Oracle Key Vault 21.5

nShield® HSM Integration Guide

28 Jul 2023

Contents

1. Introduction

This guide describes how to integrate Entrust nShield Hardware Security Module (HSM) with Oracle Key Vault.

The HSM generates and stores a Root of Trust which protects the security objects used by Oracle Key Vault to safeguard user keys and credentials. The HSM can be used in FIPS 140 Level 2 or Level 3 mode to meet compliance requirements.

Note that:

- An Oracle Key Vault cluster node can have multiple HSMs enrolled, as long as the HSMs are in the same Security World.
- An existing Oracle Key Vault deployment cannot be migrated to use an HSM as a Root of Trust.
- Oracle Key Vault can function only if the RoT stored in the HSM is available.
- To restart or restore Key Vault in HSM mode when Operator Card Set (OCS) protection is used, the OCS for the HSM must be in slot 0 of the HSM.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Oracle Key Vault in the following configurations:

Product	Version
Operating System	Oracle Linux 7 64-bit
Oracle Key Vault Version	21.5

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
12.60.11	12.50.11 (FIPS Certified)	12.60.10	✓	✓	✓

Security World Software	Firmware	Image	OCS	Softcard	Module
12.80.4	12.50.11 (FIPS Certified)	12.80.4	✓	✓	✓
12.80.4	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓
13.3.2	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓

1.2.2. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.3.2	13.2.2 (FIPS Pending)	13.3.2	✓	✓	✓

1.3. Supported nShield functionality

Feature	Support
Key generation	Yes
1-of-N Operator Card Set	Yes
FIPS 140 Level 3 support	Yes
Key management	Yes
k-of-N Operator Card Set	No
Common Criteria support	Yes
Key import	Yes
Softcards	Yes
Load sharing	Yes
Key recovery	Yes
Module-Only key	Yes
Fail over	Yes

1.4. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.
- If nShield Remote Administration is to be used: nShield Remote Administration User Guide_.
- Oracle Key Vault documentation (https://docs.oracle.com/en/database/oracle/key-vault).

In addition, the integration between nShield HSMs and Oracle Key Vault requires:

- A separate non-HSM machine on the network to use as the Remote File System for the HSM. The RFS machine can also be used as a client to the HSM, to allow presentation of Java Cards using nShield Remote Administration. See the nShield Remote Administration User Guide_.
- PKCS #11 support in the HSM.
- A correct quorum for the Administrator Card Set (ACS).
- Operator Card Set (OCS), Softcard, or Module-Only protection.

  If OCS protection is to be used, a 1-of-N quorum must be used.

- Firewall configuration with usable ports:
  - 9004 for the HSM (hardserver).
  - 8200 for Key Vault.

Furthermore, the following design decisions impact how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140 Level 3 standards.

  If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. The OCS can also provide key protection for the Vault master key. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.

- Whether to instantiate the Security World as recoverable or not.

> Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.5. More information

For more information about OS support, contact your Oracle Key Vault sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

ℹ Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

2. Procedures

The high-level procedure to install and configure one or more Oracle Key Vault servers with one or more nShield HSMs is as follows:

1. Install the required number of instances of Oracle Key Vault. For instructions, see the Oracle Key Vault documentation.
2. Install and configure the required number of HSMs and the Security World software, including setting up the Remote File System (RFS) or Remote Administration. For instructions, see the *Installation Guide* for your HSM.
    - nShield HSMs require a separate non-HSM machine on the network to use as the RFS. You must set up this machine and copy the nShield Security World Software files to it before you install the HSM client software on Oracle Key Vault servers.
    - All enrolled HSMs must be in the same Security World and must have access to the OCS in slot 0 if OCS-protection is used. If the HSM whose slot 0 is used is enrolled on each of the Key Vault servers, the Key Vault web user interface has access to all of the HSMs, as long as they are in the same Security World.
    - If dynamic slots are to be used on the HSMs, set up Remote Administration and configure slot mapping.
3. Install the HSM client software on the Oracle Key Vault server(s).
4. Enroll the Key Vault(s) as client(s) of the HSM(s).
5. Enable HSM mode in the Oracle Key Vault web user interface.
6. For a high-availability Oracle Key Vault environment, enroll your HSM and configure initialization of the HSM in each of the nodes.

2.1. Install HSM client software on the Key Vault server

Perform these steps on the Oracle Key Vault server.

For a high-availability Oracle Key Vault environment, perform these steps:

1. In a primary-standby architecture, on both the primary and the standby.
2. In a cluster architecture, on each Key Vault instance to be added to the cluster.

> Primary-Standby configuration is deprecated in Oracle Key Vault version 21.5. Oracle recommends the use of an multi-master cluster deployment instead. See https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/deprecated-features-oracle-key-vault-21.5.html.

To install HSM client software on the Key Vault server:

1. Log into the Oracle Key Vault server as the `support` user using SSH:

   ```
   $ ssh support@<okv_instance>
   <Enter the support user password when prompted>
   ```

2. Switch to root:

   ```
   $ su root
   ```

3. Install the latest version of the Security World software as described in the *Installation Guide* for the HSM.

   > ℹ Entrust recommends that you uninstall any existing nShield software before installing the new nShield software.

