



Bring Your Own Key for Oracle Cloud and Entrust Cryptographic Security Platform Key Management Vault

Integration Guide

2025-08-13

Table of Contents

1. Introduction	1
1.1. Documents to read first	1
1.2. Product configurations	1
1.3. Features tested	1
1.4. Requirements	2
2. Procedures	3
2.1. Prerequisites	3
2.2. Create a CloudKey Vault in the Key Management Vault server	3
2.3. OCI Setup	5
2.4. Testing the Integration	11
3. Additional resources and related products	23
3.1. nShield Connect	23
3.2. nShield as a Service	23
3.3. KeyControl BYOK	23
3.4. KeyControl as a Service	23
3.5. Entrust products	23
3.6. nShield product documentation	23

Chapter 1. Introduction

This document describes the integration of Oracle Cloud Infrastructure (OCI) Bring Your Own Key (BYOK), referred to as OCI BYOK in this guide, with the Entrust Cryptographic Security Platform Key Management Vault.

1.1. Documents to read first

- [Entrust Cryptographic Security Platform Key Management Vault: nShield® HSM Integration Guide](#). This document is also available from the [Entrust Document Library](#).
- [Cryptographic Security Platform Vault for Cloud Keys](#).
- [Configuring Vault Authentication for Cryptographic Security Platform Vault for Cloud Keys](#).
- [Cryptographic Security Platform Vault BYOK Overview](#)
- [Configuring OCI for Cryptographic Security Platform Vault BYOK](#).
- Also refer to the documentation for OCI in the [Oracle Cloud Infrastructure Documentation](#).

1.2. Product configurations

Entrust has successfully tested the integration of Cryptographic Security Platform Key Management Vault with OCI BYOK in the following configurations:

Vendor	Product	Version
Oracle	Oracle Cloud	N/A
Entrust	Cryptographic Security Platform	1.0
Entrust	Key Management Vault	10.4.5
VMware	vSphere	8.0

1.3. Features tested

Entrust has successfully tested the following features:

Feature	Tested
API Key Generation	✓

Feature	Tested
API Key Rotation	✓
OCI API Connection	✓
OCI Compartment Creation	✓
OCI Vault Creation	✓
OCI Vault Master Encryption Key Creation	✓
OCI Bucket Creation	✓
CloudKey Creation for OCI Vault Master Encryption Key.	✓
Disabling and Enabling cloud key	✓

1.4. Requirements



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

Chapter 2. Procedures

2.1. Prerequisites

Before you perform the integration, complete the following tasks:

1. Deploy and configure Entrust Key Management Vault.
2. Ensure that you have access to Oracle Cloud Infrastructure (OCI).
3. If the OCI user is not in the administrators group, create a policy that allows the user to manage keys and vaults.
4. Ensure that the OCI user was created in the default identity domain for the tenancy, because users in non-default identity domains are not supported.
5. Ensure that the endpoints whitelisted for OCI BYOK work:

If your organisation restricts outbound access to the public internet, the following endpoints will need to be whitelisted for OCI BYOK to work:

- <https://cloud.oracle.com/>
- <https://kms.<region>.oraclecloud.com>

This endpoint must be individually whitelisted for each region you want to use.

- <https://identity.<region>.oci.oraclecloud.com>

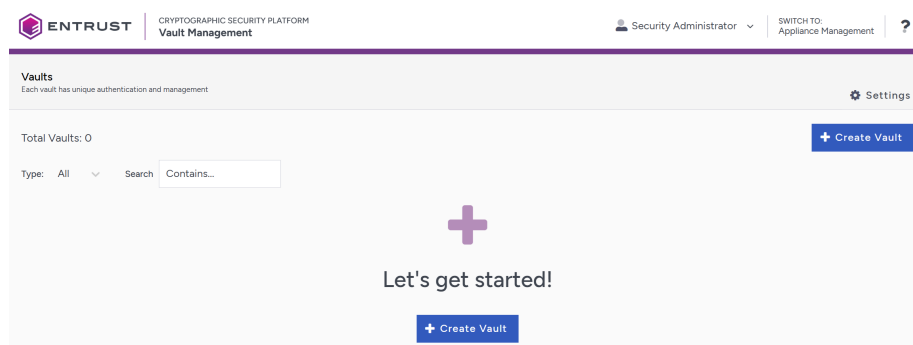
This endpoint must be individually whitelisted for each region you want to use).

- <https://<vaultid>-management.kms.<region>.oraclecloud.com>

This endpoint must be individually whitelisted for each vault you want to use. The URL can be found on the vault information tile in the OCI console.

2.2. Create a CloudKey Vault in the Key Management Vault server

1. Log in to the Key Management Vault server in your web browser using the **secroot** credentials.
2. If you are not in the Vault Management interface, select **SWITCH TO: Manage Vaults** in the menu header
3. Select **Create Vault**.



