VMWare

Cloud Director

10.6

Integration Guide

ESKM

8.54.0

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	2026-08-11
Status	PUBLISHED
Document No.	IG-2026-0036

Table of Contents

1 Introduction

1.1 About This Guide

This guide provides information on how to configure VMware Cloud Director to work with the Utimaco Enterprise Secure Key Manager (ESKM). It describes only the features in VMware Cloud Director, VMware vCenter Server, and ESKM that are necessary for the configuration and integration.

The integration is based on the underlying vCenter Server configuration, through which key management and encryption operations are performed using ESKM as an external Key Management Server (KMS).

For more information on installing an Utimaco Enterprise Secure Key Manager, refer to the *"Installing Hardware"* chapter in the Utimaco Enterprise Secure Key Manager Installation and Replacement Guide.

1.2 Target Audience

This guide is intended for VMware Cloud Director and Utimaco ESKM administrators.

1.3 Purpose of the Integration

The purpose of this integration is to enable VMware Cloud Director to leverage centralized and secure key management through ESKM for encrypted workloads in VMware-based cloud environments.

By integrating ESKM as the external Key Management Server (KMS) through VMware vCenter Server, encryption keys used for virtual machine protection are securely generated, stored, and managed outside of the virtualization platform. VMware Cloud Director builds on this configuration by orchestrating multi-tenant cloud environments that inherit encryption capabilities from the underlying vCenter infrastructure.

Additionally, the integration includes the use of a u.trust GP HSM to provide hardware-backed protection for root keys and key-encryption keys. This ensures that critical cryptographic material is safeguarded within a secure hardware boundary, enhancing the overall security posture of the environment.

This integration aims to:

- Enable secure deployment of encrypted virtual machines in multi-tenant cloud environments
- Centralize key management using ESKM
- Ensure separation between key management and workload execution
- Provide hardware-based protection for sensitive cryptographic material
- Support security and compliance requirements for enterprise and service provider environments

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
CA	Certificate Authority
CSR	Certificate Signing Request
CN	Common Name
SAN	Subject Alternative Name

Abbreviation	Meaning
IP	Internet Protocol
KMIP	Key Management Interoperability Protocol
KMS	Key Management Server
ESKM	Enterprise Secure Key Manager
RSA	Rivest-Shamir-Adleman
ECDSA	Elliptic Curve Digital Signature Algorithm
VM	Virtual Machine

Table 1: Abbreviations

1.5 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`

Convention	Use	Example
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 marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 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.

2.2 Overview of VMware Cloud Director

VMware Cloud Director is a cloud management platform designed to enable service providers and enterprises to deliver multi-tenant infrastructure and application services based on VMware vSphere environments. It provides a centralized interface to provision, manage, and monitor virtual data centers, virtual machines, networking, and storage resources across multiple tenants.

VMware Cloud Director operates on top of VMware vCenter Server and ESXi hosts, leveraging their capabilities for compute, storage, networking, and security. It introduces an abstraction layer that allows administrators to define Provider Virtual Data Centers (Provider VDCs) and allocate resources to tenant-specific Organization Virtual Data Centers (Org VDCs).

In the context of encryption and key management, VMware Cloud Director relies on the underlying vCenter Server configuration. All cryptographic operations, including virtual machine encryption and key handling, are performed through vCenter and its configured Key Management Server (KMS).

2.3 Joint Value Proposition

The integration of VMware Cloud Director with ESKM enables secure, multi-tenant cloud environments with centralized and hardware-backed key management.

VMware Cloud Director provides an abstraction layer on top of VMware vSphere, allowing service providers and enterprises to deliver isolated virtual data centers to multiple tenants. By leveraging the encryption capabilities of the underlying vCenter Server, Cloud Director enables tenants to deploy and manage encrypted virtual machines as part of their cloud workloads.

Through the integration with ESKM as the external Key Management Server (KMS), all cryptographic keys used for virtual machine encryption are centrally managed outside of the

virtualization platform. This ensures that key control remains independent from tenant workloads and infrastructure operations.

When combined with a u.trust GP HSM, ESKM further enhances security by protecting root keys and key-encryption keys within certified hardware, ensuring that sensitive cryptographic material is never exposed in software.