4. Create the Security World as described in the *User Guide*, creating the ACS and OCS that you require.

5. As root on the Key Vault server, add the `nfast` group to the `oracle` user:

   ```
   root# usermod -a -G nfast oracle
   ```

6. Switch to the `oracle` user and verify the installation:

   ```
   root# su oracle
   oracle$ PATH=/opt/nfast/bin:$PATH
   oracle$ export PATH
   oracle$ enquiry
   ```

   The mode should say `operational` in the output. For example:

   ```
   Server:
   enquiry reply flags  none
   enquiry reply level  Six
   serial number        nnnn-nnnn-nnnn
   mode                 operational
   version              12.60.7
   speed index          15843
   ```

7. Restart the Oracle Key Vault server for the group change to take effect.

   > ℹ To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

8. As the `root` user, set firewall rules to enable port 9004 for the hardserver (the client process in the nShield Security World software that communicates with the HSM).

2.2. Enroll Key Vault as a client of the HSM

To enroll Key Vault as a client of the HSM:

1. Add the Key Vault server IP address to the client list on the HSM using the front panel or via an update to the Connect configuration file. For instructions, see the *User Guide* for your HSM.
   a. Select privileged on any port.
   b. For a high-availability Oracle Key Vault environment, add the IP addresses of all Key Vault servers to the client list on all HSMs.
2. Switch to the `oracle` user:

   ```
   root# su oracle
   oracle$ PATH=/opt/nfast/bin:$PATH
   oracle$ export PATH
   ```

3. To obtain the ESN and keyhash for the `nethsmenroll` command in the next step, run the `anonkneti` command:

   ```
   anonkneti <HSM IP address>
   ```

4. On the Key Vault server, enroll with the HSM:

   ```
   oracle$ nethsmenroll --privileged <HSM IP address> <HSM ESN> <HSM keyhash>
   ```

5. Run the following command:

   ```
   enquiry
   ```

   Verify that the HSM mode is operational and the hardware status is OK.

6. Configure TCP sockets:

   ```
   oracle$ config-serverstartup --enable-tcp --enable-privileged-tcp
   ```

7. Switch to root and restart the hardserver:

   ```
   oracle$ su root
   root# /opt/nfast/sbin/init.d-ncipher restart
   ```

8. On the Remote File System machine, run the following command:

   ```
   rfs-setup --gang-client --write-noauth <IP address of your Key Vault server>
   ```

9. If OCS protection is intended but the Security World has not been created yet, edit the `cardlist` file to enable Java Cards for use through dynamic slots. If the Security World has been created with this RFS, this configuration is already enabled.

   a. Go to the following directory on the RFS:

   ```
   #/opt/nfast/kmdata/config
   ```

   b. Open the `cardlist` file in a text editor.

   c. Add an asterisk (*) to authorize all Java Cards for dynamic slots.

   If only certain Java Cards are authorized for this use, list them by their serial number. For example:

   ```
   4286005559064791
   4286005559064792
   4286005559064793
   ```

   d. Copy the updated `cardlist` file from the RFS to all clients.

10. On the Key Vault server as the `oracle` user, run the following commands:

```
oracle$ rfs-sync --setup <IP address of Remote File System machine>
oracle$ rfs-sync --update
```

11. As the `root` user, create the `/opt/nfast/cknfastrc` configuration file for PKCS#11 variables. For information on these variables, see the *User Guide* for your HSM.

   a. OCS protection.

   If you are using OCS or Module protection, set `cknfastrc`:

   ```
   CKNFAST_NO_ACCELERATOR_SLOTS=1
   CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm
   ```

   b. Softcard Protection.

   If you are using Softcard protection, then `CKNFAST_LOADSHARING` must be set. This is not supported alongside the Module-only Key protection settings. See also [{xref_known-issues}].

   ```
   CKNFAST_LOADSHARING=1
   CKNFAST_NO_ACCELERATOR_SLOTS=1
   CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm
   ```

   c. Module Protection.

   If you are using Module-Only protection, set `cknfastrc`:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

12. On the Key Vault Server, test PKCS#11 access as follows:

    ```
    oracle$ /opt/nfast/bin/ckcheckinst
    ```

    Select a slot number to run a library test. Various slots are displayed, depending on your configuration.

    Example 1:

    ```
    0 Fixed token "accelerator"
    1 Operator card "OKV_OCS"
    ```

    Example 2:

    ```
    0  Operator card     "OKV_OCS"
    1  Soft token        "OKV_Softcard"
    ```

    Test execution:

    ```
    Test                      Pass/Failed
    ----                      -----------

    1 Generate RSA key pair   Pass
    2 Generate DSA key pair   Pass
    3 Encryption/Decryption   Pass
    4 Signing/Verification    Pass

    Deleting test keys         ok

    PKCS#11 library test successful.
    ```

2.3. Enable HSM mode in Key Vault

After installing HSM software and enrolling Key Vault as an HSM client, you can enable HSM mode with nShield HSM(s) from the Key Vault web user interface. This will protect the Oracle Key Vault Root of Trust key with the HSM.