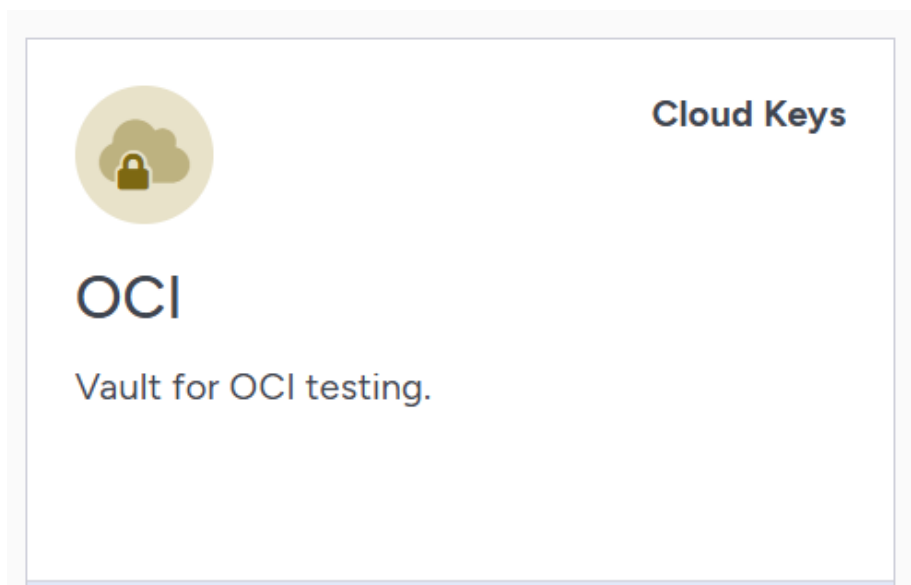
4. Create a **CloudKey** Vault:

- For **Type**, select **Cloud Keys**.
- For **Name**, enter a vault name.
- For **Description**, enter a description for the vault.
- For **Admin Name**, enter the name of the vault administrator.
- For **Admin Email**, enter a valid email for the administrator.



A temporary password will be emailed to the administrator's email address when the vault is created. Use this password the first time that you sign in to the CloudKey Vaults space in Key Management Vault. In a closed gap environment where email is not available, the password for the user is displayed when you first create the vault. Copy this password and send it to the user.

5. Select **Create Vault**.
6. Select **Close** when the vault creation completes.
7. The newly created vault is added to the vault dashboard.



8. Go to the displayed URL and sign in with the credentials given.

When you sign in for the first time, the system will prompt you to change the password.

2.3. OCI Setup

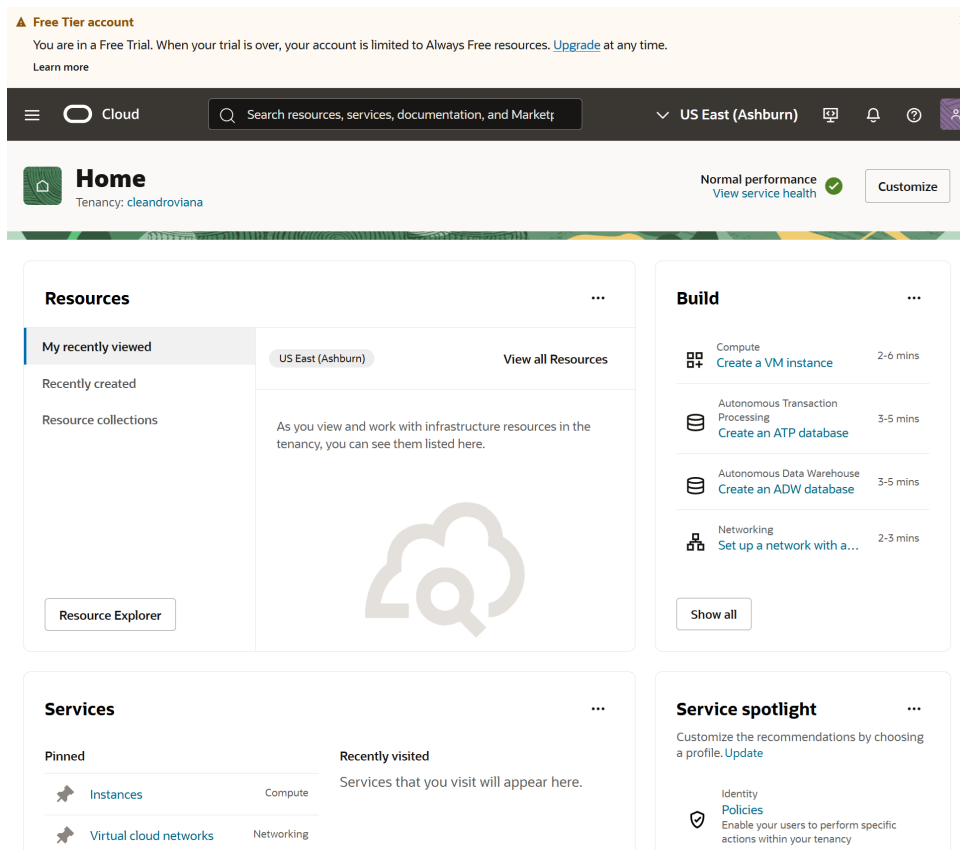
Setting up OCI from scratch is a multi-step process that involves creating an account, configuring networks, provisioning resources, and deploying your applications or services. Use the following steps as a general guide to get started:

2.3.1. Create an Oracle Cloud Account

Visit the Oracle Cloud website and create an account: <https://cloud.oracle.com/>

2.3.2. Log In to Oracle Cloud Console

Use your credentials to log in to the Oracle Cloud Console. This is your central location for configuring and managing OCI resources.



2.3.3. Add an API Key for the OCI User

The API key provides a configuration file snippet that contains the connection information that allows you to connect to the Entrust Cryptographic Security Platform Key Management Vault.



It might take up to 5 minutes for a new API key to become active on OCI. If you attempt to create your Cloud Service Provider account before the API key is active, it will fail with the following error: **Failed to validate Access Credentials OCI returned error: Client is unauthorized. null** Wait for a few minutes before you attempt to recreate your Cloud Service Provider account. For more information, see [Adding a Cloud Service Provider Account for OCI](#).


1. In OCI, navigate to the user that got created for you when you signed up for OCI.


You can find the **Users** link under the **Services spotlight** section in the console.


Service spotlight

...

