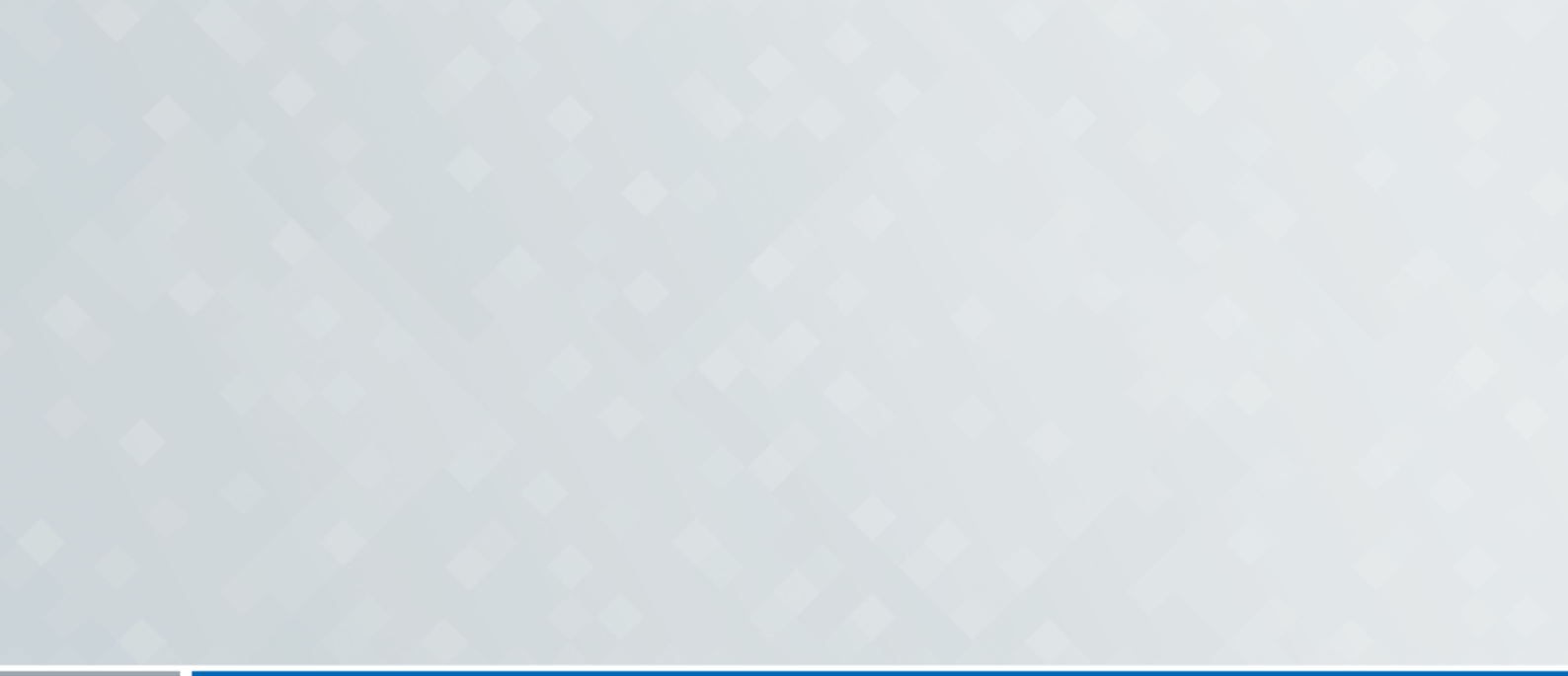




Oracle

Cloud Infrastructure HYOK

Integration Guide

ESKM

8.54.x



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	2026-10-09
Status	PUBLISHED
Document No.	IG-2026-0097
All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1	About This Guide	5
1.1	Target Audience	5
1.2	Purpose of the Integration	5
1.3	Abbreviations	6
1.4	Document Conventions	7
2	Product Overview	9
2.1	Overview of the Partner Product	9
2.2	Overview of ESKM	9
2.3	Joint Value Proposition	9
3	Integration Requirements and Prerequisites	11
3.1	Tested Versions	11
3.2	Supported Platforms	11
3.3	Hardware and Software Requirements	11
3.4	Prerequisites	11
4	Installing and Configuring ESKM	12
5	Installing and Configuring OCI	14
6	Integration Steps on Utimaco ESKM	15
6.1	Add an OCI-HYOK Cloud Instance	15
6.2	Delete an OCI-HYOK Cloud Instance	17
6.3	Manage OCI-HYOK Keys	18
6.4	Create a Key	21
7	Integration Steps on OCI	24
7.1	Prepare the Private Network	24
7.2	Direct VPN Configuration	26
7.3	Create the Confidential Resource Application	29
7.4	Create the Confidential Client Application	32
7.5	Obtain the Identity Domain URL	34
7.6	Configure OAuth Trust in the ESKM	34
7.7	Create the OCI External KMS Private Endpoint	36
7.8	Create the Cloud instance in the External KMS	37
7.9	Create the External Key Management Vault in OCI	39

8	Verification and Testing	41
8.1	Functional Testing.....	41
8.1.1	Create the Key Reference in OCI.....	41
8.1.2	Rotate the Key in OCI.....	43
8.1.3	Disable the Key in OCI	45
8.1.4	Modify the Key in OCI	46
8.1.5	Encrypt with the Key in OCI	47
8.1.6	Delete the Key in OCI	48
8.2	Logs and Validation Steps.....	50
9	Troubleshooting	51
9.1	Common Issues and How to Resolve Them	51
9.2	Log Locations and Interpretation	52
10	Contact and Support Information.....	53
11	Appendices	54
11.1	References (links to external docs).....	54
11.2	Command Summary (CLI commands used)	54

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 **Hold Your Own Key (HYOK)** 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 while enabling Oracle Cloud Infrastructure Key Management Service (OCI KMS) and supported OCI services to use keys that remain under the control of the ESKM environment.

This guide focuses only on the configuration and integration aspects required for the OCI–ESKM HYOK 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 that are created and securely managed within the Utimaco Enterprise Secure Key Manager (ESKM) while keeping the key material under the control of the ESKM environment.

In the HYOK model, cryptographic keys remain within ESKM and are not uploaded or transferred into Oracle Cloud Infrastructure Key Management Service (OCI KMS). OCI uses a reference to the externally managed key to perform supported cryptographic operations while the key material remains under the control of ESKM.

The integration aims to:

- Enable OCI services to use customer-controlled cryptographic keys for supported encryption operations.

- Keep cryptographic key material within the Utimaco ESKM environment.
- Enable OCI to reference and use externally managed keys without importing the key material 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
HYOK	Hold 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

Abbreviation	Meaning
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
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

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.

For the HYOK integration, OCI provides the cloud-side capabilities required to use cryptographic keys that are managed externally through the Utimaco Enterprise Secure Key Manager (ESKM).

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 maintain cryptographic keys within the ESKM environment while allowing supported OCI services to use externally managed keys.

In the HYOK model, cryptographic keys are created and managed within the Utimaco ESKM environment and are not transferred to or stored as key material within OCI KMS. OCI uses the externally managed key through the integration with ESKM, while ESKM remains responsible for the management and lifecycle of the cryptographic key.

The HYOK integration provides customers with greater control over their cryptographic keys by keeping the key material within the ESKM environment while enabling its use by supported OCI services.

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 their cryptographic key material and its lifecycle 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.

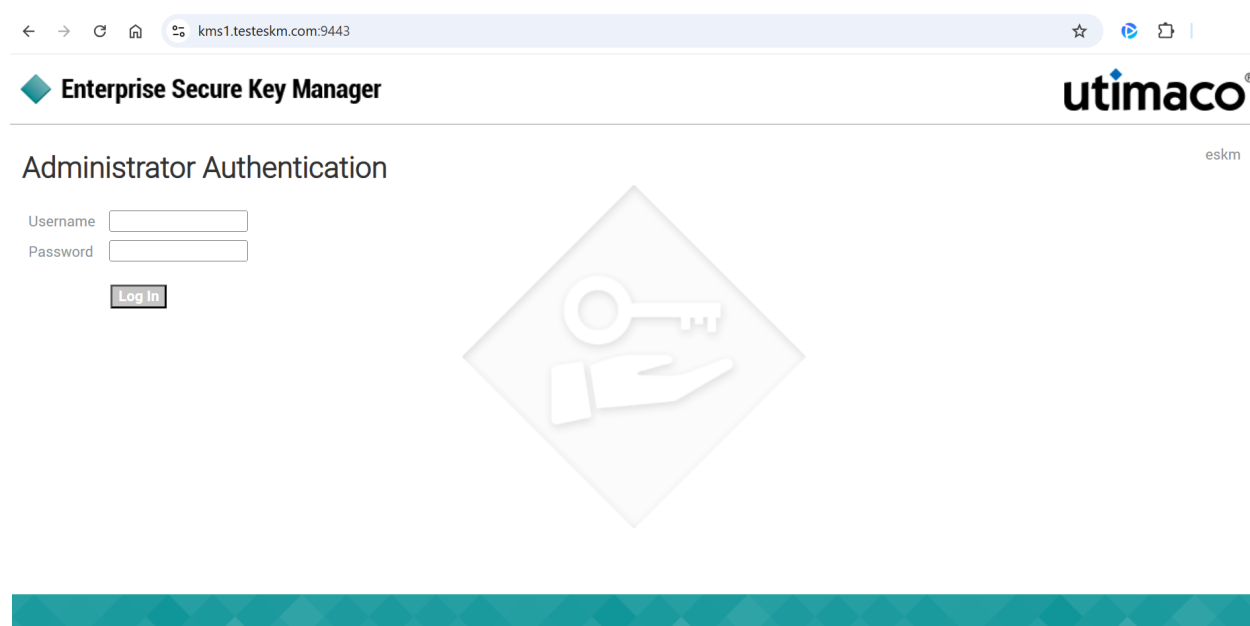


Figure 1 : ESKM login page

The screenshot displays the Enterprise Secure Key Manager (ESKM) home page. The top navigation bar includes 'Home', 'Security', and 'Device'. The left sidebar shows 'Summary', 'Search', and 'What's New'. The main content area is titled 'Home' and 'System Summary'. The 'System Summary' section provides the following details:

Product:	Enterprise Secure Key Manager L1
Unit ID:	UL14NFAB6HJK
Hardware Platform:	Cloud Platform
Software Version:	8.54.0 (vESKM 8.54)
Date:	09/08/2025
Time:	23:27:31
Time Zone:	Pacific Time
System Uptime:	26 days, 18:59:13
Licenses:	100
Licenses in Use:	25

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.

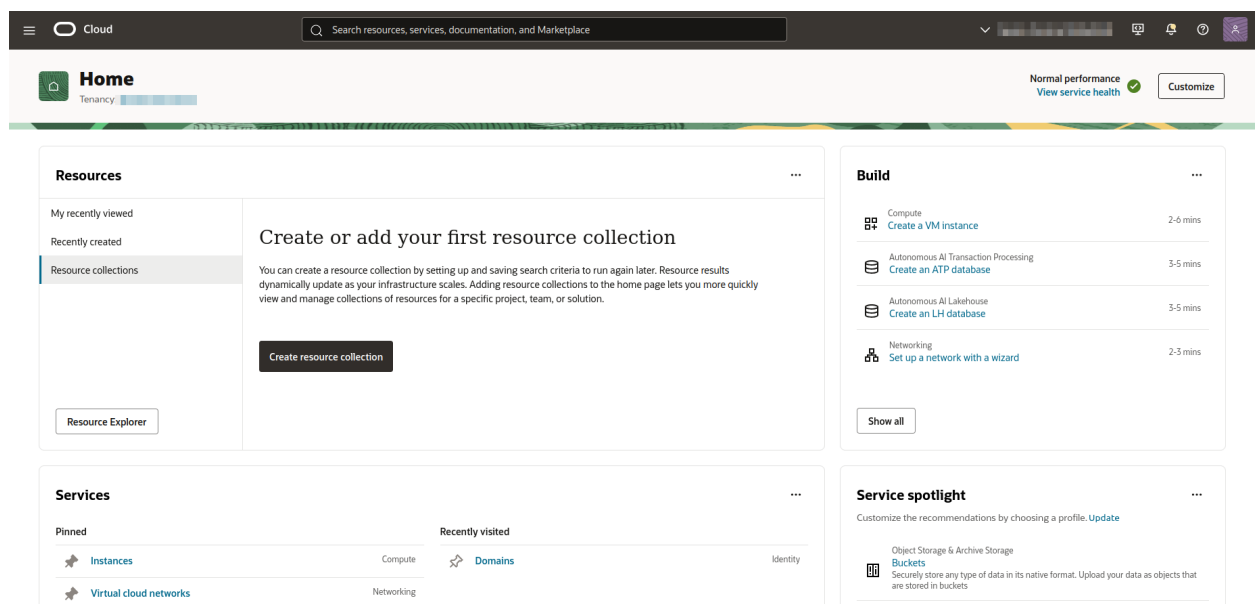


Figure 3 : OCI Login

6 Integration Steps on Utimaco ESKM

This section describes the configuration steps required on Utimaco Enterprise Secure Key Manager (ESKM) to establish the HYOK integration. The following sections guide you through the ESKM-side configuration, including the creation of the OCI-HYOK cloud instance and the management of cryptographic keys that remain under the control of ESKM while being referenced by 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 externally managed cryptographic keys is not covered and must be performed separately according to the requirements of the corresponding OCI service.

