ENTRUST

SECURING A WORLD IN MOTION

Oracle Key Vault

nShield® HSM Integration Guide

Version: 1.10

Date: Thursday, November 26, 2020

Information in this document is subject to change without notice.

nCipher Security Limited makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. nCipher Security Limited shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Where translations have been made in this document English is the canonical language.

nCipher Security Limited
Registered Office: One Station Square,
Cambridge, CB1 2GA, United Kingdom
Registered in England No. 11673268

nCipher is an Entrust company.

Contents

1 Introduction

The nShield Hardware Security Module (HSM) can be used to generate and store a Root of Trust (RoT) that protects security objects used by Oracle Key Vault to safeguard users' keys and credentials. The HSM can be used in FIPS 140-2 Level 2 or Level 3 mode to meet compliance requirements. An Oracle Key Vault cluster node can have multiple HSMs enrolled, as long as the HSMs are in the same Security World.

ℹ An existing Oracle Key Vault deployment cannot be migrated to use an HSM as a RoT.

ℹ Oracle Key Vault can function only if the RoT stored in the HSM is available.

ℹ 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

We have successfully tested nShield HSM integration with Oracle Key Vault in the following configurations:

Operating System (Remote File System)	Oracle Key Vault Version	nShield Support	nShield Firmware Version	Security World Software Version
Red Hat Enterprise Linux 7 64-bit	18.3.0.0.0 18.2.0.0.0	Connect XC	12.60.2 3.4.2	v12.60

1.2 Supported nShield functionality

Feature	Support	Feature	Support	Feature	Support
Key generation	Yes	1-of-N Operator Card Set	Yes	Strict FIPS 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

1.3 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 have an impact on how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140-2 Level 3 standards.
    - If using FIPS Restricted mode, 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.

1.4 This guide

This guide describes how to integrate an nShield HSM with Oracle Key Vault.

1.5 More information

For more information about contacting nCipher, see *Contact Us* at the end of this guide.

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. If you have 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.

If you have a high availability Oracle Key Vault environment, perform these steps:

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

To install HSM client software on the Key Vault server:

1. Log in to 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. Go to the root directory and create the directories ctls and hwsp:

```
root# cd /root
root# mkdir ctls
root# mkdir hwsp
```

4. Transfer the ctls and hwsp packages from the RFS to the Oracle Key Vault server. Assuming that the nShield Security World Software ISO is mounted on the RFS:

```
root# scp root@<RFS_IP>:/mnt/isoimage/linux/amd64/ctls.tar.gz ctls/
root# scp root@<RFS_IP>:/mnt/isoimage/linux/amd64/hwsp.tar.gz hwsp/
```

5. Install the ctls and hwsp packages:

```
root# cd /
root# tar xvf /root/ctls/ctls.tar.gz
root# tar xvf /root/hwsp/hwsp.tar.gz
root# /opt/nfast/sbin/install
```

6. As root, perform additional edits on the Key Vault server:

```
root# usermod -a -G nfast oracle
root# cd /etc/rc.d/rc5.d
root# mv S50nc_hardserver S40nc_hardserver
root# cd /etc/rc.d/rc3.d
root# mv S50nc_hardserver S41nc_hardserver
```

7. 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
```

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

   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.

9. 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

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.

   - Select privileged on any port.
   - If you have 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 **enquiry** 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 to be used 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 folder 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 --no-authenticate <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.

If you are using OCS protection, cknfastrc needs the following set:

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

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 *Known issues* on page 24.

If you are using Module-Only protection, cknfastrc needs the following set:

```
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 slot number to run 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

