and managed directly by the Oracle Key Vault server.

The benefits of securing the cryptographic keys with Luna HSMs include:

- > Secure generation, storage and protection of the keys on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of the keys.
- > HSM audit trail*.
- > Significant performance improvements by off-loading cryptographic operations from application servers.

*Luna Cloud HSM service does not have access to the secure audit trail

Certified Platforms

- > [Certified platforms for Luna HSM](#)
- > [Certified platforms for Luna Cloud HSM](#)

Certified platforms for Luna HSM

The following platforms are certified for integrating Oracle Key Vault with Luna HSM:

HSM Type	Platforms Certified
Luna HSM	Oracle Key Vault v21.1.0.0.0 Oracle Key Vault v18.5.0.0.0 Oracle Key Vault v18.4.0.0.0 Oracle Key Vault v18.1.0.0.0 Oracle Key Vault v12.2.0.8

NOTE: This integration is tested in both HA and FIPS mode.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Certified platforms for Luna Cloud HSM

The following platforms are certified for integrating Oracle Key Vault with Luna Cloud HSM:

HSM Type	Platforms Certified
Luna Cloud HSM	Oracle Key Vault v21.1.0.0.0

Luna Cloud HSM: Luna Cloud HSM platform provides on-demand, cloud-based HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before beginning the integration, ensure you have completed the following tasks:

- > [Configure Luna HSM](#)
- > [Configure Luna Cloud HSM service](#)
- > [Set up Oracle Key Vault](#)

Configure Luna HSM

To configure Luna HSM:

1. Ensure the HSM is setup, initialized, provisioned, and ready for deployment.
2. Create a partition on the HSM for use by Oracle Key Vault.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Verify that the partition is successfully registered and configured. The command to see the registered partition is:

```
# /usr/safenet/lunaclient/bin/lunacm
```

```
lunacm (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.
```

```
Available HSMs:
Slot Id -> 0
Label -> OKV
Serial Number -> 1238696044950
Model -> LunaSA 7.4.0
Firmware Version -> 7.4.0
Configuration -> Luna User Partition With SO (PW) Key Export
With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> Non-FM
Current Slot Id: 0
```

- For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

NOTE: Follow the [Luna Network Luna HSM documentation](#) for detailed steps for creating NTLS connection, initializing the partitions, and managing various user roles.

To control user access to HSM

NOTE: This section is applicable only for Linux users.

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM, by adding them to the **hsmusers** group. The client software installation automatically creates the **hsmusers** group. The **hsmusers** group is retained when you uninstall the client software, allowing you to upgrade the software while retaining your **hsmusers** group configuration.

To add a user to hsmusers group

To allow non-root users or applications access to the HSM, assign the users to the **hsmusers** group. The users you assign to the **hsmusers** group must exist on the client workstation.

- Ensure that you have **sudo** privileges on the client workstation.
- Add a user to the hsmusers group.

```
# sudo gpasswd --add <username> hsmusers
```

Where `<username>` is the name of the user you want to add to the hsmusers group.

To remove a user from hsmusers group

- Ensure that you have **sudo** privileges on the client workstation.
- Remove a user from the hsmusers group.

```
# sudo gpasswd -d <username> hsmusers
```

Where `<username>` is the name of the user you want to remove from the **hsmusers** group. You must log in again to see the change.

NOTE: The user you delete will continue to have access to the HSM until you reboot the client workstation.

To set up Luna HSM High-Availability (HA)

Please refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

Configure Luna Cloud HSM service

You can configure Luna Cloud HSM Service in the following ways:

- > [Standalone Cloud HSM service using minimum client package](#)
- > [Standalone Cloud HSM service using full Luna client package](#)
- > [Luna HSM and Luna Cloud HSM service in hybrid mode](#)

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using [pscp](#), scp, or other secure means.
2. Login as root to the Oracle Key Vault server and create a directory /usr/safenet/lunaclient
3. Extract the .zip file into a /usr/safenet/lunaclient directory created above on your client workstation.
4. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

[Linux]

```
cvclient-min.tar
```

```
# tar -xvf cvclient-min.tar
```

5. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

[Linux]

```
Source the setenv script.
```

```
# source ./setenv
```

6. Run the LunaCM utility and verify that the Cloud HSM service is listed.

NOTE: Follow the [Luna Cloud HSM documentation](#) for detailed steps for creating service, client, and initializing various user roles.

