Oracle

Cloud Infrastructure BYOK

Integration Guide

ESKM

8.54.x

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-09-09
Status	PUBLISHED
Document No.	IG-2026-0055

Table of Contents

1 About This Guide

This guide provides information on how to configure Oracle Cloud Infrastructure (OCI) to work with the Utimaco Enterprise Secure Key Manager (ESKM) for Bring Your Own Key (BYOK) scenarios. It describes the features and configuration steps in OCI and ESKM that are necessary to establish and validate the integration.

The guide describes the configuration required to securely create and manage cryptographic keys in ESKM and upload them to Oracle Cloud Infrastructure Key Management Service (OCI KMS), where they can be used by OCI services for encryption-at-rest.

This guide focuses only on the configuration and integration aspects required for the OCI–ESKM BYOK scenario. It does not provide general installation or administration procedures for OCI or ESKM beyond those required to establish the integration.

For more information on installing and configuring the Utimaco Enterprise Secure Key Manager, refer to the applicable Utimaco Enterprise Secure Key Manager installation and administration documentation.

1.1 Target Audience

This guide is intended for Oracle Cloud Infrastructure (OCI) and Utimaco Enterprise Secure Key Manager (ESKM) administrators responsible for configuring and managing the integration between OCI and ESKM.

1.2 Purpose of the Integration

The purpose of this integration is to enable Oracle Cloud Infrastructure (OCI) services to use customer-controlled cryptographic keys managed through the Utimaco Enterprise Secure Key Manager (ESKM).

In the BYOK model, cryptographic keys are created and securely managed in ESKM before being uploaded to Oracle Cloud Infrastructure Key Management Service (OCI KMS). This allows organizations to maintain control over the generation and lifecycle management of their cryptographic keys while making the keys available to OCI services for encryption-at-rest.

The integration aims to:

- Enable OCI services to use customer-controlled cryptographic keys for encryption-at-rest.
- Enable secure upload of cryptographic keys from ESKM into OCI KMS.

- Provide centralized key management and lifecycle control through Utimaco ESKM.
- Maintain secure authentication and communication between ESKM and OCI.
- Support enterprise security and compliance requirements through controlled management of cryptographic material.

1.3 Abbreviations

Abbreviation	Meaning
API	Application Programming Interface
BYOK	Bring Your Own Key
CA	Certificate Authority
ESKM	Enterprise Secure Key Manager
HSM	Hardware Security Module
IAM	Identity and Access Management
KMS	Key Management Service
OCID	Oracle Cloud Identifier
OCI	Oracle Cloud Infrastructure
RSA	Rivest–Shamir–Adleman
TLS	Transport Layer Security

Table 1: Abbreviations

1.4 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 2: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of the Partner Product

Oracle Cloud Infrastructure (OCI) is Oracle's cloud platform providing a broad range of infrastructure and platform services, including compute, storage, databases, and security services. OCI provides the Key Management Service (KMS) and Vault capabilities for creating, storing, and managing cryptographic keys used to protect data at rest across OCI services. OCI also supports Bring Your Own Key (BYOK), allowing customers to securely import externally generated cryptographic keys into OCI KMS for use by OCI services.

2.2 Overview of ESKM

ESKM is a centralized key management solution that securely stores, distributes, and manages encryption keys throughout their lifecycle. It supports industry standards, including the KMIP, enabling integration with various enterprise applications and storage systems.

2.3 Joint Value Proposition

The integration of Oracle Cloud Infrastructure (OCI) with Utimaco Enterprise Secure Key Manager (ESKM) enables customers to generate and initially protect cryptographic keys within ESKM before securely importing them into OCI Key Management Service (KMS).

The BYOK integration provides customers with greater control over the origin and initial protection of their cryptographic keys while allowing OCI services to use the imported keys for encryption-at-rest. Cryptographic keys are generated and managed within the Utimaco ESKM environment and securely transferred to OCI using the key import and wrapping mechanisms supported by OCI.

This joint solution combines OCI's cloud-native services and encryption capabilities with the centralized key management and security capabilities of Utimaco ESKM. It enables organizations to maintain control over key generation and initial key protection while leveraging OCI services, supporting enterprise security, governance, and compliance requirements.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Utimaco ESKM Version
8.54.x

Table 3: Tested versions

3.2 Supported Platforms

- Utimaco ESKM hardware appliance.
- Utimaco ESKM virtual/cloud appliance.

3.3 Hardware and Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.x
Oracle Cloud Infrastructure (OCI)	-

Table 4: Hardware and software requirements

3.4 Prerequisites

1. Utimaco ESKM version 8.54.x or later.
2. Admin access to Utimaco ESKM.
3. Access to an Oracle Cloud Infrastructure (OCI) tenancy.

4 Installing and Configuring ESKM

The following section outlines the procedures required to configure ESKM.

The initial phase involves configuring the ESKM before proceeding to Partner Product.
For detailed configuration steps, refer to the *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to the ESKM.

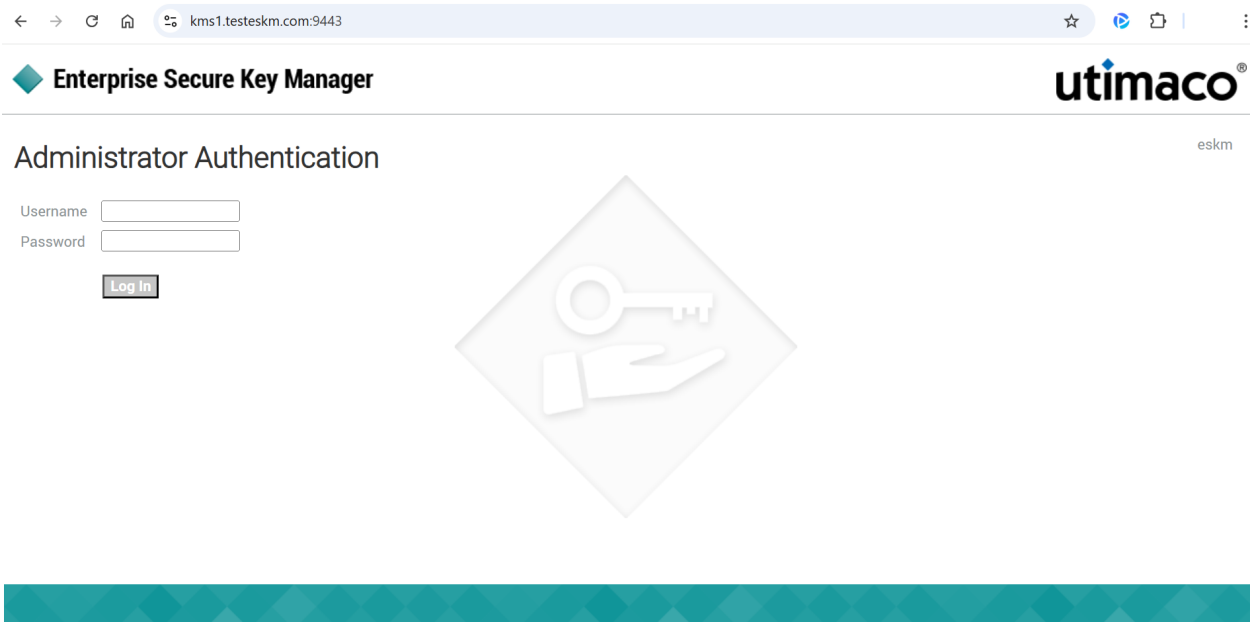

Figure 1 : ESKM login page

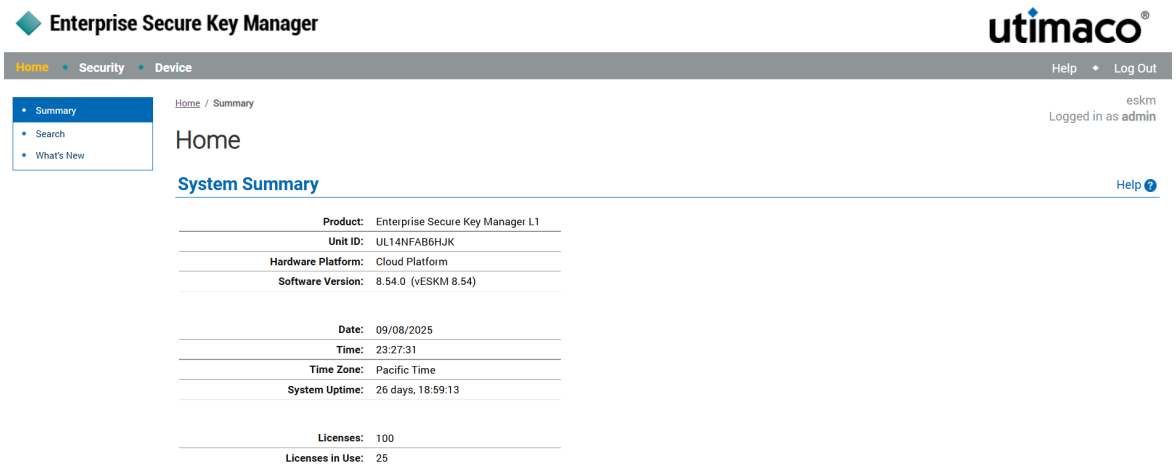

Figure 2 : ESKM home page

5 Installing and Configuring OCI

The following section outlines the procedures required to configure OCI.

The initial phase involves configuring the OCI before proceeding to Partner Product.
For detailed configuration steps, refer to the *"OCI installation Documentation"*.

After successful installation and configuration, log in to the OCI.

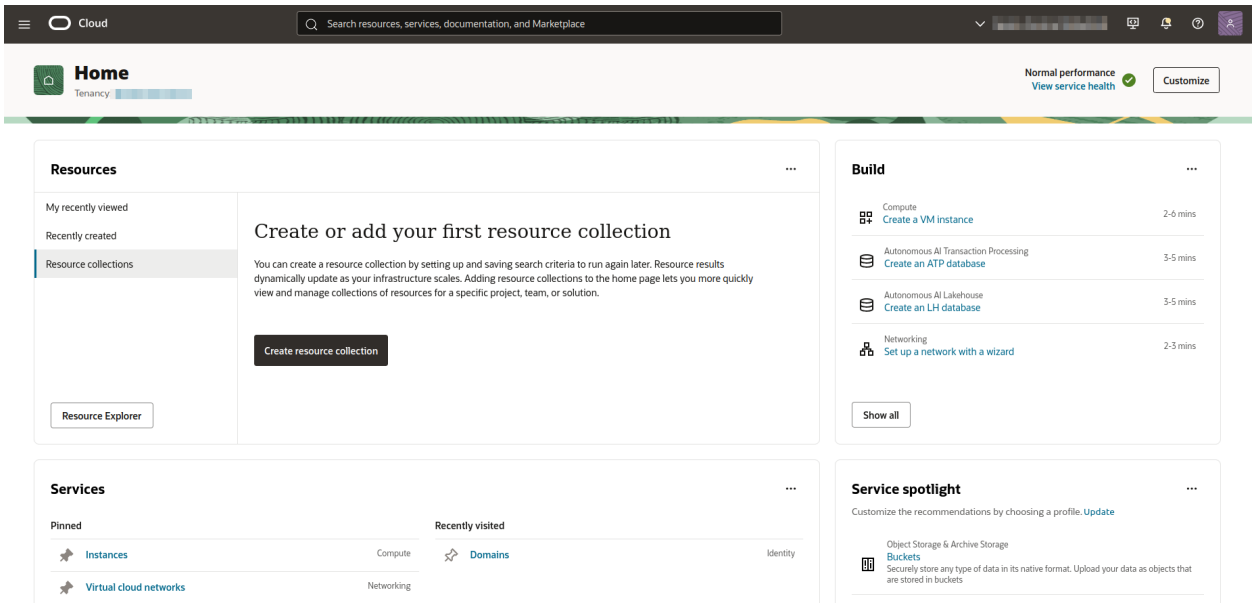

Figure 3 : OCI Login

6 Integration Steps on OCI

The following section describes the Oracle Cloud Infrastructure (OCI) configuration steps required to prepare the environment for the BYOK integration. The following sections guide you through the OCI-side configuration and the collection of the information required to establish the integration with Utimaco ESKM. The procedures assume that an OCI tenancy is already available and appropriately accessible. Therefore, the creation or initial setup of an OCI tenancy is outside the scope of this chapter. In addition, this chapter does not cover the configuration of specific OCI services that will use the imported cryptographic material. Such service-specific configuration should be performed separately according to the requirements of the corresponding OCI service.