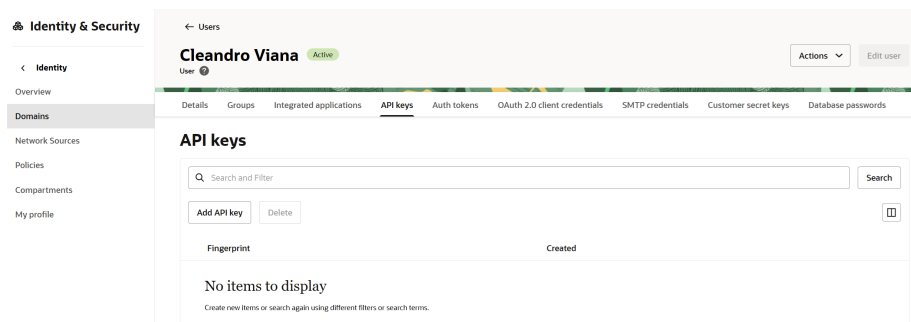
Customize the recommendations by choosing a profile. [Update](#)

Identity
 **Policies**
Enable your users to perform specific actions within your tenancy

Networking
 **Virtual Cloud Networks**
Set up and manage your VCNs, which are your private, flexible data centers in the cloud with security policies and built-in administration

Identity
 **Users**
Secure your resources by managing the users that can access your tenancy

2. Select **Users** and then the user that got created for you.
3. On the user page, select the **API Keys** tab.



4. Under **API Keys**, select **Add API Key**.
5. Add the key using your preferred method. For this guide, **Generate API key pair** was used.

The API key is an RSA key pair in PEM format. You can either generate the key pair here and download the private key, or, if you already have a key pair, you can choose to upload or paste your public key file instead.



Download the private and public keys because these files will be used later in the integration.

6. Click **Add**.

The Configuration file preview window displays the information that you need to connect to Entrust Cryptographic Security Platform Key Management Vault.

Configuration file preview

Note: This configuration file snippet includes the basic authentication information you'll need to use the SDK, CLI, or other OCI developer tool. Paste the contents of the text box into your `~/oci/config` file and update the `key_file` parameter with the file path to your private key. [Learn more](#)

```
Fingerprint
1fe9:1d:c0:bb:30:cc:42:74:ca:33:b4:d7:ff:f4:09
```

```
[DEFAULT]
user=ocid1.user.oc1..aaaaaaa443hpmnhcsxkli7ta6tea4d2cvn6crnq3zxyom3gppfz5nsu4a
fingerprint=1f:e9:1d:c0:bb:30:cc:42:74:ca:33:b4:d7:ff:f4:09
tenancy=ocid1.tenancy.oc1..aaaaaaaavugauj3y6gakzqvofrgmxbbcx5q3xxz44pkw2vwkpczchjqw2wa
region=us-ashburn-1
key_file=<path to your private keyfile> # TODO
```

Configuration file preview [DEFAULT] user=ocid1.user.oc1..aaaaaaa443hpmnhcsxkli7ta6tea4d2cvn6crnq3zxyom3gppfz5nsu4a fingerprint=1fe9:1d:c0:bb:30:cc:42:74:ca:33:b4:d7:ff:f4:09

[Copy](#)

7. Click **Copy** to copy the file, and paste it somewhere you can access later on.

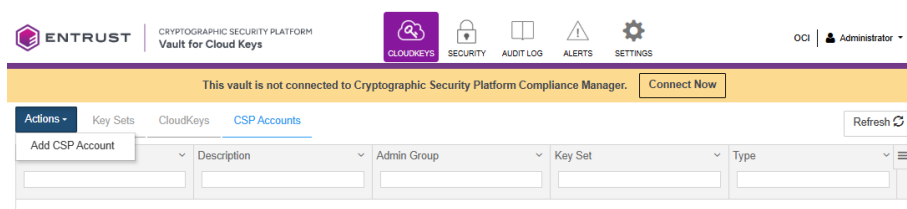
```
[DEFAULT]
user=ocid1.user.oc1..aaaaaaa443hpmnhcsxkli7ta6tea4d2cvn6crnq3zxyom3gppfz5nsu4a
fingerprint=1f:e9:1d:c0:bb:30:cc:42:74:ca:33:b4:d7:ff:f4:09
tenancy=ocid1.tenancy.oc1..aaaaaaaavugauj3y6gakzqvofrgmxbbcx5q3xxz44pkw2vwkpczchjqw2wa
region=us-ashburn-1
key_file=<path to your private keyfile> # TODO
```

2.3.4. Add a Cloud Service Provider Account for OCI



It may take up to 5 minutes for a new API key to become active on OCI. If you attempt to create your Cloud Service Provider account before the API key is active, it will fail with the following error: **Failed to validate Access Credentials OCI returned error: Client is unauthorized. null** Wait for a few minutes before you attempt to recreate your Cloud Service Provider account. For more information, see [Adding a Cloud Service Provider Account for OCI](#).

1. Log in to the Entrust Cryptographic Security Platform Key Management Vault: Cloud Keys Vault webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, select **CloudKeys**.
3. Select the **CSP Accounts** tab.
4. Select **Actions > Add Cloud Service Provider Account**.



5. On the **Details** tab of the **Add CSP Account** dialog box, enter the account details as follows:
 - For **Name**, enter the name you want to use for the Cloud Service Provider Account.