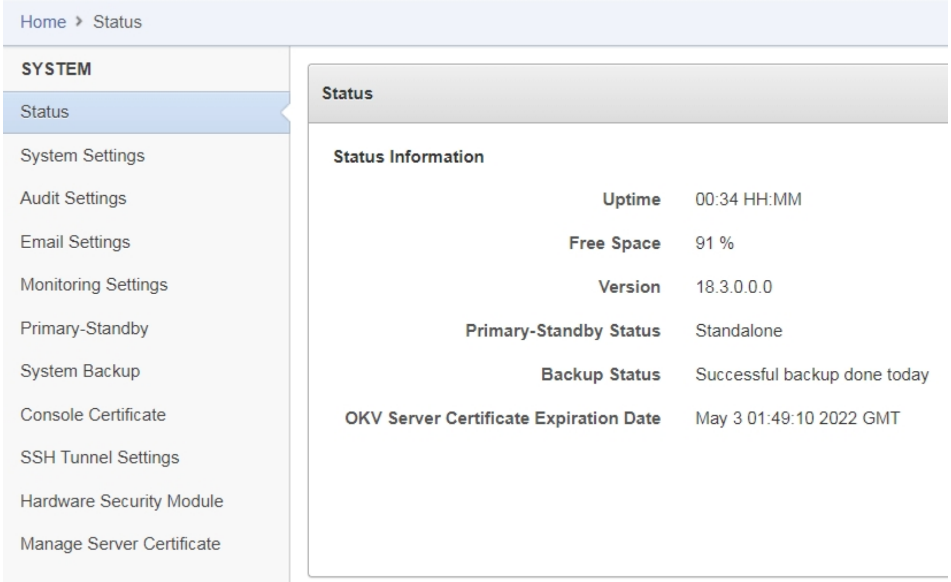
After installing HSM software and enrolling Key Vault as an HSM client, you can enable HSM mode with nShield HSM(s) from the Key Vault web user interface. This will protect the Oracle Key Vault Root of Trust key with the HSM.

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.



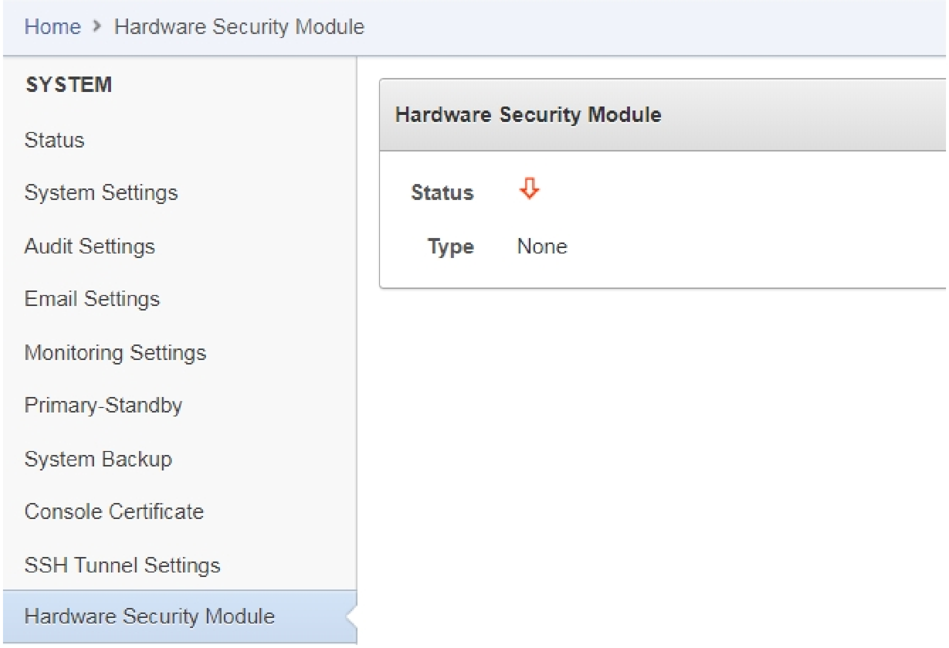
Status

Status Information

Uptime	00:34 HH:MM
Free Space	91 %
Version	18.3.0.0.0
Primary-Standby Status	Standalone
Backup Status	Successful backup done today
OKV Server Certificate Expiration Date	May 3 01:49:10 2022 GMT

3. Select Hardware Security Module in the left sidebar.

   The Hardware Security Module page appears. The red downward arrow shows the non-initialized Status. The Type field displays None.



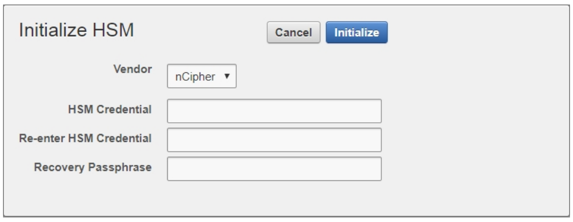
Hardware Security Module

Status	⇩
Type	None

4. Select Initialize.

   The Initialize HSM screen appears.