7. Create a directory /usr/safenet/lunaclient/lib/

```
# mkdir /usr/safenet/lunaclient/lib/
```

8. Create a link of /usr/safenet/lunaclient/libs/64/libCryptoki2.so library to /usr/safenet/lunaclient/lib/libCryptoki2_64.so.

```
# ln -svf /usr/safenet/lunaclient/libs/64/libCryptoki2.so
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
```

9. Copy the Chrystoki.conf file to /etc directory.

```
# cp /usr/safenet/lunaclient/Chrystoki.conf /etc/
```

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using `pscp`, `scp`, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Linux]
```

```
cvclient-min.tar
```

```
# tar -xvf cvclient-min.tar
```

4. Run the `setenv` script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Linux]
```

```
Source the setenv script.
```

```
# source ./setenv
```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

NOTE: Skip this step for Luna Client v10.2 or higher.

Cloud HSM Certificates

```
server-certificate.pem
```

```
partition-ca-certificate.pem
```

```
partition-certificate.pem
```

LunaClient Certificate Directory

```
[Linux default location for Luna Client]
```

```
/usr/safenet/lunaclient/cert/
```

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

Linux

```
Chrystoki.conf
```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

NOTE: Skip this step for Luna Client v10.2 or higher.

```
[XTC]
```

```
. . .
```

```

PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .
[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .

```

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```

Misc]
PluginModuleDir=<LunaClient_plugins_directory>

[Linux Default]