-
- For **Description**, enter an optional description of the Cloud Service Provider Account.
 - For **Admin Group**, select the Admin Group that you want to use for the account, for example **Cloud Admin Group**.
 - For **Type**, select **OCI**.
 - For **OCI User ID**, copy the user information (everything after **user=**) from the configuration file preview.
 - For **OCI Tenancy ID**, copy the tenancy information (everything after **tenancy=**) from the configuration file preview.
 - For **OCI Region**, copy the region information (everything after **region=**) from the configuration file preview.
 - For **OCI API Key Fingerprint**, copy the fingerprint information (everything after **fingerprint=**) from the configuration file preview.
 - For **OCI API Key Content**, click **Load File** to upload the private keyfile that you generated.
 - For **OCI API Key Passphrase**, if you generated an RSA Key Pair with a passphrase, enter the passphrase here.
 - For **OCI Storage Bucket**, if you are using a virtual private vault, enter the bucket name. This is where backups of HSM-protected keys in a virtual private vault will be stored. If you have a virtual private vault, imported keys will not be stored in the Cryptographic Security Platform Vault for Cloud Keys.
 - For **OCI Storage Namespace**, if you are using a virtual private vault, enter the namespace of the storage bucket.

Add CSP Account

X

Details

Schedule

Name *

OCI CSP Account

Description

Account for Oracle Cloud Infrastructure

Admin Group *

Cloud Admin Group

Type *

OCI

OCI User ID *

ocid1.user.oc1..aaaaaaa443hpmnhcsxkli7ta6teai4d2cvwn6crnq3zxyom3gppfz5nsu

OCI Tenancy ID *

ocid1.tenancy.oc1..aaaaaaaavgauj3y6gkzqvqofrgmxbbcx5q3xxz44pkw2vwwkpzchji

OCI Region *

us-ashburn-1

OCI API Key Fingerprint *

1f:e9:1d:c0:bb:30:cc:42:74:ca:33:b4:d7:ff:f4:09

OCI API Key Content ⓘ *

api-key.private.pem

Clear

Preview

OCI API Key Passphrase ⓘ

OCI Storage Bucket ⓘ

OCI Storage Namespace ⓘ

Cancel

Continue

6. Click **Continue**.

7. On the **Schedule** tab, determine the rotation schedule. This can be one of the following:

- Never: The api keys will never be rotated.

- Every x days: The API keys will be rotated after x days, where x is a value from 1 to 540.
- Every x weeks: The api keys will be rotated after x weeks, where x is a value from 1 to 72.
- Every x months: The api keys will be rotated after x months, where x is a value from 1 to 18.
- Every x years: The api keys will be rotated every year, where x must be "1".

8. Click **Add**.

You should be able to see the newly created CSP Account. Select it to view the details:

Details	
Name:	OCI CSP Account
Description:	Account for Oracle Cloud Infrastructure
Type:	OCI
Key Set:	Not Available
OCI User ID	ocid1.user.oc1.aaaaaaa443hpmnhcsxli7ta6teal4d2cwn6cmq3zyom3gppfz5nsu4a
OCI API Key Fingerprint	f0:9a:88:b8:3e:2e:64:f8:df:5b:e7:2e:53:be:02:14
OCI Tenancy ID	ocid1.tenancy.oc1.aaaaaaaauvgauj3y6gkzkvqofrgmxbbc5q3oxz44pkw2vwpkzchjqwv2wa
OCI Region	us-ashburn-1
OCI Storage Bucket	empty
OCI Storage Namespace	empty
Rotation Schedule:	No Scheduled Rotation
	Rotate Now

2.4. Testing the Integration

This section demonstrates one possible usage of Entrust Cryptographic Security Platform Key Management Vault in the integration. The following steps set up an OCI storage bucket where the contents are encrypted with an encryption key generated by Entrust Cryptographic Security Platform Key Management Vault and uploaded to an OCI vault.

2.4.1. Rotate the Access Credentials from Entrust Cryptographic Security Platform Key Management Vault

1. Log in to the Entrust Key Management Vault Cloud Keys Vault webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Select the **CSP Accounts** tab.
4. Select the **CSP Account** created earlier.
5. In the **Details** tab, under the **Rotation Schedule**, select **Rotate Now**.

This should rotate the API Keys. To check the rotation, you can check the **API Keys** tab in the User's page under OCI. You should see a new fingerprint for the key.

API keys

Q Search and Filter		Search
Add API key	Delete	
<input type="checkbox"/>	Fingerprint	Created
<input type="checkbox"/>	d3:a4:78:41:37:62:41:50:82:e2:98:2c:e4:fe:cd:5b	Tue, Jul 22, 2025, 19:12:24 UTC
<input type="checkbox"/>	6b:20:7f:77:d0:f2:73:0f:c7:16:1c:2f:93:ee:5b:70	Tue, Jul 22, 2025, 19:04:23 UTC
Page 1 of 1 (1 - 2 of 2 total items)		Items per page 10

2.4.2. Create a Compartment in OCI that will be used for the testing.

1. In the OCI UI, search for **compartments**.
2. Under **Services**, select **compartments**.
3. Select **Create Compartment**.
4. In the **Create Compartment** dialog, enter the following details:
 - For **Name**, enter a name for the compartment.
 - For **Description**, enter a description for the compartment.
 - For **Parent Compartment**, use the default parent compartment.
 - For the other fields, leave the default values.

The screenshot shows the 'Create Compartment' dialog in the OCI console. The 'Name' field is filled with 'KCV Compartment' and the 'Description' field is filled with 'Test KCV Integration'. The 'Security Zone' is set to 'None' and the 'Parent Compartment' is set to 'cleandrovia (root)'. There is a section for adding tags with 'Tag namespace', 'Tag key', and 'Tag value' fields. The 'Create Compartment' button is highlighted at the bottom.

