

Oracle Primavera Cloud

Bring Your Own Keys (BYOK) Setup Guide



G58914-02
August 2026



Oracle Primavera Cloud Bring Your Own Keys (BYOK) Setup Guide,

G58914-02

Copyright © 2014, 2026, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

1	Overview	
2	Submit a Service Request to Enable BYOK	
3	Parameters Required for the BYOK Setup	
4	Create Tag Namespace	
5	Create Tag Key Definitions	
6	Create the ADB Key	
7	Create the Object Storage Bucket Key	
8	Create Policies	
9	Verify the Vault Replica Exists	
10	Update the Service Request with the Vault OCID	
11	Appendices	
	Create a Compartment	1
	Create a Vault	1
	Replicate the Vault in <REGION_2>	2

Import an External Key	2
Re-Keying with New BYOK Keys	2

1

Overview

Note

This feature is only available for customers in the Oracle UK Sovereign Cloud (OC4) who have purchased the license for Oracle Primavera Cloud Service, BYOK for United Kingdom Sovereign Cloud.

Bring Your Own Key (BYOK) lets you use and manage your own encryption keys to secure data in Oracle Primavera Cloud environments.

By default, Oracle Primavera Cloud encrypts customer data at rest using Oracle-managed encryption keys. BYOK allows eligible customers to replace Oracle-managed keys with customer-managed keys while Oracle continues to manage the Primavera Cloud service.

With BYOK, your organization maintains ownership and lifecycle management of the encryption keys used to protect supported Primavera Cloud resources. You create, disable, and delete the keys in your OCI tenancy according to your organization's security and compliance requirements.

Benefits of BYOK

BYOK helps organizations:

- Maintain full control of encryption keys used to protect Primavera Cloud data.
- Meet internal security, governance, and regulatory requirements.
- Manage key lifecycle operations, including re-keying and retirement.
- Use Oracle Cloud Infrastructure Vault to securely store and manage encryption keys.
- Continue using Oracle-managed Primavera Cloud services while retaining control of encryption keys.
- Oracle does not require customers to manually share encryption key OCIDs. Oracle securely discovers the required resources through OCI IAM policies and defined tags.

Prerequisite

The customer tenancy must be in same regions (primary and disaster recovery) as the Oracle Primavera Cloud tenancy.

Setting up BYOK

The BYOK configuration process involves the following steps:

1. [Submit a Service Request to Enable BYOK.](#)
2. Oracle prepares your Primavera Cloud environment and provides you with the information required to configure your environment in the Service Request.
3. Create a Tag Namespace and Tag Key Definitions
 - a. [Create Tag Namespace](#)

- b. [Create Tag Key Definitions](#)
- 4. Create Keys
 - a. [Create the ADB Key](#)
 - b. [Create the Object Storage Bucket Key](#)
- 5. [Create Policies](#)
- 6. [Verify the Vault Replica Exists](#)
- 7. [Update the Service Request with the Vault OCID](#)

Your encryption keys remain in your OCI tenancy throughout this process. Oracle accesses the keys only through tightly scoped OCI Identity and Access Management (IAM) policies that you configure.

2

Submit a Service Request to Enable BYOK

You must submit a Service Request to initiate the process for setting up BYOK.

For instructions on submitting a Service Request, go to [My Oracle Support](#) site, sign in, and then select **Service Requests (SRs)**.

When filling out the Service Request, be sure to select **Oracle Primavera Cloud Service for United Kingdom Government** as the Product.

After Oracle has prepared your environment, the parameters will be provided to you in the Service Request. These parameters will be needed during the set up process. For a list of those parameters, see [Parameters Required for the BYOK Setup](#).

3

Parameters Required for the BYOK Setup

There are a number of parameters that are needed during the process of setting up BYOK. There are parameters that are provided to you in the Service Request after Oracle has prepared your environment. There are parameters that are based on how you set up your environment.

Review these parameters to be sure you have all the information you need before you begin.