/usr/safenet/lunaclient/plugins/

```

10. Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.
11. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

Linux

Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

12. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

NOTE: Refer to [Luna Cloud HSM documentation](#) for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the [Standalone Cloud HSM service using full Luna client package](#) section above.

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up Oracle Key Vault

Oracle Key Vault is a software appliance that is delivered as an ISO image. We recommend installing Oracle Key Vault on its own dedicated physical server. The Oracle Key Vault ISO image consists of a pre-configured operating system, an Oracle database, and the Oracle Key Vault application.

For detailed information about installing Oracle Key Vault, refer to *Oracle Key Vault Documentation*.

Configuring Oracle Key Vault to use Thales Luna HSM

This section demonstrates how to initialize the Luna HSM so that a root of trust (RoT) can be created and used by Oracle Key Vault. To configure Oracle Key Vault to use Luna HSM:

1. Add the Oracle user to the **hsmusers** group and reboot the Oracle Key Vault for the change to take effect. Login with support user and then switch to root to perform below steps.

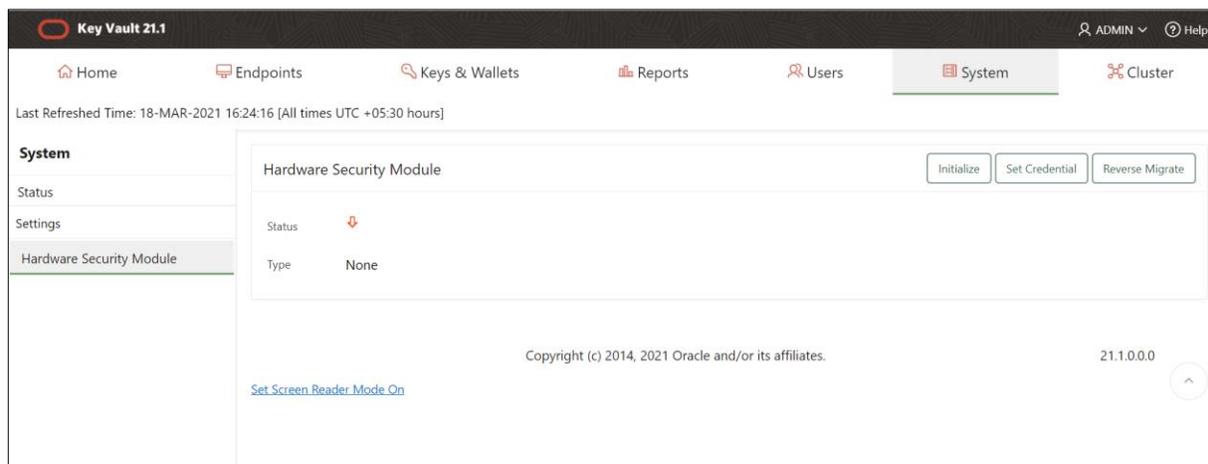
```
# gpasswd --add oracle hsmusers
# reboot
```

NOTE: Skip this step if you are using *Standalone Cloud HSM service using minimum client package*.

2. Oracle Key Vault provides a management console which can be accessed through `https://<Oracle_Key_Vault_Server_IP>` in the web browser.
3. Log in to the Oracle Key Vault management console as a user with system administrative privileges.

NOTE: The System Admin user credentials are created during Oracle Key Vault installation and configuration.

4. Click the **System** tab.
5. For Oracle Key Vault v21.1 in the left sidebar, click **Settings**. Under **Network Services**, click on **HSM**.
6. For Oracle Key Vault v18.5 or below in the left sidebar, click **Hardware Security Module**.
7. At this point, the HSM is not initialized. You will see a red arrow pointing down in the **Status** field.



8. Click **Initialize**. The **Initialize HSM** dialog will appear on the screen.

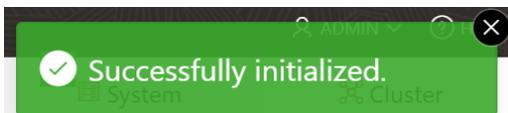
9. Open the **Vendor** drop-down menu and select **Thales Luna**.

NOTE: In earlier versions of Oracle Key Vault (18.4 or lower), open the Vendor drop-down menu and select Safenet.

10. Enter the **HSM Credential**, **Recovery Passphrase**. The HSM Credential is the partition password. The Recover Passphrase was set during the Post Installation setup of Oracle Key Vault. Select **Use Token Label** and enter the **Token Label**.

NOTE: Earlier versions of Oracle Key Vault (18.3 or lower) do not support selecting Token Label. Using Token Label you can choose any token if multiple tokens are registered.

11. Click **Initialize**. On success, you will see the following message.



12. Once initialized, verify the HSM **Status**. You will see a green arrow pointing up with partition HSM details.

NOTE: If you change the HSM credential following HSM initialization, you also need to update the HSM credential on the Oracle Key Vault server using the **Set Credential** button.

13. Verify the master encryption key generated on the partition by executing partition contents in lunacm.

```

lunacm:>par con

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:          OKV 18.1 HSM Key Number
Handle:         115
Object Type:    Data
Object UID:     5600000025000003cb640800

Label:          OKV 18.1 HSM Root Key
Handle:         96
Object Type:    Symmetric Key
Usage Limit:    none
Object UID:     5400000025000003cb640800