5. From the Vendor list, select nCipher:



Initialize HSM

Vendor: nCipher

HSM Credential

Re-enter HSM Credential

Recovery Passphrase

6. Enter a password two times: first in HSM Credential and second in Re-enter HSM Credential.

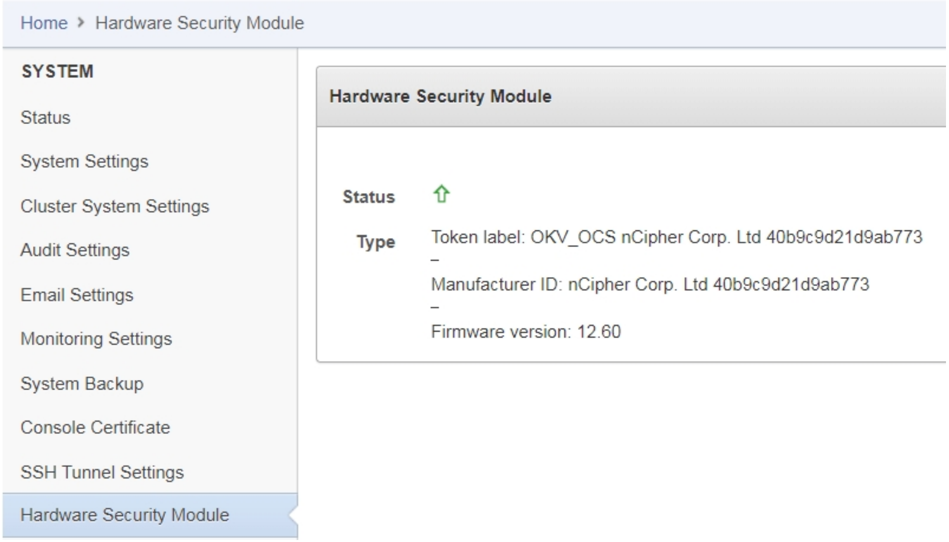
   - If you are using OCS protection, then your OCS passphrase needs to be entered in twice with your card presented in slot 0.
   - If you are using Softcard protection, then the Softcard passphrase needs to be entered twice.
   - If you are using Module-Only protection, enter a password that you set up for this credential check.

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

7. Enter the recovery passphrase for Oracle Key Vault.

8. Select Initialize.

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



Hardware Security Module

Status ⇧

Type Token label: OKV_OCS nCipher Corp. Ltd 40b9c9d21d9ab773
–
Manufacturer ID: nCipher Corp. Ltd 40b9c9d21d9ab773
–
Firmware version: 12.60

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

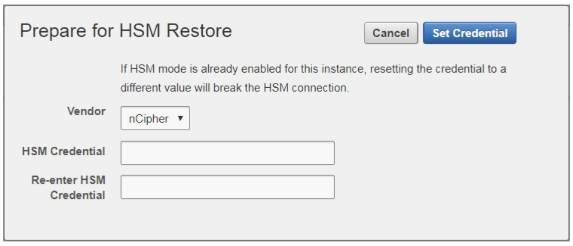
   Only the first two numbers of the firmware are displayed.

9. 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 nCipher, then select the **Set Credential** button.



Prepare for HSM Restore

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

Vendor: nCipher

HSM Credential:

Re-enter HSM Credential:

2.4 Enable the HSM in a primary-standby high availability deployment

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.