Table 3-1 Parameters Provided by Oracle

Parameter	Used for
OPC_TENANCY_OCID	Oracle Primavera Cloud Tenancy OCID for creating cross-tenancy IAM policies.
OPC_BYOK_DG_OCID	OCID of opc_byok_dg Dynamic Group in Oracle Primavera Cloud tenancy.
REGION_1	Primary region for creating regional IAM policies and vault configuration.
REGION_2	Disaster recovery region for configuring vault replication for disaster recovery.

The following parameters are provided by you. If these are not already configured, you can follow the link to complete the steps before you continue with the configuration process.

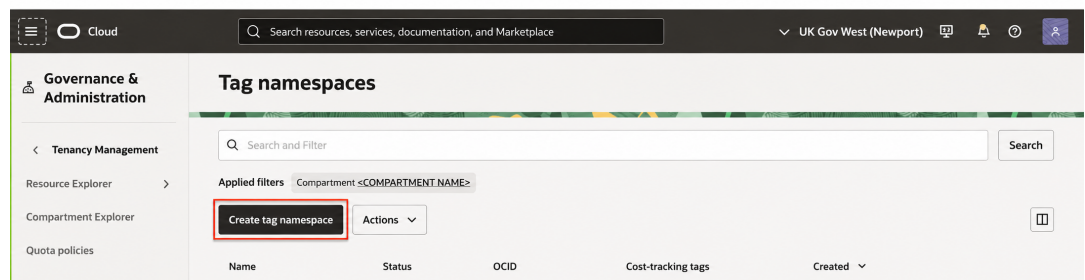
Table 3-2 Parameters Provided by Customer

Parameter	Used for
COMPARTMENT_NAME	Name of the compartment in which the Vault that will be used for Oracle Primavera Cloud BYOK is located. • If the Vault exists in the root compartment, the COMPARTMENT_NAME is the root compartment name. • If a suitable compartment does not exist and a new compartment is preferred, follow the instructions to Create a Compartment.
VAULT_NAME	Name of the Vault in <COMPARTMENT_NAME> in which to create keys for Oracle Primavera Cloud BYOK. If a suitable vault does not exist and a new vault is preferred, follow the instructions to Create a Vault .
VAULT_OCID	OCID of the Vault <VAULT_NAME>.

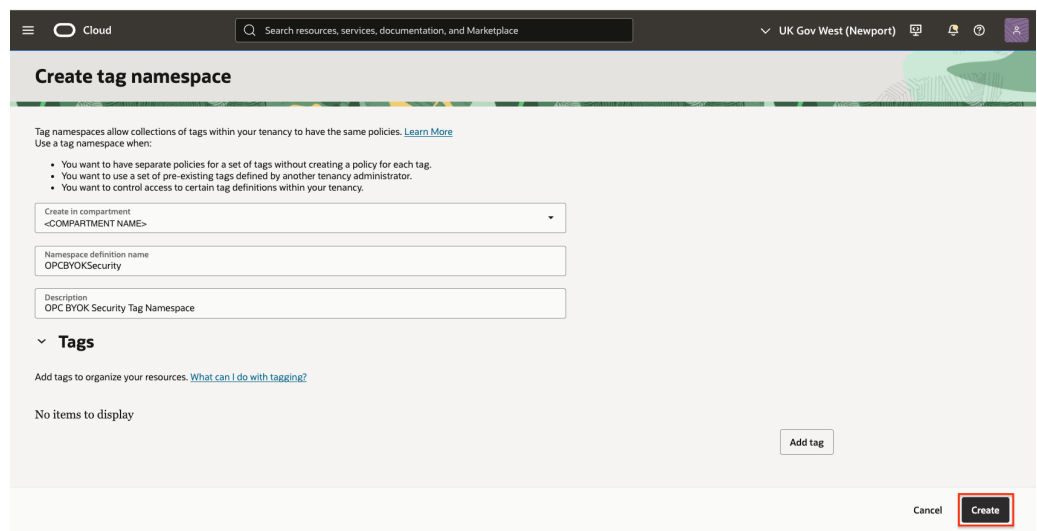
4

Create Tag Namespace

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Governance & Administration**, and in the **Tenancy Management** section, select **Tag Namespaces**.
3. On the **Tag namespaces** page, select **Create tag namespace**.



