

---

# Oracle Key Vault: Integration Guide

---

THALES LUNA HSM AND LUNA CLOUD HSM

## Document Information

<b>Document Part Number</b>	007-000318-001
<b>Revision</b>	G
<b>Release Date</b>	31 January 2023

## Trademarks, Copyrights, and Third-Party Software

Copyright © 2023 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
Configure Oracle Key Vault to use Luna HSM .....	10
Upgrade considerations when Luna HSM is configured .....	14
Backing up and restoring Oracle Key Vault in HSM Mode .....	17
Back up Oracle Key Vault in HSM mode .....	18
Restore Oracle Key Vault in HSM mode .....	19
Enable Luna HSM in OKV Multi-Master Cluster .....	21
Configure Luna HSM for a multi-master cluster starting with single node (recommended) .....	21
Configure Luna HSM for a multi-master cluster with multiples nodes .....	27
Contacting customer support .....	30
Customer support portal .....	30
Telephone support .....	30

## Overview

This document guides security administrators through the steps for integrating Oracle Key Vault with Luna HSM or Luna Cloud HSM. You can use Luna HSM 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 Client Version
Luna HSM	Oracle Key Vault v21.5.0.0.0 Oracle Key Vault v21.4.0.0.0 Oracle Key Vault v21.3.0.0.0 with Multi-Master Cluster	UC 10.4
	Oracle Key Vault v21.1.0.0.0	UC 10.3
	Oracle Key Vault v18.5.0.0.0 with Multi-Master Cluster Oracle Key Vault v18.4.0.0.0 Oracle Key Vault v18.1.0.0.0 Oracle Key Vault v12.2.0.8	UC 10.2

**NOTE:** This integration is tested in both HA mode 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
```

You should see the following output:

```
lunacm (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.
Available HSMs:
Slot Id ->                0
Label ->                  TPA01
Serial Number ->          1312109862206
```

```

Model -> LunaSA 7.7.1
Firmware Version -> 7.7.1
Bootloader Version -> 1.1.2
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 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.

**NOTE:** The removed user will have HSM access until you reboot the client workstation.

## To set up Luna HSM High-Availability (HA)

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 the primary stop functioning for some reason, all calls are 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`.
 

```
# mkdir -p /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 soft 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. Open the `Chrystoki.conf` file in file editor and update the `Chrystoki2` section as follows:

```
Chrystoki2 = {
    LibUNIX = /usr/safenet/lunaclient/lib/libCryptoki2.so;
    LibUNIX64 = /usr/safenet/lunaclient/lib/libCryptoki2_64.so;
}
```

10. 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/
```



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

```
[Linux]
```

```
Chrystoki.conf
```

- Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
- 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
. . .
```

- 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/
```

- Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.
- 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/
```

- 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.

## To configure 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. It is recommended that you should install 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 Luna HSM so that a root of trust (RoT) can be created and used by Oracle Key Vault. It is assumed that you have followed the guidelines explained in the [Prerequisites](#) section and ensured that Luna Client is connected with Luna HSM on Oracle Key Vault.

### Configure Oracle Key Vault to use Luna HSM

**NOTE:** The steps explained here are valid for new Oracle Key Vault installation as well as for upgradation from a lower version of Oracle Key Vault to Oracle Key Vault 21.x. Execute the steps as per your Oracle Key Vault and Luna Client versions.

1. Login to Oracle Key Vault server through SSH as user `support`, and switch user (su) to `root`.

**NOTE:** Skip steps 1-9 if you are using Luna Client v6.x or Standalone Luna Cloud HSM service with minimum client package.

2. Add the Oracle user to the `hsmusers` group.

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

3. Reboot the Oracle Key Vault for the changes to take effect.

```
# reboot
```

4. Login to Oracle Key Vault server through SSH as user `support`, and switch user (su) to `root`.

**NOTE:** Skip steps 4-9 and start directly from step 10 if you are using Oracle Key Vault v21.2 or lower. These steps are applicable for Oracle Key Vault v21.3 onwards.

5. From Oracle Key Vault v21.3 onwards, Oracle provides an interface to enable your Luna HSM using Luna client other than v6.x. Go to the following directory:

```
# cd /usr/local/okv/hsm/generic
```

6. Open the `okv_hsm.conf` file in file editor and update as follows:

**Note:** All parameters are required but `PRESERVED_FILES` parameter will not be used until the next major version upgrade.

```
# The vendor name, to be displayed on the HSM page on the management
console.
VENDOR_NAME="Thales_Luna"

# The location of the PKCS#11 library. This file must be preserved on
upgrade.
PKCS11_LIB_LOC="/usr/safenet/lunaclient/lib/libCryptoki2_64.so"

# A colon-separated list of the full paths of files and directories
that must be preserved on upgrade.

PRESERVED_FILES="/usr/safenet/lunaclient:/etc/Chrystoki.conf:/usr/safe
net/lunaclient/lib/libCryptoki2_64.so"
```

7. Open the `okv_hsm_env` file in file editor and update as follows:

```
# Below is an example. Remove the '#' character to uncomment the line.
#EXAMPLE_ENV_VAR_NAME="EXAMPLE_ENV_VAR_VALUE"

ChrystokiConfigurationPath="/etc"
```

8. Open the `okv_hsm_mid_upgrade` file in file editor and update as follows:

**NOTE:** This script is used during upgrades only, when you upgrade the Oracle Key Vault. If you are upgrading from Oracle Key Vault v21.3 to any above version. You must refer the [Upgrade considerations when Luna HSM is configured](#).