6.1 Add an OCI-HYOK Cloud Instance

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

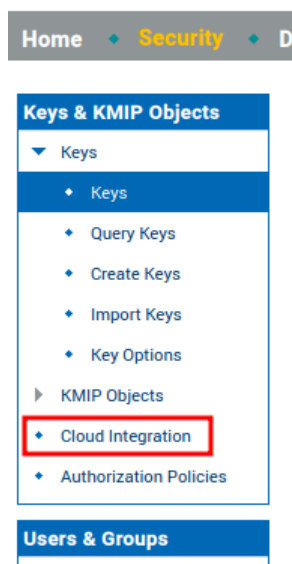


Figure 4 : Cloud Integration

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

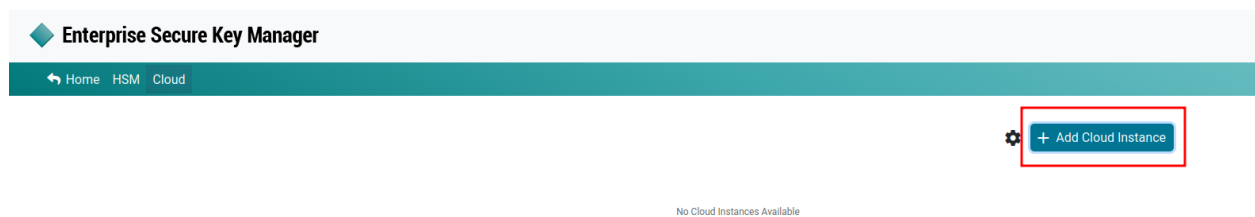


Figure 5 : Add Cloud Instance

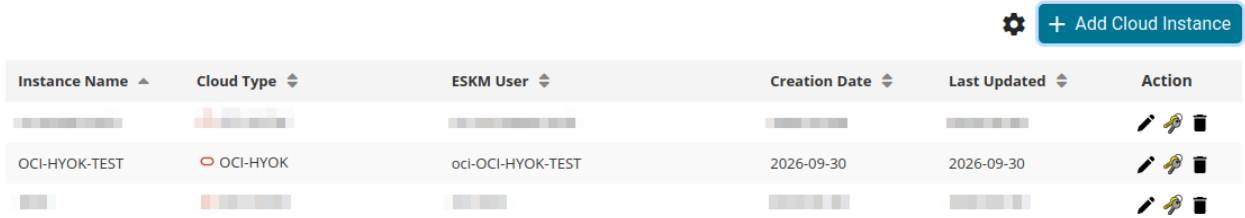
3. Enter an **Instance Name** and select **OCI-HYOK** from the **Cloud Type** dropdown list.

The screenshot shows a modal dialog box titled 'Add Cloud Instance'. The dialog has a teal header bar with a question mark icon and a close button. Inside the dialog, there are two input fields. The first field is labeled '*Instance Name' and contains the text 'OCI-HYOK-TEST'. The second field is labeled '*Cloud Type' and is a dropdown menu with the text 'Select' and a downward arrow. At the bottom right of the dialog, there are two buttons: 'Verify' and 'Cancel'.

Figure 6 : Add Cloud Instance — OCI Configuration

4. Click **Verify**.

5. Verify that the instance was created successfully.



Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
OCI-HYOK-TEST	OCI-HYOK	oci-OCI-HYOK-TEST	2026-09-30	2026-09-30	  

Figure 7 : OCI-HYOK Cloud Instance

6.2 Delete an OCI-HYOK Cloud Instance

1. Go to ESKM Management Console > Security > Cloud Integration.
2. Select and Click the Cloud Instance to be deleted.
3. Click The Delete Icon.



Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
ESKM-vault	OCI-HYOK	oci-ESKM-vault	2026-09-08	2026-09-08	  
HYOK-TEST	OCI-HYOK	oci-HYOK-TEST	2026-09-28	2026-09-28	  

Figure 8 : Delete Cloud Instance

4. Confirm the Delete prompt.

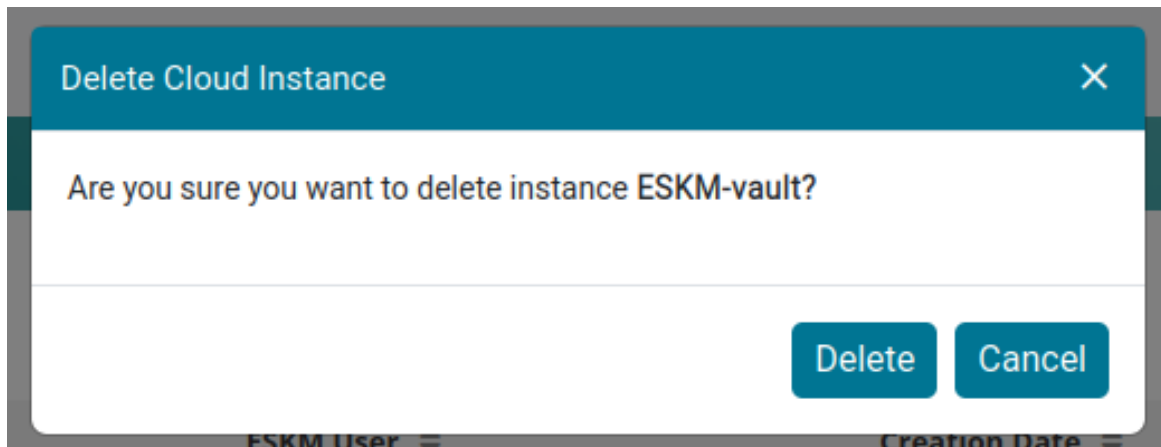


Figure 9 : Delete Instance Confirmation

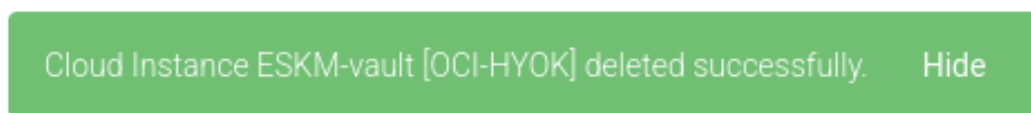
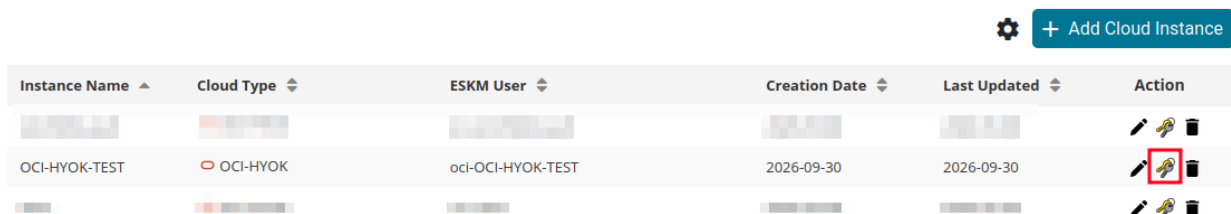


Figure 10 : Cloud Instance Deleted

6.3 Manage OCI-HYOK Keys

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



The table displays a list of cloud instances. The row for "OCI-HYOK-TEST" is highlighted. In the "Action" column of this row, the "Manage Keys" icon (a key) is highlighted with a red square. Above the table, there is a settings gear icon and a button labeled "+ Add Cloud Instance".

Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
OCI-HYOK-TEST	OCI-HYOK	oci-OCI-HYOK-TEST	2026-09-30	2026-09-30	[REDACTED] Manage Keys [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Figure 11 : OCI-HYOK Cloud Instance — Manage Keys

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

<< Cloud Instance: ○ vault4 + Create Key

Key Name ▾	Source ▴	Status ▴	ESKM Key Owner ▴	Action
oci-94d95470-f444-4fd5-a1c3-2f84e83ec30a	oci-94d95470-f444-4fd5-a1c3-2f84e83ec30a(ESKM)	Active	oci-vault4	Select ▾
oci-691ea8b1-0bcd-42a6-95c8-863359ce5dc0	oci-691ea8b1-0bcd-42a6-95c8-863359ce5dc0(ESKM)	Active	oci-vault4	Select ▾