This architecture provides the following benefits:

- Secure Multi-Tenancy
  VMware Cloud Director enables multiple tenants to operate in isolated environments, while ESKM ensures that encryption keys are centrally managed and protected across all tenants.
- Centralized and Independent Key Management
  Encryption keys are managed outside of the cloud management platform, reducing the risk of unauthorized access and enabling clear separation of responsibilities.
- Hardware-Backed Key Protection
  Integration with u.trust GP HSM ensures that critical keys are stored and processed within secure hardware boundaries.
- Consistent Encryption Across Cloud Workloads
  All encrypted virtual machines deployed through VMware Cloud Director inherit the key management and encryption policies configured at the vCenter level.
- Improved Security and Compliance
  Centralized key control, auditability, and hardware-based protection support regulatory requirements and strengthen overall cloud security posture.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	VMWare Cloud	VMWare vCenter	ESKM Version
Linux Ubuntu 22.04	10.6	8.0	8.54.5

Table 3: Tested versions

3.2 Supported Platforms

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

3.3 Hardware and Software Requirements

Software	Software Requirements
ESKM	8.54.5
VMWare vCenter	>8.0 <8.OU3
VCloud Director	>10.6

Table 4: Hardware and software requirements

3.4 Prerequisites

1. ESKM version 8.54.5 or later.
2. Admin access to ESKM.
3. VMware vCenter Server deployed and configured (supported version).
4. Administrative access to vCenter Server.

5. VMware Cloud Director deployed and accessible.
6. Provider-level administrative access to VMware Cloud Director.
7. A configured and trusted Key Provider in vCenter using ESKM via KMIP (see VMware vCenter/ESXI and ESKM integration guide).
8. Network connectivity and hostname resolution between VMware Cloud Director, vCenter Server, and ESKM.
9. (Optional) u.trust GP HSM integrated with ESKM, including configured crypto user and key material.

4 Installation and Configuration

The following section outlines the procedures required to configure ESKM.

4.1 Setting Up ESKM

The initial phase involves configuring the ESKM before proceeding to VMWare Cloud Director. 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.