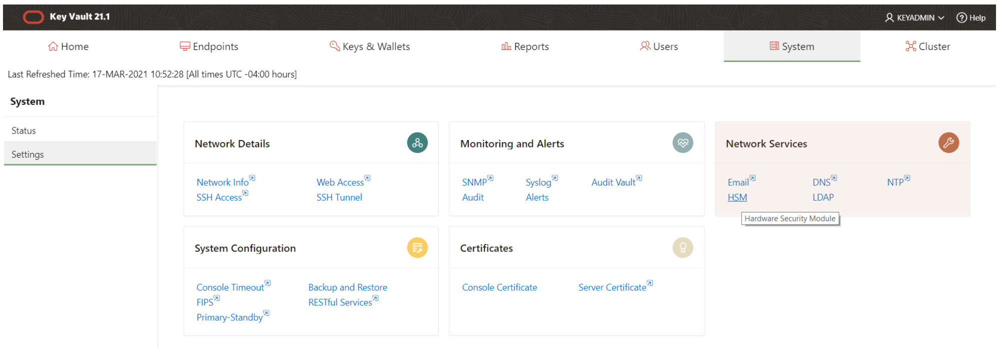
1. Log into the Oracle Key Vault web user interface as a Key Administrator.

   The **Oracle Key Vault Home** page appears.

2. Select the **System** tab.

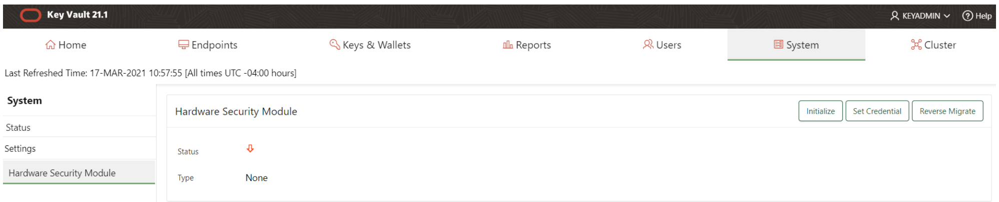
   The **Status** page appears.

3. Select **Settings** on the Left menu.
4. Under **Network Services**, select **HSM**.



Last Refreshed Time: 17-MAR-2021 10:52:28 [All times UTC -04:00 hours]

The **Hardware Security Module** page appears.



Last Refreshed Time: 17-MAR-2021 10:57:55 [All times UTC -04:00 hours]

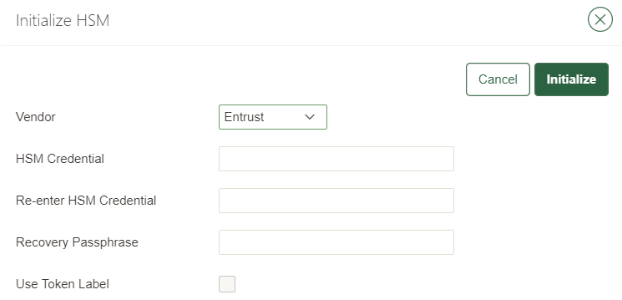
Status ↓

Type None

The red downward arrow shows the non-initialized **Status**. The **Type** field displays **None**.

5. Select **Initialize**.

The **Initialize HSM** dialog appears.



Vendor: Entrust

HSM Credential

Re-enter HSM Credential

Recovery Passphrase

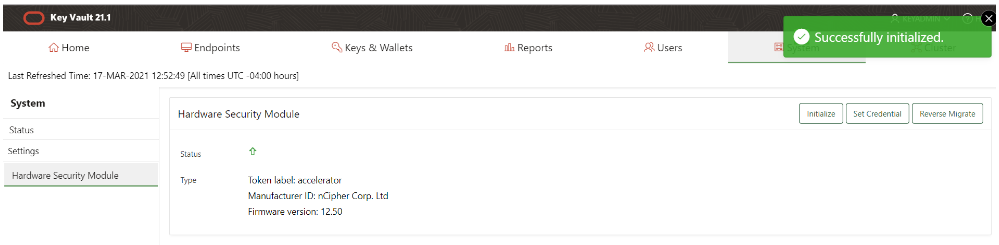
Use Token Label □

6. From the **Vendor** list, select **Entrust**.
7. Enter a password two times: first in **HSM Credential** and second in **Re-enter HSM Credential**.
   - If you are using OCS protection, then your OCS passphrase needs to be entered twice with your card presented in slot 0.
   - If you are using Softcard protection, then the Softcard passphrase needs to be entered twice.
   - If you are using Module-Only protection, enter a password that you set up for this credential check.

The password will be needed in the future, for example for reverse migration.

8. Enter the recovery passphrase for Oracle Key Vault.
9. If you are using token labels, used for OCS protection and Softcards for instance, check the **Use Token Label** checkbox and enter the name of the token.
10. Select **Initialize**.

    At the end of a successful initialize operation, the **Hardware Security Module** page appears. The initialized **Status** is indicated by an green upward arrow. The **Type** field shows details of the HSM in use.



Successfully initialized.

Last Refreshed Time: 17-MAR-2021 12:52:49 [All times UTC -04:00 hours]

Hardware Security Module

Status ⇧

Type Token label: accelerator
Manufacturer ID: nCipher Corp. Ltd
Firmware version: 12.50

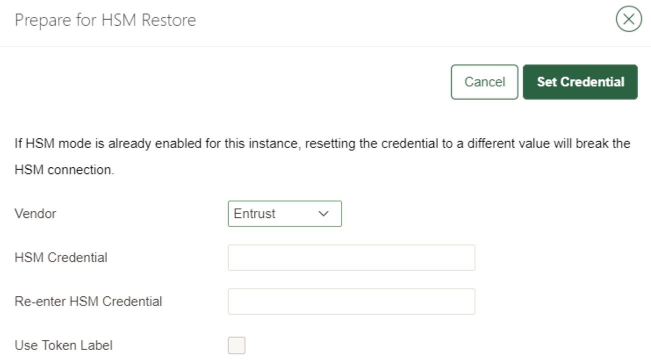
The **Token** label is **accelerator** if Module-Only protection is used.