⏮ ⏪ 1 ⏩ ⏭ 5 ▾

Figure 12 : OCI-HYOK Keys

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

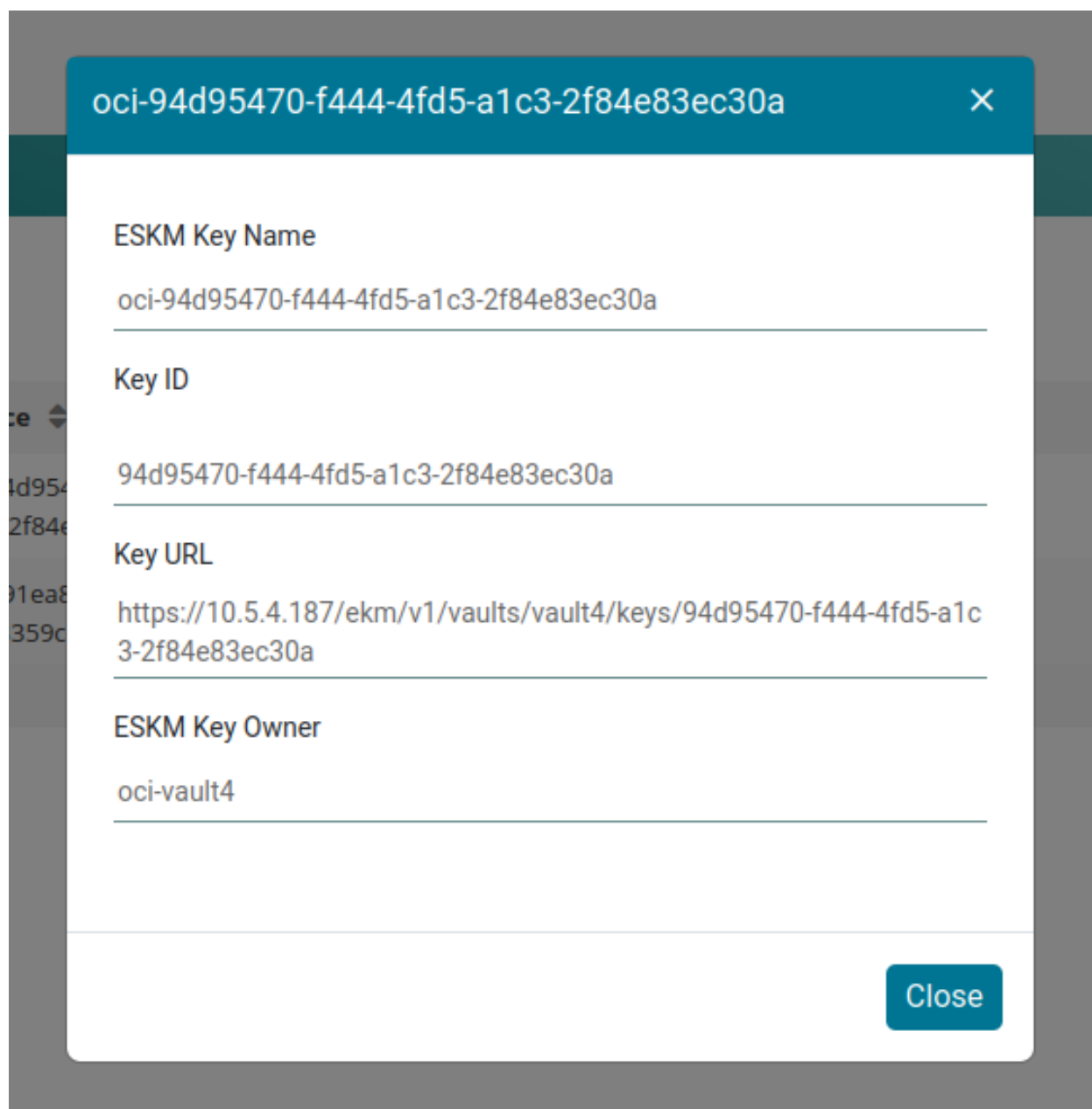


Figure 13 : OCI-HYOK Key details

5. To delete a Key, change the **Action** to **Delete**.

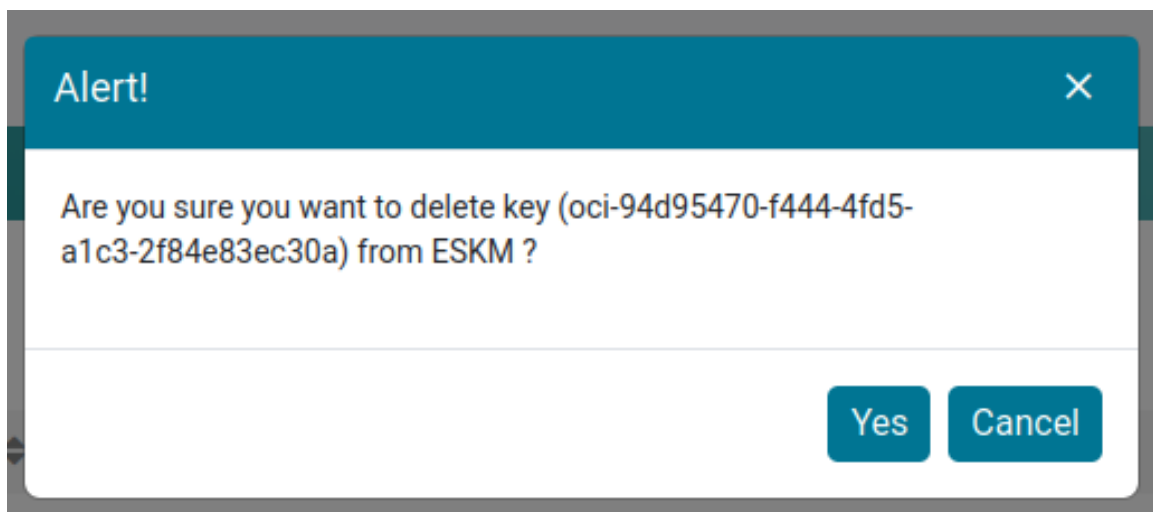


Figure 14 : OCI-HYOK Key deletion

6.4 Create a Key

1. From the OCI-HYOK Keys page, click **Create Key**.

<< Cloud Instance: vault4

+ Create Key

No Keys Available

Figure 15 : Create Key

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

Create Key

1 Key Selection ————— 2 Summary

*Algorithm
AES-256

ESKM Key Owner
oci-vault4

Create Cancel

Figure 16 : Key Selection – ESKM Key Name and Algorithm

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

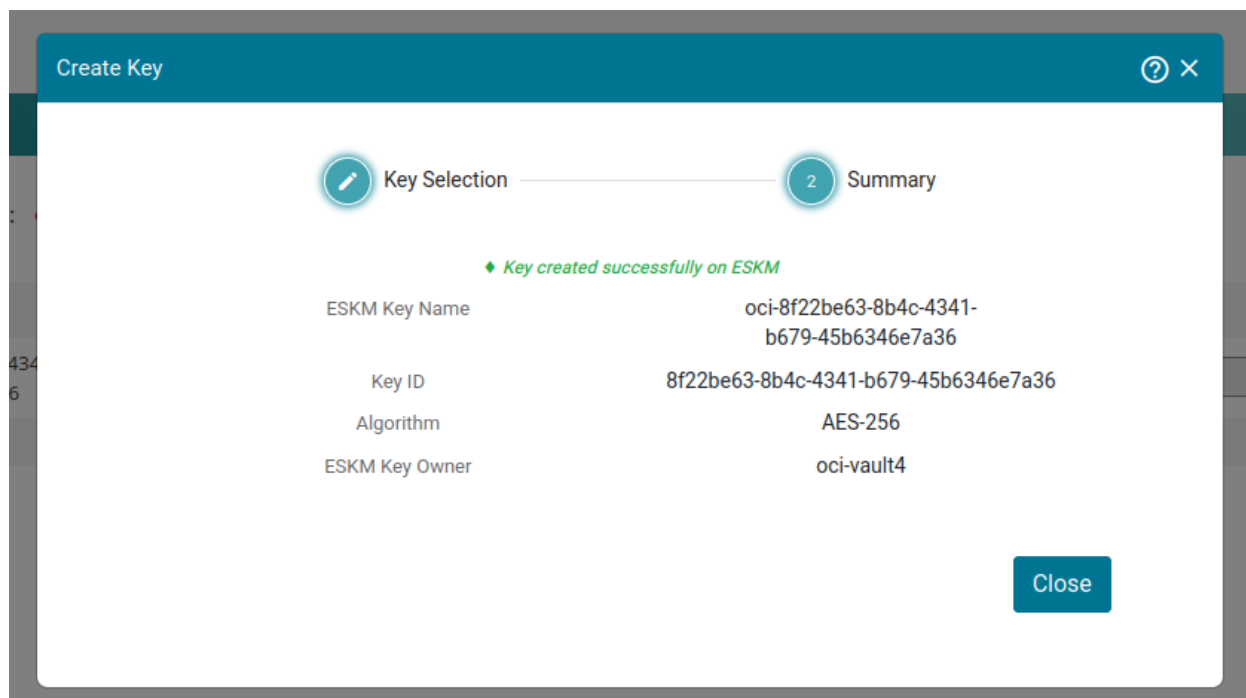


Figure 17 : Key Summary



The Key ID will be useful later on when creating the key Reference in OCI.

7 Integration Steps on OCI

The following section describes the Oracle Cloud Infrastructure (OCI) configuration steps required to prepare the environment for the HYOK 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 externally managed cryptographic keys. Such service-specific configuration should be performed separately according to the requirements of the corresponding OCI service.

7.1 Prepare the Private Network

The HYOK integration requires a private network connection between OCI and the external KMS.

1. Log in to the **OCI Console**.
2. In the OCI Console, go to **Networking** → **Virtual Cloud Networks**.
3. Select the VCN to be used for the Private Endpoint.
4. Verify that the VCN has the required IPv4 CIDR configured.

Create a Virtual Cloud Network

Name
VCN_HYOK

Create In Compartment

IPv4 CIDR Blocks

You can assign up to 16 IPv4 CIDR blocks to a VCN. There must be at least one IPv4 CIDR block assigned to a VCN. [Learn more](#).

IPv4 CIDR Blocks
10.1.0.0/16

☒ 10.1.0.0/16

IPv4 Example: 10.0.0.0/16

Assign an Oracle allocated IPv6 /56 prefix.
☐

Selecting this option allows a single Oracle assigned IPv6 prefix to your Virtual Cloud Network. [Learn More](#)

BYOIPv6 Prefix

Search and Filter

Add IPv6 Prefixes Remove

IPv6 prefix	IP range	Total IPs
No items to display		

Create new items or search again using different filters or search terms.

Cancel Save as stack Create VCN

Figure 18 : Create a Virtual Cloud Network

5. From the VCN, go to **Subnets**.

6. Click **Create Subnet**.

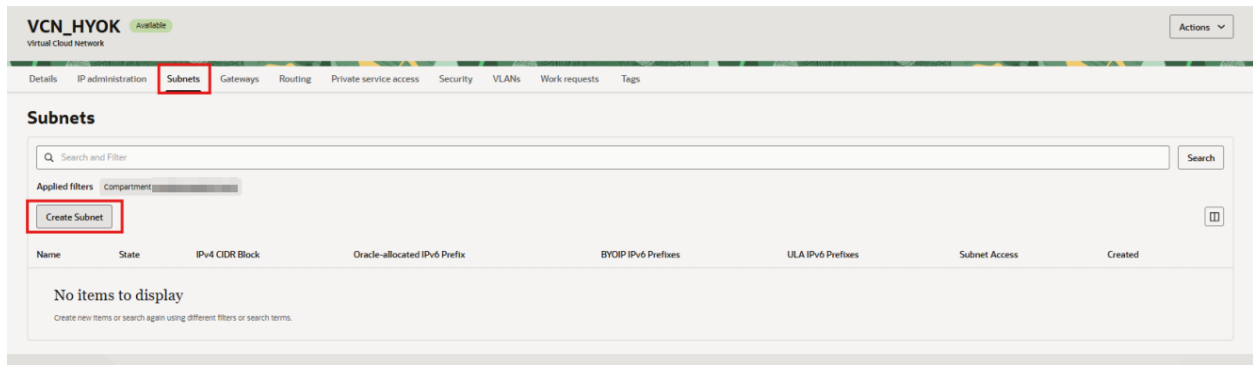


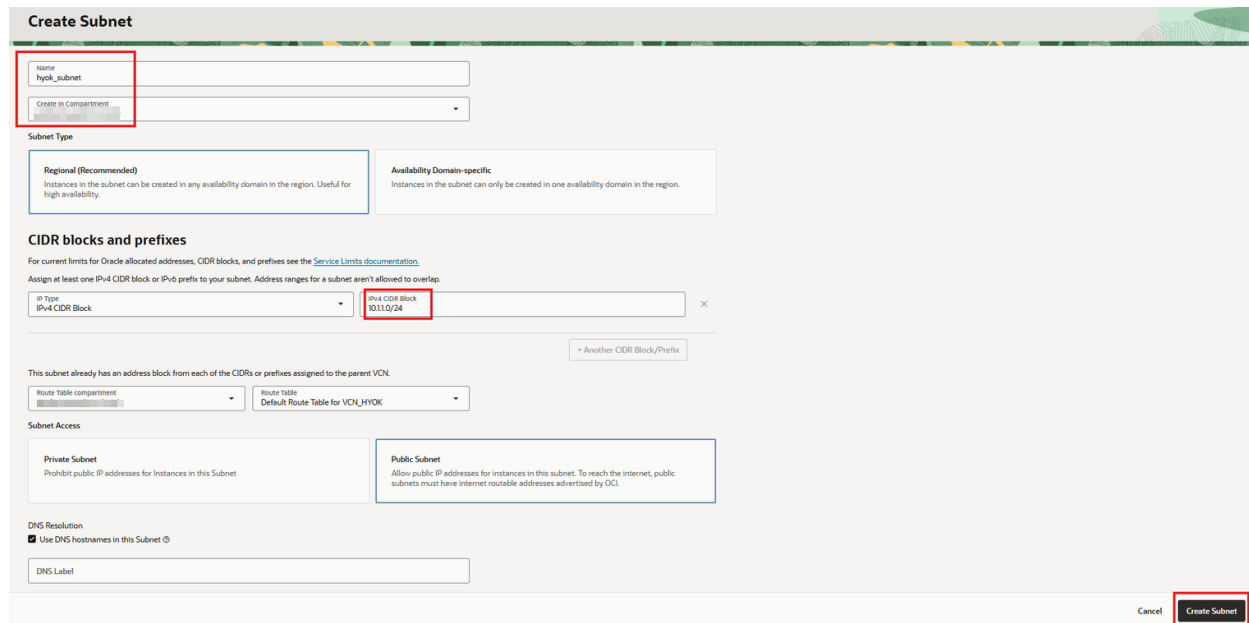
Figure 19 : Subnets menu in VCN

7. Enter the subnet **Name** and **Compartment**.

8. Define the subnet CIDR within the VCN CIDR range.

9. Leave the remaining values at their default settings unless additional network configuration is required.

10. Click **Create Subnet**.



Create Subnet

Name:

Create in Compartment:

Subnet Type

Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.

