



ENTRUST

SECURING A WORLD IN MOTION

Oracle Key Vault 21.1

nShield® HSM Integration Guide

Version: 1.12

Date: Wednesday, March 24, 2021

Copyright © 2020-2021 nCipher Security Limited. All rights reserved.

Copyright in this document is the property of nCipher Security Limited. It is not to be reproduced modified, adapted, published, translated in any material form (including storage in any medium by electronic means whether or not transiently or incidentally) in whole or in part nor disclosed to any third party without the prior written permission of nCipher Security Limited neither shall it be used otherwise than for the purpose for which it is supplied.

Words and logos marked with ® or ™ are trademarks of nCipher Security Limited or its affiliates in the EU and other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries.

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, UK CB1 2GA
Registered in England No. 11673268

nCipher is an Entrust company.

Entrust, Datacard, and the Hexagon Logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

Contents

1. Introduction	4
1.1. Product configurations	4
1.2. Supported nShield hardware and software versions	5
1.3. Supported nShield functionality	5
1.4. Requirements	6
1.5. More information	6
2. Procedures	7
2.1. Install HSM client software on the Key Vault server	7
2.2. Enroll Key Vault as a client of the HSM	9
2.3. Enable HSM mode in Key Vault	11
2.4. Enable the HSM in a primary-standby high availability deployment	14
2.5. Configure an HSM for a multi-master cluster	16
2.6. Reverse migration operations to a local wallet	20
2.7. Configure backup of the Key Vault server in HSM mode	25
2.8. Restore from a Key Vault backup in HSM mode	25
2.9. Restart or restore in HSM mode using nShield Remote Administration	26
3. Known issues	27
Contact Us	28

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.



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



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

We have 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	21.1

1.2. Supported nShield hardware and software versions

We have 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	12.60.10	✓	✓	✓

1.2.2. Connect +

Security World Software	Firmware	Image	OCS	Softcard	Module
12.60.11	12.50.8	12.60.10	✓	✓	✓

1.3. 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

1.4. 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 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.

1.5. More information

For more information about OS support, contact your Oracle Key Vault sales representative or Entrust nShield Support, <https://nshieldsupport.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. 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. Install the latest version of the Security World software as described in the *Installation Guide* for the HSM.



We recommend 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, perform additional edits on the Key Vault server:

- a. 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.



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

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.