4. On the **Create tag namespace** page:
 - a. In the **Create in compartment** list, select <COMPARTMENT_NAME>.
 - b. In the **Namespace definition name** field, enter: OPCBYOKSecurity.
 - c. In the **Description** field, enter: OPC BYOK Security Tag Namespace.
 - d. Select **Create**.



5

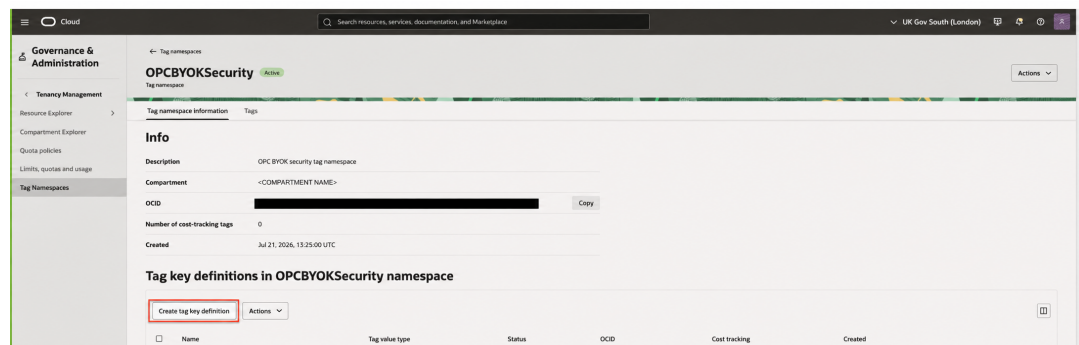
Create Tag Key Definitions

Add the following three tags to the OPCBYOKSecurity tag namespace.

- ADBKey
- BucketKey
- IsCurrent

To create namespace tags:

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Governance & Administration**, and in the **Tenancy Management** section, select **Tag Namespaces**.
3. On the **Tag namespaces** page, select **OPCBYOKSecurity**.
4. On the **OPCBYOKSecurity Tag names** page, select **Create tag key definition**.



5. On the **Create tag definition** page:
 - a. In the **Tag key** field, enter: ADBKey.
 - b. In the **Description** field, enter: BYOK Key Tag for OPC ADB Encryption
 - c. Select **Create**.

Create tag definition

This tag key definition will be created in the **OPCBYOKSecurity** namespace

Tag key
ADBKey

Description
BYOK Key Tag for OPC ADB Encryption

Cost-tracking
☐

Cost-tracking tags are passed to the billing system to allow you to filter your bill and view usage by tag. See [Using Cost-tracking Tags](#).

Tag value type

Static value
User can enter a string to set the value for this key

A list of values
User selects from a list to set the value for this key

Cancel **Create**

6. Repeat the process using the following tag key and description:
 - a. **Tag Key:** BucketKey
 - b. **Description:** BYOK Key Tag for OPC Bucket Encryption
7. Repeat one more time with the following tag key and description:
 - a. **Tag Key:** IsCurrent
 - b. **Description:** BYOK Key Tag for Identifying Current Key

OPC BYOK security tag namespace Active Actions

Tag namespace information Tags

Info

Description OPC BYOK security tag namespace

Compartment <COMPARTMENT NAME>

OCID [REDACTED] Copy

Number of cost-tracking tags 0

Created Jul 21, 2026, 13:25:00 UTC

Tag key definitions in OPCBYOKSecurity namespace

Create tag key definition Actions

Name	Tag value type	Status	OCID	Cost tracking	Created
IsCurrent	String	Active	...5uam0az2a	No	Aug 21, 2026, 16:55 UTC
BucketKey	String	Active	...yhhvu34q	No	Aug 21, 2026, 16:55 UTC
ADBKey	String	Active	...hgwv2qca	No	Aug 21, 2026, 16:54 UTC

After all tag definitions are created, the key definitions are shown in the OPCBYOKSecurity Tag namespace **Status** column as **Active**.