CIDR blocks and prefixes
For current limits for Oracle allocated addresses, CIDR blocks, and prefixes see the [Service Limits documentation](#).
Assign at least one IPv4 CIDR block or IPv6 prefix to your subnet. Address ranges for a subnet aren't allowed to overlap.

IP Type:

+ Another CIDR Block/Prefix

This subnet already has an address block from each of the CIDRs or prefixes assigned to the parent VCN.

Route Table compartment:

Route Table:

Subnet Access

Private Subnet
Prohibit public IP addresses for instances in this Subnet.

Public Subnet
Allow public IP addresses for instances in this subnet. To reach the internet, public subnets must have Internet routable addresses advertised by OCI.

DNS Resolution
☒ Use DNS hostnames in this Subnet

DNS Label:

Cancel

Figure 20 : Create Subnet

7.2 Direct VPN Configuration



This section is only needed if the ESKM is inside a private network, if the ESKM has a public address configured this step shouldn't be configured.

The Private Network configuration in OCI needs the establishment of a Site-to-Site VPN in order to connect the OCI private network with the ESKM private network.

1. In the OCI Console, go to **Networking** → **Customer-premises equipment**.
2. Select **Create CPE**.
3. Insert the Name and select the Compartment.
4. Insert the Customer-premises public IP address.
5. Select the CPE Vendor and Platform/Version.
6. **Create CPE**.

Create CPE

Name
CPE-VON-Prod-Shared

Create in compartment
[selected]

Allow IPSec over FastConnect
☒

IPSec over FastConnect lets you use IPSec encryption for traffic sent over FastConnect private virtual circuits. The CPE IP address provided can be an RFC 1918 address if this CPE is reachable over a private virtual circuit.

IP address
12.3.4

CPE vendor information
Used by the CPE configuration helper to produce vendor-specific content that helps a network engineer configure your CPE.

Vendor
Cisco

Platform/Version
ASA Route-Based VPN 971 or later

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

No items to display

Add tag

Cancel Save as Stack Create CPE

Figure 21 : Create a CPE

7. Go to **Networking** → **Site-to-Site VPN**.
8. **Create IPSec Connection**.
9. Define the Name and select the Compartment, CPE and Network Dynamic Route Gateway created before.
10. Introduce `<IP_ADDRESS>/32` as the static route to the on-premise network.
11. Expand **Tunnel 1** and select **IKEv2** and **Static Route**.

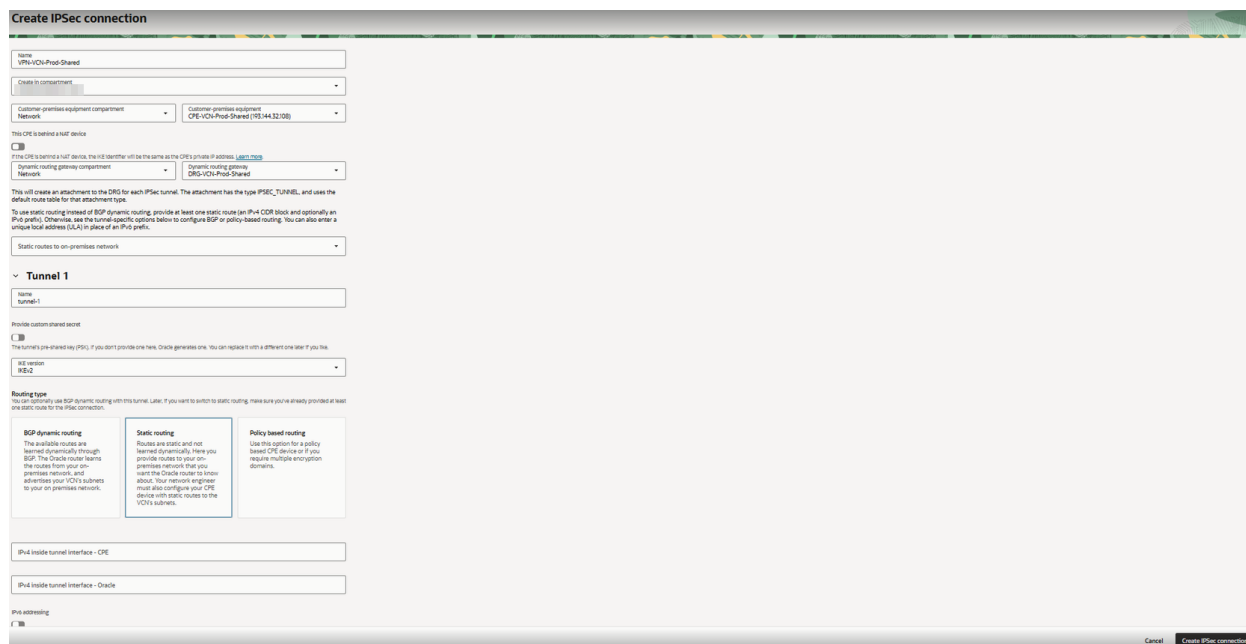


Figure 22 : Create IPsec connection

12. Expand **Tunnel 2** and select **IKv2** and **Static Routing**.



To define the **algorithms** used in the **IKEv2 phases**, expand the **advanced options** and the desired phase. Some companies may have restrictions with the allowed algorithms.

13. Create IPsec Connection.

14. In the Site-to-Site VPN panel, select the created IPsec VPN panel, select the **created IPsec Connection** → **Tunnels** → **tunnel-1**.

15. Copy the Oracle VPN IP address and the Shared Secret.

16. Use these parameters to configure the ESKM network side.



The Site-to-Site VPN tunnels are commonly managed in the gateway's firewall. If the ESKM environment's firewall requires the modification of the algorithms or the session key lifetime, it can be done by selecting the **Edit** button, **Advanced Options** – > **Phase One/Two** → **Set custom configurations**.

7.3 Create the Confidential Resource Application

The Confidential Resource Application is used as the OAuth Resource Server for the HYOK integration.

1. In the **OCI Console**, go to **Identity & Security** > **Domains**.
2. Select the domain to be used for the integration.
3. Go to **Integrated Applications**.
4. Click **Add Application**.
5. Select **Confidential Application**.