6.1 Configure OCI Domain

The following section describes the configuration required on Oracle Cloud Infrastructure (OCI) before establishing the integration with Utimaco Enterprise Secure Key Manager (ESKM).

The OCI environment is organized into domains, which provide the administrative boundary for OCI resources and identities. Each domain is associated with an Oracle Cloud Identifier (OCID) and a deployment region.

1. Log in to the **OCI Console**.
2. Select the domain to be used for the integration.
3. Verify that the domain is associated with the required OCI region.

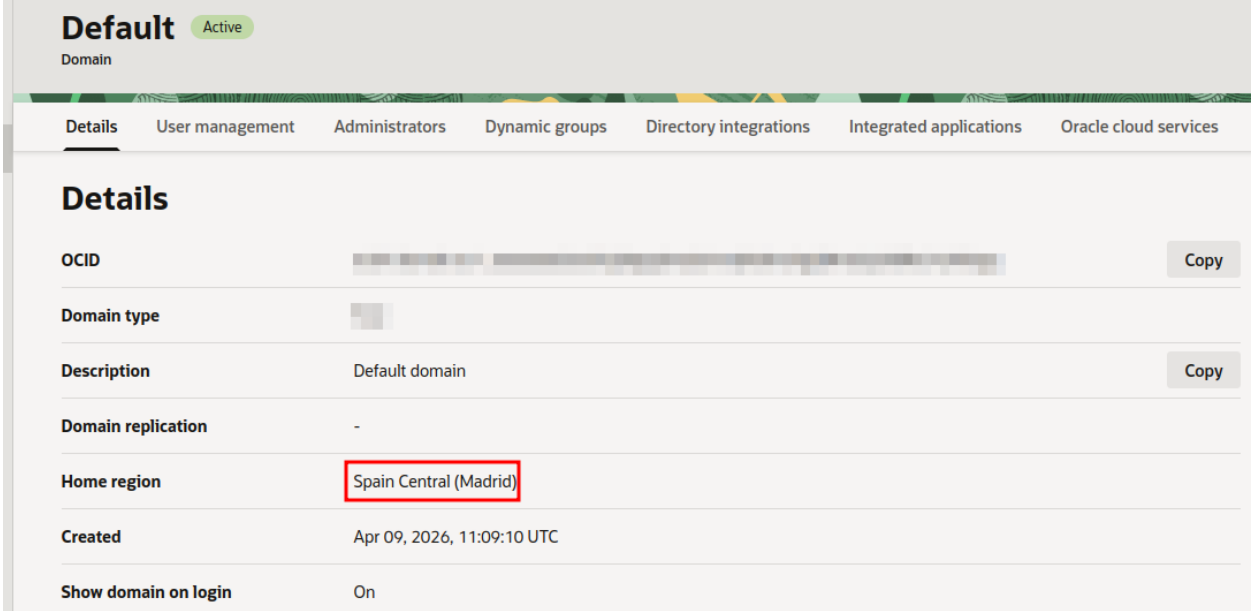

Figure 4 : OCI Domain

6.2 Create OCI Users

OCI users are used to access and manage resources within the OCI environment. Users must be created within the domain and assigned the permissions required for their respective roles.

1. In the **OCI Console**, go to **Identity & Security** > **Domains**.
2. Select the **Default** domain.
3. Select **User Management**.
4. Click **Create User**.

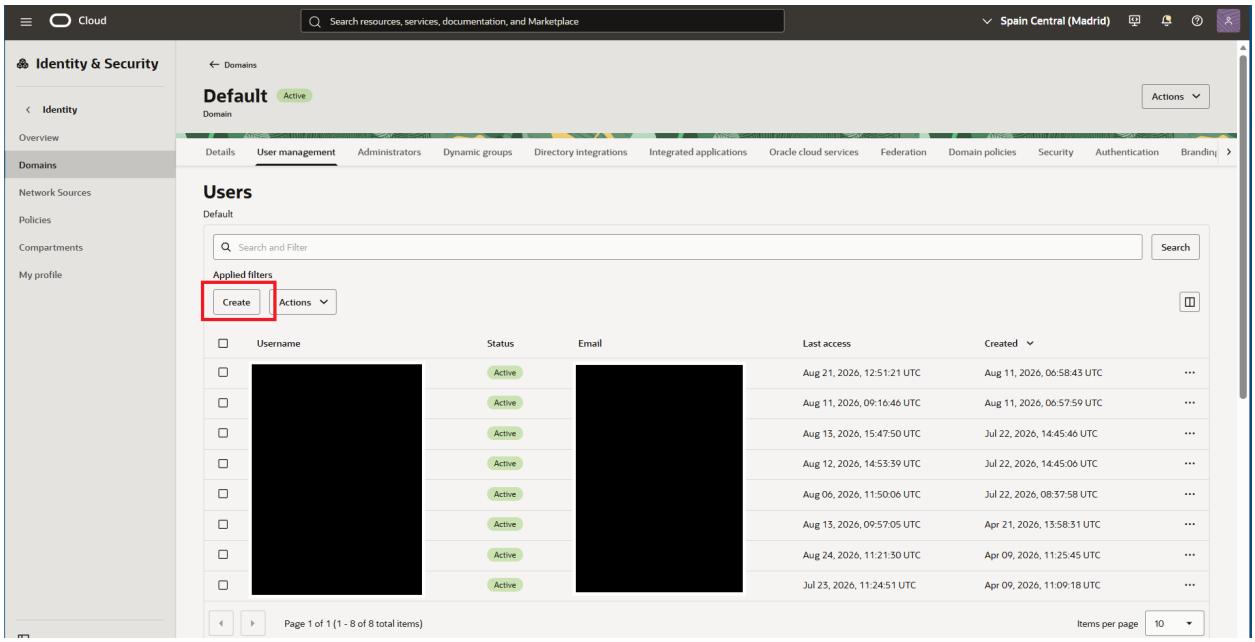

Figure 5 : OCI User Create

5. Enter the required user information, including the user name and email address.
6. Configure the required authentication settings.

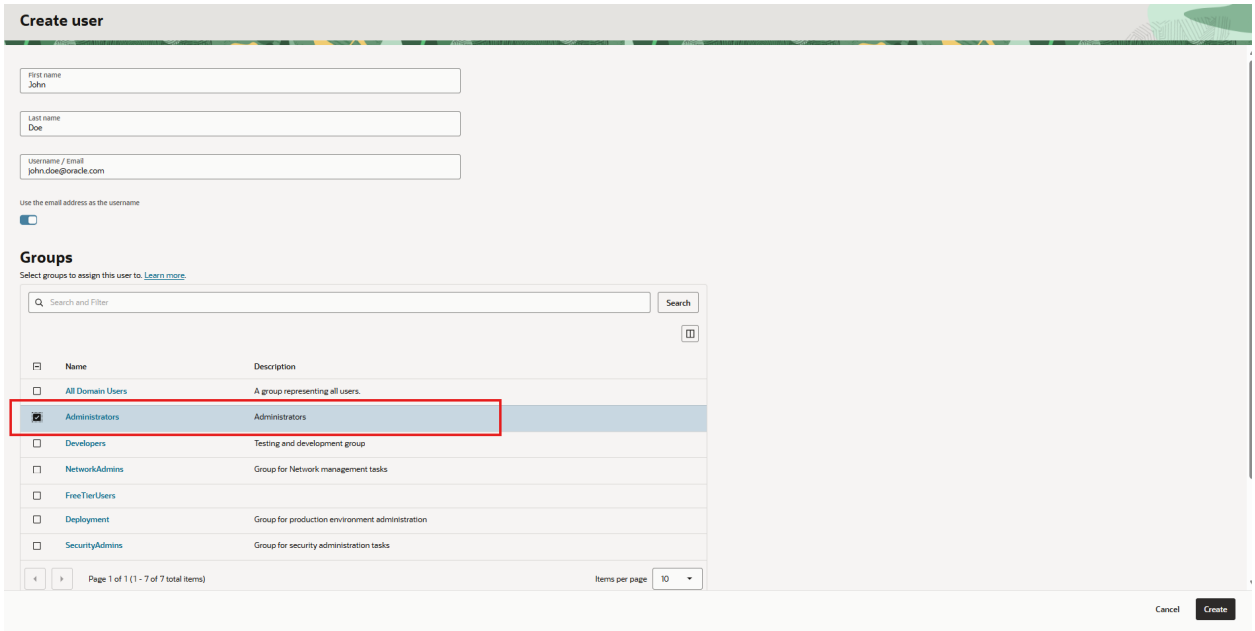

Figure 6 : OCI User Creation

7. Enable **multi-factor authentication (MFA)** for the user.
8. Add the user to the **Administrators** group.
9. Click **Create**.

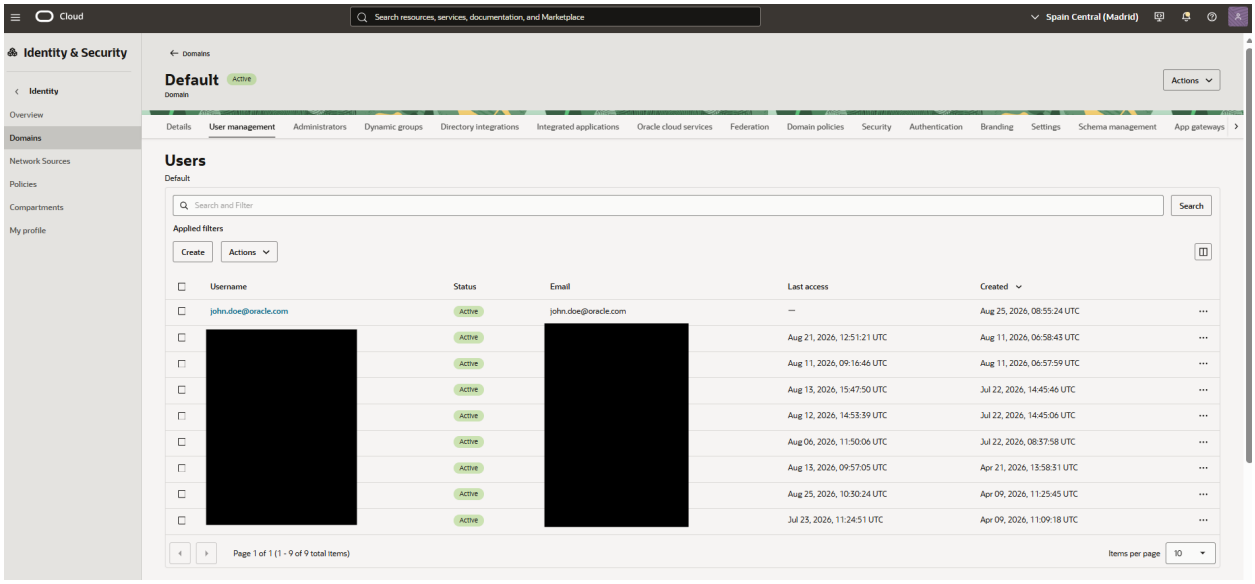

Figure 7 : User Created

Users can subsequently be assigned to one or more groups according to their required access permissions.

6.3 Create OCI Vault

The following procedure describes how to create the OCI Vault required for the OCI-BYOK integration. The Vault is used to store the keys imported from the Utimaco ESKM.