Only the first two numbers of the firmware are included.

11. After a successful initialize operation of the nShield HSM, run the following command as the `oracle` user on the Key Vault server:

```
oracle$ /opt/nfast/bin/rfs-sync --commit
```

If you change the HSM credential on the HSM after initialization, you must also update the HSM credential on the Oracle Key Vault server: In the **Vendor** list select **Entrust**, then select `Set Credential`.



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

Vendor: Entrust

HSM Credential

Re-enter HSM Credential

Use Token Label □

2.4. Enable the HSM in a Primary-Standby high availability deployment

> Primary-Standby configuration is deprecated in Oracle Key Vault version 21.5. Oracle recommends the use of an multi-master cluster deployment instead. See https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/deprecated-features-oracle-key-vault-21.5.html.

In a high availability Oracle Key Vault installation, you must enable the HSM(s) separately on the servers that you plan to designate as primary and standby before pairing them in a high availability configuration. On the primary server, the HSM(s) will be enabled through the Oracle Key Vault web user interface. On the standby server, the command line interface with SSH will be used to enable the HSM(s).

1. Install Oracle Key Vault on two servers that you mean to designate as primary and standby.
2. Install the nShield Security World software on each Oracle Key Vault server, see Install HSM client software on the Key Vault server.
3. Enroll the primary and standby nodes as clients of the HSM, see Enroll Key Vault as a client of the HSM.
4. From the Oracle Key Vault web user interface, initialize the intended primary server for HSM mode with nShield HSM(s), see Enable HSM mode in Key Vault.
5. On the primary server, run the following commands as the `oracle` user:

```
$ ssh support@<okv_primary_instance>
<Enter password when prompted>
$ su root
root# su oracle
oracle$ rfs-sync --commit
oracle$ cd /usr/local/okv/hsm/wallet
oracle$ scp cwallet.sso support@<okv_standby_instance>:/tmp
oracle$ scp enctdepwd support@<okv_standby_instance>:/tmp
oracle$ cd /usr/local/okv/hsm/restore
oracle$ scp ewallet.p12 support@<okv_standby_instance>:/tmp
```

6. On the standby server, run the following commands as the `root` user:

```
$ ssh support@<okv_standby_instance>
<Enter password when prompted>
$ su root
root# cd /usr/local/okv/hsm/wallet
root# mv /tmp/enctdepwd .
root# mv /tmp/cwallet.sso .
root# chown oracle *
root# chgrp oinstall *
root# cd /usr/local/okv/hsm/restore
root# mv /tmp/ewallet.p12 .
root# chown oracle *
root# chgrp oinstall *
```

7. Continuing as the `root` user, open the `okv_security.conf` file for writing:

   ```
   root# vi /usr/local/okv/etc/okv_security.conf
   ```

   A sample `okv_security.conf` file before enabling HSM mode:

   ```
   SNMP_ENCRYPTION_PWD="01:10:bf3f58671448a5ac2dba1682daf22a92235382c1f9f5b1ab28b3815a70bf2dc3:AlMBqgMWi4PtI2cY1j4Y7Q==
   "
   SNMP_AUTHENTICATION_PWD="01:10:e4dc49617faca046e7e3585f27dbfbe282f16123b762fda17dba6233cab815ec:1a+Gnv9+uF6HsV7peDhm
   /g=="
   SNMP_USERNAME="root"
   SMTP_TRUSTSTORE_PWD="changeit"
   HSM_ENABLED="0"
   FIPS_ENABLED="0"
   HSM_FIPS_ENABLED="1"
   OKV_OCI_INSTALL="DISABLED"
   HSM_TOKEN_LABEL=""
   HSM_KEY_EXTRACTABLE="0"
   OKVAG_LINK_UI="https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/"
   LDAP_TRACE_LEVEL="1"
   OKV_AVS_STATUS="DISABLED"
   OKV_AVS_OKV_HOST_ID=""
   OKV_AVS_AVDF_IP_ADDRESS=""
   HSM_REVERSE_MIGRATE_ENABLED="1"
   ```

8. Make updates to the `okv_security.conf` file as follows:

   a. Set the `HSM_ENABLED` variable to 1. If the variable does not exist, add it and set its value to 1:

      ```
      HSM_ENABLED="1"
      ```

   b. Add the following line:

      ```
      HSM_PROVIDER="2"
      ```

   c. If using Softcards or OCS cards, enter the name of the Card Set:

      ```
      HSM_TOKEN_LABEL="card_set_name"
      ```

9. On the standby server, run `rfs-sync --update` as the `oracle` user:

   ```
   root# su oracle
   oracle$ /opt/nfast/bin/rfs-sync --update
   ```

10. Without restarting the Oracle Key Vault instances, navigate to the web user interfaces of the primary and standby servers and configure primary-standby via the Oracle Key Vault web user interface. For information on the configuration and settings, see the Oracle documentation.