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* on page 6.
3. Enroll the primary and standby nodes as clients of the HSM, see *Enroll Key Vault as a client of the HSM* on page 8.
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* on page 10.
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$ 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="snmp_encryption_password"
   SNMP_AUTHENTICATION_PWD="snmp_auth_password"
   SNMP_USERNAME="snmpuser"
   SMTP_TRUSTSTORE_PWD="smtp_truststore_password"
   HSM_ENABLED="0"
   FIPS_ENABLED="0"
   HSM_FIPS_ENABLED="1"
   ```

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

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

   ```
   HSM_ENABLED="1"
   ```

   Add the following line:

   ```
   HSM_PROVIDER="2"
   ```

9. On the standby server, run the rfs-sync --update command 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 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.

2.5.1 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.

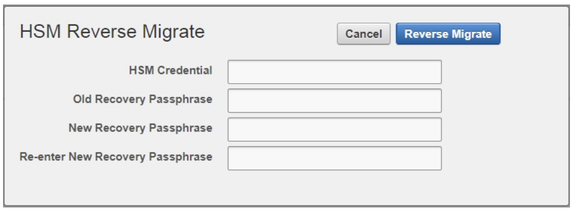
   The Status page appears.

3. Select Hardware Security Module in the left sidebar.

   The Hardware Security Module page appears.

4. Select Reverse Migrate.

   The HSM Reverse Migrate dialog box is displayed.



HSM Reverse Migrate

HSM Credential

Old Recovery Passphrase

New Recovery Passphrase

Re-enter New Recovery Passphrase

5. On the HSM Reverse Migrate dialog box, enter the following details:

   a. Enter the HSM credential in the HSM Credential field. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. Enter the old recovery passphrase in the Old Recovery Passphrase field.
   c. Enter the new recovery passphrase in the New Recovery Passphrase and Re-enter New Recovery Passphrase fields.

6. Select Reverse Migrate.
7. The Hardware Security Module page appears. The red downward arrow indicates the Status.

2.5.2 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.

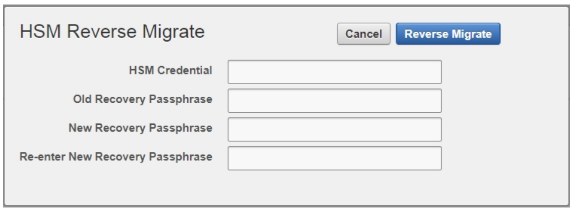
   The Status page appears.

3. Select Hardware Security Module in the left sidebar.

   The Hardware Security Module page appears.

4. Select Reverse Migrate.

   The HSM Reverse Migrate dialog box is displayed.



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

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

7. On the standby server, log in through 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
```

- Delete the line HSM_PROVIDER="2".
- Change the value of the parameter HSM_ENABLED to 0.

8. 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
```

9. Switch user (su) to oracle:

```
$ su oracle
```

10. Run the following command:

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

11. Enter the new recovery passphrase that you specified in Step 5.

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

The primary-standby deployment is successfully reverse migrated.

2.5.3 Reverse migrate a multi-master cluster

You can reverse migrate a multi-master cluster 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.

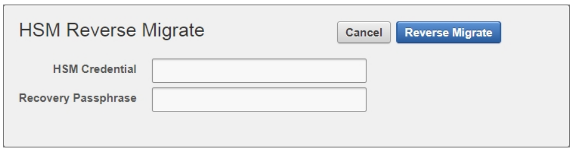
   The Status page appears.

3. Select Hardware Security Module in the left sidebar.

   The Hardware Security Module page appears.

4. Select Reverse Migrate.

   The HSM Reverse Migrate dialog box is displayed.



5. In the HSM Reverse Migrate dialog box, enter the following details:

   a. Enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.

   b. Enter the recovery passphrase.

6. Select Reverse Migrate.

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

2.6 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.

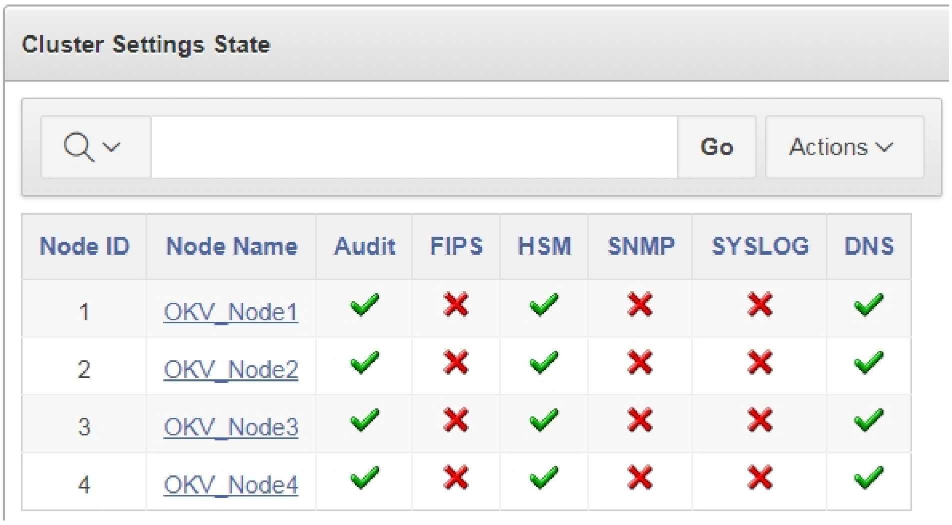
2.6.1 Configure an HSM for a multi-master cluster with a single node

To use an HSM with a multi-master cluster, you should start with a single HSM-enabled node and add additional HSM-enabled nodes.

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

1. Configure the first node of the cluster.
2. Configure the HSM on the first node before adding any new nodes. If there is already more than one node in the cluster, then configure the HSM for a multi-master cluster with multiple nodes. See *Configure an HSM for a multi-master cluster with multiple nodes* on page 19.
3. HSM-enable the candidate node before adding it to the cluster.
4. Add the HSM-enabled candidate node to the cluster using a controller node that is also HSM-enabled.

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



Node ID	Node Name	Audit	FIPS	HSM	SNMP	SYSLOG	DNS
1	OKV_Node1	✓	✗	✓	✗	✗	✓
2	OKV_Node2	✓	✗	✓	✗	✗	✓
3	OKV_Node3	✓	✗	✓	✗	✗	✓
4	OKV_Node4	✓	✗	✓	✗	✗	✓

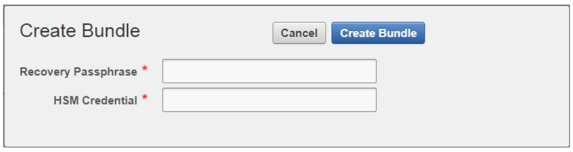
An enabled HSM does not mean that the HSM is active. The status only indicates whether the HSM is enabled for these nodes. To check whether the HSM is active, use the status information on the Hardware Security Module page of the web user interface.

2.6.2 Configure an HSM for a multi-master cluster with multiple nodes

You can configure HSM for multiple nodes by copying information from an HSM-enabled node to the non-enabled nodes.

For instructions to configure an HSM for a multi-master cluster, see *Configure an HSM for a multi-master cluster with a single node* on page 18. If the first node to be HSM-enabled is in a cluster that already has multiple nodes, then you must manually copy information from that HSM-enabled Oracle Key Vault to the other Oracle Key Vault installations in the cluster before you can enable HSM in any other nodes. If the first node to be HSM-enabled has a read-write peer, then the read-write peer will not be able to decrypt the information from the HSM-enabled node until the bundle is copied and applied successfully to the read-write peer.

1. Log in to the Oracle Key Vault web user interface as a Key Administrator.
2. Select the System tab.
3. On the left side of the System page, select Hardware Secure Module.
4. On the HSM-enabled node, select Create Bundle on the Hardware Security Module page.
5. Enter the recovery passphrase.



Create Bundle

6. Log in to the HSM-enabled node through SSH as the **support** user.

```
ssh support@<hsm_enabled_node>
```

7. Switch to the **root** user.

```
su root
```

8. Copy the bundle to each node using the node IP addresses:

```
scp /usr/local/okv/hsm/hsmbundle support@<ip_address>:/tmp
```

9. Log in to each node in the cluster, except the original HSM-enabled node, using the node IP address:

```
ssh support@<ip_address>
```

10. Switch to the **root** user.