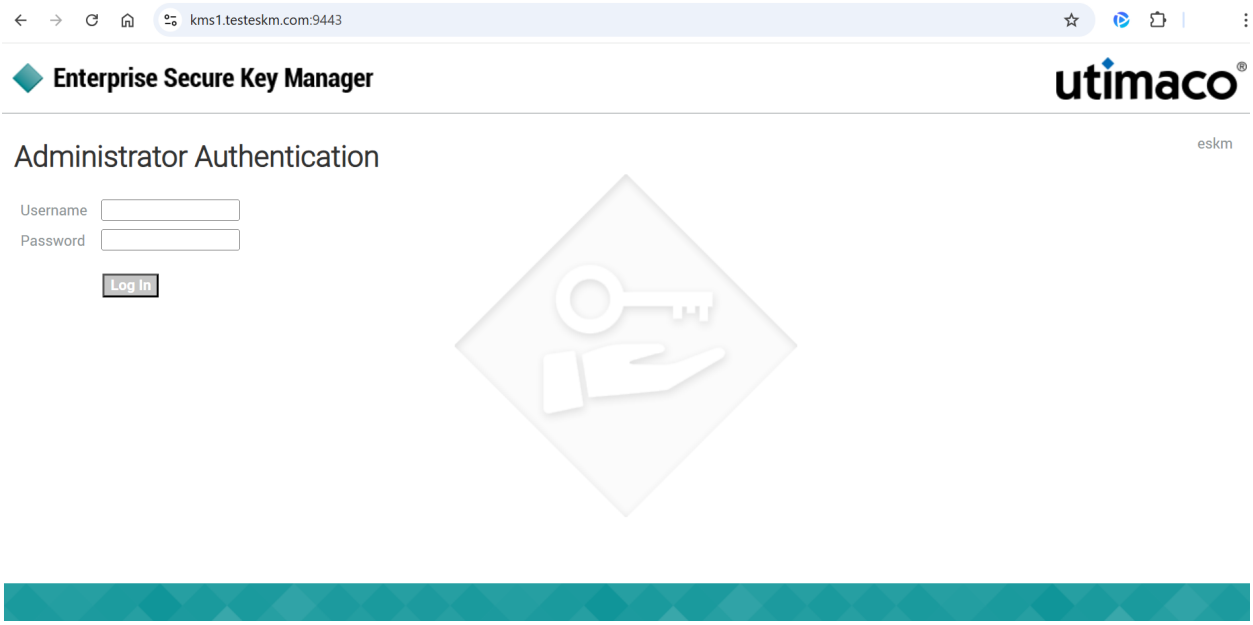

Figure 1 : ESKM Login Page

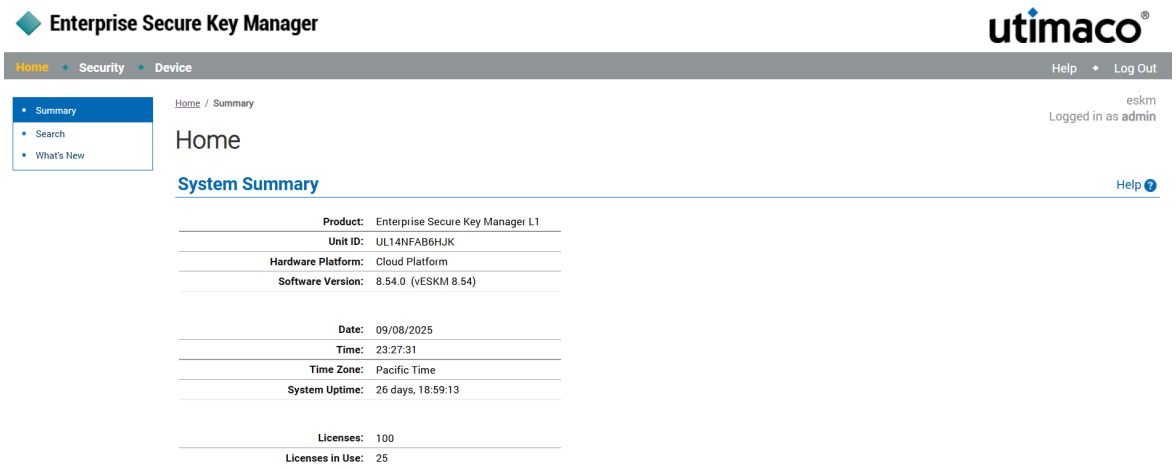

Figure 2 : ESKM Home Page

4.2 Setting Up VMWare Cloud Director

The initial phase involves deploying and configuring VMware Cloud Director before proceeding with the integration steps.

For detailed installation and configuration instructions, refer to the official VMware Cloud Director documentation available on the VMware website.

After successful deployment and initial configuration, access the VMware Cloud Director portal using a web browser:

```
https://<VCD-IP>/provider
```

Log in using the provider administrator credentials configured during the deployment process.

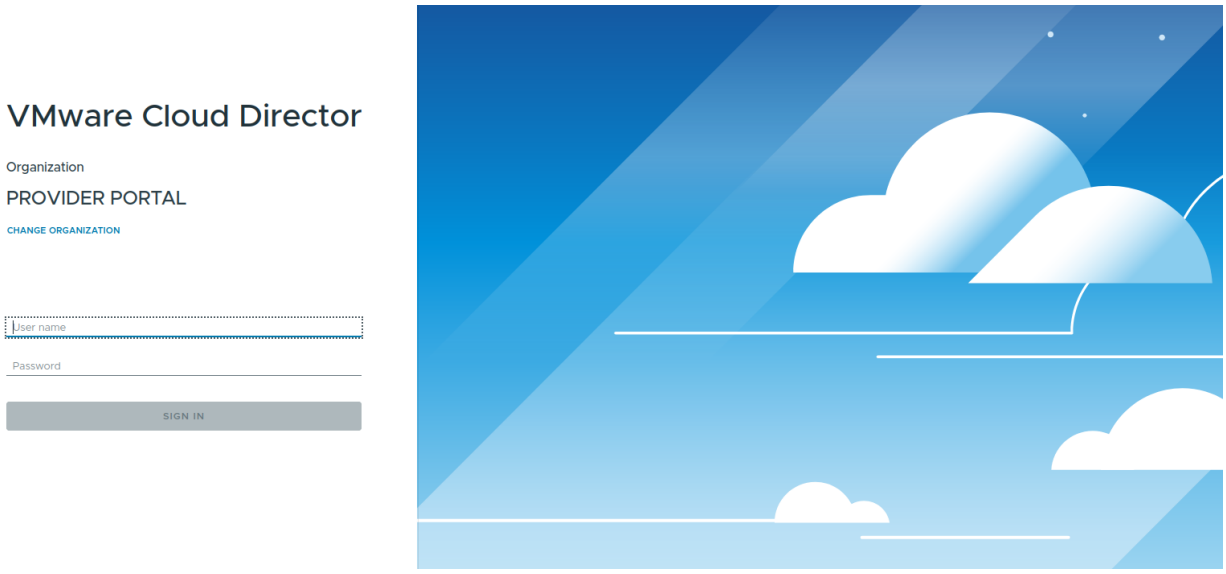

Figure 3 : VMware Cloud Login Page

4.3 Network and Security Configurations

The integration requires proper network connectivity and name resolution between all components involved in the architecture.