5. Select **Create Compartment**.
6. Refresh the page and you should see the compartment listed.

Compartments						
Create Compartment						
Name	Status	OCID	Authorized	Security Zone ⓘ	Subcompartments	Created
cleandrovia	Active	...aue2ea	Yes	-	2	-
KCV-Compartment	Active	...o3baoa	Yes	-	0	Wed, Jul 23, 2025, 19:55:51 UTC

2.4.3. Create a Policy

Create a policy that allows storage buckets to access the master encryption keys present in the test compartment.

1. In the OCI UI, search for **policies**.
2. Under **Services**, select **policies**.
3. Select **Create Policy**.
4. In the **Create Policy** dialog, enter the following details:
 - For **Name**, enter the name of the policy.
 - For **Description**, enter a description for the policy.
 - For **Compartment**, select the compartment created earlier.
 - Under **Policy Builder**, select **Show Manual Editor** and enter the following text:

Allow service blockstorage, objectstorage-us-ashburn-1 to use keys in compartment KCV-Compartment



us-ashburn-1 is the region and **KCV-compartment** is the compartment created earlier.

5. Select **Create**.

Create Policy

Name
KCV-Policy

Description
Test KCV Integration

Compartment
KCV-Compartment

Policy Builder

Hide manual editor

Allow service blockstorage, objectstorage-us-ashburn-1 to use keys in compartment KCV-Compartment

Example: Allow group [group_name] to [verb] [resource-type] in compartment [compartment_name] where [condition]

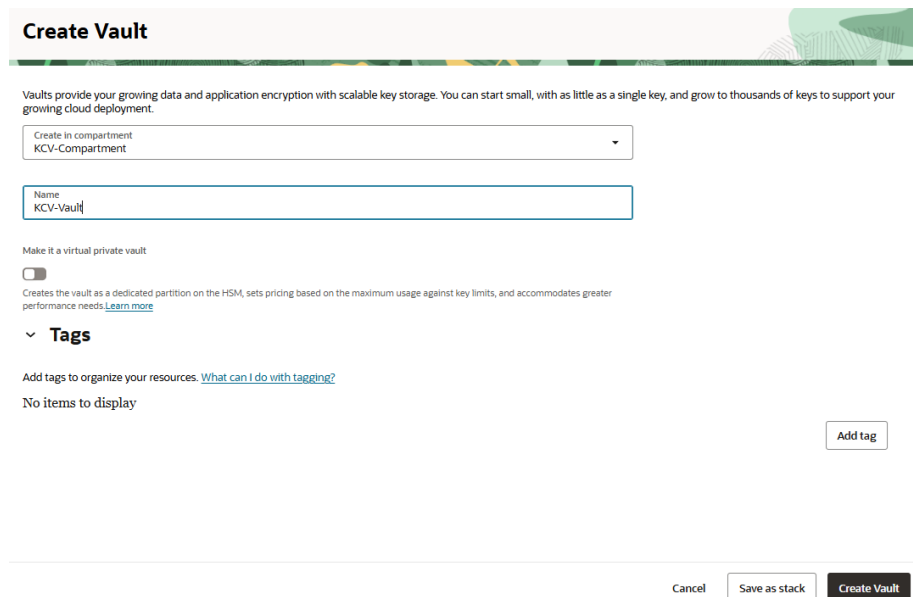
Cancel Create

2.4.4. Create a Vault

Now create a vault in the compartment created earlier.

1. In the OCI UI, search for **vault**.

2. Under **Services**, select **vault**.
3. Select **Create Vault**.
4. In the **Create Vault** dialog, enter the following details:
 - For **Create in Compartment**, select the compartment created earlier.
 - For **Name**, enter a name.
 - For the other fields, leave the default values.
5. Select **Create Vault**.



Create Vault

Vaults provide your growing data and application encryption with scalable key storage. You can start small, with as little as a single key, and grow to thousands of keys to support your growing cloud deployment.

Create in compartment
KCV-Compartment

Name
KCV-Vault

Make it a virtual private vault
☐

Creates the vault as a dedicated partition on the HSM, sets pricing based on the maximum usage against key limits, and accommodates greater performance needs. [Learn more](#)

Tags

Add tags to organize your resources. [What can I do with tagging?](#)

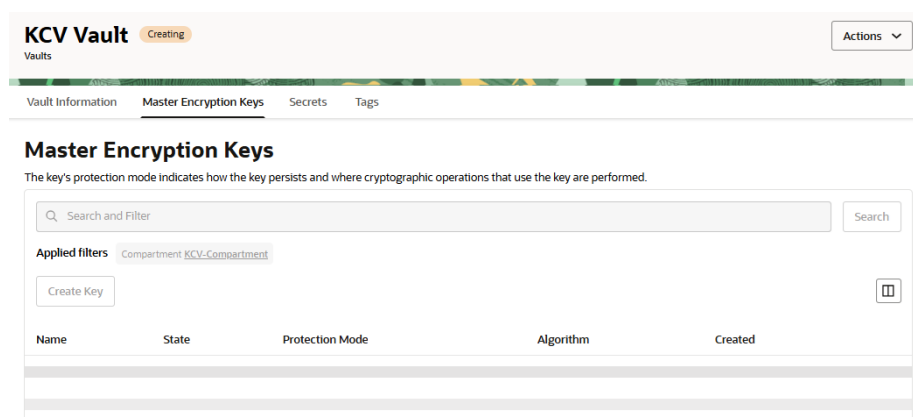
No items to display

Add tag

Cancel Save as stack Create Vault

6. Select the **Master Encryption Keys** tab in the vault that you just created.

There are no encryption keys.



KCV Vault Creating Actions

Vaults

Vault Information Master Encryption Keys Secrets Tags

Master Encryption Keys

The key's protection mode indicates how the key persists and where cryptographic operations that use the key are performed.