- a. OCS protection

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

```
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 [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, `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.

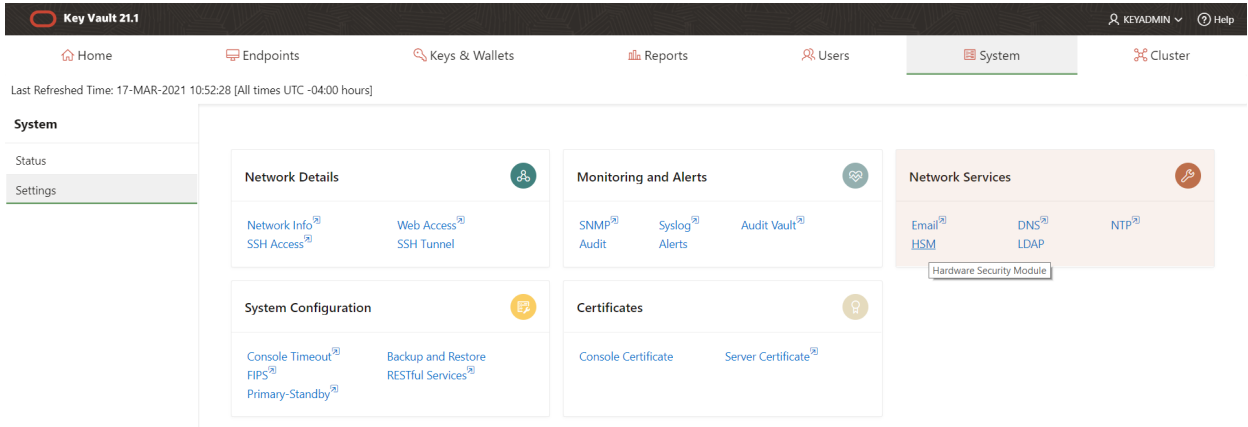
1. Log into the Oracle Key Vault web user interface as a Key Administrator.

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

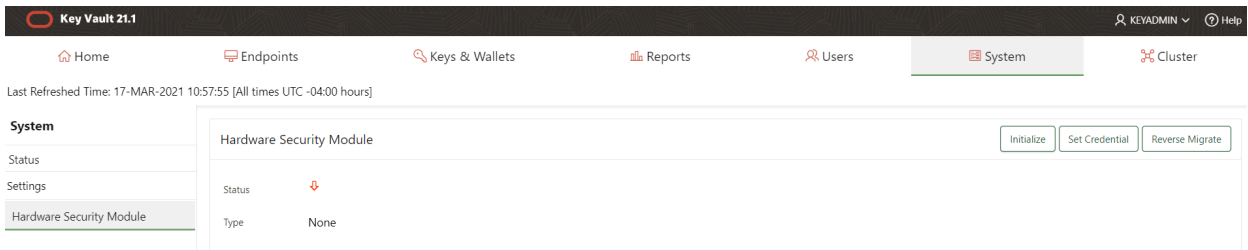
2. Select the **System** tab.

The **Status** page appears.

3. Select **Settings** on the Left menu and then Select **HSM** under **Network Services**.



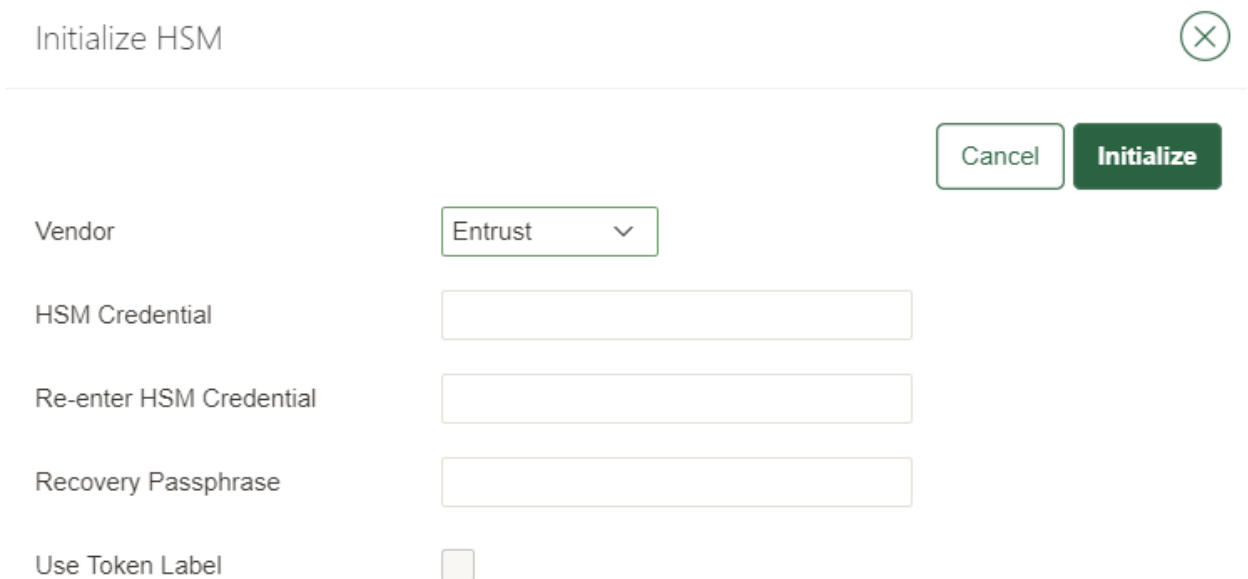
The **Hardware Security Module** page appears.



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

4. Select **Initialize**.

The **Initialize HSM dialog** appears.



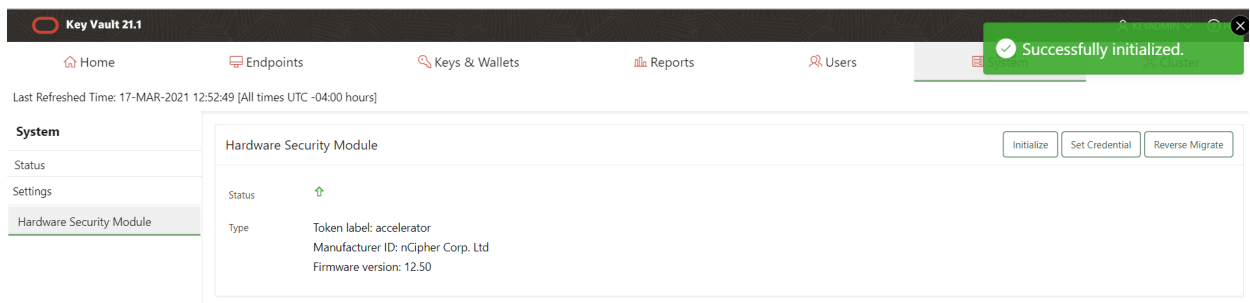
5. From the **Vendor** list, select **Entrust**:
6. Enter a password two times: first in **HSM Credential** and second in **Re-enter HSM Credential**.
 - If you are using OCS protection, then your OCS passphrase needs to be entered in twice with your card presented in slot 0.
 - If you are using Softcard 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. 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.
9. 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 displays details of the HSM in use.



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



Only the first two numbers of the firmware are displayed.

10. 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 the **Set Credential** button.

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

Entrust

HSM Credential

Re-enter HSM Credential

Use Token Label

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. 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="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"
OKV_OCI_INSTALL="DISABLED"
HSM_TOKEN_LABEL=""
HSM_KEY_EXTRACTABLE="0"
OKVAG_LINK_UI="https://docs.oracle.com/en/database/oracle/key-vault/21.1/okvag/"
LDAP_TRACE_LEVEL="1"
```