```
#####
#
# Do not make changes above this line
#####
#
# For now, this script does nothing, so log it and exit.
logger -t "${LOGTAG}" -p "${LOGDEBUG}" "Adding hsmusers group"
```

```

sudo groupadd hsmusers
exit ${DBFW_PM_CHANGED}

# Until changes are added, exit indicating that no changes occurred.
#exit ${DBFW_PM_NO_CHANGE_REQUIRED}

# If changes are made and were successful, you should exit like the
commented code below:
#exit ${DBFW_PM_CHANGED}

```

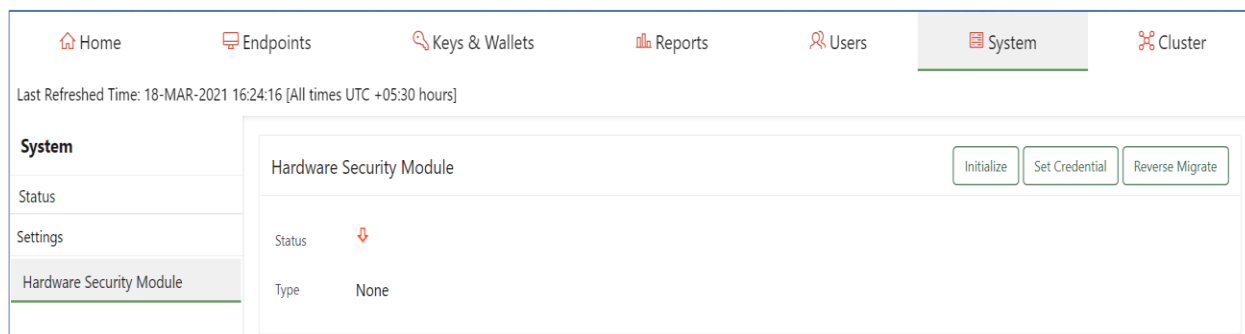
9. Reboot the Oracle Key Vault for the changes to take effect.

```
# reboot
```

10. Oracle Key Vault provides a management console which can be accessed through [https://<Oracle\\_Key\\_Vault\\_Server\\_IP>](https://<Oracle_Key_Vault_Server_IP>) in the web browser.
11. 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.

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



15. Click **Initialize**. The **Initialize HSM** dialog will appear on the screen.
16. Open the **Vendor** drop-down menu and select the Vendor.

For Oracle Key Vault v21.3 onwards, when using Luna Client other than v6.x, you must choose Vendor as per the `VENDOR_NAME` defined in `okv_hsm.conf` file.

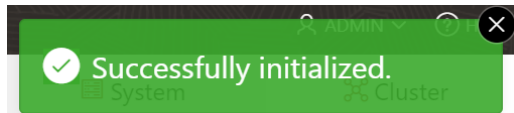
For Oracle Key Vault v21.2 or below, choose **Thales** as a Vendor listed at top position.

**NOTE:** In earlier versions of Oracle Key Vault (18.4 or lower), Select the SafeNet in Vendor drop-down menu, Thales is available since Oracle Key Vault v18.5 onwards.

17. Enter the **HSM Credential** and **Recovery Passphrase**. The HSM Credential is the partition password. The Recovery Passphrase was set during the post Installation setup of Oracle Key Vault. Select the **Use Token Label** checkbox and then enter the **Token Label**.

**NOTE:** Earlier versions of Oracle Key Vault (18.3 or lower) do not support using the Token Label. From Oracle Key Vault 18.4 onwards, use Token Label and provide the name of the desired partition to use, even if multiple partitions are registered.

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



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

**NOTE:** If you change the HSM credential after HSM initialization, you must need to update the HSM credential on the Oracle Key Vault server using the `Set Credential` option.

20. Verify the master encryption key generated on the partition by executing the 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.

## Upgrade considerations when Luna HSM is configured

**Note:** These steps are applicable for Oracle Key Vault v21.3 onwards when you integrated and enabled Oracle Key Vault to use Luna Client other than v6.x.

Follow the [Oracle Key Vault Upgrade documentation](#) for upgrading your Oracle Key Vault. The instructions provided here are required when Luna HSM is integrated and enabled for RoT.

If you have Oracle Key Vault v21.3 or above installed using Luna Client other than v6.x and you are upgrading to higher version of the Oracle Key Vault that is supported, create the pre-upgrade or post-upgrade script mentioned below and execute them as instructed.

**NOTE:** These pre-upgrade or post-upgrade scripts are useful for Oracle Key Vault administrators to ensure that all Luna HSM-related configurations are as expected before the upgrade begins and after the upgrade completes.

1. Log in to Oracle Key Vault server through SSH as user `support` and switch user (`su`) to `root`.
2. Create pre-upgrade or post-upgrade scripts in the `/opt` directory and execute them when necessary.
3. Create a `pre-upgrade-luna.sh` with the following contents that will check the Luna HSM connectivity before upgrade.

```

#!/bin/bash
chown -R root:root /etc/Chrystoki.conf
chmod 644 /etc/Chrystoki.conf

```

```

chmod -R g-s /usr/safenet/lunaclient/cert
chown -R root:root /usr/safenet/lunaclient/cert
chmod -R 755 /usr/safenet/lunaclient/cert
chmod -R g-s /usr/safenet/lunaclient/configData
chown -R root:root /usr/safenet/lunaclient/configData
chmod -R 755 /usr/safenet/lunaclient/configData
chmod -R g-s /usr/safenet/lunaclient/data
chown -R root:root /usr/safenet/lunaclient/data
chmod -R 777 /usr/safenet/lunaclient/data
sudo -u oracle /usr/safenet/lunaclient/bin/vtl listslots

```

4. Create a `post-upgrade-luna.sh` with the following contents that will check the Luna HSM connectivity after upgrade.