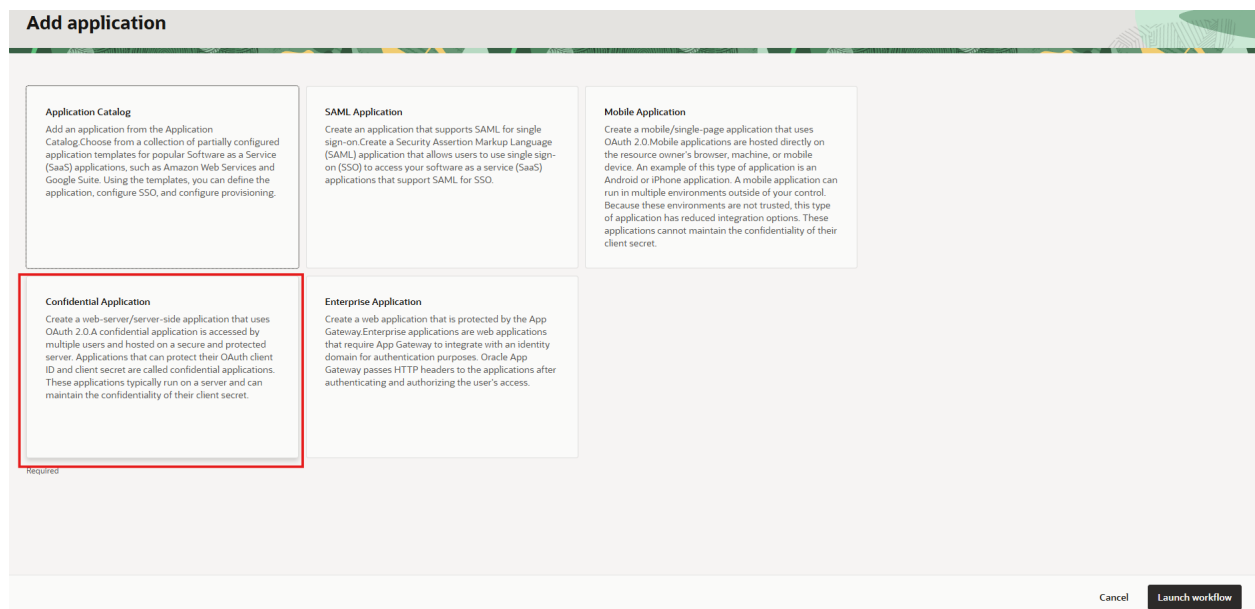


Figure 23 : Add a Confidential Application

6. Click **Launch workflow**.
7. Enter the application name:

<RESOURCE_APP_NAME>

8. Click **Create**.

9. Select the application and go to **Actions** → **Activate**.

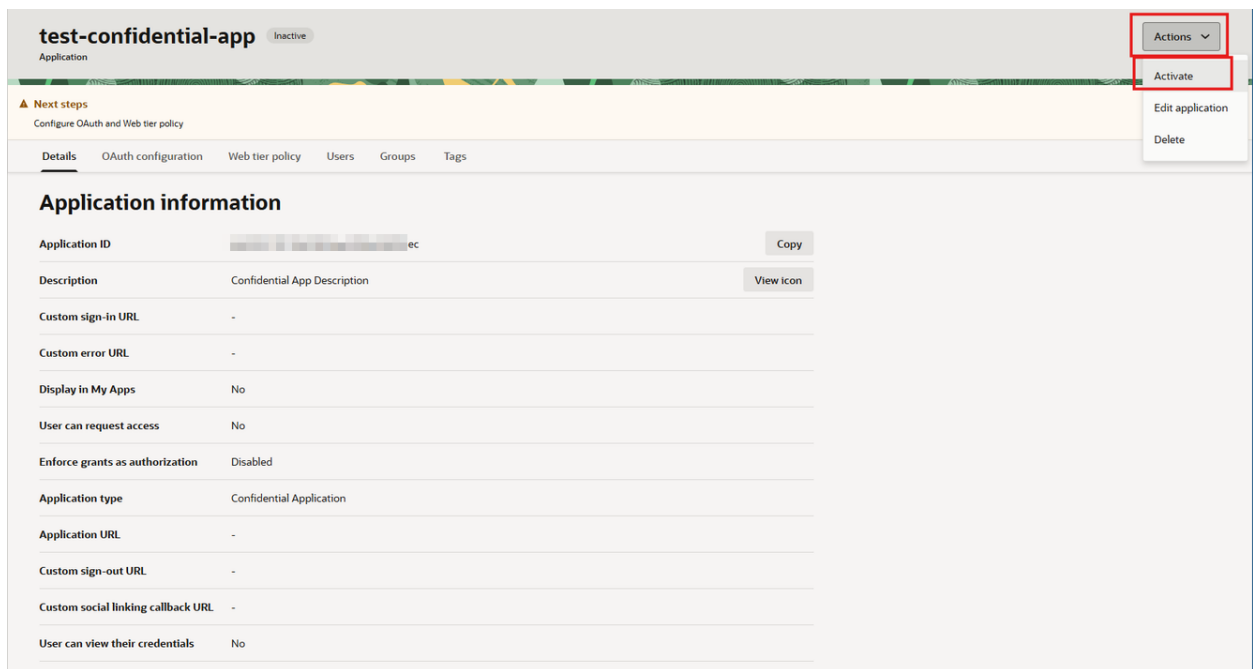


Figure 24 : Activate the Confidential Application

10. Go to **OAuth Configuration**.

11. Click **Edit OAuth Configuration**.

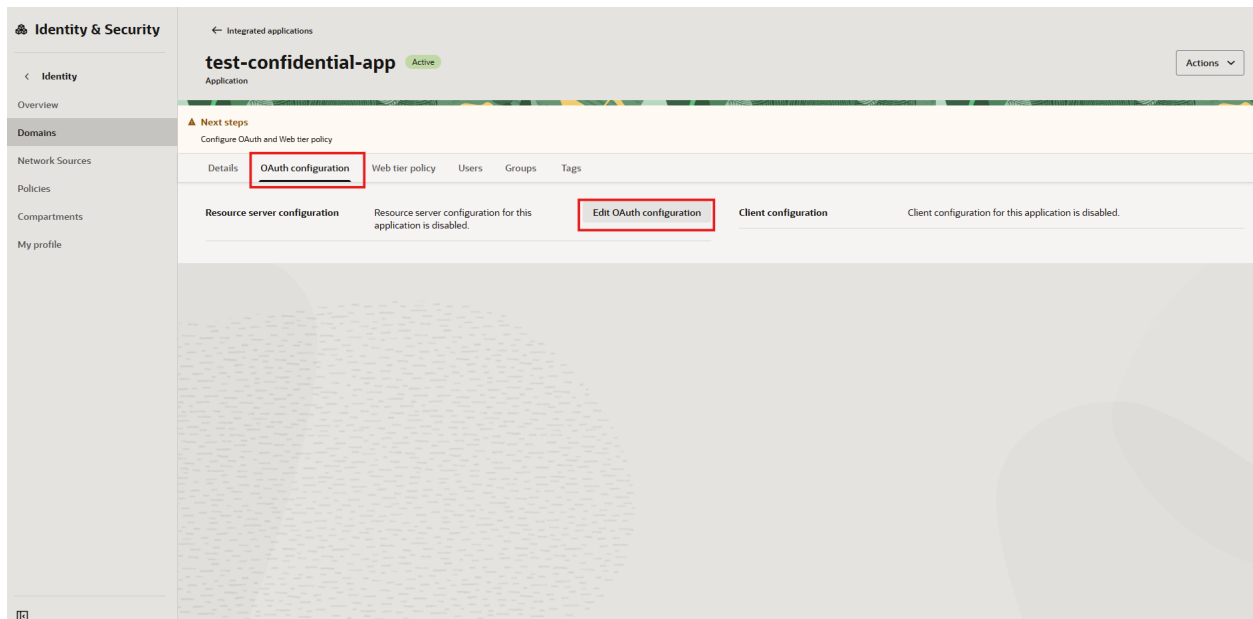


Figure 25 : Edit OAuth configuration

12. Select **Configure this Application as a Resource Server now**.
13. Enter the public IP address that will access the ESKM resources as Primary Audience.
14. Activate the **Add Scope** and click **Add**.

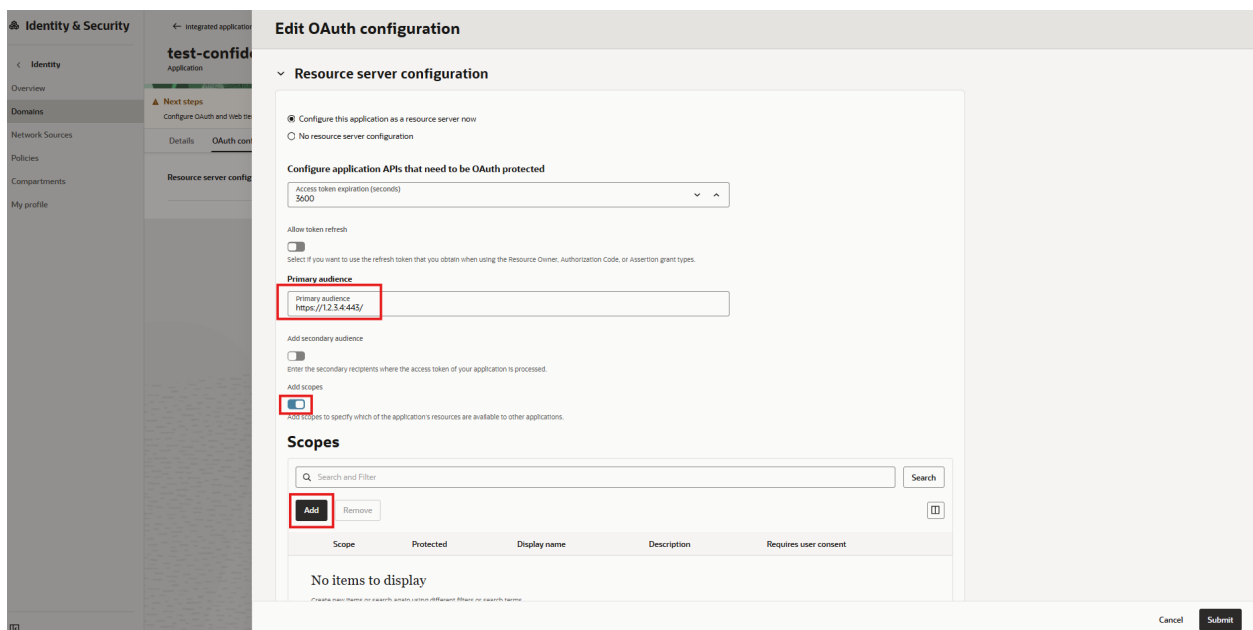


Figure 26 : Resource Server Configuration

15. Insert the Scope and click **Add**.

16. Click **Submit**.



The Resource Server application and the Confidential Client Application can be the same application. If the same application is used, configure the Resource Server first so that the OAuth scope is available when configuring the client.

7.4 Create the Confidential Client Application

The Confidential Client Application is used by the external KMS to authenticate with OCI.



If the Resource Server application and the Confidential Client Application are the same application, then move to step 5.

1. In **Integrated Applications**, click **Add Application**.
2. Select **Confidential Application**.
3. Enter the application name:
`<CLIENT_APP_NAME>`
4. Select the application and go to **Actions** → **Activate**.
5. Go to **OAuth Configuration**.
6. Click **Edit OAuth Configuration**.
7. Select **Configure this Application as a Client now**.
8. Configure the application to use **Client Credentials**.

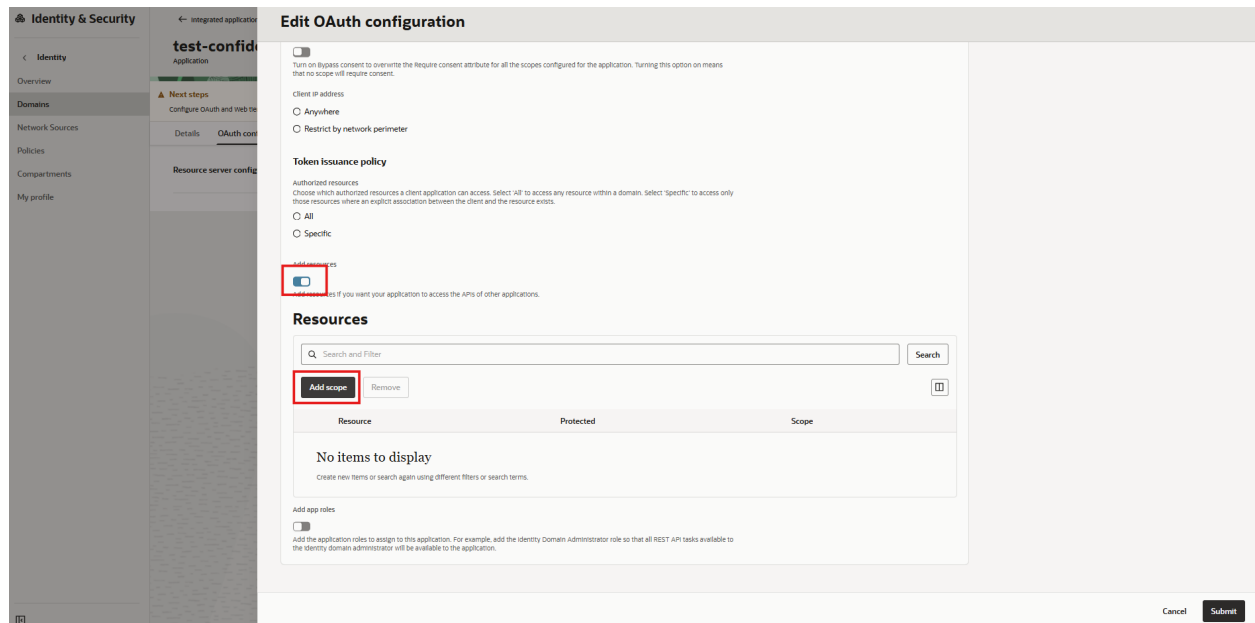


Figure 27 : Add scope as a resource

9. Associate the application with the scope created for `<RESOURCE_APP_NAME>`.
10. Click **Create**.
11. Open the OAuth configuration.
12. Record the following values available in the General Information section:
 - Client ID
 - Client Secret

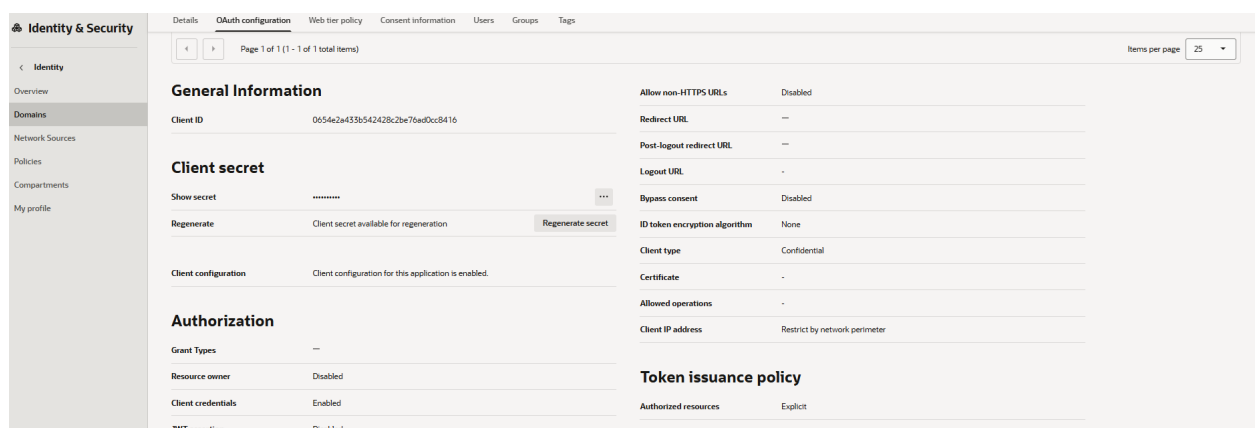


Figure 28 : Client ID and Secret



Store the Client Secret securely. It is required later when configuring the external KMS.

7.5 Obtain the Identity Domain URL

The Identity Domain URL is required to configure the OAuth connection with the external KMS.

1. In the OCI Console, go to **Identity & Security** → **Domains**.
2. Select the domain used for the integration.
3. Copy the **Domain URL**.

Record the value as:

<ID_DOMAIN_URL>

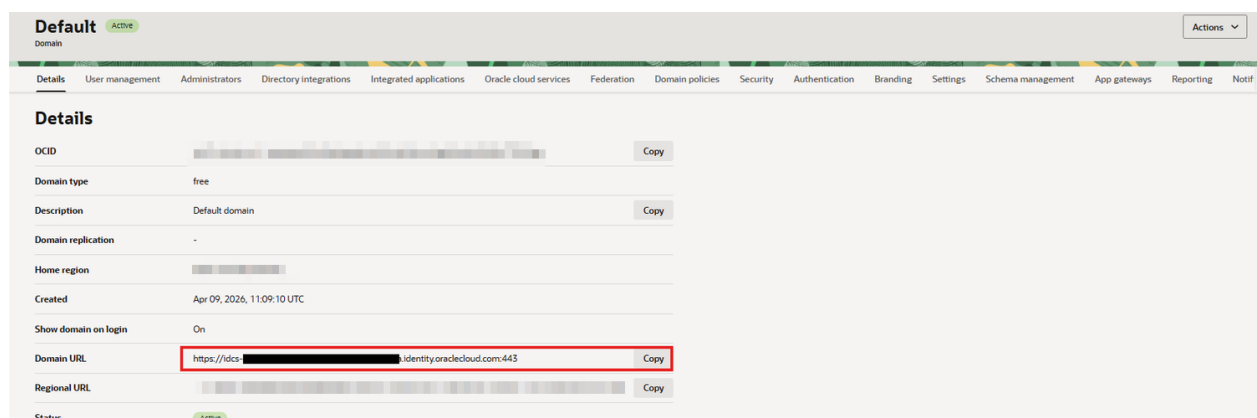


Figure 29 : Domain URL



When the OpenID Configuration endpoint is required, use:

<ID_DOMAIN_URL>/well-known/openid-configuration

7.6 Configure OAuth Trust in the ESKM

In the ESKM, create or configure the **Identity Provider** for OCI.