Number of objects: 2

Command Result : No Error

lunacm:>

```

This completes the Integration of Oracle Key Vault with Thales Luna HSM.

Backing up and restoring Oracle Key Vault in HSM Mode

You can back up and restore Key Vault data when HSM mode is enabled. It is recommended that you should back up data periodically to reduce down time and recover from unexpected data losses and system failures. Backup can be done on local as well as on remote destination, but it is advised to choose remote destination. There are two types of backups: **One-Time** and **Periodic**. For the purpose of demonstration, this guide uses **One-Time** backup.

> [Back up Oracle Key Vault in HSM mode](#)

> [Restore Oracle key Vault in HSM mode](#)

Back up Oracle Key Vault in HSM mode

1. Log in to the Oracle Key Vault management console as a user with System Administrator privileges.
2. For Oracle Key Vault v21.1, select the **System**→**Settings** and then click **Backup and Restore** under **System Configuration**. A list of scheduled and completed backups will be displayed.
3. For Oracle Key Vault v18.5 or below, select the **System** tab and then click **System Backup** on the left sidebar. A list of scheduled and completed backups will be displayed.
4. Click **Manage Backup Destinations**. This will display a list of all backup destinations.
5. Click **Create**.
6. Enter the following information for the backup location:
 - **Destination Name:** Specify any destination name.
 - **Transfer Method:** This is by default set to SCP to allow secure copy of files.

- **Hostname:** Enter the IP address of the backup destination. If DNS is configured enter the Hostname.
- **Port:** Enter Port number for SCP. The default port number is 22.
- **Destination Path:** Enter the Actual path on the backup destination.
- **Username:** Enter the username who has read-write permission of Destination Path.
- **Authentication Method:** Select the authentication method as key-based or password based.
 - For key based enter the public key.
 - For password based enter the password.

Create Backup Destination

Destination Name * BackupServer

Transfer Method scp sftp

Hostname * 10.164.78.89

Port * 22

Destination Path * /okv/backup

User Name * root

Authentication Method Key-based Authentication Password Authentication

Password *

Re-enter Password *

Cancel Save

7. Click **Save**. Oracle Key Vault validates the destination. If the validation fails, the destination is not created.

NOTE: You can edit these settings at any time except when restoring from a backup.

8. After the destination is created, click **System Backup**→**Backup**.
9. Enter the following information for the backup:
 - **Name:** Enter a name to identify the backup.
 - **Start Time:** Select a time for the backup to start. If you want to start it now, select **Now**.
 - **Destination:** Select a local or remote destination.
 - **Type:** Select **One-Time** or **Periodic**. If **Periodic** is selected, specify the time when the backup will be performed.

Backup

Name * OKVBACKUP

Start Time * 25-MAR-2021 19:30

Destination * BACKUPSERVER

Type * ONE-TIME PERIODIC

Days 7 Hours 00 Mins 00

Cancel Schedule

10. Click **Schedule**. This will enable you to check the backup status as **ACTIVE**, **ONGOING**, **PAUSED** or **DONE**. When the backup is in progress, its status will appear as **ONGOING**. Once the backup is completed its status will appear as **DONE**.

Completed Backups									
Name	Type	Destination	Status	Run Index	Run Error	Schedule Time	Start Time	Backup Time	Last Full Backup Time
OKVBACKUP	Backup Once	BACKUPSERVER	DONE	1		25-MAR-2021 19:35:21	25-MAR-2021 19:35:22	25-MAR-2021 19:49:27	25-MAR-2021 19:49:27

row(s) 1 - 1 of 1

11. You can verify the backup files on backup destination.