```

#!/bin/bash
gpasswd --add oracle hsmusers
chown -R root:hsmusers /etc/Chrystoki.conf
chmod 660 /etc/Chrystoki.conf
chmod -R 755 /usr/safenet/lunaclient/bin
chmod -R 755 /usr/safenet/lunaclient/lib
chmod -R 755 /usr/safenet/lunaclient/plugins
chown -R root:hsmusers /usr/safenet/lunaclient/cert
chmod -R 2770 /usr/safenet/lunaclient/cert
chmod 664 /usr/safenet/lunaclient/cert/client/*
chmod 664 /usr/safenet/lunaclient/cert/server/*
chown -R root:hsmusers /usr/safenet/lunaclient/configData
chmod -R 2770 /usr/safenet/lunaclient/configData
chmod 664 /usr/safenet/lunaclient/configData/token/001/*
chown -R root:hsmusers /usr/safenet/lunaclient/data
chmod -R 2770 /usr/safenet/lunaclient/data
chmod -R 2777 /usr/safenet/lunaclient/data/*
sudo -u oracle /usr/safenet/lunaclient/bin/vtl listslots

```

5. While upgrading, you must run `pre-upgrade-luna.sh` before running the upgrade command `/usr/bin/ruby /images/upgrade.rb --confirm` mentioned in the [Oracle Key Vault Upgrade documentation](#).

**Caution:** Do not run the Oracle Key Vault `upgrade.rb` script without running the `pre-upgrade-luna.sh`. Otherwise, the Oracle Key Vault upgrade may fail. As mentioned

in the Oracle Key Vault documentation, you must have pre-upgrade backup of the OKV server to start again in case of failure.

6. Ensure that the output of the `pre-upgrade-luna.sh` displays the Luna SA information similar to the image below:

```
[root@okv opt]# ./pre-upgrade-luna.sh
v1 (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.

Number of slots: 1

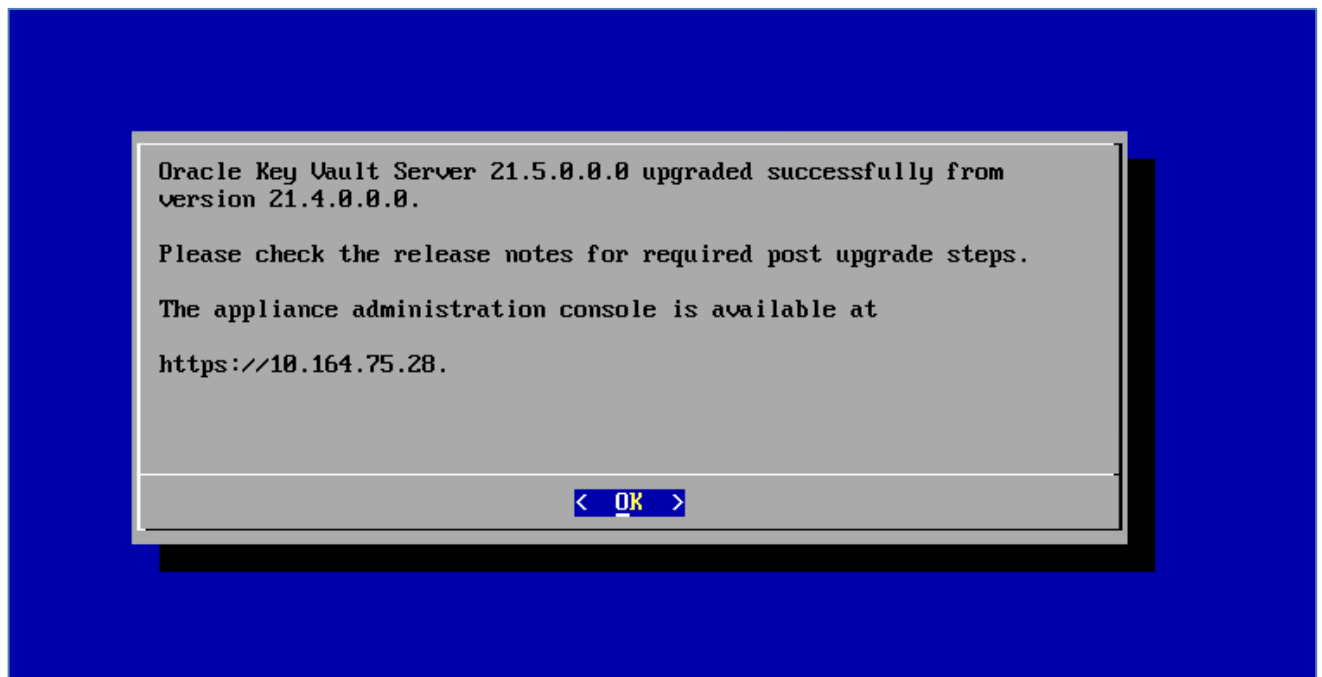
The following slots were found:

Slot Description          Label          Serial #          Status
=====
 0 HA Virtual Card Slot  TPA-HA        11312109862206   Present
[root@okv opt]#
```

7. Follow the Oracle Key Vault Upgrade documentation and run the upgrade script provided with the upgrade ISO.

```
root# /usr/bin/ruby /images/upgrade.rb -confirm
```

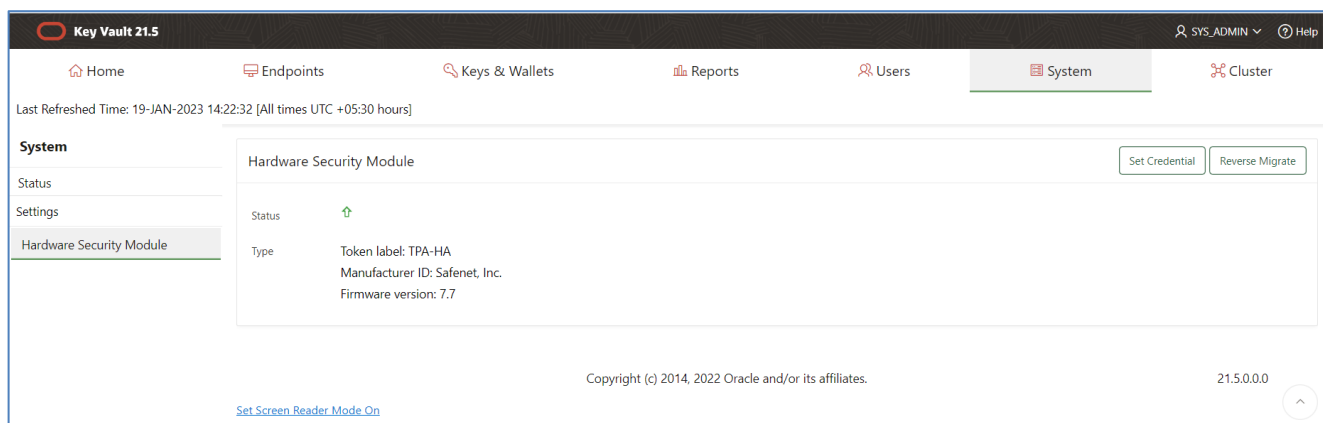
When the upgrade gets completed successfully, the screen with heading `Oracle Key Vault Server new_software_release` appears, wherein `new_software_release` indicates the release number of the upgraded version.



8. Log in to the Oracle Key Vault management console as a user with system administrative privileges.
9. Click the **System** tab.
10. Click **Settings**. Under **Network Services**, click **HSM**.
11. In the left sidebar, click **Hardware Security Module**.



## 12. Verify that Luna HSM is enabled in the upgraded Oracle Key Vault version.



## 13. Login to Oracle Key Vault server through SSH as user `support`, and switch user (`su`) to `root`.

## 14. Execute `post-upgrade-luna.sh` and ensure that Luna HSM information appears after the post upgrade with the output “Adding user oracle to group hsmusers”, as indicated in the image below.