1. In the **OCI Console**, go to **Identity & Security** > **Key Management** > **Vaults**.
2. Click **Create Vault**.

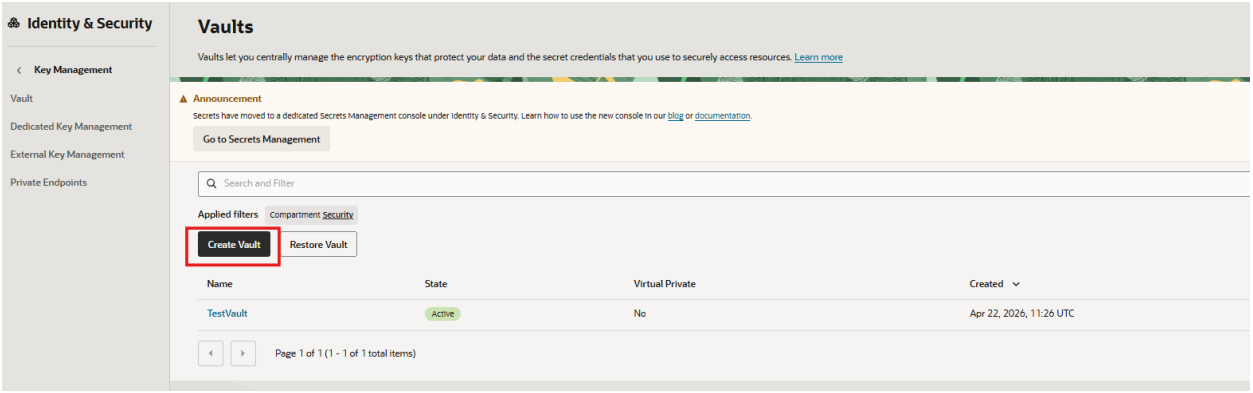

Figure 8 : Create Vault

3. Select the required **Compartment**.
4. Enter a name for the Vault.

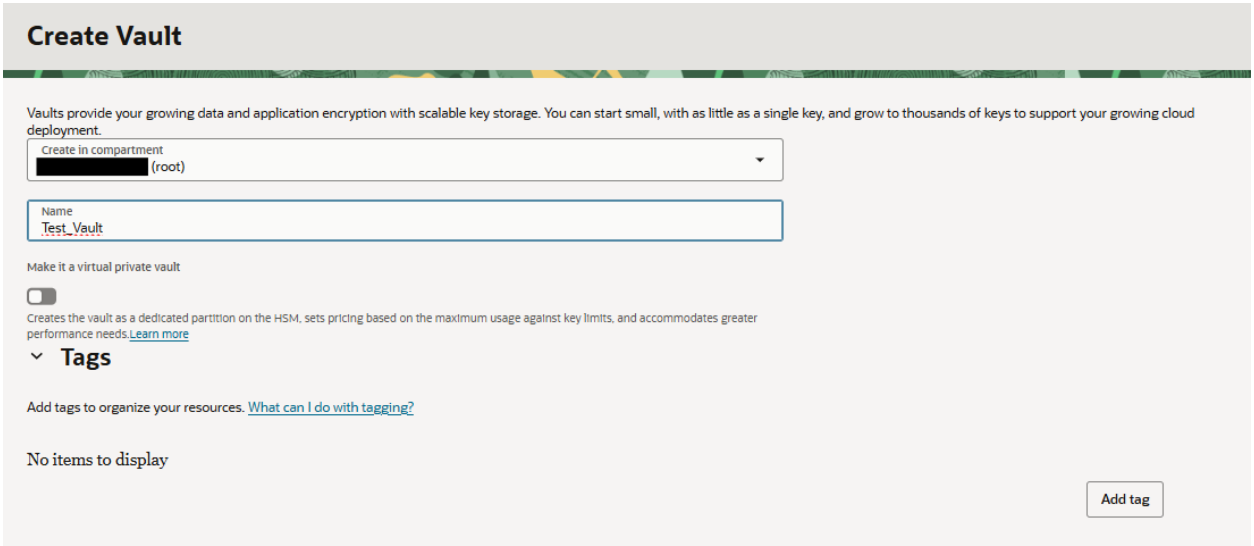

Figure 9 : Vault Creation

5. Complete the Vault creation.

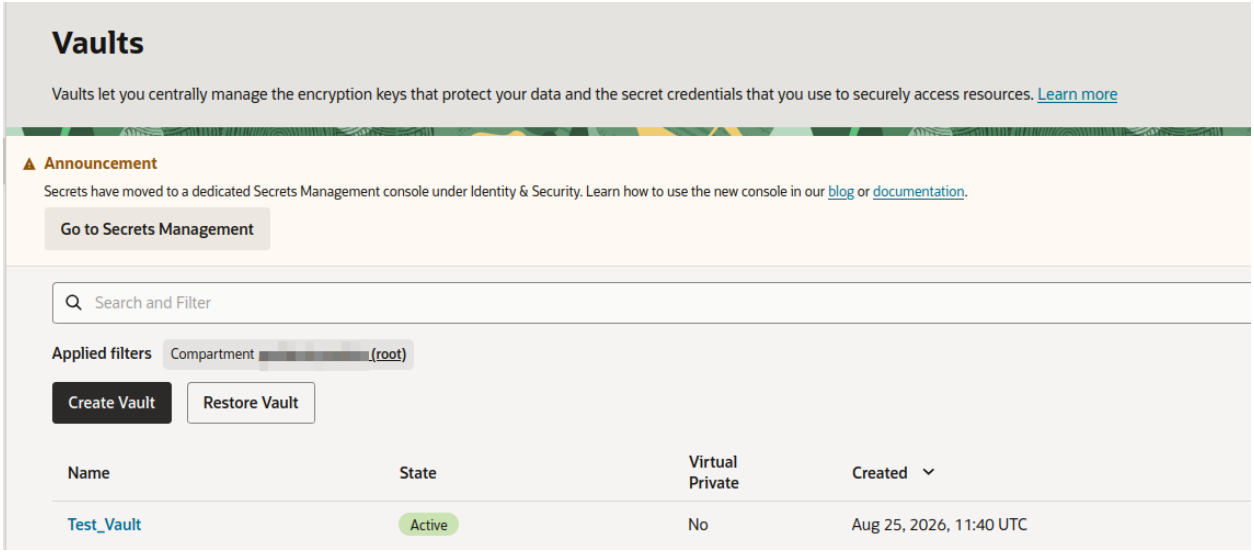

Figure 10 : Vault Created

6.4 Create API Key

The following procedure describes how to create an API key for the OCI user used by the OCI-BYOK integration. The API key enables external applications, such as Utimaco ESKM, to authenticate when accessing OCI resources.

1. In the **OCI Console**, go to **Identity & Security** > **Identity** > **My Profile**.
2. Select **Tokens and Keys**.
3. In the **API Keys** section, click **Add API Key**.

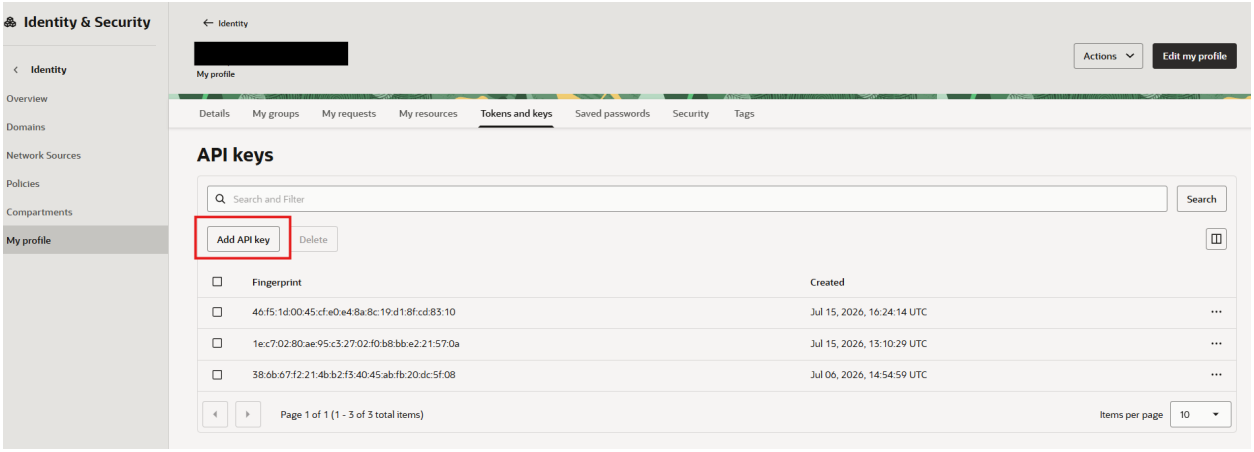

Figure 11 : Add API Key

4. Select **Generate API Key**.
5. Download the generated **Private Key** and **Public Key**.

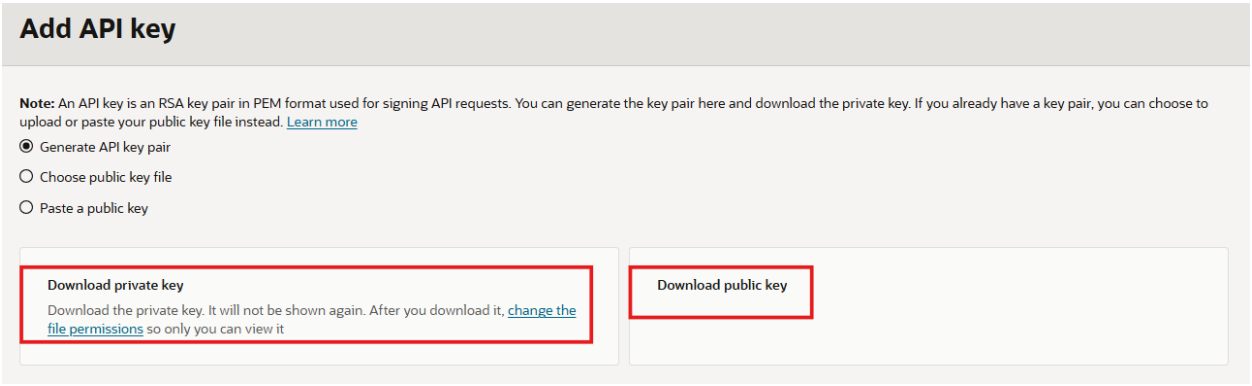

Figure 12 : API Key Generation

6. Store the downloaded **Private Key** securely. The private key cannot be retrieved again from the OCI Console after leaving the API key configuration page.
7. Click **Add** and Complete the API key configuration.