Ensure the following:

- Network connectivity is established between:
  - VMware Cloud Director and VMware vCenter Server
  - VMware vCenter Server and ESKM
  - ESKM and the u.trust GP HSM (if applicable)
- All components can resolve each other using DNS or appropriate hostname mapping.
- Required ports are open and not blocked by firewalls or network policies.

Failure to meet these requirements may result in connectivity issues, failed integrations, or inability to perform encryption operations.

5 Integration Steps

5.1 Configuration on ESKM

It is essential to configure the ESKM to ensure secure and efficient key management. This section guides you through the necessary steps to configure ESKM for Partner Product integration.

5.1.1 Create a Local CA

The local CA signs and verifies the server certificate and may also sign client certificate requests. Follow these steps to create and install a local CA.

1. Go to the **Security** tab.
2. Click on the **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Create Certificate** section.
4. Enter a **Certificate Authority Name** and a **Common Name**. These may have the same value, such as ESKMLocalCA.
5. Enter your **Organizational information**.
6. Select the **Algorithm** (for example, RSA-2048).
7. Select **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.
8. Click on **Create**.

Figure 4 : Create Local CA

5.1.2 Create a Server Certificate

You must create an ESKM certificate to enable secure communication between Partner Product and the ESKM.

To create an ESKM server certificate, perform the following steps:

1. In the **ESKM Management** console, go to **Security** > **Certificates and CAs** and click **Certificates**.
2. Enter **Certificate Name**, **Country Name**, **State or Province Name**, **Locality Name**, **Organization Name,** and **Organizational Unit Name**.
3. Select **RSA-2408** from the **Algorithm** dropdown list.
4. Select the previously created CA certificate name from the **Local CA** dropdown list.
5. Select **Server** from the **Certificate Purpose** dropdown list.
6. Click **Create**.

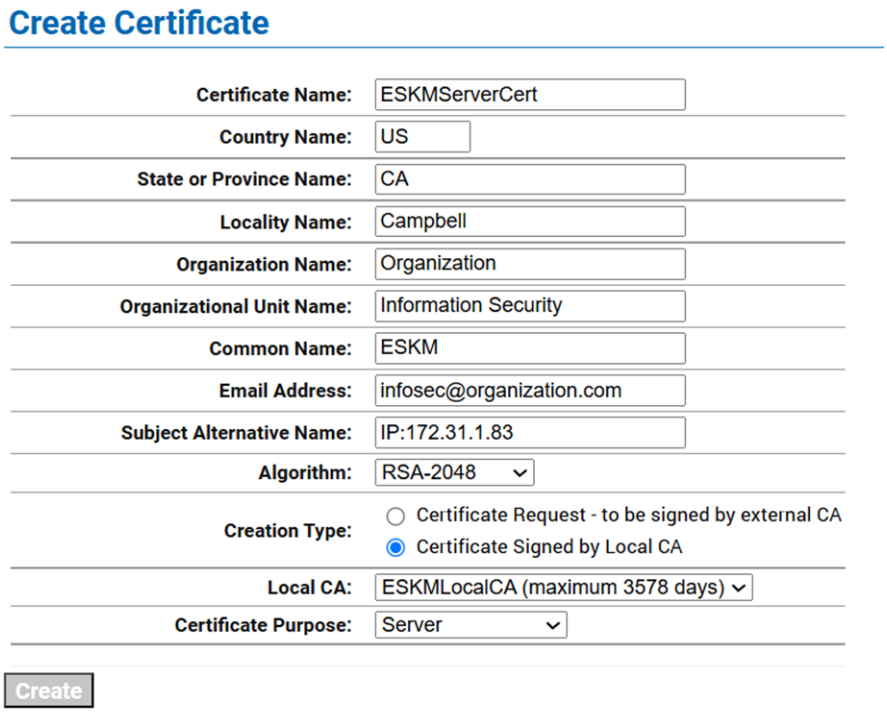

Figure 5 : Create Certificate

5.1.3 Configure the KMIP Server

1. In the **ESKM Management** console, go to **Device** > **KMIP Server** > **KMIP Server**.
2. Select the relevant KMIP Port.
3. Select the created server certificate as the **Server Certificate** for the KMIP server.
4. Select the created Local CA from the dropdown list.
5. Click **Save.**