```
[root@okv opt]# ./post-upgrade-luna.sh
Adding user oracle to group hsmusers
v1 (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.

Number of slots: 1

The following slots were found:

Slot Description          Label                Serial #             Status
=====
  0 HA Virtual Card Slot TPA-HA                11312109862206      Present
[root@okv opt]#
```

## 15. Proceed to follow the post-upgrade steps as per the [Oracle Key Vault documentation](#).

In case `post-upgrade-luna.sh` fails to display Luna HSM information, contact Thales Customer support. Do not restart the Oracle Key Vault server.

## 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 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 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

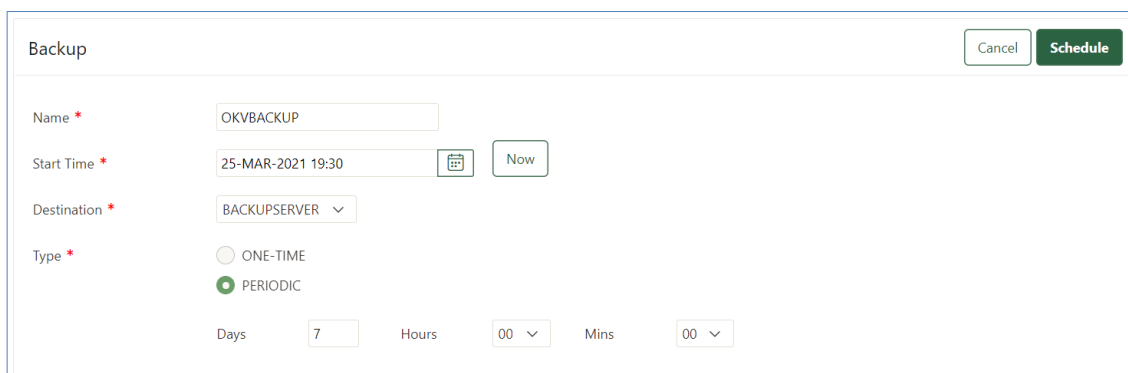
1. Log in to the Oracle Key Vault management console as a user with System Administrator privileges.
2. For Oracle Key Vault v21.1 or above, select the **System** > **Settings** and then click **Backup and Restore** under **System Configuration**. A list of scheduled and completed backups will be displayed.
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:
  - a. **Destination Name:** Specify any destination name.
  - b. **Transfer Method:** This is by default set to SCP to allow secure copy of files.
  - c. **Hostname:** Enter the IP address of the backup destination. If DNS is configured enter the Hostname.
  - d. **Port:** Enter Port number for SCP. The default port number is 22.
  - e. **Destination Path:** Enter the Actual path on the backup destination.
  - f. **Username:** Enter the username with read-write permission of Destination Path.
  - g. **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.

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.



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 or above, click **Settings**. Under **Network Services**, click **HSM**.
3. For Oracle Key Vault v18.5 or below in the left sidebar, click **Hardware Security Module**.
4. Validate the HSM status if the **Status** appears as disabled. Click **Set Credential**. The **Prepare for HSM Restore** dialog appears.

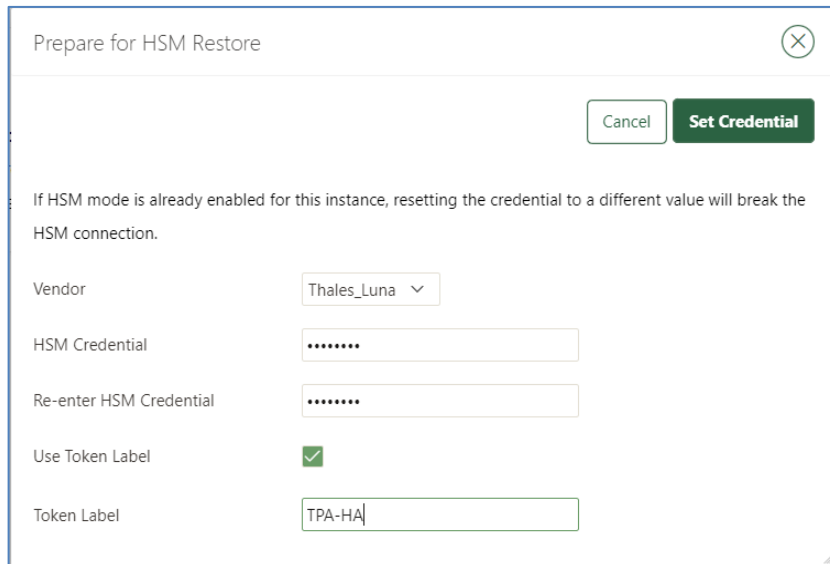
**NOTE:** Skip step 4-6, if HSM status appears to be enabled with Green Arrow pointing towards UP.

5. Open the **Vendor** drop-down menu and select the **Vendor**.

- For Oracle Key Vault v21.3 onwards, when using Luna Client other than v6.x, you must choose Vendor as per the **VENDOR\_NAME** defined in `okv_hsm.conf` file.
- For Oracle Key Vault v21.2 or below, choose **Thales** as a Vendor listed at top position.

**NOTE:** In earlier versions of Oracle Key Vault (18.4 or lower), select **SafeNet** in Vendor drop-down menu. **Thales** is available since Oracle Key Vault v18.5 onwards.

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



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

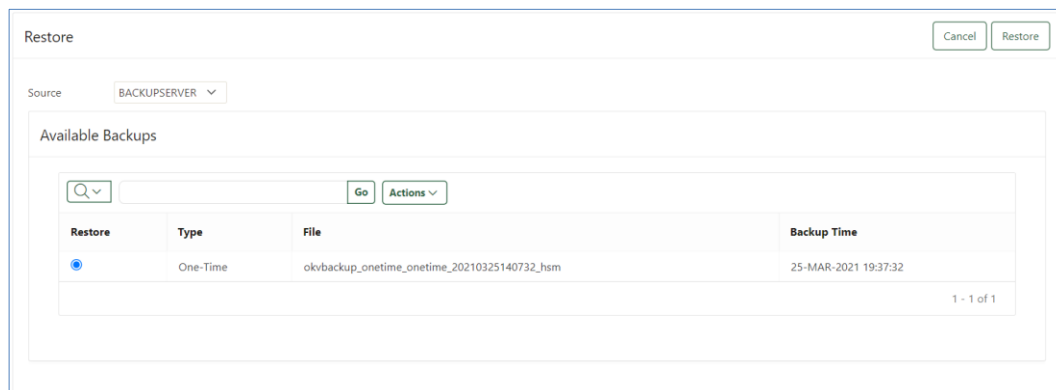
Token Label TPA-HA

**NOTE:** Earlier versions of Oracle Key Vault (v18.3 or below) do not facilitate to select Token Label. Using Token Label you can choose any token if multiple tokens are registered.

7. For Oracle Key Vault v21.1 or above, click **Settings** from the left sidebar and select **Backup and Restore** from **System Configuration**.

8. For Oracle Key Vault v18.5 or below, click **System Backup** from the left sidebar.

9. 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

Search: [ ] 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

10. Click **Restore**.

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

Last Restore Details			
Restore Time	Destination Name	Run Error	Status
19-JAN-2023 18:09:33	BACKUP_SERVER	-	ONGOING

row(s) 1 - 1 of 1

**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.

## Enabling Luna HSM in OKV Multi-Master Cluster

You can configure Luna HSM in a multi-master cluster with a single node or multiple nodes by using one of the following methods:

**NOTE:** In a multi-master Oracle Key Vault installation, any Key Vault node in the cluster can use any HSM. The nodes in the multi-master cluster will use different TDE wallet passwords and RoT keys and may or may not use different HSM credentials, depending on how you choose to configure each cluster node.

- > [Configure Luna HSM for a multi-master cluster starting with single node \(recommended\)](#)
- > [Configure Luna HSM for a multi-master cluster with multiples nodes](#)

### Configure Luna HSM for a multi-master cluster starting with single node (recommended)

To use an HSM with a multi-master cluster, you should start with a single HSM-enabled node and then add additional HSM-enabled nodes using the node induction process. Here are the steps:

- > [Convert an existing Oracle Key Vault server into the first node of the cluster](#)
- > [HSM-enable the first node](#)
- > [HSM-enable the candidate node before adding it to the cluster](#)
- > [Add the HSM-enabled candidate node to the cluster using an HSM-enabled \(first\) controller node](#)

**NOTE:** If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled. The Add Node to Cluster page on the controller node will require HSM credentials of the controller node.

## Convert an existing Oracle Key Vault server into the first node of the cluster

To create a cluster, convert an existing standalone Oracle Key Vault server into the first node of the cluster. This first node is called the initial node or controller node. You can use this node to add one or more nodes to the cluster. The node operates in read-only restricted mode until it is part of a read-write pair. To convert a node into first node, complete the following tasks:

1. Perform a server backup.
2. Log into the Oracle Key Vault management console as a user who has the System Administrator role.
3. If the Oracle Key Vault server was upgraded from a release earlier than Oracle Key Vault release 12.2 (bundle patch 8), then generate and activate (rotate) a new certificate for the node.
4. Select the **Cluster** tab.
5. The Configure as Candidate Node page appears, with the IP address of the current server listed in the **Current Server IP** field.
6. On the **Configure as Candidate Node** page, enter the following information:

- a. **First Node of Cluster:** Select the **Yes** button.
  - b. **Node Name:** Enter a unique name for this node. You cannot change this name after it has been accepted in the name resolution process.
  - c. **Cluster Name:** Enter a name for this cluster of nodes. You cannot change this name after it has been accepted in the name resolution process.
  - d. **Cluster Subgroup:** Enter a name for this sub-group of nodes, such as a data center name or a logical group name. You cannot change this name after it has been accepted in the name resolution process.
7. Click the **Convert to Candidate Node** button. After the conversion process is completed, the **Cluster Management** page will appear on screen and you'll be able to operate the node in read-only restricted mode. You can verify this by checking the **Cluster Details**, as shown below.