2.5. Configure an HSM for a multi-master cluster

You can configure HSMs in a multi-master cluster with a single node or multiple nodes. 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 can use different TDE wallet passwords (recovery passwords), RoT keys, and HSM credentials.

> To ensure complete security, you must HSM-enable all Oracle Key Vault nodes in the cluster.

> Entrust recommends that you read https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/managing_multimaster.html for details on how to set up clusters.

This guide will set up the cluster from scratch. If you already have a cluster in place, read the documentation above.

To use an HSM within a cluster, start with a single node and add additional nodes as required.

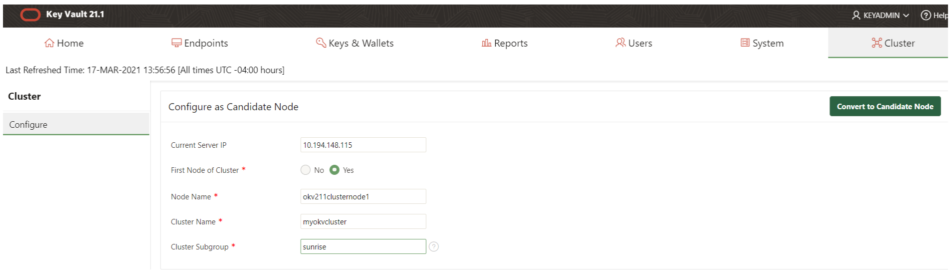
There are two different procedures for configuring an HSM for a multi-master cluster. The first is configuring an HSM for a multi-master cluster starting with a single node and the second is configuring an HSM for a multi-master cluster starting with multiple nodes. Both will be described in this document but Oracle recommends the first method.

2.5.1. Oracle recommendation to configure an HSM for a multi-master cluster starting with a single node

Oracle recommends the following steps to configure an HSM for a multi-master cluster starting with a single node:

1. Convert an Oracle Key Vault server into the first node of the cluster.
   a. Create the cluster by configuring the first node of the cluster.
   b. Select the **Cluster** tab.
   c. On the left menu, select **Configure**.

   The **Configure as a Candidate Node** page appears. For example:



Last Refreshed Time: 17-MAR-2021 13:56:56 [All times UTC -04:00 hours]

Configure as Candidate Node

Current Server IP: 10.194.148.115

First Node of Cluster *: ○ No ● Yes

Node Name *: okv211clusternode1

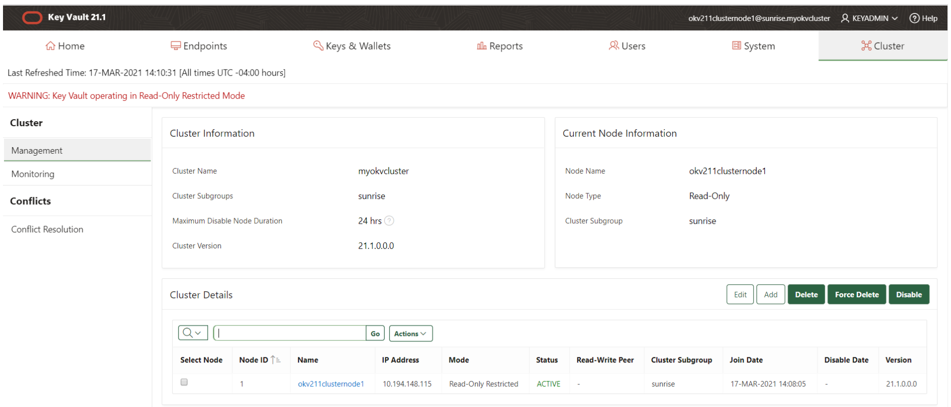
Cluster Name *: myokvcluster

Cluster Subgroup *: sunrise

- For **Current Server IP**, enter the server IP address.
- For **First Node of Cluster**, select **Yes** if this is the first node, otherwise set it to **No**.
- **Node Name** is pre-populated with the host name of the OKV server.
- For **Cluster Name**, enter the name for the cluster.
- For **Cluster SubGroup**, enter the name of the group.

> If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled.

d. Select **Convert Candidate Node**. The **Cluster Information** page appears.



Last Refreshed Time: 17-MAR-2021 14:10:31 [All times UTC -04:00 hours]

WARNING: Key Vault operating in Read-Only Restricted Mode

Cluster Information

Cluster Name	myokvcluster
Cluster Subgroups	sunrise
Maximum Disable Node Duration	24 hrs
Cluster Version	21.1.0.0.0

Current Node Information

Node Name	okv211clusternode1
Node Type	Read-Only
Cluster Subgroup	sunrise

Cluster Details

Select Node	Node ID	Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Version
□	1	okv211clusternode1	10.194.148.115	Read-Only Restricted	ACTIVE	-	sunrise	17-MAR-2021 14:08:05	-	21.1.0.0.0

2. HSM-enable the first node before adding any new nodes, see Enable HSM mode in Key Vault.
3. HSM-enable the candidate node before adding it to the cluster, see Enable HSM mode in Key Vault.
4. Add the HSM-enabled candidate node to the cluster using a controller node that is also HSM-enabled. Note the following:
   a. If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled.
   b. The Add Node to Cluster page on the controller node will require the controller node's HSM credential.

Refer to https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/managing_multimaster.html for details on how to add a candidate node to the cluster.