```
su root
```

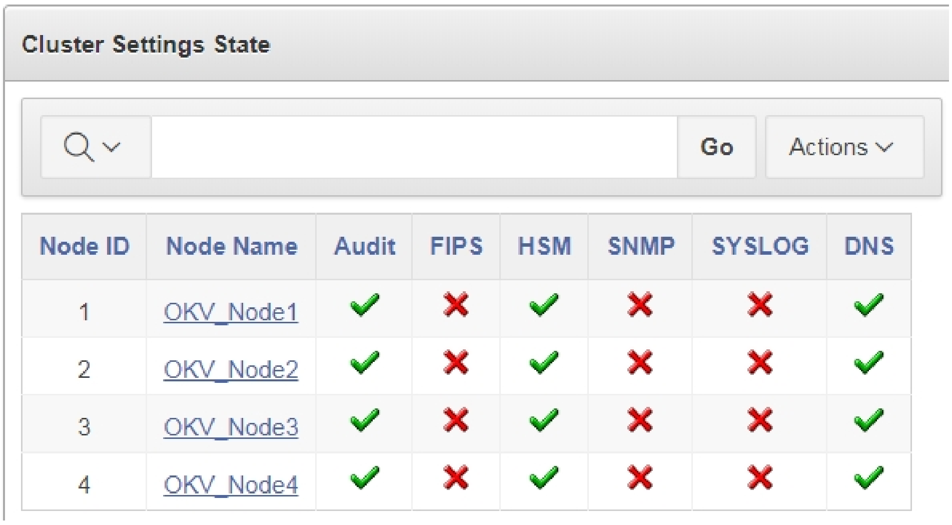
11. Perform the following steps on each node to copy the bundle to the /usr/local/okv/hsm location and apply user and group ownership:

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

12. On each node except the original HSM-enabled node, select Apply Bundle on the Hardware Security Module page. 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.

13. Proceed to HSM-enable each of these nodes in the same way that you HSM-enabled the first node. Also verify that each HSM is enabled:
    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:



Node ID	Node Name	Audit	FIPS	HSM	SNMP	SYSLOG	DNS
1	OKV_Node1	✓	✗	✓	✗	✗	✓
2	OKV_Node2	✓	✗	✓	✗	✗	✓
3	OKV_Node3	✓	✗	✓	✗	✗	✓
4	OKV_Node4	✓	✗	✓	✗	✗	✓

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.

14. After HSM-enabling a node in a cluster, the `rfs-sync --update` command must be run on all other nodes to ensure that all nodes have up-to-date Security World files.
15. After you have HSM-enabled all nodes and verified the replication between all nodes, remove the `hsmbundle` file from all of the nodes.

2.7 Configure backup of the Key Vault server in HSM mode

1. Install a new Key Vault server.
2. Install the nShield Security World Software as described in *Install HSM client software on the Key Vault server* on page 6.
3. From the Key Vault web user interface, add the backup destination on the System Backup page, just as you would in non-HSM mode.
4. 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.
- 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. Select Hardware Security Module in the left sidebar.

   The Hardware Security Module page appears. On restore, the Status is disabled first, then enabled after the restore completes.
5. Select Set Credential.

   The Prepare for HSM Restore screen appears.
6. From the Vendor list, select nCipher and enter the HSM credential twice as requested.
7. 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.
8. Go to the Restore page via the Key Vault web user interface 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. This way, when the Oracle Key Vault server comes back up, it can still access the keys from the HSM using the OCS in slot 0.

3 Known issues

Issue	Action for Integrator
If you want to use softcards as a means of protection, you need to set CKNFAST_LOADSHARING=1 in cknfastrc, but this causes the firmware version to display as 0.0 when the Oracle Key Vault server is initialized with the HSM.	None.

Contact Us

Web site:	https://www.entrust.com
Support:	https://nshieldsupport.entrust.com
Email Support:	nShield.support@entrust.com
Online documentation:	Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa

United Kingdom:	+44 1223 622444 One Station Square Cambridge CB1 2GA UK

Americas

Toll Free:	+1 833 425 1990
Fort Lauderdale:	+1 954 953 5229 Sawgrass Commerce Center – A Suite 130, 13800 NW 14 Street Sunrise FL 33323 USA

Asia Pacific

Australia:	+61 8 9126 9070 World Trade Centre Northbank Wharf Siddeley St Melbourne VIC 3005 Australia
Japan:	+81 50 3196 4994
Hong Kong:	+852 3008 3188 31/F, Hysan Place 500 Hennessy Road Causeway Bay Hong Kong

To get help with
Entrust nShield HSMs

nShield.support@entrust.com

nshieldsupport.entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

ENTRUST
SECURING A WORLD IN MOTION