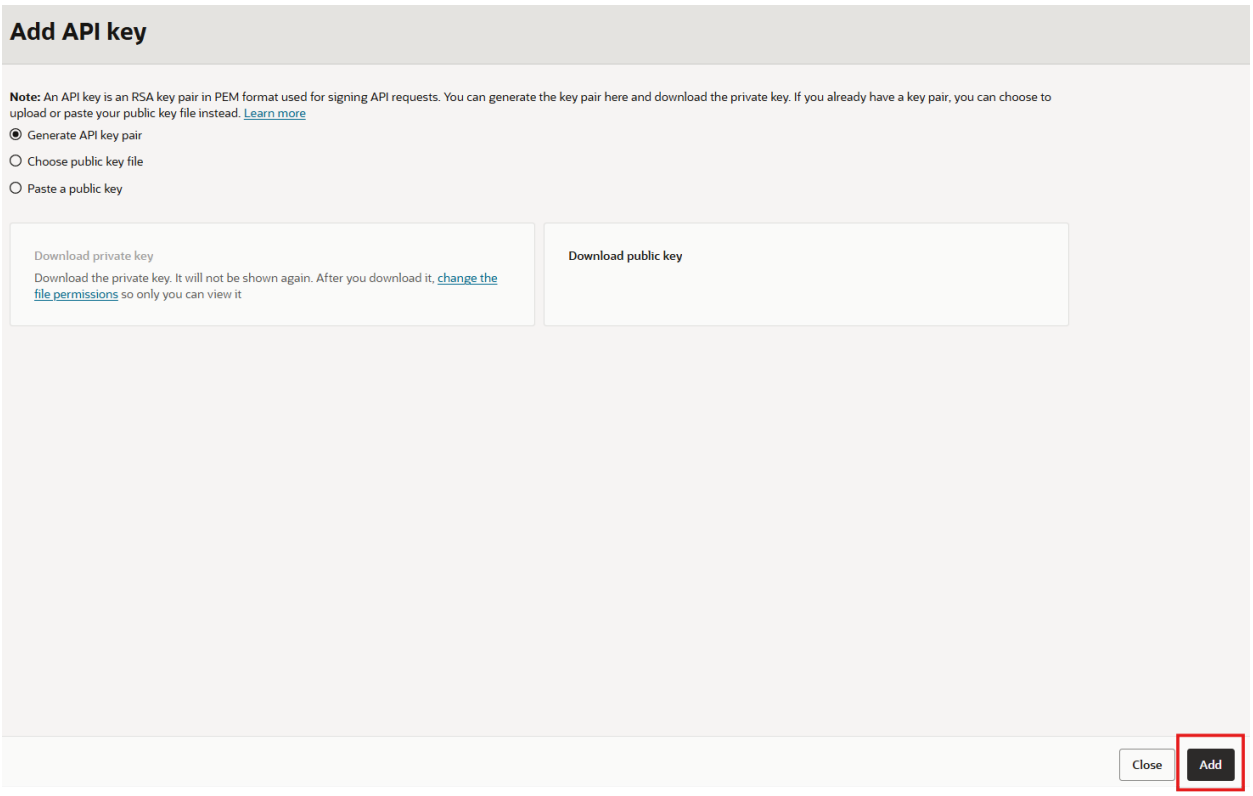

Figure 13 : API Key Added

6.5 Verify OCI Configuration

Before proceeding with the configuration of the OCI-BYOK cloud instance on ESKM, verify that the following OCI information is available and valid. These values are required later during the subsequent integration steps on the ESKM side.

6.5.1 Tenancy OCID

1. In the **OCI Console**, go to **Governance & Administration** > **Account Management** > **Tenancy Details**.
2. Verify that the **Tenancy OCID** is available and valid.

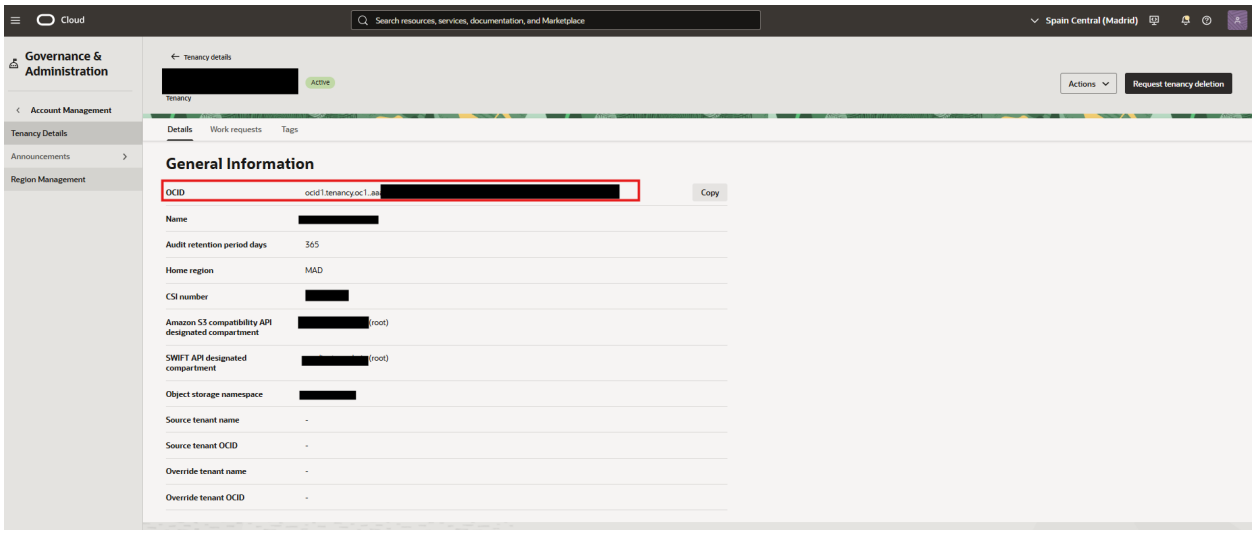

Figure 14 : Tenancy OCID

6.5.2 User OCID

1. In the **OCI Console**, go to **Identity & Security** > **Identity** > **Domains** > **Default** > **User Management**.
2. Select the user created for the integration.
3. Verify that the **User OCID** is available and valid.

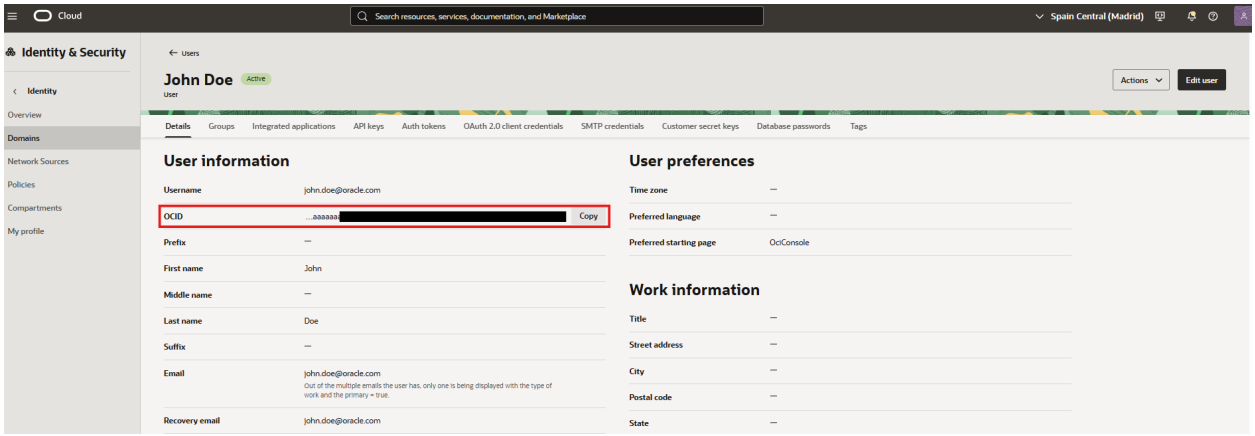

Figure 15 : User OCID

6.5.3 Fingerprint and Private Key

1. In the **OCI Console**, go to **Identity & Security** > **Identity** > **My Profile** > **Tokens and Keys**.
2. Verify that the **Fingerprint** associated with the OCI API key is available.
3. Verify that the corresponding **Private Key** is available for the ESKM configuration.

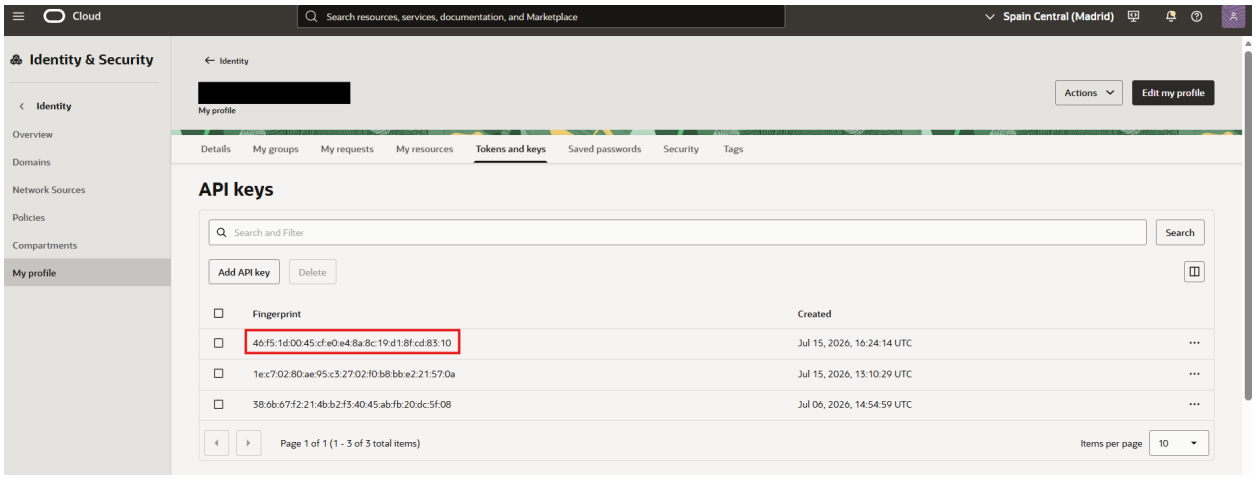

Figure 16 : Fingerprint

The **Private Key** should have been downloaded during the Create API Key Section.

6.5.4 Region

1. In the **OCI Console**, go to **Governance & Administration** > **Account Management** > **Region Management**.
2. Verify the region in which the Vault is deployed.

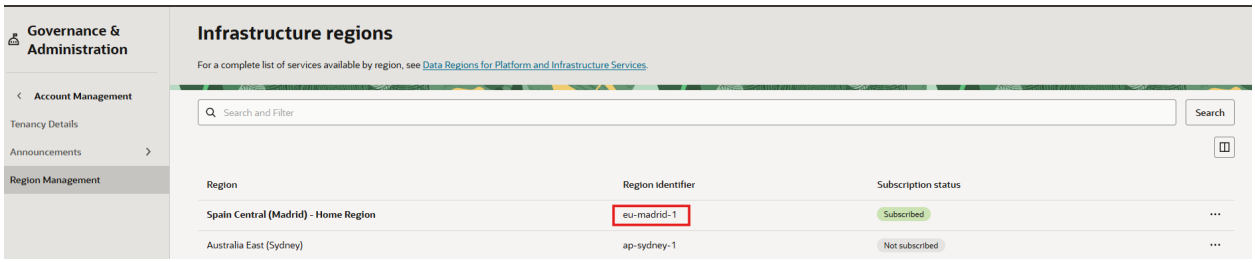

Figure 17 : Region

6.5.5 Compartment OCID

1. In the **OCI Console**, go to **Identity & Security** > **Identity** > **Compartments**.
2. Select the **root compartment**.
3. Verify that the **Compartment OCID** is available and valid.

Figure 18 : Compartment OCID

6.5.6 Vault OCID

1. In the **OCI Console**, go to **Identity & Security** > **Key Management** > **Vaults**.
2. Select the Vault created for the integration.
3. Verify that the **Vault OCID** is available and valid.