2.5.2. Oracle recommendation to configure an HSM for a multi-master cluster with multiple nodes

Oracle recommends the following steps to configure an HSM for a multi-master cluster with multiple nodes:

1. Convert an Oracle Key Vault server into the first node (the controller node) of the cluster. The steps for this are described above.
2. Add the candidate nodes to the cluster using the controller node.

   Refer to https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/managing_multimaster.html for details on how to add a candidate node to the cluster.

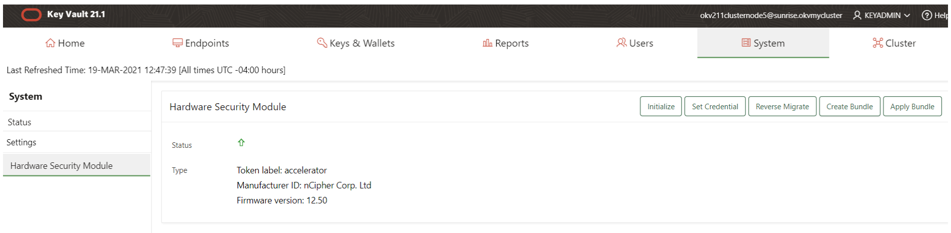
3. HSM-enable the controller node (first node).

   Follow instructions to enable HSM mode on the first node of the cluster, see Enable HSM mode in Key Vault.

4. If multiple nodes are being used in the cluster, create an HSM bundle from the controller node and apply it to the candidate node(s).

   You can configure HSM for the other nodes by copying information from the HSM-enabled controller node in the cluster. You do that by creating a bundle and applying the bundle to the candidate nodes in the cluster.

   a. On the controller node of the cluster (first node), log into the Oracle Key Vault web user interface as a Key Administrator.
   b. Select the **System** tab.
   c. On the left side of the **System** page, select **Settings**.
   d. Under **Network Services**, select **HSM**. The **Hardware Security Module** page appears.



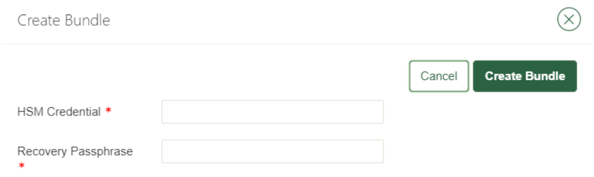
Last Refreshed Time: 19-MAR-2021 12:47:39 [All times UTC -04:00 hours]

Status ⇧

Type Token label: accelerator
Manufacturer ID: nCipher Corp. Ltd
Firmware version: 12.50

> The controller node must be HSM enabled first.

   e. Select **Create Bundle**.



HSM Credential *

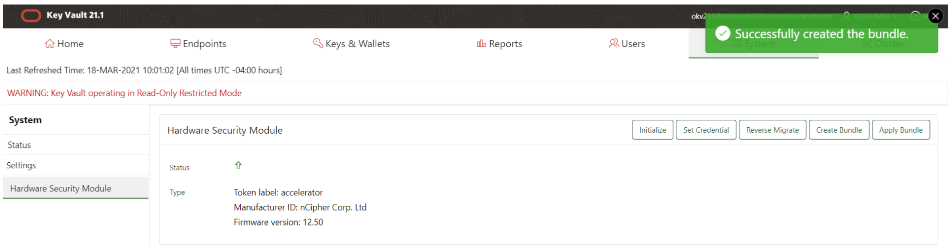
Recovery Passphrase *

   f. Enter the HSM Credentials.

g. Enter the recovery passphrase.

h. Select **Create Bundle**.

   A message indicating the bundle was created successfully appears.



Successfully created the bundle.

Last Refreshed Time: 18-MAR-2021 10:01:02 [All times UTC -04:00 hours]

WARNING: Key Vault operating in Read-Only Restricted Mode

Hardware Security Module

Status ⇧

Type Token label: accelerator
Manufacturer ID: nCipher Corp. Ltd
Firmware version: 12.50

i. Log into the controller (first node) HSM-enabled node through SSH as the support user:

```
% ssh support@HSMENABLEDNODEIP
```

j. Copy the bundle to the candidate node using the node IP addresses:

```
% sudo scp /usr/local/okv/hsm/hsmbundle support@CANDIDATENODEIPADDRESS:/tmp
```

k. Log into the candidate node in the cluster, except the original HSM-enabled node, using the node IP address:

```
% ssh support@CANDIDATENODEIPADDRESS
```

l. Perform the following steps to copy the bundle to the /usr/local/okv/hsm location and apply user and group ownership:

```
% sudo cp /tmp/hsmbundle /usr/local/okv/hsm/
% sudo chown oracle:oinstall /usr/local/okv/hsm/hsmbundle
```

m. On the candidate node, select **Apply Bundle** on the **Hardware Security Module** page in the Web interface. Enter the recovery passphrase.

   If you plan on reverse-migrating the original HSM-enabled node, you must apply the bundle immediately on all nodes first.

5. HSM-enable the candidate node.

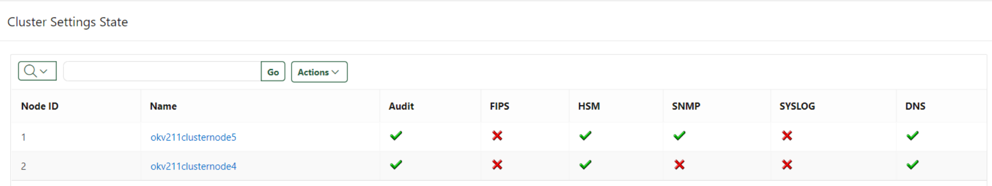
   Follow instructions to enable HSM mode on the candidate node of the cluster when using multiple nodes, see Enable HSM mode in Key Vault.