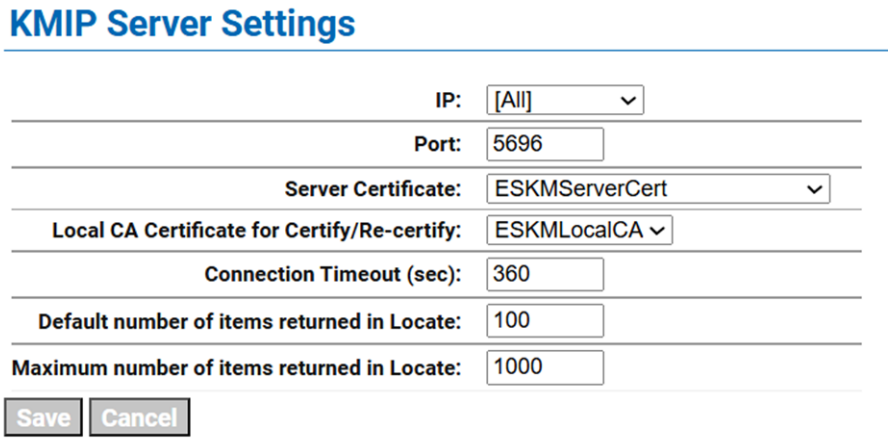

Figure 6 : KMIP Server Configuration

5.1.4 HSM Integration

The vESKM or ESKM L2 appliance can be integrated with the Utimaco CryptoServer LAN Hardware Security Module (HSM) which is a special “trusted” network computer performing a variety of cryptographic operations:

- key management, key exchange, encryption etc.
- Is built on top of specialized hardware.
- The hardware is well-tested and certified in Utimaco's special laboratories.
- Has a security-focused OS.
- Has limited access via a network interface that is strictly controlled by internal rules
- Actively hides and protects cryptographic material.

To configure the HSM integration in ESKM, perform the following steps:

1. Log in to the ESKM Management Console.
2. Select the **Device** tab.
3. In **Device Configuration**, click **HSM Integration**.
4. The HSM Integration dashboard is displayed.