6

Create the ADB Key

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
3. On the **Vaults** page, select the **Vault** list and select <VAULT_NAME>.
4. On the **Vaults** details page, select **Master encryption keys**.
5. Select **Create Key**.
6. On the **Create Key** page, enter the following:
 - a. In the **Create in Compartment** list, select the <COMPARTMENT_NAME>.
 - b. In the **Protection Mode** list, select **HSM**.
 - c. In the **Name** field, enter: OPCBYOKADBKey1. Or, you can enter whatever name you choose.
 - d. In the **Key Shape: Algorithm** list, select **AES (Symmetric key used for Encrypt and Decrypt)**.
 - e. In the **Key Shape: Length** list, select **256 bits**.
 - f. **Import External Key**: By default, this toggle is off. It indicates OCI will create the key. If you want to import an external key, follow the instructions in [Import an External Key](#) to wrap the external key and upload, and then return here to continue.
7. In the **Tags** section, select **Add tag**.
 - a. In the **Namespace** list, select: **OPCBYOKSecurity**.
 - b. In the **Key** list, select **ADBKey**.
 - c. In the **Value** field, enter **true**.
8. In the **Tags** section, select **Add tag**.
 - a. In the **Namespace** list, select: **OPCBYOKSecurity**.
 - b. In the **Key** list, select **IsCurrent**.
 - c. In the **Value** field, enter **true**.
9. Click **Create Key**.

Cloud

Search resources, services, documentation, and Marketplace

UK Gov West (Newport)

Create Key

Create in Compartment
<COMPARTMENT NAME>

Protection Mode
HSM

Name
OPCBYOKADBKey1

Key Shape: Algorithm
AES (Symmetric key used for Encrypt and Decrypt)

Key Shape: Length
256 bits

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

Import External key
☐

Tags

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

Namespace OPCBYOKSecurity	Key ADBKey	Value true	X
Namespace OPCBYOKSecurity	Key IsCurrent	Value true	X

Add tag

Cancel

Create Key

Terms of Use and Privacy

Cookie Preferences

Copyright © 2026, Oracle and/or its affiliates. All rights reserved.

7

Create the Object Storage Bucket Key

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
3. On the **Vaults** page, select the **Vault** list and select <VAULT_NAME>.
4. On the **Vaults** details page, select **Master encryption keys**.
5. Select **Create Key**.
6. On the **Create Key** page, enter the following:
 - a. In the **Create in Compartment** list, select the <COMPARTMENT_NAME>.
 - b. In the **Protection Mode** list, select **HSM**.
 - c. In the **Name** field, enter: **OPCBYOKBucketKey1**.
 - d. In the **Key Shape: Algorithm** list, select **AES (Symmetric key used for Encrypt and Decrypt)**.
 - e. In the **Key Shape: Length** list, select **256 bits**.
 - f. **Import External Key**: By default, this toggle is off. It indicates OCI will create the key. If you want to import an external key, follow the instructions in [Import an External Key](#) to wrap the external key and upload, and then return here to continue.
7. In the **Tags** section, select **Add tag**.
 - a. In the **Namespace** list, select: **OPCBYOKSecurity**.
 - b. In the **Key** list, select **BucketKey**.
 - c. In the **Value** field, enter **true**.
8. In the **Tags** section, select **Add tag**.
 - a. In the **Namespace** list, select: **OPCBYOKSecurity**.
 - b. In the **Key** list, select **IsCurrent**.
 - c. In the **Value** field, enter **true**.
9. Click **Create Key**.

Cloud

Search resources, services, documentation, and Marketplace

UK Gov West (Newport)

Create Key

Create in Compartment
<COMPARTMENT NAME>

Protection Mode
HSM

Name
OPCBYOKBucketKey1

Key Shape: Algorithm
AES (Symmetric key used for Encrypt and Decrypt)

Key Shape: Length
256 bits

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

Import External key
☐

Tags

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

Namespace OPCBYOKSecurity	Key BucketKey	Value true	×
Namespace OPCBYOKSecurity	Key IsCurrent	Value true	×