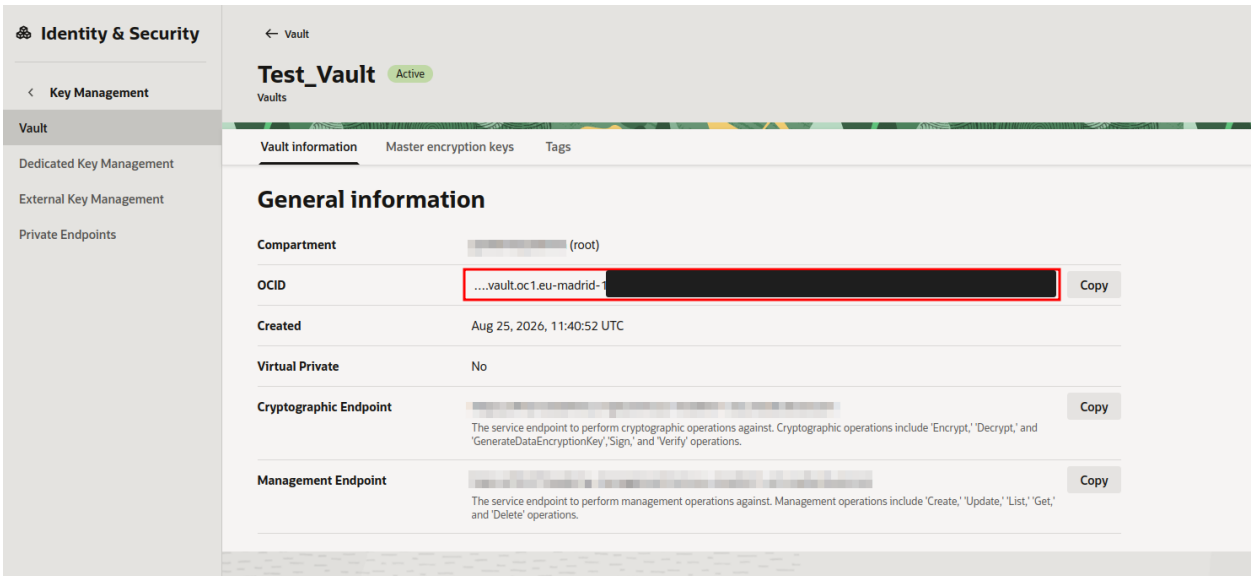

Figure 19 : Vault OCID

7 Integration Steps on Utimaco ESKM

This section describes the configuration steps required on Utimaco Enterprise Secure Key Manager (ESKM) to establish the BYOK integration. The following sections guide you through the ESKM-side configuration, including the creation of the OCI-BYOK cloud instance and the management and upload of cryptographic keys to OCI. The procedures assume that ESKM is already installed, configured, and accessible to an administrator. Therefore, the installation and general administration of ESKM are outside the scope of this chapter. The required OCI configuration and connection information is also assumed to have been prepared as described in the preceding section. Configuration of specific OCI services that will consume or use the imported cryptographic material is not covered and must be performed separately according to the requirements of the corresponding OCI service.

7.1 Add an OCI-BYOK Cloud Instance

1. Go to **ESKM Management Console** > **Security** > **Cloud Integration**.

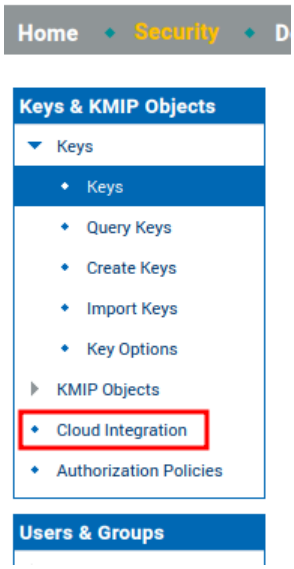

Figure 20 : Cloud Integration

2. Go to **Cloud** and click **Add Cloud Instance**.

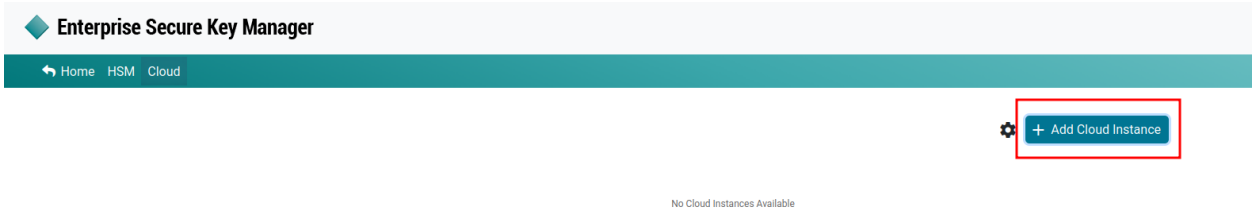

Figure 21 : Add Cloud Instance

3. Enter an **Instance Name** and select **OCI-BYOK** from the **Cloud Type** dropdown list.

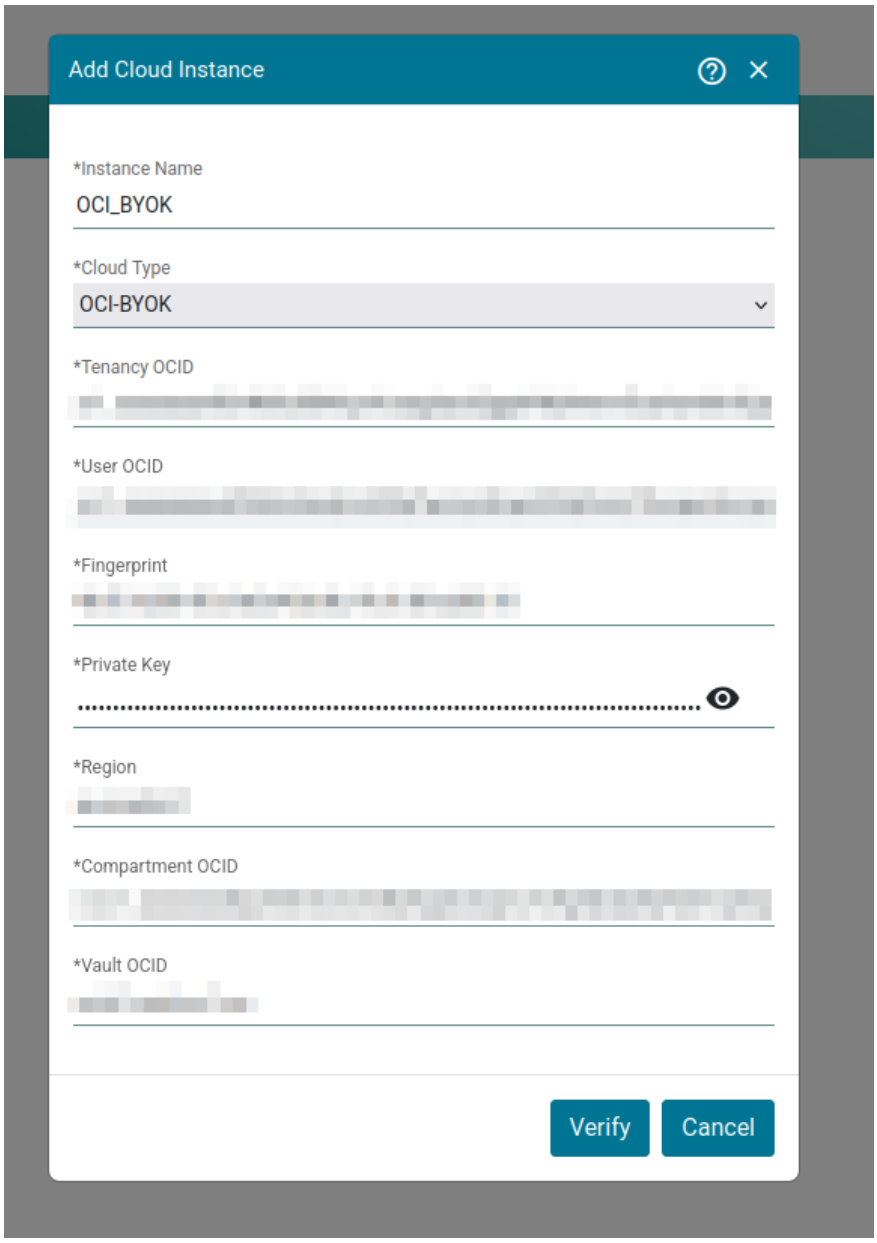

Figure 22 : Add Cloud Instance — OCI Configuration

4. Enter the required OCI information in the following fields:

    a. **Tenancy OCID**

    b. **User OCID**

    c. **Fingerprint**

    d. **Private Key**

    e. **Region**

    f. **Compartment OCID**

g. **Vault OCID**

5. Click **Verify** to verify the OCI configuration.

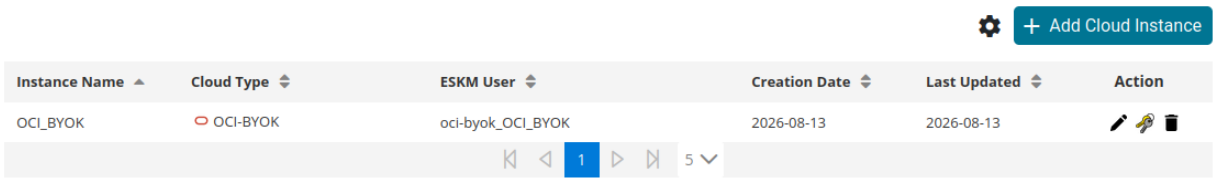

Figure 23 : OCI-BYOK Cloud Instance

7.2 Manage OCI-BYOK Keys

1. Go to **ESKM Management Console** > **Security** > **Cloud Integration**.
2. Locate the configured **OCI-BYOK** cloud instance and click **Manage Keys icon**.

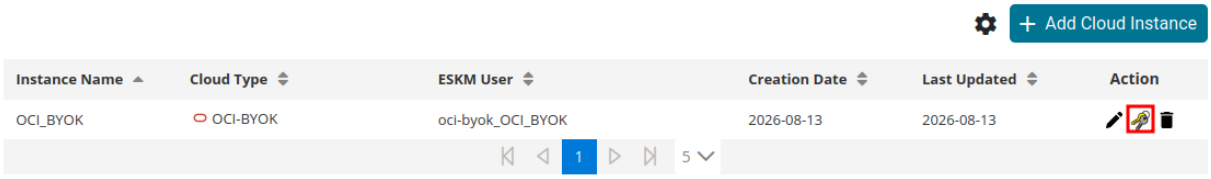

Figure 24 : OCI-BYOK Cloud Instance — Manage Keys

3. The **OCI-BYOK Keys** page is displayed.

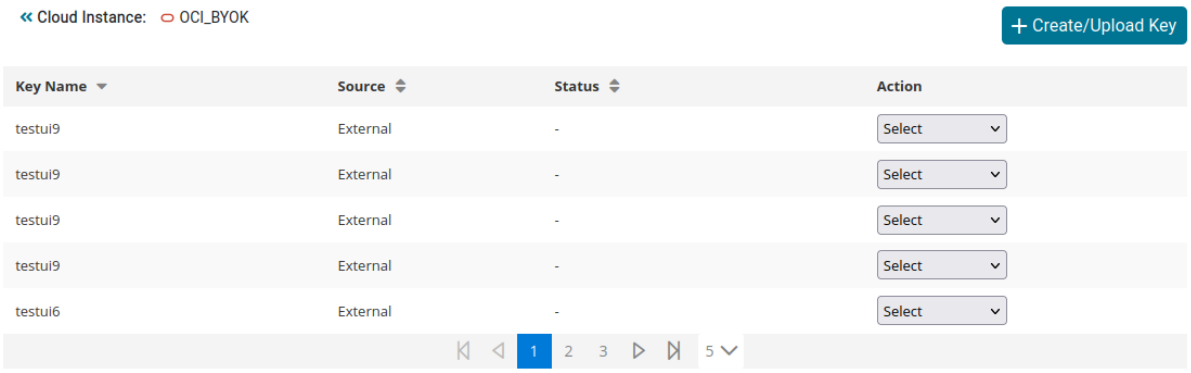

Figure 25 : OCI-BYOK Keys

4. Click the desired key from the list to view its details, then click **Close** when done.

7.3 Create and Upload a Key

1. From the **OCI-BYOK Keys** page, click **Create/Upload Key**.

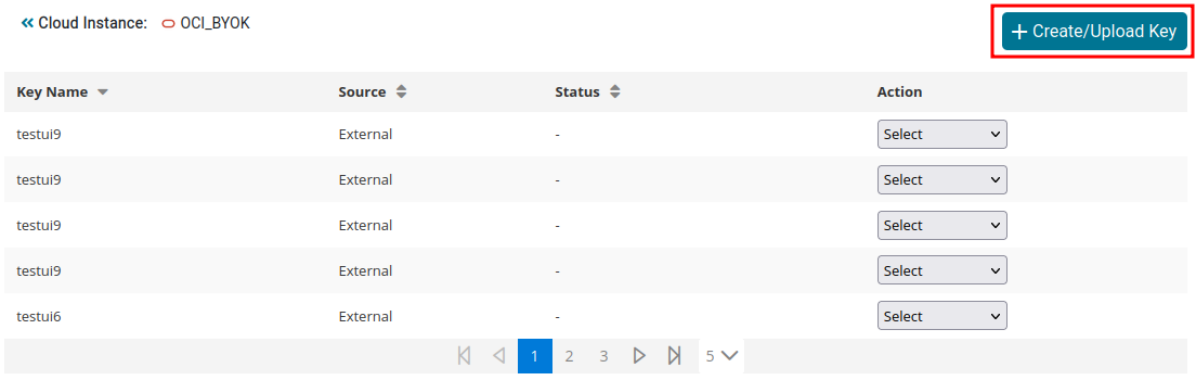

Figure 26 : Create/Upload Key

2. Select **Create Key & Upload**.
3. Enter the **ESKM Key Name** and select the required **Algorithm.**
4. Click **Create**.