Search and Filter Search

Applied filters Compartment KCV-Compartment

Create Key

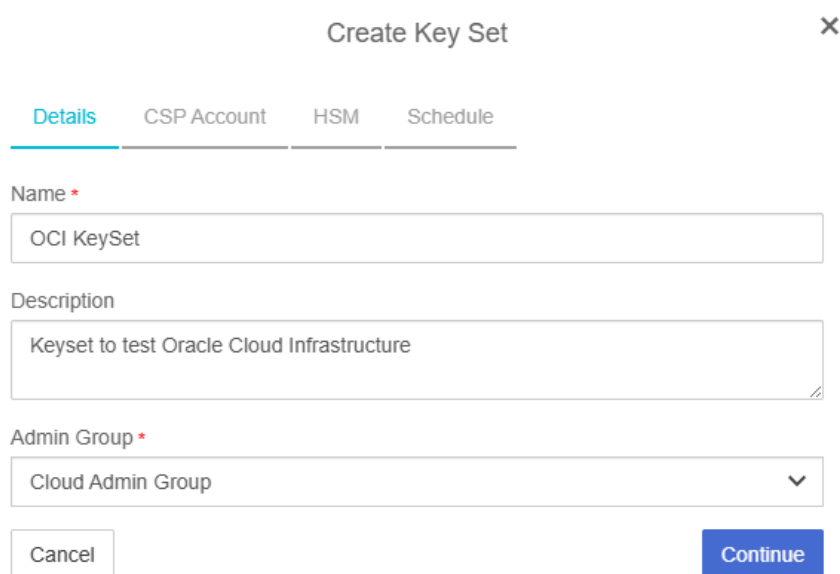
Name	State	Protection Mode	Algorithm	Created
------	-------	-----------------	-----------	---------

The next step is to use the Entrust Key Management Vault to create the encryption keys for the OCI vault, therefore bringing your own key to the vault.

2.4.5. Create a New KeySet

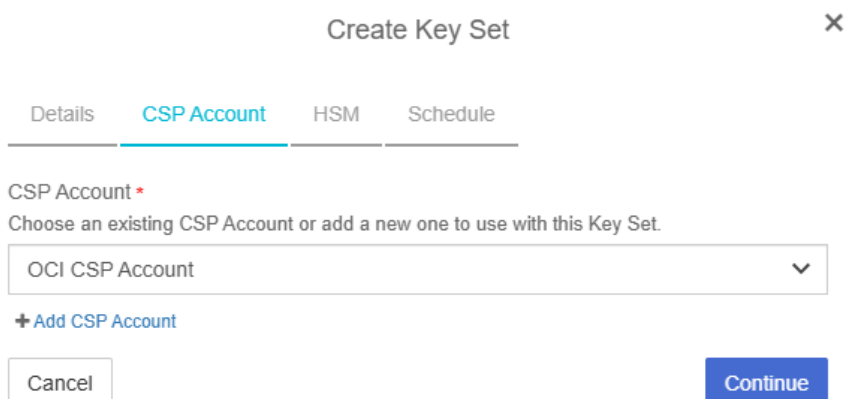
Back in the Entrust Key Management Vault CloudKey Vault webGUI, create a KeySet.

1. In the top menu bar, select **CloudKeys**.
2. Select the **KeySets** tab.
3. Select **Create a Key Set Now**.
4. In the **Choose the Type of Keys in this key set** dialog, select **OCI Key**.
5. In the **Create Key Set** dialog, in the **Details** tab, enter the following details:
 - For **Name**, enter a name for the keyset.
 - For **Description**, enter a description for the keyset.
 - For **Admin Group**, select **Cloud Admin Group**.



The screenshot shows the 'Create Key Set' dialog box with the 'Details' tab selected. The dialog has a title bar with 'Create Key Set' and a close button. Below the title bar are four tabs: 'Details' (active), 'CSP Account', 'HSM', and 'Schedule'. The 'Details' tab contains three input fields: 'Name' with the value 'OCI KeySet', 'Description' with the value 'Keyset to test Oracle Cloud Infrastructure', and 'Admin Group' with a dropdown menu showing 'Cloud Admin Group'. At the bottom are 'Cancel' and 'Continue' buttons.

6. Select **Continue**.
7. In the **Create Key Set** dialog, in the **CSP Account** tab, enter the following details:
 - For **CSP Account**, select the CSP Account created earlier.



The screenshot shows the 'Create Key Set' dialog box with the 'CSP Account' tab selected. The dialog has a title bar with 'Create Key Set' and a close button. Below the title bar are four tabs: 'Details', 'CSP Account' (active), 'HSM', and 'Schedule'. The 'CSP Account' tab contains a dropdown menu for 'CSP Account' with the value 'OCI CSP Account'. Below the dropdown is a link '+ Add CSP Account'. At the bottom are 'Cancel' and 'Continue' buttons.

8. Select **Continue**.

9. In the **Create Key Set** dialog, in the **HSM** tab:

- If Key Management Vault has been set with an HSM, select the HSM and then **Continue**.
- If not, just select **Continue**.

10. In the **Create Key Set** dialog, in the **Schedule** tab, select the rotation schedule.

11. Select **Apply**.

The KeySet gets created.

Key Set Name	Description	Admin Group	Type	Keys
OCI KeySet	Keyset to test Oracle Cloud In...	Cloud Admin Group	OCI	0

12. Check whether the KeySet has access to the Vaults in OCI that belong to the CSP Account created earlier.

13. Select the newly created KeySet.

When you select the KeySet, the **Details** Tab for the KeySet gets displayed.

14. Select the **Key Vault** Tab to view the vaults.

You should see the OCI Vaults associated with the CSP account in the KeySet. The Vault created earlier should be listed.