1. In Device --> REST Server --> Advanced REST Settings select Edit.
2. Activate the Enable OCI HYOK checkbox.
3. Use `<ID_DOMAIN_URL>/admin/v1/SigningCert/jwk` as the OCI HYOK JWKS URL.
4. Set the OCI HYOK Issuer field as `identity.oraclecloud.com`.
5. Save.

Advanced REST Settings

Enable ETSI QKD 14:	☐
ETSI QKD 14 Port:	7443
ETSI QKD 14 CA:	[None]
Enable Google Workspace:	☐
Google Workspace Server Certificate:	[None]
IDP JWKS Endpoint:	
IDP Client ID:	
IDP Issuer:	
Enable Azure EKM Proxy:	☐
Azure EKM Proxy Server Certificate:	[None]
Azure EKM Proxy Server name:	[None]
Azure EKM Proxy CA:	[None]
Enable OCI HYOK:	☒
OCI HYOK JWKS URL:	https://idcs-26bd05a584ef4
OCI HYOK Issuer:	identity.oraclecloud.com

Figure 30 : Enable OCI HYOK in the ESKM

7.7 Create the OCI External KMS Private Endpoint

The Private Endpoint provides the private connection between OCI and the external KMS.

1. In the OCI Console, go to **Identity & Security** → **Private Endpoints**.
2. Click **Create Private Endpoint**.

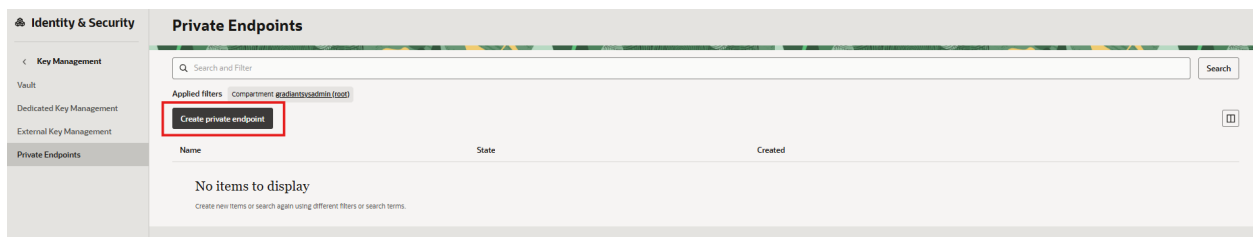


Figure 31 : Create Private Endpoint

3. Enter the Private Endpoint name:

<EKMS_PRIVATE_ENDPOINT_NAME>

4. Select the VCN created previously.
5. Select the required subnet.
6. Enter the external KMS destination:

<KMS_PRIVATE_IP/FQDN>



If the KMS has a private IP instead of a public IP, it will be necessary to configure a VPN / FastConnect. This configuration must be performed both in OCI and the KMS network.

7. Enter port **443**, or the port configured for the ESKM service.

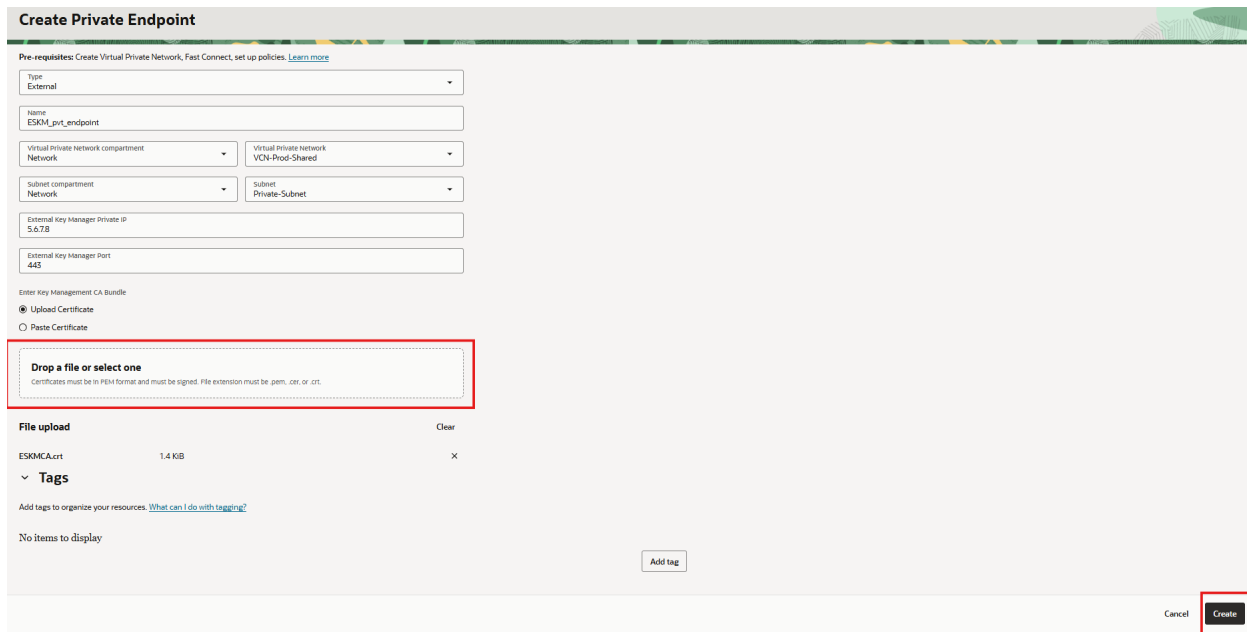


Figure 32 : Create Private Endpoint parameters

8. Upload the CA bundle used to sign the ESKM's service certificate:

<KMS_CA_BUNDLE>

9. Click **Create**.

10. Verify that the Private Endpoint is in the expected active state.

7.8 Create the Cloud instance in the External KMS

The External Vault used for the OCI HYOK integration corresponds to the **cloud instance created in ESKM**.

You can either use an existing ESKM cloud instance or create a new one by following the procedure described in IG-2026-0097 Add an OCI-HYOK Cloud Instance .

1. In the ESKM Management Console, go to the **Cloud Instances** section.
2. Select the cloud instance to be used for the OCI HYOK integration.
3. Click **Edit**.

 [+ Add Cloud Instance](#)

Instance Name ▲	Cloud Type ▼	ESKM User ▼	Creation Date ▼	Last Updated ▼	Action
vault3	 OCI-HYOK	oci-vault3	2026-09-11	2026-09-11	  
vault4	 OCI-HYOK	oci-vault4	2026-09-24	2026-09-24	  

  1 2 **3**   5 ▼

Figure 33 : Edit Cloud Instance

- From the cloud instance configuration, copy the **External Vault URL**.

Edit Cloud Instance? ×

Instance Name

vault4

Cloud Type

OCI-HYOK

Vault URL

https://10.5.4.187/ekm/v1/vaults/vault4

Note: This instance is not editable.

Cancel

Figure 34 : ESKM Vault URL

Record the value as:

<EXTERNAL_VAULT_URL>



The External Vault URL is required when creating the External Vault in OCI.

7.9 Create the External Key Management Vault in OCI

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

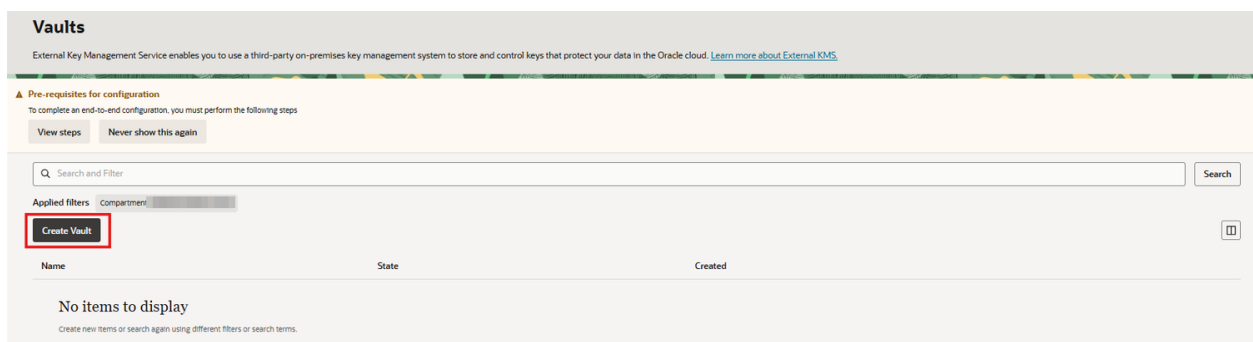


Figure 35 : Create External Key Management Vault

3. Enter the Vault name:

<EKMS_VAULT_NAME>

4. Select the desired Compartment.

5. Enter in the IDCS Account URL:

<ID_DOMAIN_URL>

6. Enter the required OAuth information.
7. Select the Private Endpoint created previously.
8. Enter the External Vault URL:

<EXTERNAL_VAULT_URL>

Create Vault

Pre-requisites:

- Register third-party key management system as confidential resource App in IDCS [Learn more](#).
- Create external vault in External Key Manager and register KMS client application id.
- Create Private Endpoint in OCI KMS.

Name:

Create in compartment:

IDCS Account name URL:

Client Application ID:

Client Application Secret:

Private Endpoint compartment:

Private Endpoint:

External Vault URL:

> Advanced options

Cancel **Create Vault**

Figure 36 : External Key Management parameters

9. Click **Create Vault**.

10. Wait until the External Vault reaches the **Active** state.

Identity & Security			
Vaults			
External Key Management Service enables you to use a third-party on-premises key management system to store and control keys that protect your data in the Oracle cloud. Learn more about External KMS			
Search and Filter Search			
Applied filters: compartment idcs			
Create Vault			
Name	State	Created	
ESKM-vault4	Active	Thu, Sep 24, 2026, 12:44:07 UTC	...
ESKM-vault3	Active	Mon, Sep 14, 2026, 12:35:58 UTC	...
ESKM-vault2	Active	Thu, Sep 10, 2026, 11:34:20 UTC	...
ESKM-vault	Active	Fri, Aug 14, 2026, 09:50:38 UTC	...

Figure 37 : External Key Management Vault activated



The OCI External Key Management service is a paid resource. An OCI account with the required service availability and billing configuration is required to create the External Vault.

8 Verification and Testing

8.1 Functional Testing

8.1.1 Create the Key Reference in OCI

1. In the OCI Console, open the External Vault created previously.
2. Go to **Keys**.
3. Click **Create Key Reference**.

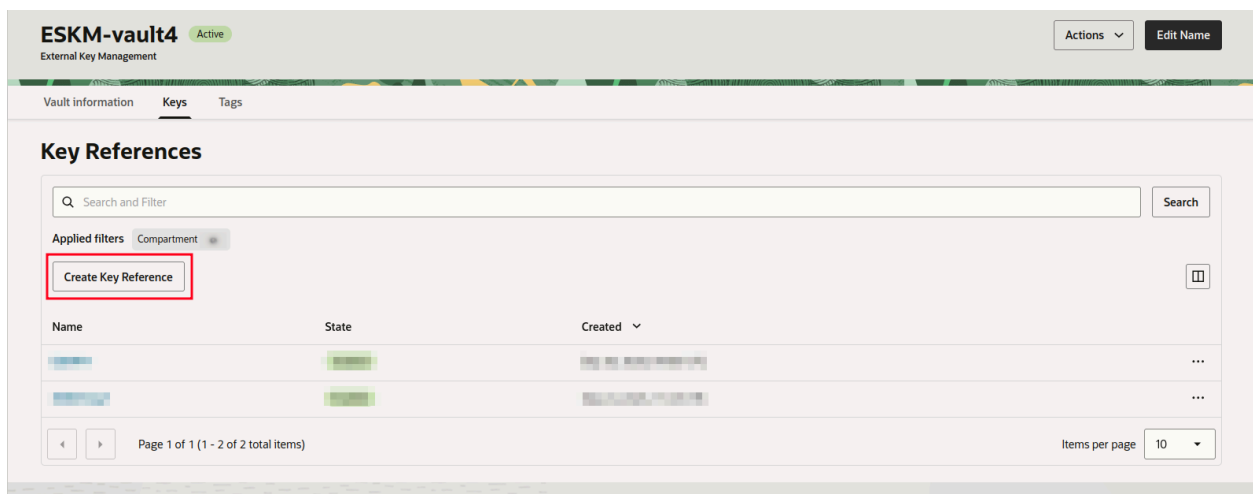


Figure 38 : Create Key Reference

4. Enter the external key identifier created in the ESKM previously:

<EXTERNAL_KEY_ID>

Create Key Reference

Create in Compartment

Name
ESKM-HYOK-KEY

Key Shape: Algorithm
AES

Key Shape: Length
256 bits

External Key ID
8f22be63-8b4c-4341-b679-45b6346e7a36

› **Advanced options**

Figure 39 : Key Reference Information

5. Enter the required algorithm and key length, if requested.
6. Enter the Key Reference name.
7. Click **Create**.
8. Verify that the Key is created and has the expected status.