```
[root@localhost ~]# ls /okv/backup/
okvbackup_onetime.mgr  okvbackup_onetime_onetime_20210325140732_hsm  okvinit.bkp
```

Restore Oracle Key Vault in HSM mode

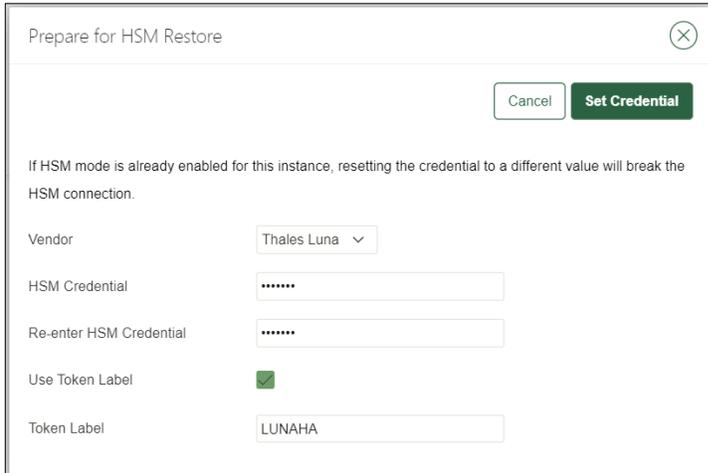
NOTE: Only backups taken in HSM mode can be restored to an HSM-enabled Oracle Key Vault. Before restoring a backup, you must ensure that the system can access both the HSM and Root of Trust (RoT) used to take the backup. To restore a backup, you must have installed the Luna Client Application on the Oracle Key Vault server and register the partition that was used at the time of backup prior to this procedure.

1. Log in to the Oracle Key Vault management console as a user with System Administrative privileges.
2. For Oracle Key Vault v21.1 in the left sidebar, click **Settings**. Under **Network Services** click on **HSM**.
3. For Oracle Key Vault v18.5 or below in the left sidebar, click **Hardware Security Module**.
4. The **Status** will appear as disabled. Click **Set Credential**. The **Prepare for HSM Restore** dialog will appear on the screen.
5. Click the **Vendor** drop-down menu and select **Thales Luna**.

NOTE: In earlier versions of Oracle Key Vault (18.4 or lower), open the Vendor drop-down menu and select Safenet.

- Enter the partition password in the **HSM Credential** field. Select **Use Token Label** and enter the **Token Label**. Click **Set Credential**.

NOTE: Earlier versions of Oracle Key Vault do not facilitate to select Token Label. Using Token Label you can choose any token if multiple tokens are registered.



Prepare for HSM Restore

Cancel Set Credential

If HSM mode is already enabled for this instance, resetting the credential to a different value will break the HSM connection.

Vendor Thales Luna

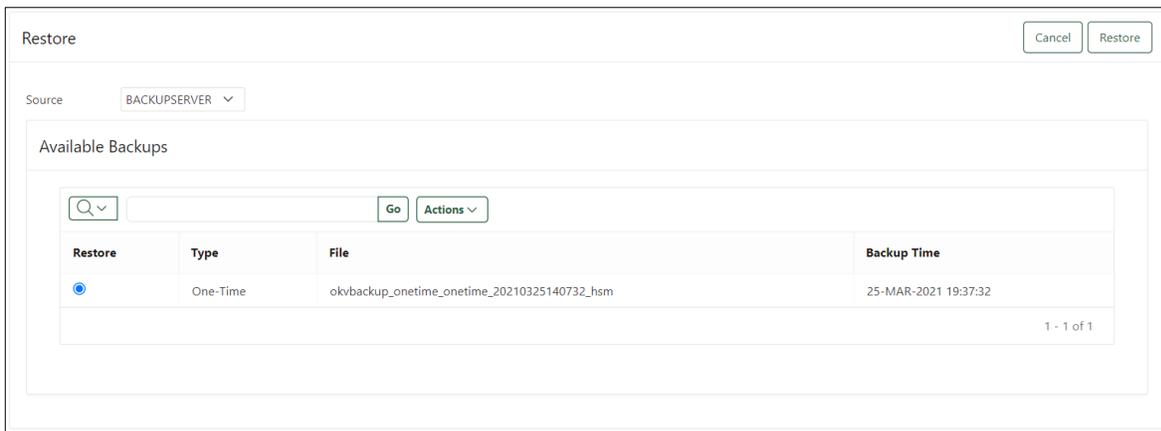
HSM Credential

Re-enter HSM Credential

Use Token Label

Token Label LUNAHA

- For Oracle Key Vault v21.1, click **Settings** from the left sidebar and select **Backup and Restore** from **System Configuration**.
- For Oracle Key Vault v18.5 or below, click **System Backup** from the left sidebar.
- Click **Restore**. Select the **Source** where the backup files are stored. It will list all the backups available on the source. Select the backup that you want to restore.



Restore

Cancel Restore

Source BACKUPSERVER

Available Backups

Go Actions

Restore	Type	File	Backup Time
<input checked="" type="radio"/>	One-Time	okvbackup_onetime_onetime_20210325140732_hsm	25-MAR-2021 19:37:32

1 - 1 of 1

- Click **Restore**.
- Now enter the **Recovery Passphrase** that was set during the Post Installation Step of Oracle Key Vault and click **Restore**. The restore process will start. You will see the **Status** as **ONGOING**.

NOTE: During the Restore process, the Oracle Key Vault management console may not work. Avoid changing any configuration until the restore is completed.

The system will be restored from the backup and then restarted. The system will be available after the completion of restore process.

Contacting customer support

If you encounter a problem during this integration, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer support portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.