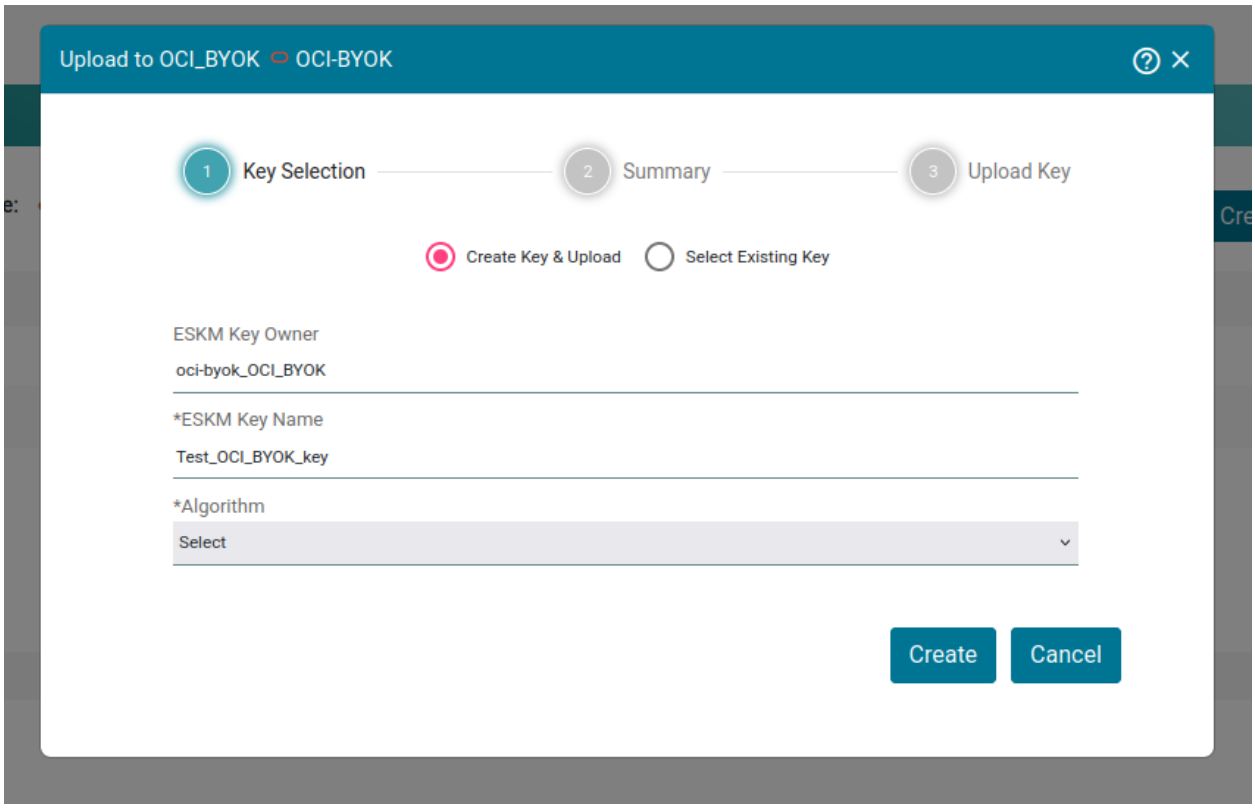

Figure 27 : Key Selection — ESKM Key Name and Algorithm

5. Review the key information displayed on the **Key Summary** page.

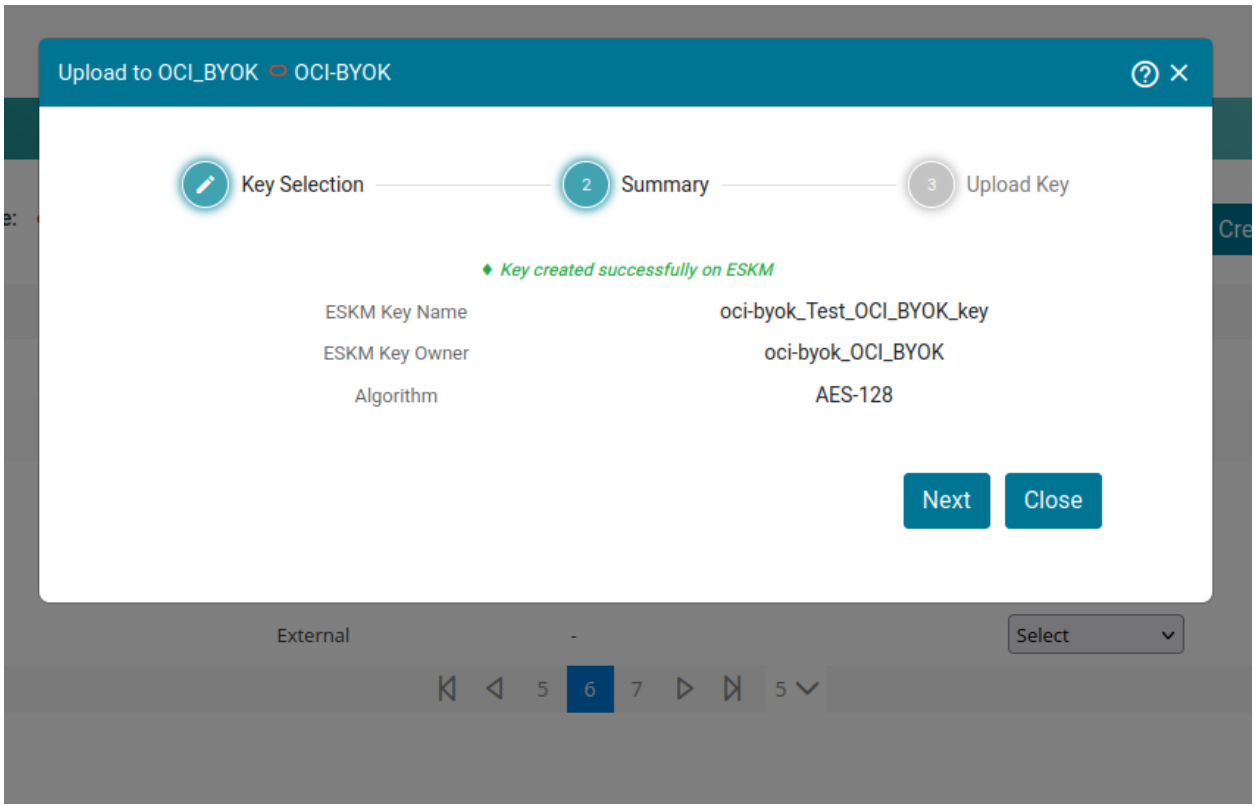

Figure 28 : Key Summary

6. Click **Next**.
7. Verify the **Cloud Key Name** and **Vault OCID**.
8. Add the required tags, if applicable.

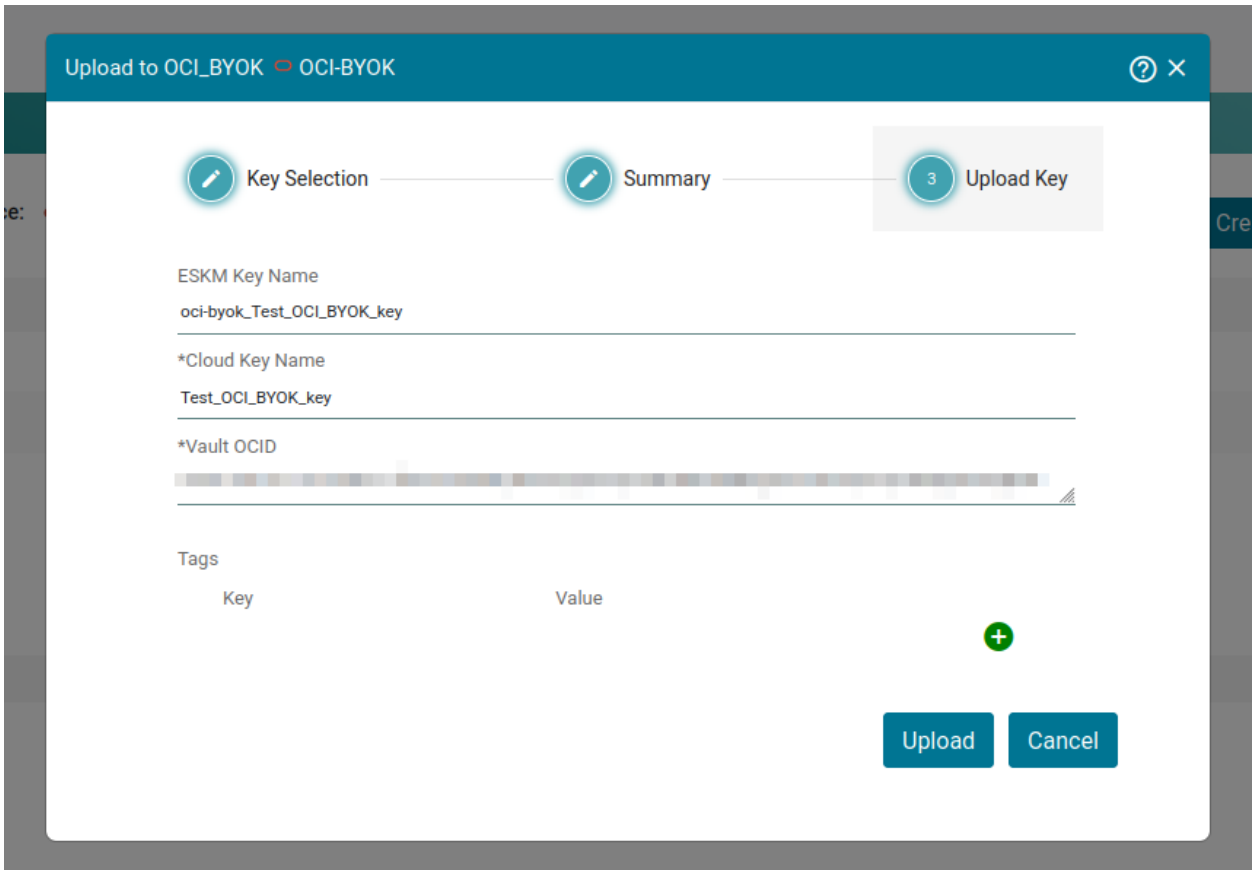

Figure 29 : Upload Key

9. Click **Upload** to upload the key to OCI.

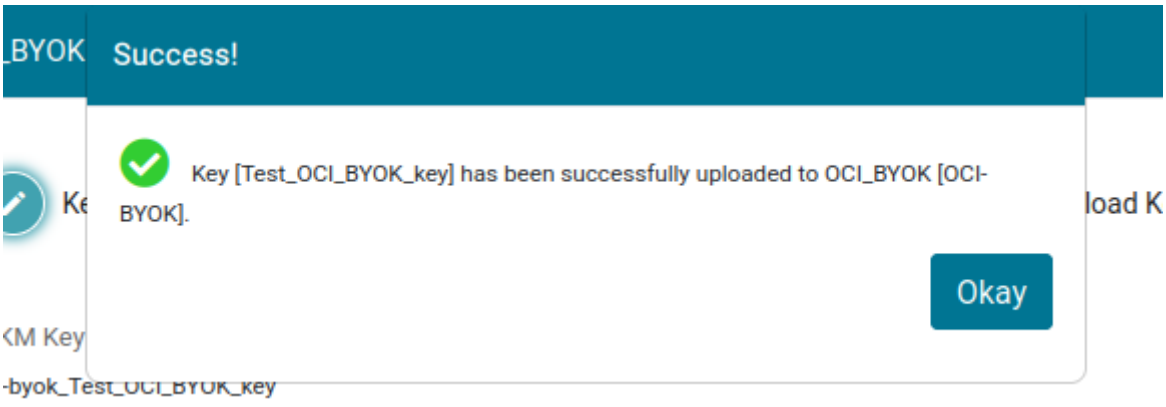

Figure 30 : Successful Key Upload

Alternatively, an existing key can be uploaded to OCI without creating a new key.