ESKM-vault4 Active

Actions Edit Name

Vault Information **Keys** Tags

Key References

Search

Applied filters

Create Key Reference

Name	State	Created	
ESKM-HYOK-KEY	Enabled	Oct 4, 2026, 17:12 UTC	...
	Enabled		...
	Enabled		...

Page 1 of 1 (1 - 3 of 3 total items)Items per page 10

Figure 40 : Key Reference Created



The Key Reference is associated with the key managed by the external KMS. The cryptographic key remains under the control of the external KMS.

8.1.2 Rotate the Key in OCI

1. In the OCI Console, open the **External Vault** and select **Keys**.
2. Select the HYOK Key Reference and open **Key Reference Versions**.
3. Select **Rotate Key Reference**.

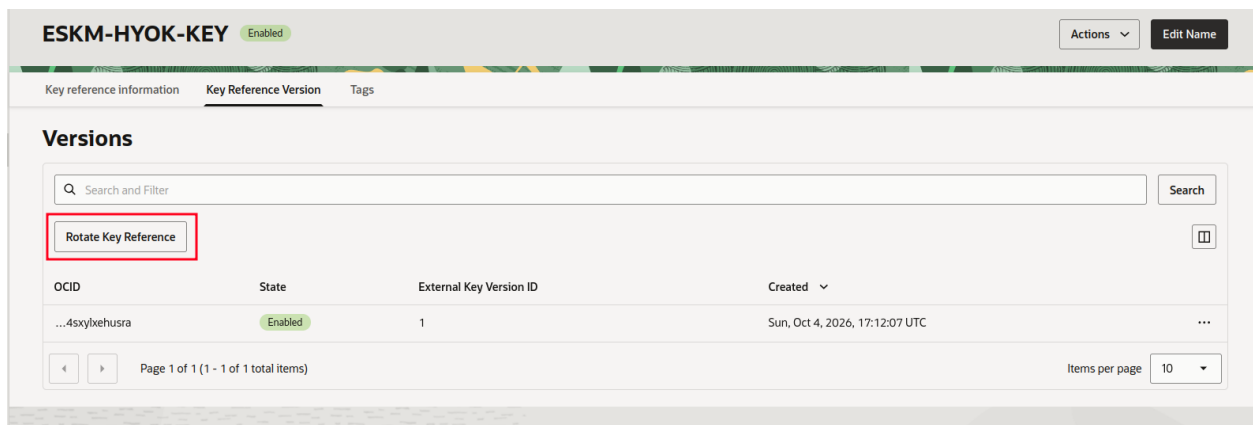


Figure 41 : Rotate Key Reference

4. Leave the **External Key Version ID** field empty.



The External Key Version ID is optional. If a specific key version has already been generated in ESKM, its ID can be entered. If the field is left empty, OCI creates a new Key Reference Version using the latest key version available in the External Key Manager.

5. Confirm the rotation when prompted.

Rotate Key Reference

If you do not enter an external key version ID, a new key reference version will be created for the latest key version available in the External Key Manager. Are you sure you want to rotate the key reference "ESKM-HYOK-KEY"?

Key version ID supplied by your external key management system.

Cancel Rotate Key Reference

Figure 42 : Rotate Key Reference Information

6. Verify that the new Key Reference Version is displayed as **Enabled**.

ESKM-HYOK-KEY Enabled Actions Edit Name

Key reference information **Key Reference Version** Tags

Versions

Search

Rotate Key Reference ⌵

OCID	State	External Key Version ID	Created	
...3ap4m7nuq	Enabled	1	Sun, Oct 4, 2026, 21:58:08 UTC	...
...4sxylxehusra	Enabled	1	Sun, Oct 4, 2026, 17:12:07 UTC	...

⏪ ⏩ Page 1 of 1 (1 - 2 of 2 total items) Items per page 10

Figure 43 : Key Reference Rotated

8.1.3 Disable the Key in OCI

1. In the **External Vault**, go to **Keys**.
2. Select the HYOK Key Reference and open **Actions**.
3. Select **Disable** and confirm the operation.

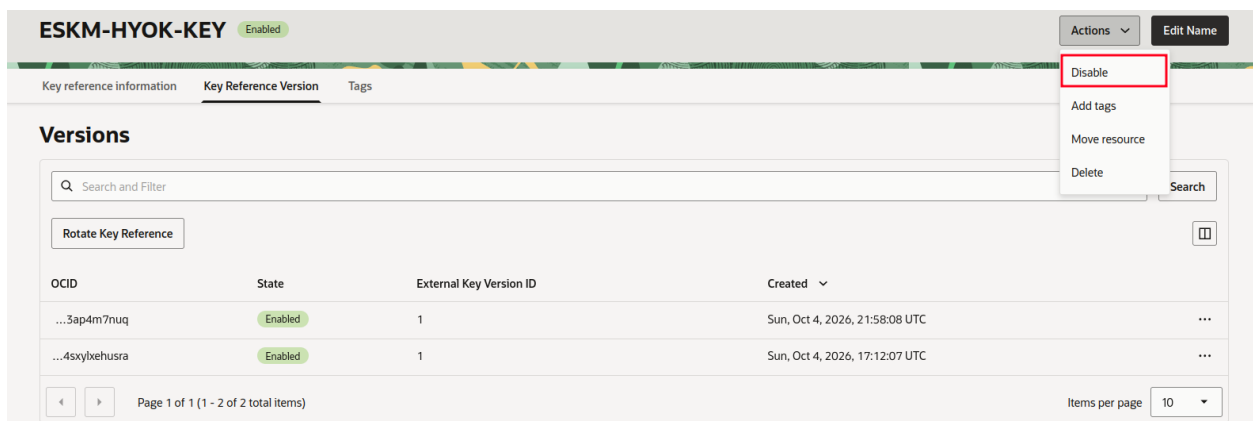


Figure 44 : Disable Key Reference

4. Verify that the Key Reference status changes to **Disabled**.

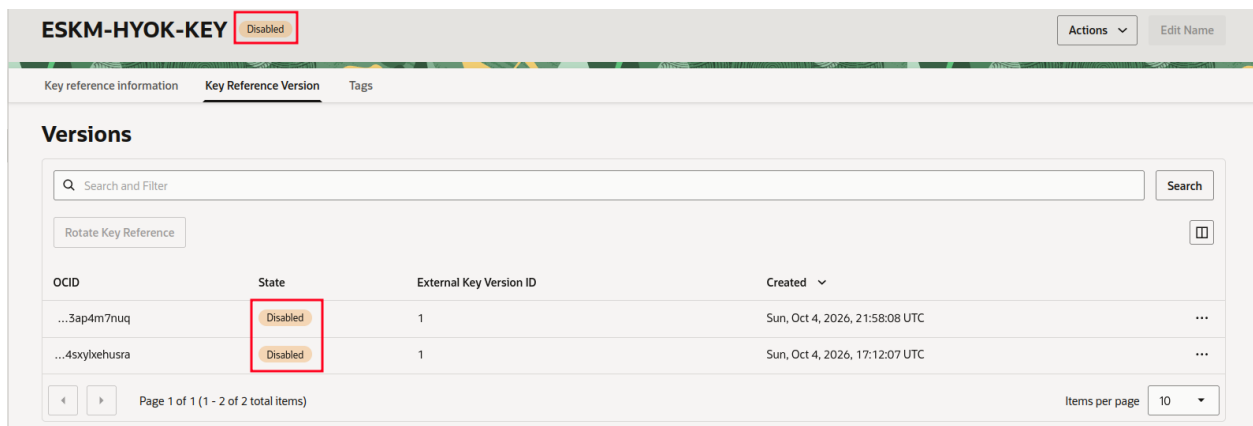


Figure 45 : Key Reference Disabled



A disabled Key Reference cannot be used for cryptographic operations.

8.1.4 Modify the Key in OCI

For HYOK, the key material itself cannot be modified in OCI. To test modification of the OCI-side resource:

1. In the **External Vault**, go to **Keys**.
2. Select the HYOK Key Reference.
3. Select **Edit Name** and modify the available key name.