Select Node	Node ID ↑	Node Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Node Version
<input type="checkbox"/>	1	<a href="#">okv005056aa3535</a>	10.124.138.135	Read-Only Restricted	ACTIVE	-	mysubgroup	7/14/2021 1:14:26 PM	-	18.5.0.0.0

## HSM-enable the first node

Refer to [Configuring Oracle Key Vault to use Thales Luna HSM](#) to enable the HSM on the first node.

## HSM-enable the candidate node before adding it to the cluster

Refer to [Configuring Oracle Key Vault to use Thales Luna HSM](#) to enable HSM on candidate node.

## Add the HSM-enabled candidate node to the cluster using an HSM-enabled first (controller) node

1. Perform a backup of the controller node before continuing.
2. Ensure that the following network requirements are in place:
  - a. There is good network connectivity between the servers that host the controller node and the candidate node.
  - b. The ports that are required for Oracle Key Vault are open in the network firewall. These ports are described in Network Port Requirements in [Oracle Key Vault Documentation](#).
3. Log into the first (controller) node Oracle Key Vault management console as a user who has the System Administrator role. You can use any existing node, including the first node that does not have a read-write peer to be the controller for this operation. If necessary, add a read-only node first.
4. Select the **Cluster** tab.
5. Click **Add**.
6. In the **Recovery Passphrase of the Cluster**, enter the recovery passphrase. This value will be used later when you pair with the candidate node.

**Add Candidate Node to Cluster** Cancel Add Node

This OKV cluster node, also referred to as the "Controller" node for this cluster operation will add the "Candidate" node to the cluster. The controller node and candidate node need to exchange information, like the IP Address and Certificates in order for the Controller node to seed the candidate node.

Ensure that the candidate node has been configured with the controller node information before clicking "Add Node".

The seeding process of the candidate node can be tracked from the cluster Management page by clicking the name of the candidate node. Once the candidate node is part of the cluster, its status will show as ACTIVE on the Management page of the controller node.

**Add Cluster Details**

Recovery Passphrase of the Cluster \*

7. Select **Yes** for **Add Node as Read-Write Peer**.
8. Enter the following details under **Add Candidate Node Details**. When you enter these details, do not save any of this information or click the **Add Node** button until you reach Step 9.
  - a. **Node ID:** Select a unique ID for the candidate node. Remember that after you create this ID, you cannot change it.
  - b. **Node Name:** Enter a unique name of the candidate node. After you create this name, you cannot change it.
  - c. **Cluster subgroup:** Enter the sub-group name for the candidate node. You can provide an existing subgroup name. If you provide a subgroup name that does not exist, it will be created. Remember that you cannot change the subgroup of this node after the node joins the cluster.

- d. **IP Address:** Enter the IP address of the candidate node.

**Add Candidate Node Details**

Add Node as Read-Write Peer ⓘ \*  No  Yes

Node ID ⓘ \* 02 Ensure the Candidate node ID is unique in the cluster!

Node Name \* node2

Cluster Subgroup ⓘ \* mysubgroup

Cluster Name mycluster

IP Address \* 10.124.138.136

Certificate of Candidate Node ⓘ \*

9. In a new browser window, log into the Oracle Key Vault management console of the candidate node as a user who has the System Administrator role.
10. Select the **Cluster** tab. The **Configure as Cluster Candidate** page is displayed.
11. For **First Node of Cluster**, select **No**.
12. For **Recovery Passphrase of the Cluster**, enter the recovery passphrase of the cluster that you created earlier for the controller node.

**Convert to Candidate Node**

**Configure as Candidate Node**

Current Server IP 10.124.138.136

First Node of Cluster \*  No  Yes

This OKV server, also referred to as the "Current Server", will be converted to a "Candidate" node before it can be added to the cluster by a "Controller" node in the cluster. The controller node and this server need to exchange information, like the IP address and certificates in order for the controller node to seed this server after it is converted to a candidate node.

During the seeding process, all the data on this candidate node will be deleted and the candidate node will also be rebooted.

This server will be part of the cluster, once the status of the converted candidate node is ACTIVE on the Management page of the controller node.

**Add Cluster Details**

Recovery Passphrase of the Cluster \*

13. For **IP Address**, enter the IP address of the controller node.



14. In the browser window for the controller node, scroll to the bottom of the screen. Select and copy the entire node certificate.

The screenshot shows the 'Add Controller Node Details' form. The 'Certificate of Controller Node' field is selected, displaying a long certificate string. The string starts with '-----BEGIN CERTIFICATE-----' and ends with '-----END CERTIFICATE-----'. The certificate content is a base64-encoded X.509 certificate.

15. In the browser window for the candidate node, paste the certificate copied from the controller node into the **Certificate of the Controller Node** field.

The screenshot shows the 'Add Controller Node Details' form. The 'Certificate of Controller Node' field is pasted with the certificate string from the controller node. The string is the same as in the previous screenshot, starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'.

**CAUTION:** Check the recovery passphrase, IP address, and the pasted certificate very carefully to ensure that you copied it correctly. If there is an error after you click Convert to Candidate Node, you will need to reinstall Oracle Key Vault.

16. Click **Convert to Candidate Node**. After the conversion is completed, the screen gets refreshed and displays the certificate of the candidate node. The **Adding Candidate Node to Cluster** page is displayed. This can take several minutes.
17. Select and copy the entire candidate node certificate.

The screenshot shows the 'Adding Candidate Node to Cluster' page. The 'Candidate Node Certificate' field is selected, displaying a long certificate string. The string starts with '-----BEGIN CERTIFICATE-----' and ends with '-----END CERTIFICATE-----'. The certificate content is a base64-encoded X.509 certificate.

18. In the browser window of the controller node, paste the certificate copied from the candidate node into the **Certificate of Candidate Node** box.

**Add Candidate Node Details**

Add Node as Read-Write Peer  No  Yes

Node ID  Ensure the Candidate node ID is unique in the cluster!

Node Name

Cluster Subgroup

Cluster Name

IP Address

Certificate of Candidate Node 