Add tag

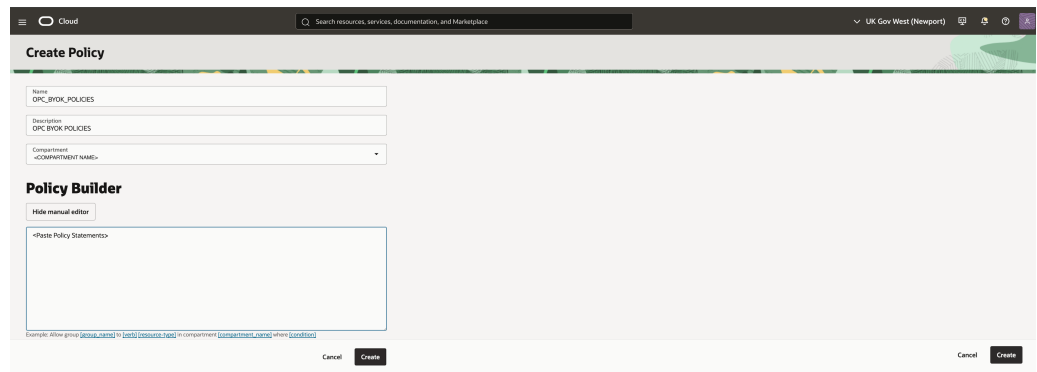
Cancel Create Key

8

Create Policies

These policies must be created in the root compartment regardless of which compartment the vaults are created in. The policies are only created once.

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Identity** section, select **Policies**.
3. On the **Policies** page, select **Create Policy**.
4. On the **Create Policy** page:
 - a. In the **Name** field, enter: OPC_BYOK_POLICIES.
 - b. In the **Description** field, enter: OPC BYOK POLICIES.
 - c. In the **Policy Builder** section, select **Show manual editor**.



- d. In the text field, enter the following policy statements.

```
define tenancy opc-tenancy as <OPC_TENANCY_OCID>
define dynamic-group opc_byok_dg as <OPC_BYOK_DG_OCID>
allow service objectstorage-<REGION_1> to use keys in compartment
<COMPARTMENT_NAME> where ALL { target.vault.id = '<VAULT_OCID>',
target.resource.tag.OPCBYOKSecurity.BucketKey = 'true' }
allow service objectstorage-<REGION_2> to use keys in compartment
<COMPARTMENT_NAME> where ALL { target.vault.id = '<VAULT_OCID>',
target.resource.tag.OPCBYOKSecurity.BucketKey = 'true' }
admit dynamic-group opc_byok_dg of tenancy opc-tenancy to use vaults in
compartment <COMPARTMENT_NAME> where target.vault.id = '<VAULT_OCID>'
admit dynamic-group opc_byok_dg of tenancy opc-tenancy to inspect keys
in compartment <COMPARTMENT_NAME> where target.vault.id = '<VAULT_OCID>'
admit dynamic-group opc_byok_dg of tenancy opc-tenancy to use keys in
compartment <COMPARTMENT_NAME> where ALL { target.vault.id =
'<VAULT_OCID>', ANY { target.resource.tag.OPCBYOKSecurity.BucketKey =
'true', target.resource.tag.OPCBYOKSecurity.ADBKey = 'true' } }
admit dynamic-group opc_byok_dg of tenancy opc-tenancy to use key-
```

```
delegate in compartment <COMPARTMENT_NAME>
admit dynamic-group opc_byok_dg of tenancy opc-tenancy to associate
keys in compartment <COMPARTMENT_NAME> with buckets in tenancy opc-
tenancy
allow service keymanagementservice to manage vaults in tenancy
```

Replace the following parameter values in the policy statements:

- <COMPARTMENT_NAME> = Name of the Compartment that contains the customer BYOK Vault with <VAULT_OCID> in the customer tenancy.

If the compartment is not in the root compartment but belongs to another compartment, the <COMPARTMENT_NAME> should include the parent compartment separated by colon, such as <COMPARTMENT_NAME> = parent compartment:compartment

For example, if the compartment COMP3 is a sub-compartment of COMP2 which is a sub-compartment of COMP1, the <COMPARTMENT_NAME> should be specified as: COMP1:COMP2:COMP3

- <VAULT_OCID> = OCID of customer BYOK Vault which will be provided by the customer.
- <OPC_TENANCY_OCID> = Oracle Primavera Cloud Tenancy OCID in the Oracle Primavera Cloud tenancy. Provided by Oracle in the Service Request.
- <OPC_BYOK_DG_OCID> = Oracle Primavera Cloud BYOK Dynamic Group OCID in the Oracle Primavera Cloud tenancy. Provided by Oracle in the Service Request.
- <REGION_1> = Oracle Primavera Cloud Primary Region Identifier. Provided by Oracle in the Service Request.
- <REGION_2> = Oracle Primavera Cloud Disaster Recovery Region Identifier. Provided by Oracle in the Service Request.