6. Verify that each HSM is enabled in the cluster:

a. In the Oracle Key Vault web user interface, select the **Cluster** tab.

b. Select **Monitoring** in the left sidebar.

c. Check that the Cluster Settings State has all green ticks for HSM:



Cluster Settings State

Node ID	Name	Audit	FIPS	HSM	SNMP	SYSLOG	DNS
1	okv211clusternode5	✓	✗	✓	✓	✗	✓
2	okv211clusternode4	✓	✗	✓	✗	✗	✓

An enabled HSM does not mean that the HSM is active. The status only indicates whether the HSM is enabled for these nodes. To check whether the HSM is active, use the status information on the **Hardware Security Module** page of the web user interface.

The FIPS column is specific to Oracle Key Vault and does not indicate nShield HSM FIPS compliance. Entrust nShield HSM's are FIPS 140 Level 2 and 3 compliant.

7. After you have HSM-enabled all nodes and verified the replication between all nodes, remove the `hsmbundle` file from all of the nodes.

2.6. Reverse migration operations to a local wallet

Reverse migrating an HSM-enabled Oracle Key Vault server reverts the Key Vault server to using the recovery passphrase to protect the TDE wallet. This operation is necessary if the HSM that protects Oracle Key Vault must be decommissioned.

- Reverse migrating a standalone deployment

  You can reverse migrate a standalone deployment by using the Oracle Key Vault web user interface.

- Reverse migrating a primary-standby deployment

  To reverse migrate a primary-standby deployment, use both the Oracle Key Vault web user interface and the command line.

- Reverse migrating a multi-master cluster

  You can reverse migrate a multi-master cluster by using the Oracle Key Vault web user interface.

2.6.1. Reverse migrate a standalone deployment

You can reverse migrate a standalone deployment by using the Oracle Key Vault web user interface.

1. Log into the Oracle Key Vault web user interface as a Key Administrator.

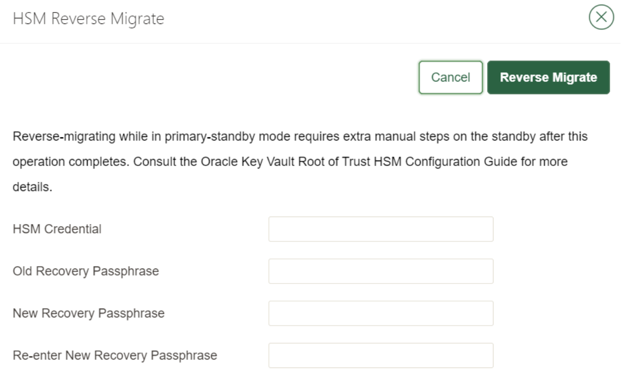
   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.
4. Under **Network Services**, select **HSM**.
5. Select **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box appears.



Reverse-migrating while in primary-standby mode requires extra manual steps on the standby after this operation completes. Consult the Oracle Key Vault Root of Trust HSM Configuration Guide for more details.

HSM Credential	
Old Recovery Passphrase	
New Recovery Passphrase	
Re-enter New Recovery Passphrase	

6. In the **HSM Reverse Migrate** dialog box, enter the following details:
   a. For **HSM Credential**, enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. For **Old Recovery Passphrase**, enter the old recovery passphrase.
   c. For **New Recovery Passphrase**, enter the new recovery passphrase. Repeat this in **Re-enter New Recovery Passphrase**.
7. Select **Reverse Migrate**.
8. The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

2.6.2. Reverse migrate a primary-standby deployment

To reverse migrate a primary-standby deployment, use both the Oracle Key Vault web user interface and the command line.

1. On the primary server, log into the Oracle Key Vault web user interface as a Key Administrator.

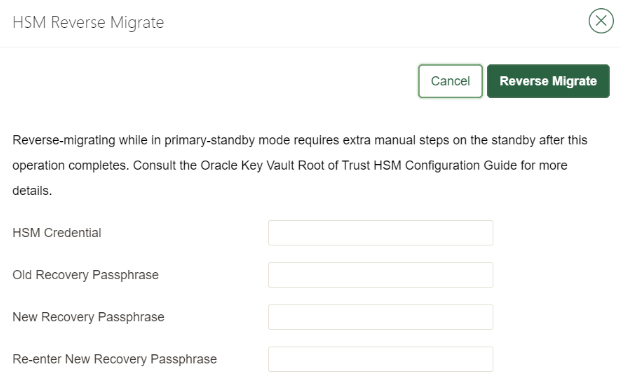
   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.
4. Under **Network Services**, select **HSM**.
5. Select **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box appears.

   Reverse-migrating while in primary-standby mode requires extra manual steps on the standby after this operation completes. Consult the Oracle Key Vault Root of Trust HSM Configuration Guide for more details.