The **Search** option allows you to select an existing key that was created in another cloud instance through the dashboard and use it for the upload operation.

1. From the **OCI-BYOK Keys** page, click **Create/Upload Key**.
2. Select "**Select Existing Key**".

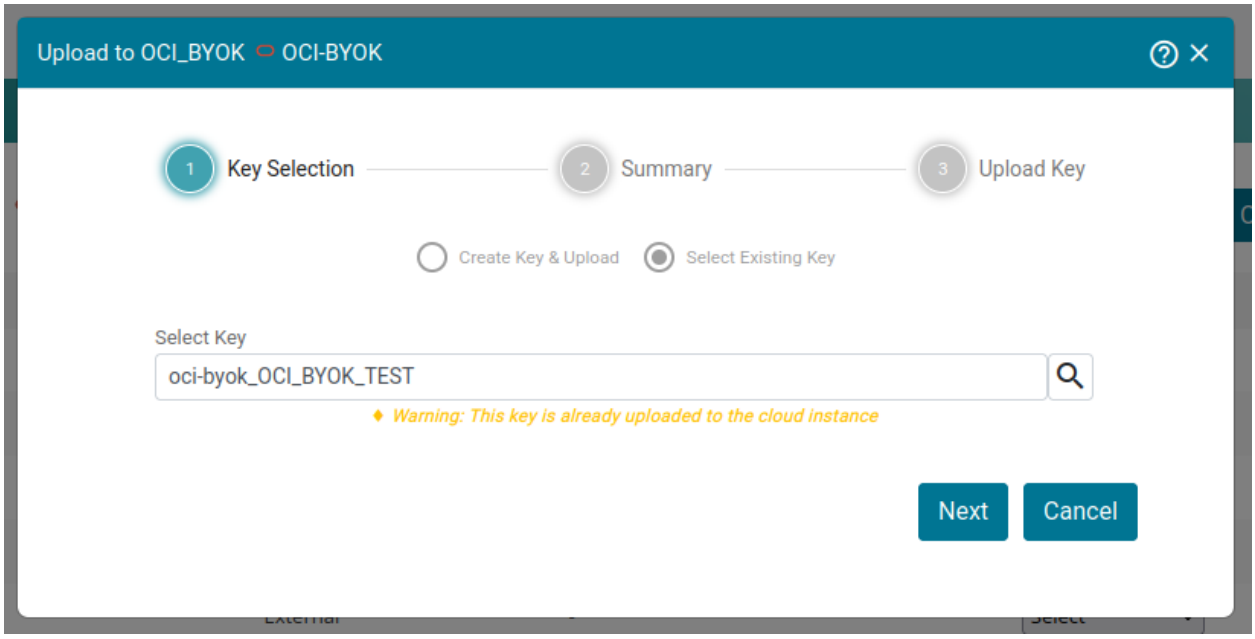

Figure 31 : Upload Key Selection

If the key is already uploaded to the cloud instance or is owned by another cloud instance, a warning will be displayed to the user.

3. Select the key to be uploaded and Click **Next**.
4. Review the key information displayed on the **Key Summary** page.

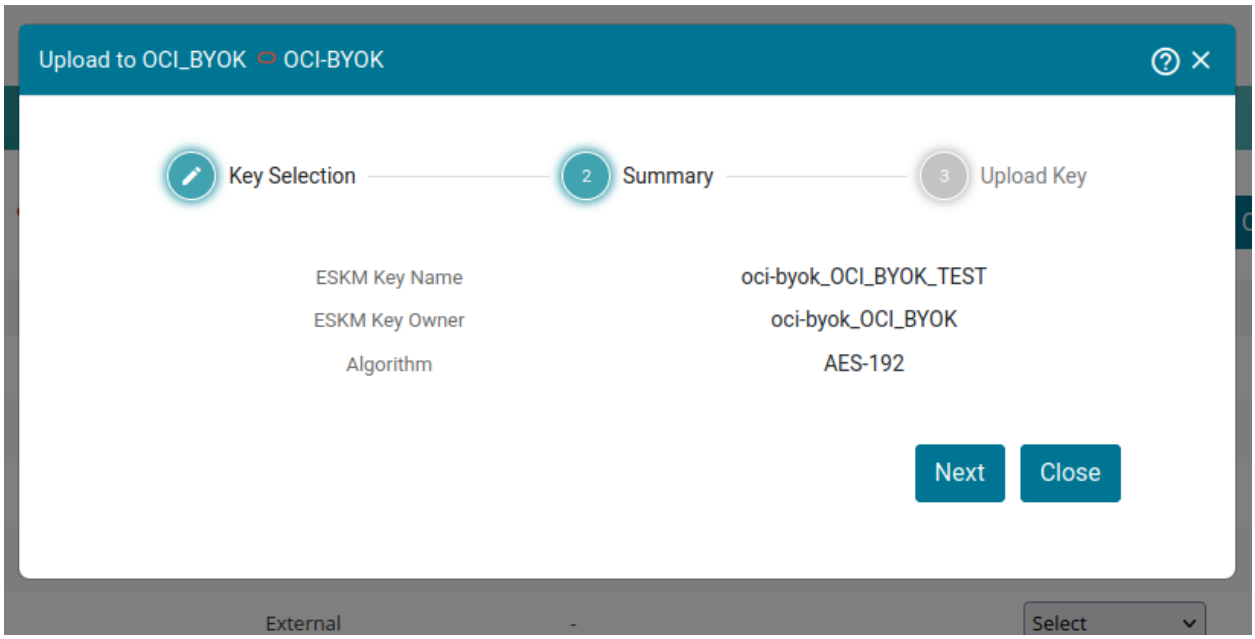

Figure 32 : Upload Key Summary

5. Click **Next**.

6. Add the required tags, if applicable.

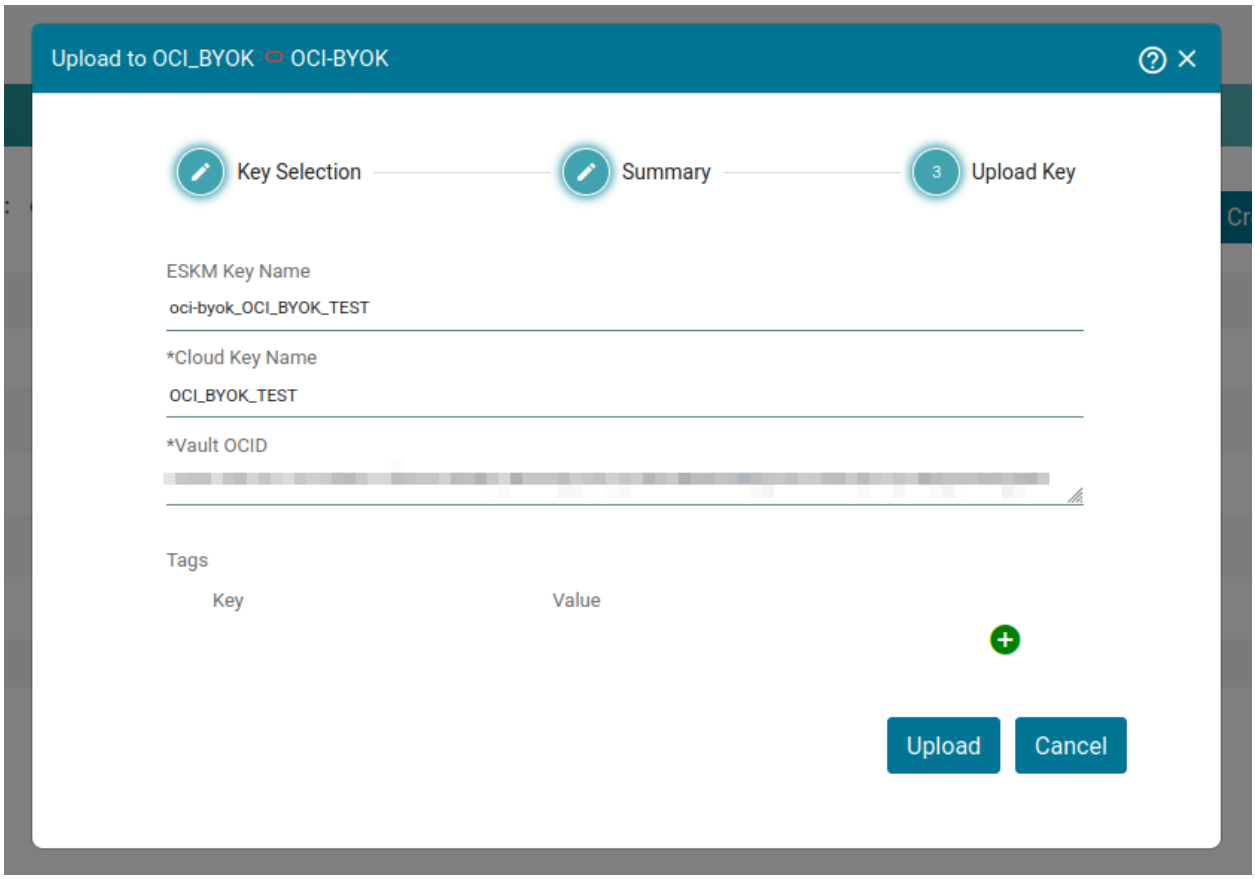

Figure 33 : Upload Key

7. Click **Upload**.

7.4 Edit an OCI-BYOK Key

1. Locate the configured **OCI-BYOK** cloud instance and click **Manage Keys**.
2. Select the key to be modified and click **Edit** from the **Action** column.