Name	OCID	Virtual Private Vault
test	ocid1.vault.oc1.iad.ejuib3saab5q.abuwcljs2qxq3th3ibnrswo633gwxqehjzbsyzgkxou3nbhv3d5nfdclaq	No
KCV Vault	ocid1.vault.oc1.iad.ejuicq2aahly.abuwcljsibhq4iz5xr5pmqe62eqwewx62h72fio3c6ao6fhyjjs542562q	No
myvault	ocid1.vault.oc1.iad.ejuibypmaaazk.abuwclj5twhsgzr34fpln5ftzg2glg24xsrxvprlripxn22s4molpkzgneq	No

2.4.6. Create a master encryption key in the OCI vault

Create a Cloud Key (BYOK) in the OCI vault created earlier. This will be the master encryption key for a storage bucket.

1. Log in to the Entrust Key Management Vault CloudKey Vault webGUI.
2. In the top menu bar, select **CloudKeys**.
3. Select the **CloudKeys** tab.
4. For **Key Set**, select the Key Set created earlier.
5. For **Key Vault**, select the Vault created earlier in OCI.
6. Under the **Actions** Menu, select **Create CloudKey**.
7. In the **Create CloudKey** dialog, in the **Details** tab, enter the following details:
 - The Type, Key Set and Key Vault values should be already set.
 - For **Compartment**, select the compartment created earlier in OCI.
 - For **Name**, enter a name for the Key.
 - For **Description**, enter a description for the key.

The screenshot shows the 'Create CloudKey' dialog box with the 'Details' tab selected. The dialog has a title bar with 'Create CloudKey' and a close button. Below the title bar are three tabs: 'Details' (active), 'Settings', and 'Schedule'. The 'Details' tab contains the following fields:

Type	OCI
Key Set	OCI KeySet
Key Vault	KCV Vault

Below the table are three input fields:

- Compartment ***: A dropdown menu with 'KCV-Compartment' selected and a downward arrow.
- Name ***: A text input field containing 'KCV-Key'.
- Description**: A text input field containing 'Encryption key for KCV Vault in OCI'.

At the bottom of the dialog are two buttons: 'Cancel' and 'Continue'.

8. Select **Continue**.
9. In the **Create CloudKey** dialog, in the **Settings** tab:
 - Select a **Hardware Protected** option.

Hardware Protected controls whether the key is protected by HSM in OCI and not whether the key is protected by the local HSM for the CloudKey vault.

- Select the **Cipher**.
- Select **Continue**.

×

Create CloudKey

DetailsSettingsSchedule

Hardware Protected ⓘ *

☐ Yes ☒ No

Cipher *

AES-256▼

CancelContinue

10. In the **Create CloudKey** dialog, in the **Schedule** tab, leave the default values.

11. Select **Apply**.

The CloudKey gets created.

12. Select the newly created cloudkey to view its details.

If you want to rotate the key, select **Rotate**.

13. Go back to OCI and check whether the master encryption key has been successfully created in the Vault created earlier.

KCV Vault Active

Vaults

Vault Information Master Encryption Keys Secrets Tags

Master Encryption Keys

The key's protection mode indicates how the key persists and where cryptographic operations that use the key are performed.

Applied filters: Compartment: KCV-Compartment

Name	State	Protection Mode	Algorithm	Created	
KCV-Key	Enabled	SOFTWARE	AES	Wed, Jul 23, 2025, 20:57:45 UTC	...

Page 1 of 1 (1 - 1 of 1 total items) Items per page: 10

2.4.7. Test the Key Usage

Test the Key usage by creating a bucket in OCI inside the Vault that is protected by the encryption key created earlier. The contents in the bucket will be encrypted by that key. Disable the key in the Entrust Key Management Vault Cloud Key Vault which should prevent access to the bucket contents in OCI.

2.4.7.1. Create the OCI Bucket.

1. In the OCI UI, search for **buckets**.
2. Under **Service**, select **buckets**.

3. Select **Create Bucket**.

4. In the **Create Bucket** dialog, enter the following details:

- For **Name**, enter a new name or leave the default name.
- Under **Encryption**, select **Encrypt using customer-managed keys**. The dialog prompts for the Vault and Key.
- Select the Vault and Key created earlier.
- Leave the rest of the fields with the default values.

Create Bucket

Bucket Name
KCV-Bucket

Default Storage Tier
☒ Standard
☐ Archive
The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. [Learn more about storage tiers](#)

☐ Enable Auto-Tiering
Automatically move infrequently accessed objects from the Standard tier to less expensive storage. [Learn more](#)

☐ Enable Object Versioning
Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. [Learn more](#)

☐ Emit Object Events
Create automation based on object state changes using the [Events Service](#).

☐ Uncommitted Multipart Uploads Cleanup
Create a lifecycle rule to automatically delete uncommitted multipart uploads older than 7 days. [Learn more](#)

Encryption
☐ Encrypt using Oracle managed keys
Leaves all encryption-related matters to Oracle.
☒ Encrypt using customer-managed keys
Requires a valid key from a vault that you have access to. [Learn more](#)

Vault in KCV-Compartment ([Change compartment](#))
KCV Vault

Master Encryption Key in KCV-Compartment ([Change compartment](#))
KCV-Key

Create [Cancel](#)

- Select **Create**.

2.4.7.2. Upload a text file to the newly created bucket.

In the bucket, upload a text file to test the encryption.