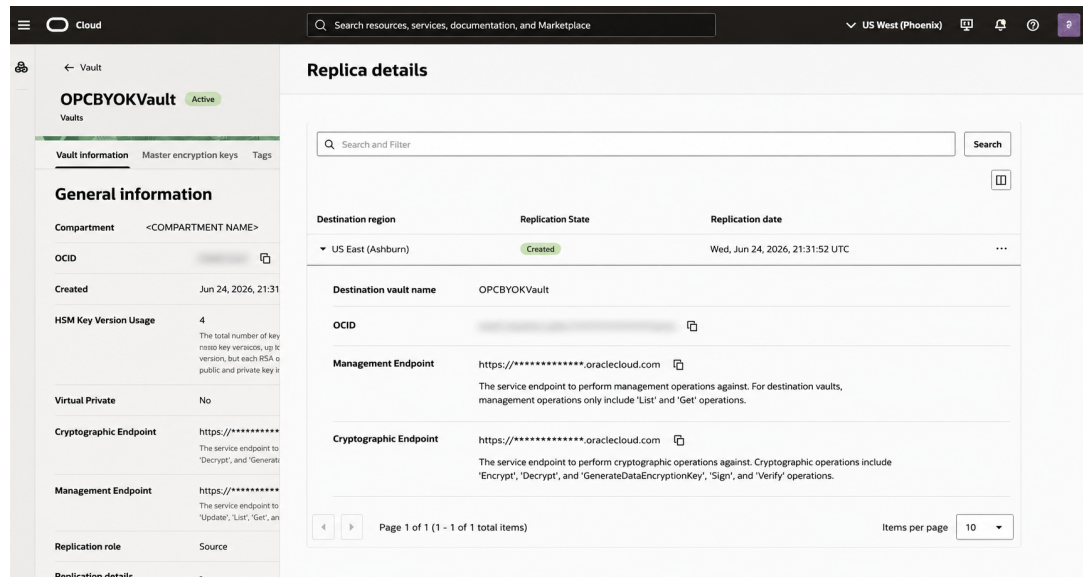
- e. Select **Create**.

Verify the Vault Replica Exists

Important: It is required that a vault replica exists in the disaster recovery region of the Oracle Primavera Cloud tenancy for BYOK encryption to work. Without a replica, the encryption process using BYOK will fail.

Verify a vault replica exists in the Oracle Primavera Cloud disaster recovery region.

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
3. On the **Vaults** page, select <VAULT_NAME>.
4. Select **Replica details**.
5. Verify there is replica for <REGION_2> under **Destination region** with a **Replication State** of **Created**. If there is no replica, proceed to [Replicate the Vault in <REGION_2>](#) to create a replica in <REGION_2>.



The screenshot shows the Oracle Cloud Console interface. On the left, the navigation menu is visible with 'Vault' selected. The main content area is titled 'Replica details' for the vault 'OPCBYOKVault'. A table lists the replica details:

Destination region	Replication State	Replication date
US East (Ashburn)	Created	Wed, Jun 24, 2026, 21:31:52 UTC

Below the table, the following details are provided:

- Destination vault name:** OPCBYOKVault
- OCID:** [Redacted]
- Management Endpoint:** https://*****.oraclecloud.com. The service endpoint to perform management operations against. For destination vaults, management operations only include 'List' and 'Get' operations.
- Cryptographic Endpoint:** https://*****.oraclecloud.com. The service endpoint to perform cryptographic operations against. Cryptographic operations include 'Encrypt', 'Decrypt', and 'GenerateDataEncryptionKey', 'Sign', and 'Verify' operations.