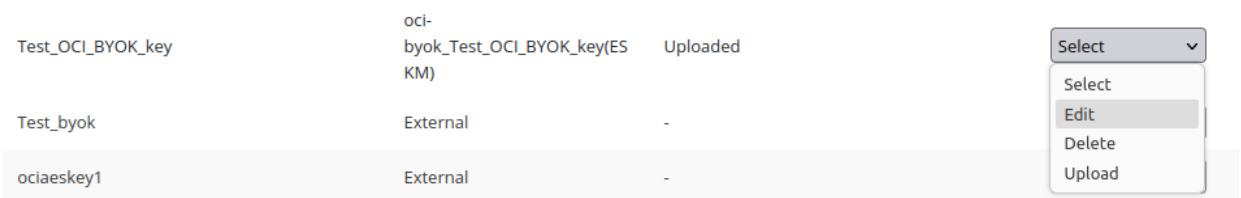

Figure 34 : Edit Action Column

3. Modify the required **key tags**.

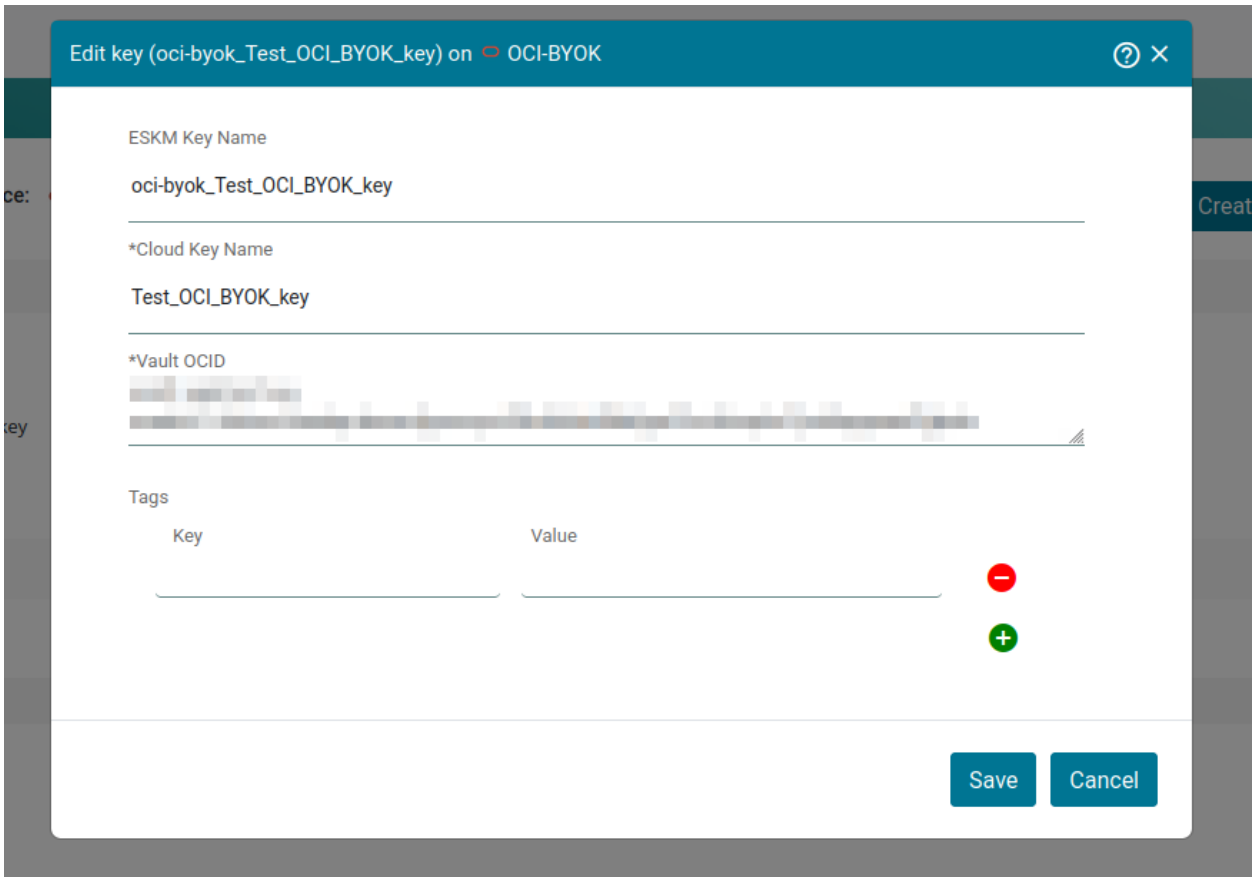

Figure 35 : Edit Key

4. Click **Save**.

Only key tags can be edited.

7.5 Delete an OCI-BYOK Key

1. Locate the configured **OCI-BYOK** cloud instance and click **Manage Keys**.
2. Select the key to be deleted and click **Delete** from the **Action** column.

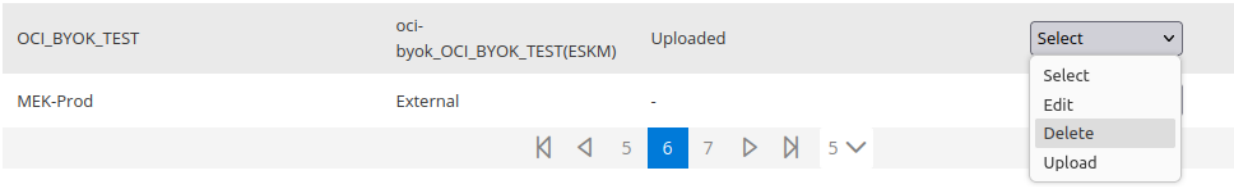

Figure 36 : Delete Action Column

3. Enter the required **Waiting period** in days.

The waiting period must be between 7 and 30 days.

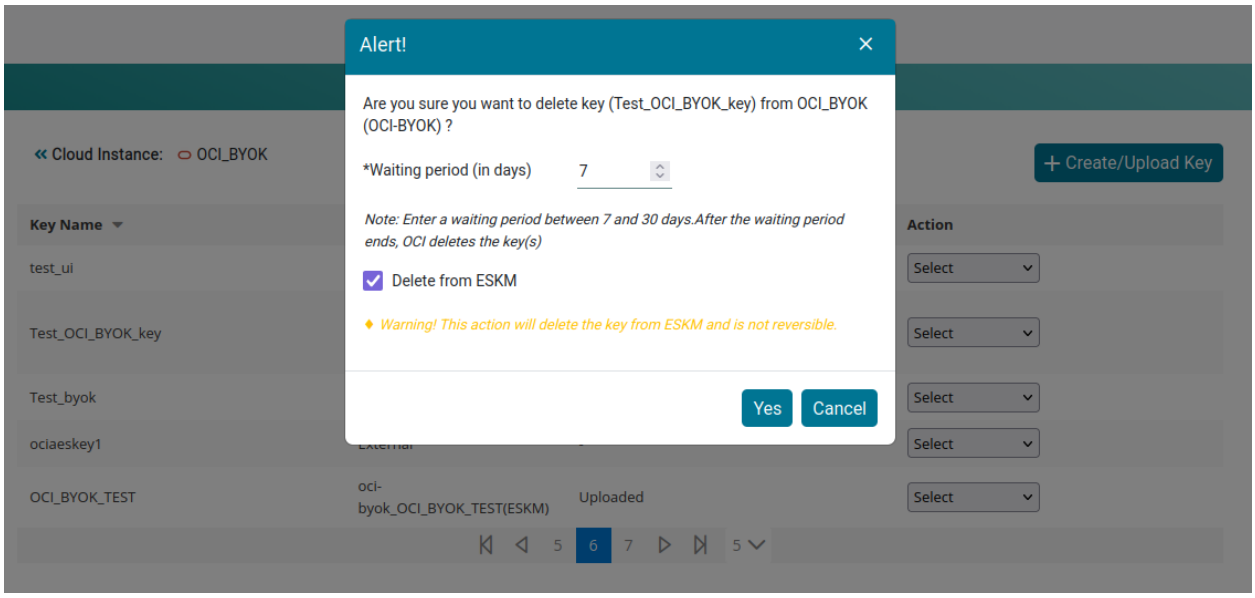

Figure 37 : Delete Key Alert

4. Click **Yes** to confirm the deletion.
5. The key remains in **Pending Deletion** status during the waiting period. After the waiting period expires, OCI deletes the key.

Deleting the key from the ESKM is irreversible.

8 Verification and Testing

8.1 Functional Testing

Verify Key Availability in OCI:

1. Log in to the **OCI Console**.
2. Navigate to **Key Management** and select the **Vault** configured for the OCI-BYOK integration.
3. Open the **Keys** section.
4. Verify that the key created and uploaded from ESKM is displayed in the OCI Vault.
5. Verify that the displayed key corresponds to the key uploaded from ESKM and that it is **Enabled**.

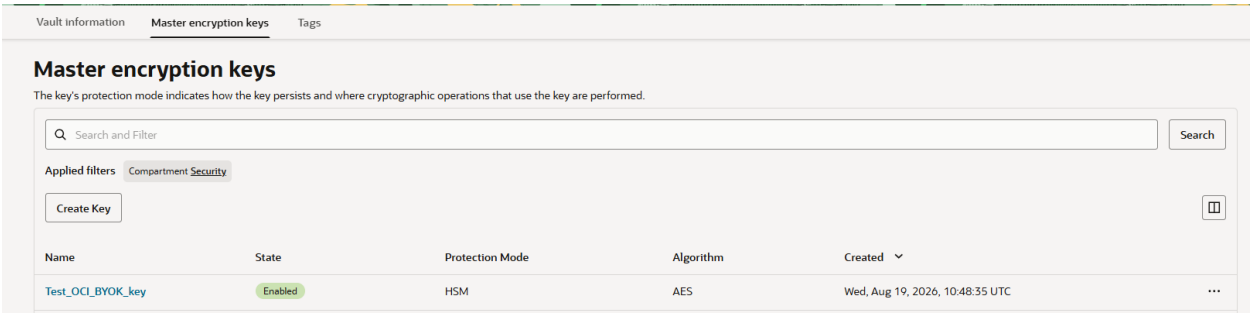

Figure 38 : Key Created in OCI Vault

8.2 Logs and Validation Steps

The ESKM logs can be used to verify the operations performed during the OCI-BYOK integration and to confirm the successful upload of the key to OCI.

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **REST**.
2. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **Audit**.
3. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **System**.

4. Review the **REST**, **Audit**, and **System** logs for the operations performed during the OCI-BYOK integration.

5. In the **Audit** log, verify that the key upload operation was successfully completed.

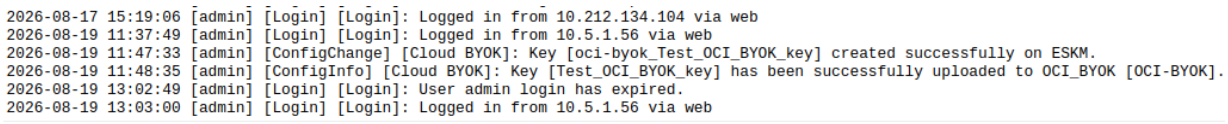

Figure 39 : Successful Upload

The successful Audit log entry confirms that the key upload operation was completed by **ESKM**. Together with the key being visible in the **OCI** Vault, this validates the successful transfer of the key as part of the OCI-BYOK integration.

9 Troubleshooting

9.1 Common issues and how to resolve them

Issue	Possible Cause	Resolution
Invalid OCID	An incorrect or incomplete OCI OCID has been provided in the ESKM OCI-BYOK cloud instance configuration.	Verify the **Tenancy OCID**, **User OCID**, **Compartment OCID**, and **Vault OCID** in the OCI Console and ensure that the values entered in ESKM are complete and correct.
Failed to verify the HTTP(S) Signature	The OCI API signing credentials configured in ESKM are invalid or do not correspond to the API signing key registered for the OCI user.	Verify that the **Private Key**, **User OCID**, and **Fingerprint** configured in ESKM correspond to the same OCI API signing key. Verify that the corresponding public key is registered for the OCI user in OCI.
Authentication or authorization failure	The OCI user does not have the required permissions to access the configured Vault or perform the requested key management operation.	Verify the IAM configuration and ensure that the OCI user used for the integration has the required permissions for the target Vault and key management operations.
Vault cannot be accessed	The configured Vault OCID, compartment, or region is incorrect, or the OCI user does not have access to the Vault.	Verify the **Vault OCID**, **Compartment OCID**, and **Region** in the ESKM configuration and verify that the OCI user has access to the target Vault.

9.2 Log locations and interpretation

You can verify the logs from Utimaco ESKM by following the steps below:

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **REST**.
2. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **Audit**.
3. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **System**.
4. Review the **REST**, **Audit** and **System** logs for operations performed during the OCI-BYOK integration.
5. Verify that the OCI requests and corresponding key management operations are completed successfully.

10 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

11 Appendices

11.1 References (links to external docs)

Title	Description	Document/Link
Utimaco Enterprise Secure Key Manager Installation and Replacement Guide	Installation and replacement procedures for Utimaco Enterprise Secure Key Manager.	
Sign In to the Oracle Cloud Infrastructure Console	Provides information on signing in to the Oracle Cloud Infrastructure Console, including first-time access and available authentication options.	https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/signingin.htm?
OCI Key Management Documentation	Documentation for Oracle Cloud Infrastructure Key Management Service (OCI KMS), including Vaults and key management.	https://docs.oracle.com/en-us/iaas/Content/KeyManagement/home.htm?

Table 5: References

11.2 Command Summary (CLI commands used)

No CLI commands are used in this integration.