```
-----BEGIN CERTIFICATE-----
MIIFFSTCCAzGgAwIBAgIJAk9xBlzRgDIsMA0GCSqGSIb3DQEBCwUAMDsXOTA3BgNV
BAMMFEFwU19DQV9DZXJ0LWZiZTJwZjZyLWFlZjEtNGMzIi1OTgzLWUzYjUzNjIz
ZWVjMDRlFw0yMTA2MjcyMjU2MjZaFw0yMzA2MjcyMjU2MjZaMDxOTA3BgNVBAMM
MEFwU19DQV9DZXJ0LWZiZTJwZjZyLWFlZjEtNGMzIi1OTgzLWUzYjUzNjIzZWVj
MDCCAlIwDQYJKoZIhvcNAQEBBQADggIPADCCAgogCggIBAsv1CR4JnICot5pZ1Su
Wna7Rmf80H5JmlJ5ZUQ9x1KkruL5WY8X5nUc6EXCiZSt/3/pBNVg02WxcLx07P+
1A6wy5wS2XavzYxJkKof35bdrBba/ALGfFtvj/3FEukLgGGuqe+6zvoEjyOR
T0Je2dm6H2G2EiWewyLzU4dofX6X+KArS8XhPYSrUWJra5JFAv9h3g5SJPa2
gQ51wSneI7LHH2p+ROR16q6NkDsQHnywC9GmBm2nn7cuhs8/vy2qtLcdABFjCD
5/tzJ9hnuwKussbqM8MIRgRAlYkYgMepSv+e9VGbz35ISYojd09Jg2GhaWkQJNF
T4X/8FleecD2bc1NwGstjToR5PefizEoqBgaIDYRKC89n9LQwsg7W82UJfFGKk
b2ar7Zur9HLyQM8XEaIVFQOgvr6aXLfARF9rDZIRzpzsucqJR/4qUo32IdmWp+9
Y6nDgvmCvaFonThCFYgaXd9AHM6EPgqtTptftH004C8j9Gr+aNIqEkrRET+hmmKWh
bXSj7nw71EK0ia5eBLYj4pEzWnvg5cYUpLJUGATbCDzHTKSufVKGaYvVdh+Y6GD
b3KbEsF/fvJl/yj2H1N16iR/27eBs6kTavE2u+uLmIgcLwDOAVET8ywkJGpLsVbz
-----
```

19. Add **HSM Credential** that is partition password.

**Add Controller Node Details**

HSM Credential

Node Name

IP Address

Certificate of Controller Node 