At the bottom, it indicates 'Page 1 of 1 (1 - 1 of 1 total items)' and 'Items per page 10'.

10

Update the Service Request with the Vault OCID

Verify a vault replica exists in the Oracle Primavera Cloud disaster recovery region.

1. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
2. On the **Vaults** page, select <VAULT_NAME>.
3. On the **Vault Information** tab, under **General information**, locate the **OCID** and select **Copy**.
4. Open the Service Request ticket, enter BYOK Keys created. Vault OCID = <VAULT_OCID>, and paste the Vault OCID into the ticket. After Oracle receives the updated ticket, Support will complete the encryption process and update your ticket when the process is complete.

Appendices

This section contains supplemental material for this document.

Create a Compartment

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Identity** section, select **Compartments**.
3. On the **Compartments** page, select **Create compartment**.
4. On the **Create compartment** page:
 - a. In the **Name** field, enter a name for your compartment. For example, you could enter: OPCBYOK
 - b. In the **Description** field, enter meaningful text to help you identify the compartment. For example, you could enter: Dedicated Compartment for Oracle Primavera Cloud BYOK vault, keys, tags, and policies.
 - c. In the **Parent compartment** list, select the root compartment.
 - d. Select **Create compartment**.

The **Status** for the compartment shows as **Creating**. This may take a minute or more. Wait until the **Status** changes to **Active**.

Create a Vault

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
3. On the **Vaults** page, select **Create Vault**.
4. In the **Create in compartment** list, select <COMPARTMENT_NAME>.
5. In the **Name** field, enter a name for your vault. For example, you could enter: OPCBYOKVault.
6. Select **Create Vault**.

The creation may take several seconds. The vault status changes from **Creating** to **Active** to indicate it is available.

Replicate the Vault in <REGION_2>

Important: The vault replica must not be removed at any time after it is created for Oracle Primavera Cloud BYOK keys to function.

To replicate the vault:

1. Sign in to the [Oracle Cloud Console](#) as an Account Administrator with appropriate privileges.
2. Open the **Navigation** menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
3. On the **Vaults** page, select <VAULT_NAME>.
4. Verify if there is replica for <REGION_2> under **Destination region** with a **Replication State** of **Created**. If there is no replica, proceed to next step to create a replica in <REGION_2>.
5. From the **Actions** menu, select **Replicate Vault**.
6. Select the <REGION_2> from the drop-down and click **Create Replica**.

The Replication State for the replica will show as **Creating**.

When the process has finished, the Replication State is **Created**.

Import an External Key

When creating a key, if you choose to import an external key, follow these instructions.

1. Wrap the external key with **OCI Vault public wrapping** key. Follow the instructions under **Wrapping the External Key Before Import** section in the topic [Creating Encryption Keys](#). This will result in a wrapped key file with extension.bin. For example, let's refer to the file as **wrappedkey.bin** file.
2. Select the **Import External Key** toggle to on.
3. Upload the wrapped key file under **External Key Data Source**. For example, **wrappedkey.bin**.
4. Return to the key creation steps.
 - [Create the ADB Key](#).
 - [Create the Object Storage Bucket Key](#).

Re-Keying with New BYOK Keys

Note

Do not delete the current keys that are being used for encryption.

1. Create a new ADB Key.
Refer to [Create the ADB Key](#). This key should have the IsCurrent tag set to true.

2. Create a new object storage bucket key.
Refer to [Create the Object Storage Bucket Key](#). This key should have the IsCurrent tag set to true.
3. Remove the IsCurrent tag from the ADB key.
 - a. Open the Navigation menu, select **Identity & Security**, and in the **Key Management** section, select **Vault**.
 - b. On the **Vault** page, from the Vault list, select the <VAULT_NAME>.
 - c. On the **Vaults** details page, select **Master encryption keys**.
 - d. Locate the currently used ADB key.
 - e. Delete the **IsCurrent** tag.
4. Remove the IsCurrent tag from the existing object storage bucket key following the process in the step above.
5. Create a Service Request ticket for re-encryption. Enter details such as: New Oracle Primavera Cloud BYOK Keys created. Requesting re-encryption of Oracle Primavera Cloud ADB and Object Storage Bucket keys.