8. Make 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"
```

If using softcards or OCS cards, enter the name of the cardset:

```
HSM_TOKEN_LABEL="card_set_name"
```

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. 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.



We recommend you read https://docs.oracle.com/en/database/oracle/key-vault/21.1/okvag/managing_multimaster.html for details on how to setup clusters.

The example we will use is to setup the cluster from scratch and if you already have a cluster in place, please read the documentation above.

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

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

1. Convert an Oracle Key Vault server into the first node of the cluster. (The controller node)
 - 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.

- Current Server IP has the server IP address.
- First Node of Cluster should be set to **Yes**, if this is the first node, otherwise set it to **No**.
- Node Name should be prefilled with the host name of the OKV server.
- Cluster Name. Enter the name for the cluster.
- 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.

Select Node	Node ID	Name	IP Address	Mode	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date	Version
<input type="checkbox"/>	1	okv211clusternode1	10.194.148.115	Read-Only Restricted	ACTIVE	-	sunrise	17-MAR-2021 14:08:05	-	21.1.0.0.0

2. If using multiple nodes, add the candidate nodes to the cluster using the controller node.

Please refer to https://docs.oracle.com/en/database/oracle/key-vault/21.1/okvag/managing_multimaster.html for details on how to add a candidate node to the cluster.

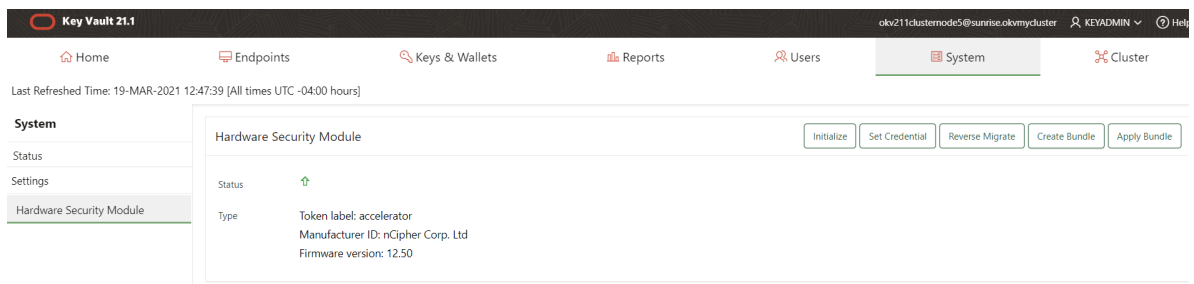
3. HSM-enable the controller node (first node).

Follow instructions to enable HSM mode on the first node of the cluster. See [Enable HSM mode in Key Vault](#) section on how to do this.

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.

- On the controller node of the cluster (first node), log in to the Oracle Key Vault web user interface as a Key Administrator
- Select the **System** tab.
- On the left side of the System page, select **Settings**.
- Select **HSM** under the **Network Services** section. The **Hardware Security Module** page appears.



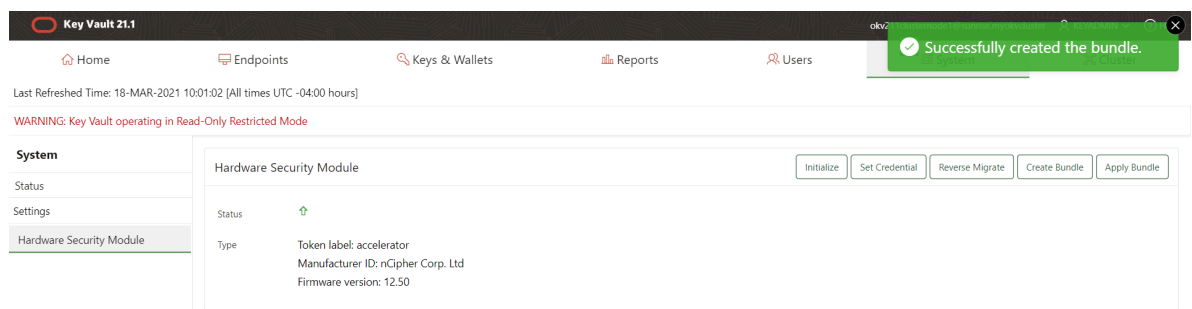
The controller node must be HSM enabled first.

- Select **Create Bundle**.

A screenshot of the 'Create Bundle' dialog box in the Oracle Key Vault interface. The dialog has a title bar with 'Create Bundle' and a close button (X). Below the title bar, there are two input fields: 'HSM Credential *' and 'Recovery Passphrase *'. To the right of the input fields are two buttons: 'Cancel' and 'Create Bundle'.

- Enter the HSM Credentials.
- Enter the recovery passphrase.
- Select **Create Bundle**.

A message indicating the bundle was created successfully appears.



- Log in to the controller (first node) HSM-enabled node through SSH as the support user.