KCV-Bucket

Edit Visibility Move Resource Re-encrypt Add tags Delete

Bucket Information Tags

General

Namespace: idvc5quozd9
Compartment: [KCV-Compartment](#)
Created: Thu, Jul 24, 2025, 14:43:23 UTC
ETag: 741a2ee4-c781-454c-b1a5-a0d3b546a5
OCID: ...0nu7kta [Show](#) [Copy](#)

Usage

Approximate Object Count: 0 objects ⓘ
Approximate Size: 0 bytes ⓘ
Uncommitted Multipart Uploads Approximate Count: 0 uploads ⓘ
Uncommitted Multipart Uploads Approximate Size: 0 bytes ⓘ

Features

Default Storage Tier: Standard
Visibility: Private
Encryption Key: KCV-Key [Assign](#) [Edit](#) [Unassign](#)
Auto-Tiering: Disabled [Edit](#) ⓘ
Emit Object Events: Disabled [Edit](#) ⓘ
Object Versioning: Disabled [Edit](#) ⓘ

Objects

Upload More Actions ▾

<input type="checkbox"/>	Name	Last Modified	Size	Storage Tier
No items found.				

1. Select the newly created bucket.
2. Under **Objects** in the bucket view, select **Upload**.
3. In the **Upload Object** dialog, upload the text file:
 - Leave the default values for all the fields.
 - In the **Choose Files from your computer** section, upload a text file.
 - Select **Upload**.
 - Select **Close**.

Upload Objects [Help](#)

Object Name Prefix *Optional*

Hello

Storage Tier

Standard

Additional checksum *Optional*

None

Choose Files from your Computer

Drop files here or [select files](#)

hello.txt 6 bytes

1 files, 6 bytes total

[Show Optional Response Headers and Metadata](#)

Upload Cancel

You should see the uploaded object in the list.

2.4.7.3. Disable the Key in the Entrust Key Management Vault

Now if you disable the key in the Entrust Key Management Vault, you can not access the objects in the OCI Vault.

In the Entrust Key Management Vault CloudKey Vault:

1. In the top menu bar, click **CloudKeys**.
2. Select the **CloudKeys** tab.
3. For **Key Set**, select the Key Set created earlier.
4. For **Key Vault**, select the Vault created earlier in OCI.
5. Select the key.
6. In the **Actions** menu, select **Disable CloudKey**.

This vault is not connected to Cryptographic Security Platform Compliance Manager. [Connect Now](#)

Actions ▾

Key Sets

CloudKeys

CSP Accounts

Refresh ↻

Create CloudKey

Disable CloudKey

Remove from Cloud

Delete CloudKey

OCI)

Key Vault: KCV Vault

	Description	Keyvault	Compartment	Hardware Pr...	Expires	Cloud Status
KCV-Key	Master encryption ke...	KCV Vault	KCV-Compartment	No	Never	AVAILABLE

Details

Tags

Versions

Sync Now

Name:

KCV-Key

Key Id:

ocid1.key.oc1.iad.ejuicq2aahly.abuwcljta3nd4mqetfiy2gub5xxzw2dbufsr4jlganjyh44dptrvg14dyna

OCI Version:

ocid1.keyversion.oc1.iad.ejuicq2aahly.a4y6ncauzryaa.abuwcljtbirez2rc4utohytjctyegctbco6td6e27plnjgymzcgls0zi46a

Description:

Master encryption key for KCV Vault in OCI

Key Type:

Symmetric

7. In the **Disable CloudKey** dialog, select **Disable**.

Disable CloudKey

X

By disabling the following CloudKey, the key will remain in the cloud but cannot be used by applications.

CloudKey

KCV-Key

KeyId

ocid1.key.oc1.iad.ejuicql2aahly.abuwcljta3nd4mqetfiy2gub5xzxzw2d
bufsr4jlganjyh44dptrvgl4dyna

Cancel

Disable

8. Test whether you can access the bucket. You should be denied access.

KCV-Bucket

Bucket Information

Error while fetching the Bucket Information:

The KMS key was disabled. The customer-managed key associated with this bucket is disabled. (KmsKeyDisabled)

9. Enable the CloudKey again in the Key Management Vault CloudKey Vault.

Select **Actions > Enable CloudKey**.

Once enabled, the bucket can be viewed again in OCI.

KCV-Bucket

Edit VisibilityMove ResourceRe-encryptAdd tagsDelete

Bucket InformationTags

General

Namespace: idvc5guoxzd9

Compartment: [KCV-Compartment](#)

Created: Thu, Jul 24, 2025, 14:43:23 UTC

ETag: 741aeee4-c781-454c-b1a6-a0dd3b54fda5

OCID: ...olru7k1a [Show](#) [Copy](#)

Usage

Approximate Object Count: 1 objects ⓘ

Approximate Size: 6 bytes ⓘ

Uncommitted Multipart Uploads Approximate Count: 0 uploads ⓘ

Uncommitted Multipart Uploads Approximate Size: 0 bytes ⓘ

Features

Default Storage Tier: Standard

Visibility: Private

Encryption Key: KCV-Key ...Idyna [Edit](#) [Unassign](#)

Auto-Tiering: ● Disabled [Edit](#) ⓘ

Emit Object Events: ● Disabled [Edit](#) ⓘ

Object Versioning: ● Disabled [Edit](#) ⓘ

Objects

UploadMore Actions

Search by prefix

<input type="checkbox"/>	Name	Last Modified	Size	Storage Tier	
<input type="checkbox"/>	<input type="checkbox"/> Hellohello.txt	Thu, Jul 24, 2025, 14:52:20 UTC	6 bytes	Standard	⋮

Chapter 3. Additional resources and related products

3.1. nShield Connect

3.2. nShield as a Service

3.3. KeyControl BYOK

3.4. KeyControl as a Service

3.5. Entrust products

3.6. nShield product documentation