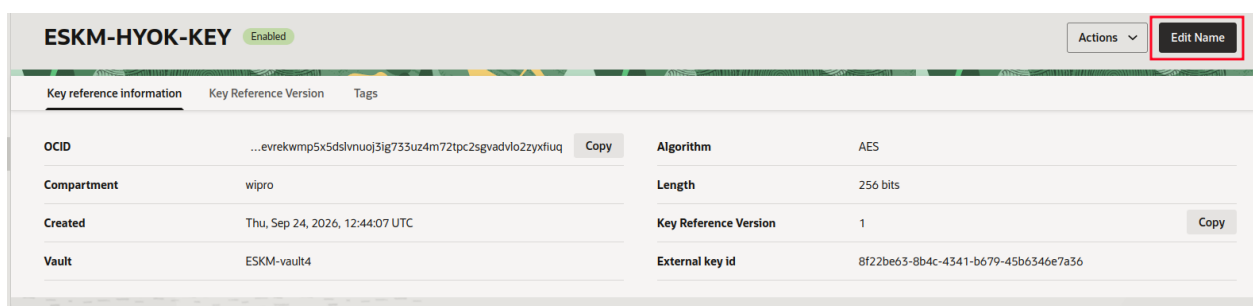


Figure 46 : Edit Key Name

4. Save the changes and verify that the modification is displayed.

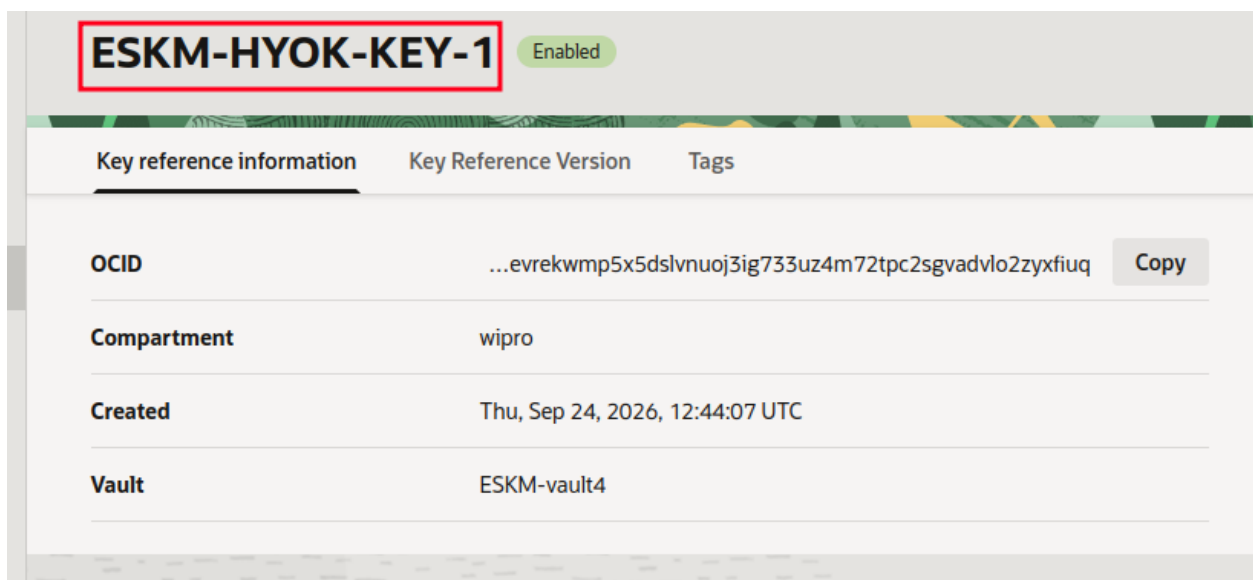


Figure 47 : Key Name Modified

8.1.5 Encrypt with the Key in OCI

1. In the OCI Console, go to **Storage** → **Block Storage** → **Block Volumes**.
2. Click **Create Block Volume**.

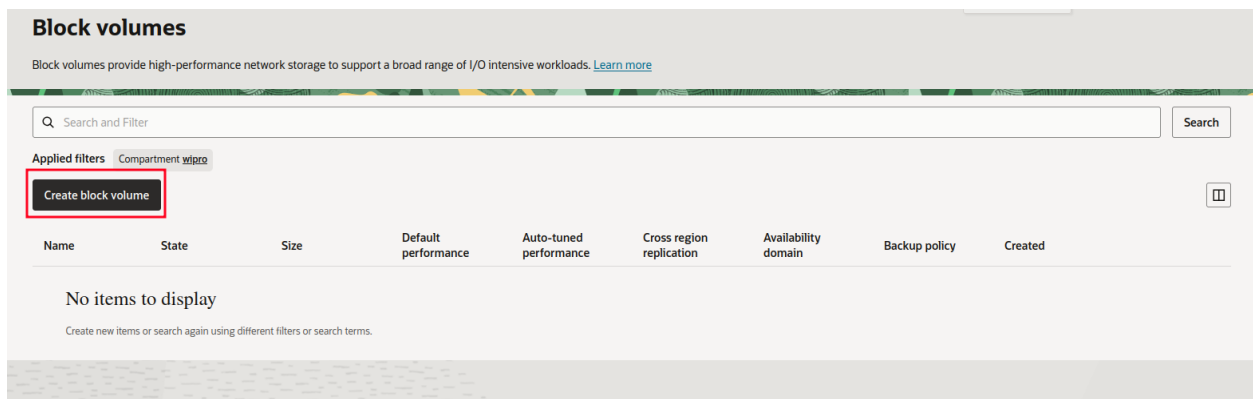


Figure 48 : Create Block Volume

3. Enter the required volume information.
4. Under **Encryption**, select **Encrypt using a customer-managed key**.
5. Select the **External Vault** created previously.
6. Select the **HYOK Key Reference**.

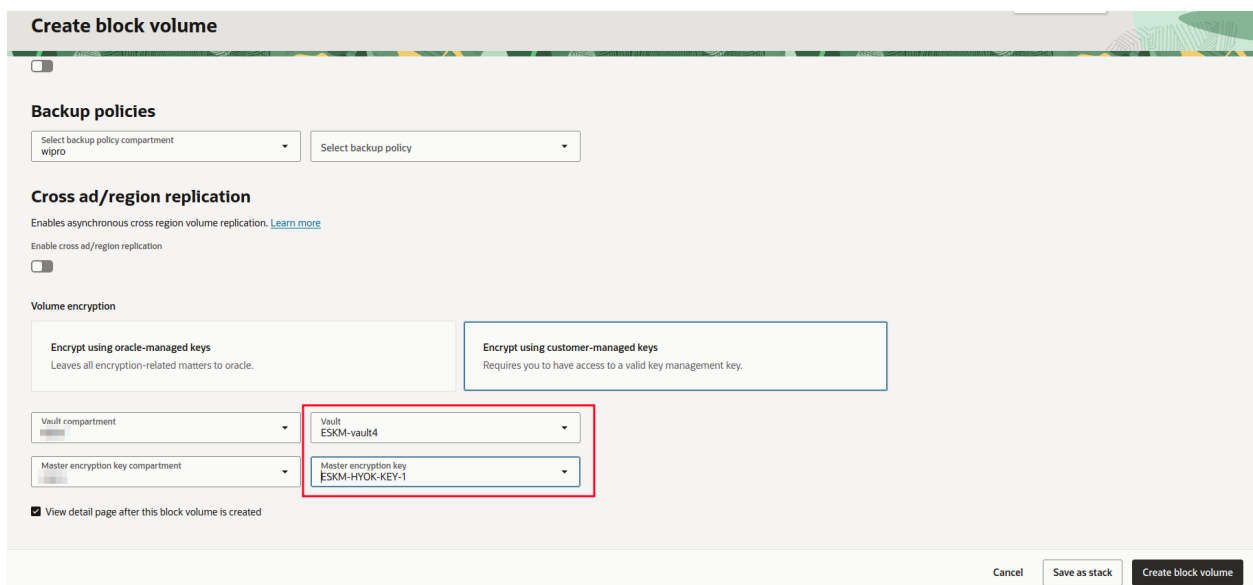


Figure 49 : Select HYOK Key Reference

7. Click **Create**.
8. Verify that the Block Volume is created successfully and that the HYOK Key Reference is displayed as the encryption key.

8.1.6 Delete the Key in OCI

1. In the **External Vault**, go to **Keys**.
2. Select the HYOK Key Reference and open its actions.

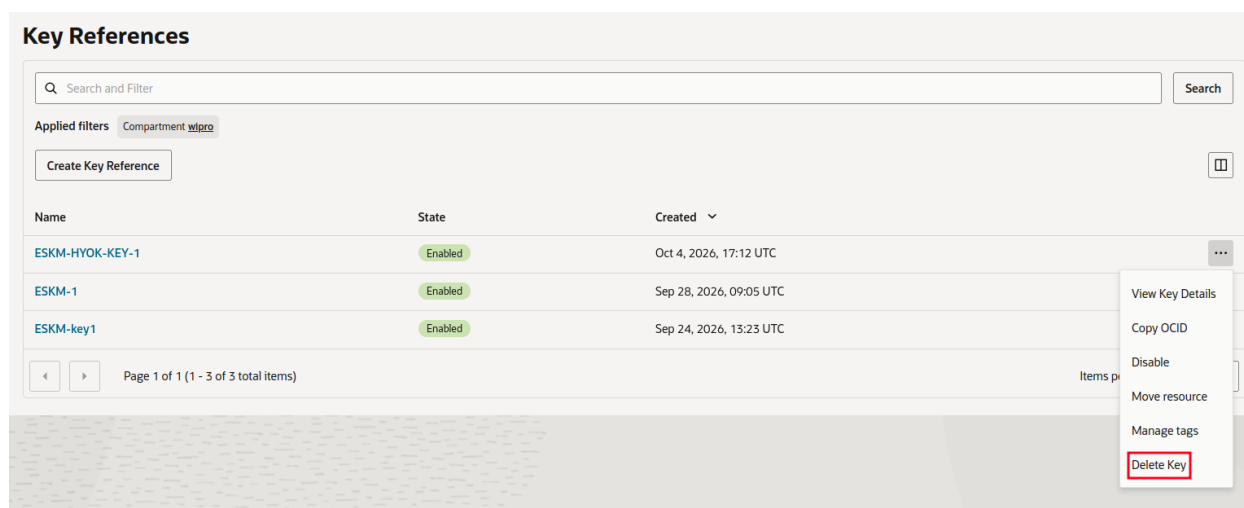


Figure 50 : Delete Key

3. Select **Delete**.

Delete Key Reference

Are you sure you want to delete the key reference "ESKM-HYOK-KEY-1"? Any data or any OCI resource such as Block Volume, Object Storage, Databases, Fusion Applications etc that are encrypted by this key will be unusable or irretrievable immediately, and is permanently unusable or irretrievable after the key has been deleted.

Confirm that you want to delete this key reference by clicking the box and typing "ESKM-HYOK-KEY-1".

Name
ESKM-HYOK-KEY-1

You can only schedule deletion 7 days from now. Within 7 days you can cancel deletion.

Select deletion date
11/3/2026

Time
22:00 UTC

Cancel

Delete Key Reference

Figure 51 : Confirm Deletion Schedule

- Confirm the deletion and verify that the Key Reference is scheduled for deletion or removed according to its current state.

ESKM-vault4 Active

External Key Management

Actions Edit Name

Vault information Keys Tags

Key References

Search and Filter

Search

Applied filters

Compartment wipro

Create Key Reference

Name	State	Created	
ESKM-HYOK-KEY-1	Pending Deletion	Oct 4, 2026, 17:12 UTC	...
ESKM-1	Enabled	Sep 28, 2026, 09:05 UTC	...
ESKM-key1	Enabled	Sep 24, 2026, 13:23 UTC	...

Page 1 of 1 (1 - 3 of 3 total items)

Items per page 10

Figure 52 : Key Pending Deletion



Deleting the Key Reference in OCI does not delete the corresponding key in ESKM. the external key remains available in the external KMS.

8.2 Logs and Validation Steps

The ESKM logs can be used to verify the operations performed during the OCI-HYOK 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-HYOK integration.
5. In the **Audit** log, verify that the key upload operation was successfully completed.

Log File: Current (Showing All Lines)

[Download Entire Log](#) [Clear](#)

```
REST Log:
[2026-10-04 18:04:12] [INFO] LOCALHOST [-] [REST] oci-vault4 Auth - [oci-vault4] - [Success] [-]
[2026-10-04 18:04:12] [ERROR] LOCALHOST [REST] oci-vault4 Get Key Custom Attributes oci-691ea8b1-0bcd-42a6-95c8-863359ce5dc0 [Custom attributes not found.] - [Failed] [-]
[2026-10-04 18:04:19] [INFO] LOCALHOST [-] [REST] oci-vault4 Auth - [oci-vault4] - [Success] [-]
[2026-10-04 18:04:19] [INFO] LOCALHOST [-] [REST] oci-vault4 KeyDelete oci-691ea8b1-0bcd-42a6-95c8-863359ce5dc0 - [Success] [-]
[2026-10-04 18:06:27] [INFO] LOCALHOST [-] [REST] oci-vault4 Auth - [oci-vault4] - [Success] [-]
[2026-10-04 18:06:27] [INFO] LOCALHOST [-] [REST] oci-vault4 KeyCreate oci-8f22be63-8b4c-4341-b679-45b6346e7a36 [AES 256 oci-vault4 Deletable Exportable Versioned] - [Success] [-]
[2026-10-04 18:06:27] [INFO] LOCALHOST [REST] Added group permissions - [Success] [Key name: oci-8f22be63-8b4c-4341-b679-45b6346e7a36; Group name: vault4; Key export: Always; Full permission: Always]
[2026-10-04 18:06:57] [INFO] LOCALHOST [-] [REST] oci-vault4 Auth - [oci-vault4] - [Success] [-]
```

Figure 53 : ESKM HYOK Logs



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-HYOK integration.

9 Troubleshooting

9.1 Common Issues and How to Resolve Them

Issue	Possible Cause	Resolution
External Vault cannot be created or verified	The External Vault URL, Private Endpoint, or OAuth configuration is incorrect or the external KMS is not reachable from OCI.	Verify the External Vault URL , Private Endpoint , and OAuth configuration. Verify that the external KMS is accessible through the configured Private Endpoint and that the required CA bundle is correct.
OAuth authentication failure	The OAuth client credentials or Identity Provider configuration are invalid or do not correspond to the OCI Identity Domain configured for the integration.	Verify the Client ID , Client Secret , Identity Domain URL , and OAuth configuration in both OCI and the external KMS. Verify that the configured OAuth scope is correct.
Private Endpoint connection failure	The VCN, subnet, destination IP/FQDN, port, or CA bundle configured for the Private Endpoint is incorrect, or the external KMS is not reachable through the configured network.	Verify the VCN , Subnet , KMS IP/FQDN , and Port configured for the Private Endpoint. Verify that the external KMS is listening on the configured port and that the required CA certificate is valid.
Key Reference cannot be created or used	The external key identifier is incorrect, the key does not exist in the external KMS, or the external KMS configuration does not allow OCI to access the key.	Verify the External Key ID in the external KMS and ensure that the key is available and enabled. Verify the tenancy, Identity Provider, OAuth client, and External Vault configuration.

Issue	Possible Cause	Resolution
Key Reference rotation fails	The specified external key version does not exist or the latest key version is not available to OCI through the external KMS.	Verify that the required key version exists in the external KMS and is available for use. If no External Key Version ID is specified, verify that the latest key version is available in the external KMS.
Cryptographic operation fails	The HYOK key is disabled or unavailable in the external KMS, or the External Vault/Key Reference configuration is incorrect.	Verify the status of the key in the external KMS and ensure that it is enabled and available. Verify the External Vault and Key Reference configuration and check the ESKM logs for the corresponding request.

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-HYOK 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.