```
-----BEGIN CERTIFICATE-----
MIIFFSTCCAzGgAwIBAgIJAk9xBlzRgDIsMA0GCSqGSIb3DQEBCwUAMDsXOTA3BgNV
BAMMFEFwU19DQV9DZXJ0LWZiZTJwZjZyLWFlZjEtNGMzIi1OTgzLWUzYjUzNjIz
ZWVjMDRlFw0yMTA2MjcyMjU2MjZaFw0yMzA2MjcyMjU2MjZaMDxOTA3BgNVBAMM
MEFwU19DQV9DZXJ0LWZiZTJwZjZyLWFlZjEtNGMzIi1OTgzLWUzYjUzNjIzZWVj
MDCCAlIwDQYJKoZIhvcNAQEBBQADggIPADCCAgogCggIBAMFJYX05jh+/q6keqWt
xZLBLEkKXc4cg0vNh9Vc+5ak5056Cw3+A-DqkRwYfEnYKjUNsXRT6R1K7EUSq
uipozX7fym9Ejw1EL+R2F3E0y8RDaKdIb7gr+uxjdes1oU17tgqGLHRI0sX18
fpyRWjys1qwyD5Rj9uXmVBUJn6yY7pJKhMOvH04hGowNvN1.IQABenYDdIqNgA
qIUkH0hTrZpqqckwSrYDdxQ1fWguYsh9GbanAsScrSmvBbnz03HNN1KK/gqkvjJ5
Uis0yqWqRiVXzicsaM2Lyy+KFigXKXh6q8SaI8Lcwp6f7Z+1kt2koEadPsg5G
/gQw/1Iwtn2Avab2J7c9rsKGIY5TOIFUJ19wlsGS3D1LJgF8g4Fz94OI04k0rPL
Khh5nmVML8FOvDD0cyY7n4NUSMqPvWkT2pT9JSLVMcEzdsMu056sbyVmm/DiYh4
-----
```

20. Click **Add Node**.

21. Click **OK** to confirm in the confirmation dialog box.

This process can take an hour or more, depending on the speed of your server, quality of network, and volume of data in the cluster. During this period, the network management interface of the Oracle Key Vault will be restarted and you might momentarily get a **Server Error 500** on the controller node.

On the candidate node, errors such as **Bad Gateway** may also appear. The candidate node will restart as part of the induction process. This is normal. During the pairing process, the status of the candidate node will appear as **PAIRING** on all cluster nodes.

**Cluster Details** Add Delete Force Delete Disable

Search:

Select Node	Node ID	Node Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Node Version
<input type="checkbox"/>	1	okv005056aa3535	10.124.138.135	Read-Only Restricted	ACTIVE	-	mysubgroup	7/14/2021 1:14:26 PM	-	18.5.0.0.0
<input type="checkbox"/>	2	node2	10.124.138.136	Read-Only Restricted	PAIRING	-	mysubgroup	7/14/2021 3:48:32 PM	-	18.5.0.0.0

1 - 2

22. Verify that after pairing is completed, the status of both the nodes is **ACTIVE** with **Read-Write Peer** mode.

**Current Node Information**

Node Name okv005056aa3535  
Node Type Read-Write  
Cluster Subgroup mysubgroup

**Cluster Information**

Cluster Name mycluster  
Cluster Subgroups mysubgroup  
Maximum Disable Node Duration ⓘ 24 hrs  
Cluster Version 18.5.0.0.0

**Cluster Details** Add Delete Force Delete Disable

Select Node	Node ID ↑↕	Node Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Node Version
<input type="checkbox"/>	1	<a href="#">okv005056aa3535</a>	10.124.138.135	Read-Write	ACTIVE	node2	mysubgroup	7/14/2021 1:14:26 PM	-	18.5.0.0.0
<input type="checkbox"/>	2	<a href="#">node2</a>	10.124.138.136	Read-Write	ACTIVE	okv005056aa3535	mysubgroup	7/14/2021 3:48:32 PM	-	18.5.0.0.0

## Configure Luna HSM for a multi-master cluster with multiples nodes

You can configure HSM for a multi-master Cluster with multiple nodes by completing these tasks:

- > [HSM-enable the first node](#)
- > [Create and copy the bundle after HSM-enabling the first node](#)
- > [Configure the remaining nodes](#)

Before proceeding to the main steps, you should have multi-master cluster setup ready with multiples nodes, as shown below:

**Current Node Information**

Node Name okv005056aa3535  
Node Type Read-Only  
Cluster Subgroup mysubgroup

**Cluster Information**

Cluster Name mycluster  
Cluster Subgroups mysubgroup  
Maximum Disable Node Duration ⓘ 24 hrs  
Cluster Version 18.5.0.0.0

**Cluster Details** Add Delete Force Delete Disable

Select Node	Node ID ↑↕	Node Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Node Version
<input type="checkbox"/>	1	<a href="#">okv005056aa3535</a>	10.124.138.135	Read-Write	ACTIVE	okv005056aa3536	mysubgroup	7/22/2021 12:39:46 PM	-	18.5.0.0.0
<input type="checkbox"/>	2	<a href="#">okv005056aa3536</a>	10.124.138.136	Read-Write	ACTIVE	okv005056aa3535	mysubgroup	7/22/2021 12:55:43 PM	-	18.5.0.0.0

## HSM-enable the first node

Follow the steps in [Configuring Oracle Key Vault to use Thales Luna HSM](#) to enable HSM on the first node. After the HSM is enabled, you can see its status in the Cluster Settings State page.

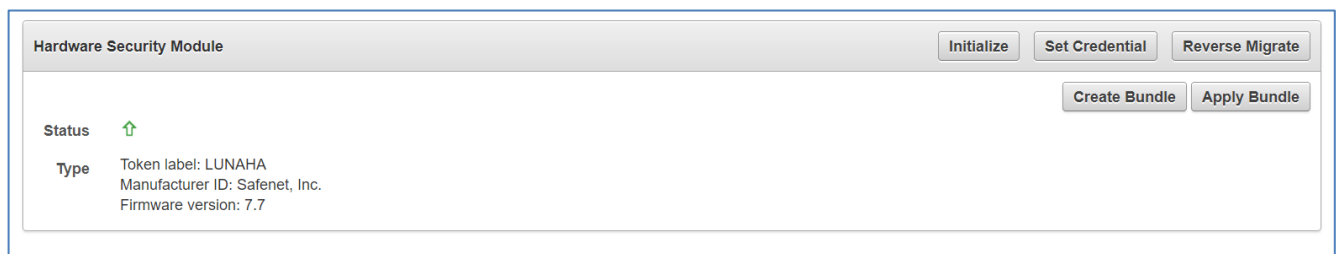
Node ID	Node Name	Audit	FIPS	HSM	SNMP	SYSLOG	DNS
1	<a href="#">okv005056aa3535</a>	✓	✗	✓	✗	✗	✓
2	<a href="#">okv005056aa3536</a>	✓	✗	✗	✗	✗	✓

1 - 2

## Create and copy the bundle after HSM-enabling the first node

After HSM-enabling the first node in the multi-master cluster, you must create a bundle and copy it to the other nodes in the cluster.

1. Log in to the **Oracle Key Vault management** console as a user who has the System Administrator role.
2. Click the **System** tab.
3. For Oracle Key Vault v21.1 or above, click **Settings**. Under **Network Services** click on **HSM**.
4. For Oracle Key Vault v18.5 or below in the left sidebar, click **Hardware Security Module**.
5. On the HSM-enabled node, click **Create Bundle** on the HSM page.



6. In the **Create Bundle** dialog box, make the following changes:
  - a. In the **HSM Credential** field, enter the HSM password.
  - b. In the **Recovery Passphrase** field, enter the recovery passphrase.
  - c. Click the **Create Bundle** button.

7. Log in to Oracle Key Vault server through SSH as user `support`, and switch user (`su`) to `root`.

- Copy the bundle to the `/usr/local/okv/hsm` location on all the other nodes using the IP address.