```
% ssh support@HSMENABLEDNODEIP
```

- Copy the bundle to the candidate node using the node IP addresses:

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

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

```
% ssh support@CANDIDATENODEIPADDRESS
```

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

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

- 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](#) section on how to do this.

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

- In the Oracle Key Vault web user interface, select the **Cluster** tab.
- Select **Monitoring** in the left sidebar.

- 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.

- 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. Select **HSM** under the **Network Services** section.
5. Select **Reverse Migrate**.

The **HSM Reverse Migrate** dialog box is displayed.

HSM Reverse Migrate ⓧ

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	<input type="text"/>
Old Recovery Passphrase	<input type="text"/>
New Recovery Passphrase	<input type="text"/>
Re-enter New Recovery Passphrase	<input type="text"/>

6. 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.
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. Select **HSM** under the **Network Services** section.
5. Select **Reverse Migrate**.

The **HSM Reverse Migrate** dialog box is displayed.

HSM Reverse Migrate ✕

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	<input type="text"/>
Old Recovery Passphrase	<input type="text"/>
New Recovery Passphrase	<input type="text"/>
Re-enter New Recovery Passphrase	<input type="text"/>

6. 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.

7. Select **Reverse Migrate**.

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

8. 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.
- Check that the parameter **HSM_TOKEN_LABEL** 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 (su) 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 in Step 5.

```
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. You will need to do this 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.

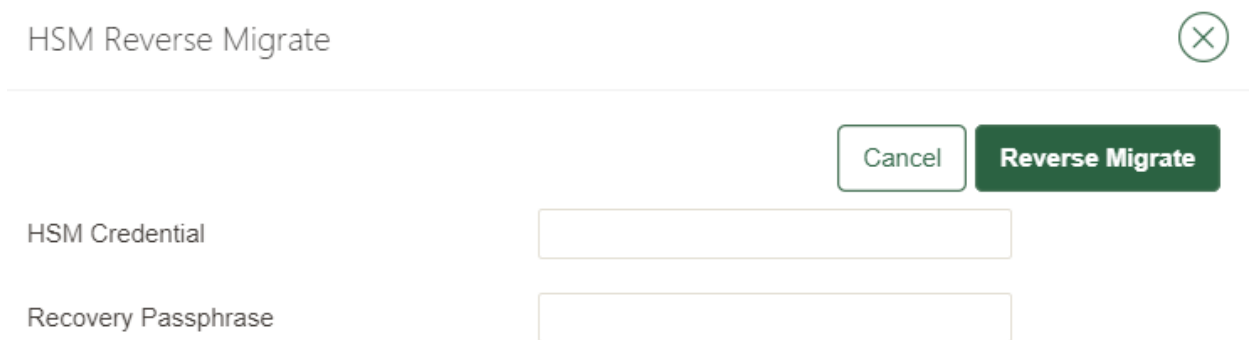
3. On the left side of the System page, select **Settings**.

4. Select **HSM** under the **Network Services** section.

The **Hardware Security Module** page appears.

5. Select **Reverse Migrate**.

The **HSM Reverse Migrate** dialog box is displayed.



HSM Reverse Migrate

Cancel Reverse Migrate

HSM Credential

Recovery Passphrase

6. 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.

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

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. Select **Backup and Restore** under the **System Configuration** section.
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.
- 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. Select **HSM** under the under the **Network Services** section.

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. Select **Backup and Restore** under the **System Configuration** section.
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. 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
<p>If you want to use softcards as a means of protection, you need to set <code>CKNFAST_LOADSHARING=1</code> in <code>cknfastrc</code>, but this causes the firmware version to display as 0.0 when the Oracle Key Vault server is initialized with the HSM.</p>	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, UK CB1 2GA

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

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