   HSM Credential

   Old Recovery Passphrase

   New Recovery Passphrase

   Re-enter New Recovery Passphrase

6. In the **HSM Reverse Migrate** dialog box, enter the following details:
   a. For **HSM Credential**, enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. For **Old Recovery Passphrase**, enter the old recovery passphrase.
   c. For **New Recovery Passphrase**, enter the new recovery passphrase. Repeat this in **Re-enter New Recovery Passphrase**.
7. Select **Reverse Migrate**.

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

8. On the standby server, log in using SSH as the `support` user, then, with the `su` command, switch to the `root` user:

   ```
   $ ssh support@<okv_standby_instance>
   $ su root
   ```

   Modify the `okv_security.conf` file:

   ```
   $ vi /usr/local/okv/etc/okv_security.conf
   ```

   a. Delete the line HSM_PROVIDER="2".

   b. Change the value of the HSM_ENABLED parameter to **0**.

   c. Check that the HSM_TOKEN_LABEL parameter is set to "".

9. On the standby server, remove the following files:

   ```
   $ cd /usr/local/okv/hsm/wallet
   $ rm -f cwallet.sso enctdepwd
   $ cd /usr/local/okv/hsm/restore
   $ rm -f cwallet.sso ewallet.p12
   $ cd /mnt/okvram
   $ rm -f cwallet.sso ewallet.p12
   $ cd /mnt/okvram/restore
   $ rm -f cwallet.sso ewallet.p12
   $ cd /usr/local/okv/tde
   $ rm -f cwallet.sso
   ```

10. Switch user to oracle:

    ```
    $ su oracle
    ```

11. Run the following command:

    ```
    /var/lib/oracle/dbfw/bin/orapki wallet create -wallet /usr/local/okv/tde -auto_login
    ```

12. Enter the new recovery passphrase that you specified above. For example:

    ```
    Enter wallet password:
    Operation is successfully completed.
    ```

The primary-standby deployment is successfully reverse migrated.

2.6.3. Reverse migrate a multi-master cluster

You can reverse migrate a multi-master cluster by using the Oracle Key Vault web user interface. This is required on each of the nodes in the cluster.

1. Log into the Oracle Key Vault web user interface as a Key Administrator.

   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

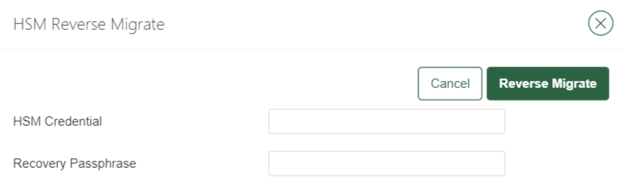
3. On the left side of the **System** page, select **Settings**.

4. Under **Network Services**, select **HSM**.

The **Hardware Security Module** page appears.

5. Select **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box appears.



HSM Reverse Migrate

HSM Credential

Recovery Passphrase

6. In the **HSM Reverse Migrate** dialog box, enter the following details:
   a. For **HSM Credential**, enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. For **Old Recovery Passphrase**, enter the old recovery passphrase.
   c. For **New Recovery Passphrase**, enter the new recovery passphrase. Repeat this in **Re-enter New Recovery Passphrase**.
7. Select **Reverse Migrate**.

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

2.7. Configure backup of the Key Vault server in HSM mode

To configure backup of the Key Vault server in HSM mode:

1. Log into the Oracle Key Vault web user interface as a Key Administrator.

   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.
4. Under the **System Configuration**, select **Backup and Restore**.
5. Add the backup destination on the **System Backup** page, just as you would in non-HSM mode.
6. Perform a backup as usual from the user interface on the web user interface.

2.8. Restore from a Key Vault backup in HSM mode

> To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

Only backups taken in HSM mode can be restored onto an HSM-enabled Oracle Key Vault. Before you restore a backup onto a system, you must ensure that the system can access both the HSM and the Root of Trust used to take the backup. You must therefore have installed the HSM on the Oracle Key Vault server and enrolled Oracle Key Vault as a client of the HSM prior to this step.

1. If OCS protection is used, present the OCS card to the HSM.
2. Log into the Oracle Key Vault web user interface as a user with system administrative privileges.

   The **Oracle Key Vault Home** page appears.

3. Select the **System** tab.

   The **Status** page appears.

4. On the left side of the **System** page, select **Settings**.
5. Under **Network Services**, select **HSM**.

   The **Hardware Security Module** page appears. On restore, the **Status** is disabled first, then enabled after the restore completes.

6. Select **Set Credential**.

   The **Prepare for HSM Restore** screen appears.

7. From the **Vendor** list, select **Entrust** and enter the HSM credential twice as requested.
8. Select **Set Credential**.

   The HSM credential will be stored in the system. This HSM credential must be entered manually to do an HSM restore because it is not stored in the backup itself.

9. On the left side of the page, select **Settings**.
10. Under the **System Configuration**, select **Backup and Restore**.
11. Select **Restore** and restore the Key Vault backup.

2.9. Restart or restore in HSM mode using nShield Remote Administration

To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

The `raserv` package of nShield software is only available on the nShield RFS machine, it is not supported on Oracle Key Vault servers. When the Oracle Key Vault server restarts or restores from a backup and Java Cards cannot be presented to the HSMs that are enrolled to that server, the restart or restore will fail.

If the HSM is also enrolled to the RFS, you can present Java Cards there when the RFS is operational. As a result, when the Oracle Key Vault server comes back up, it can still access the keys from the HSM using the OCS in slot 0.