```
# scp /usr/local/okv/hsm/hmsbundle support@ip_address:/tmp
```

### Configure the remaining nodes

After you configure the first node, you are ready to install the bundle on the remaining nodes. Complete this procedure as soon as possible after you have HSM-enabled the first node and copied the bundle to all other nodes.

- Log in to each node in the cluster using the IP address (except the original HSM-enabled node):

```
# ssh support@ip_address
```

- On each node, switch to the **root** user:

```
# su root
```

- Copy the `/tmp/hmsbundle` file to `/usr/local/okv/hsm/`.

```
# cp /tmp/hmsbundle /usr/local/okv/hsm/
```

- Change the ownership of the **hmsbundle** file to user **oracle** and group **oinstall**.

```
# chown oracle:oinstall /usr/local/okv/hsm/hmsbundle
```

- On each node, except the original HSM-enabled node, click **Apply Bundle** on the **HSM** page, and then follow these steps:
- In the **Recovery Passphrase** field, enter the recovery passphrase.
- Click the **Apply Bundle** button.

**Note:** You must apply the bundle immediately on all nodes before you reverse-migrate the original HSM-enabled node.

- Proceed to HSM-enable each of the remaining nodes in the cluster, using the steps in [Configuring Oracle Key Vault to use Thales Luna HSM](#).
- Verify that the HSM is enabled on every node in the cluster in Cluster Settings State.

Node ID	Node Name	Audit	FIPS	HSM	SNMP	SYSLOG	DNS
1	<a href="#">okv005056aa3535</a>	✓	✗	✓	✗	✗	✓
2	<a href="#">okv005056aa3536</a>	✓	✗	✓	✗	✗	✓

1 - 2

- After you have HSM-enabled on all nodes and verified the replication between all nodes, remove the **hmsbundle** file from all the nodes.

This completes the Luna HSM integration with Multi-Master OKV Cluster.

## 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.