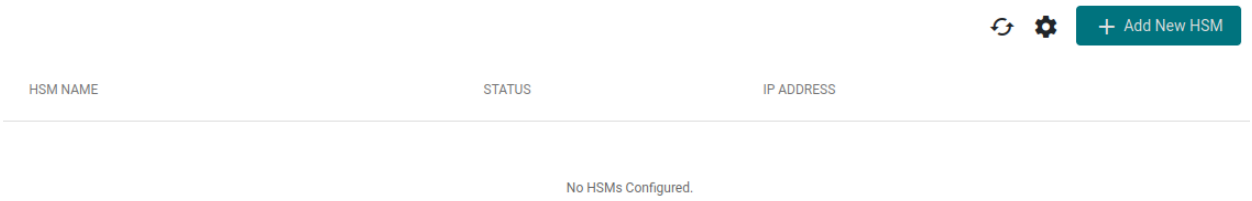

Figure 7 : HSM Integration Dashboard

5. Click **Add New HSM**.
6. Enter the required information in the configuration form:

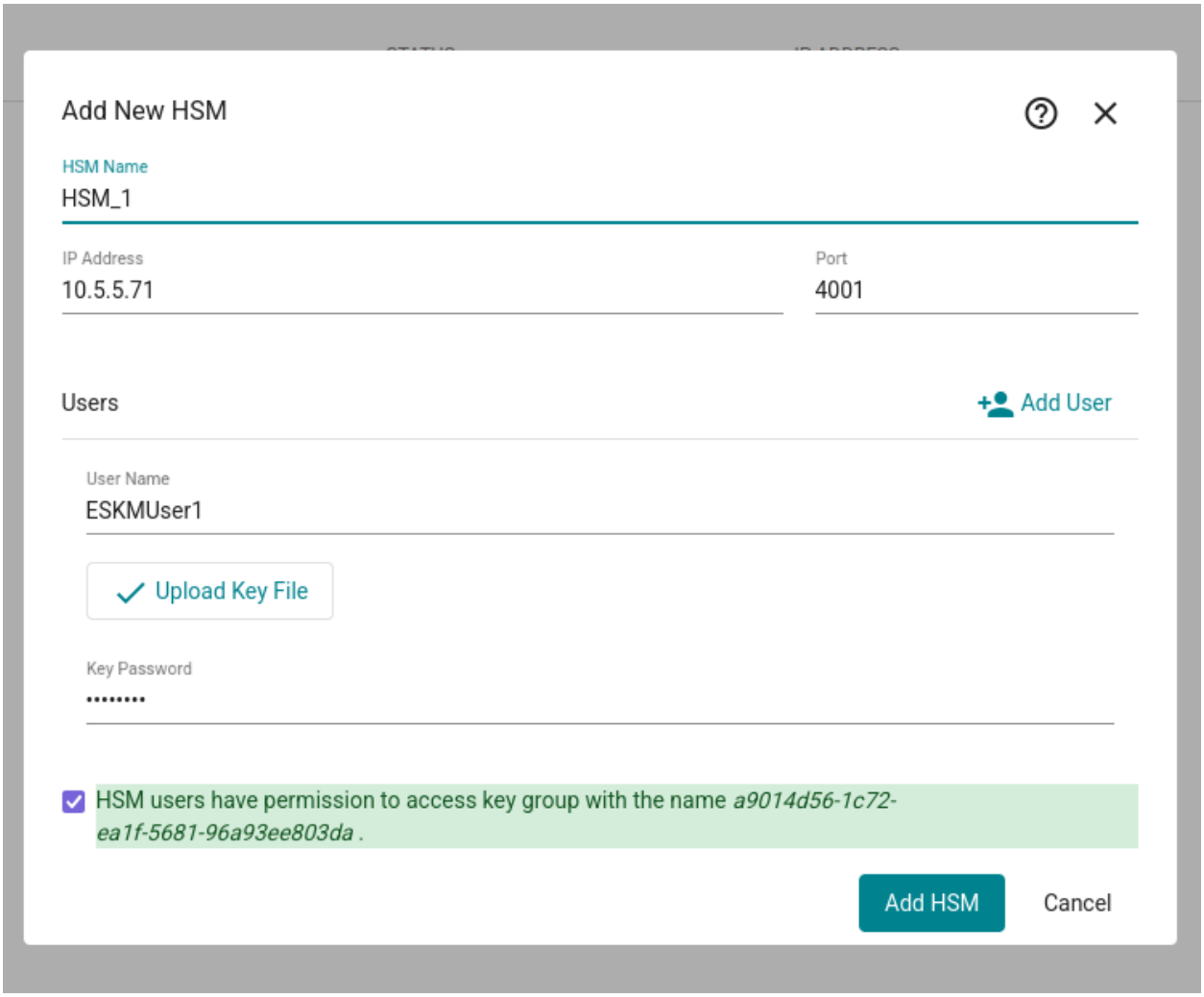

Figure 8 : Add New HSM

- Enter a name to identify the HSM.
- Enter the IP address of the HSM.
- Enter the communication port.
- Enter the Crypto User name configured on the HSM.
- Enter the password associated with the Crypto User.
- Upload the corresponding key file.

7. Click **Add HSM** to register the HSM.

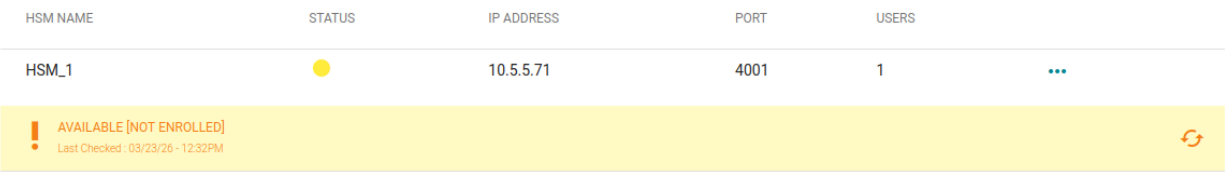

Figure 9 : HSM Added (Not Enrolled)

8. Initially, the HSM will not be enrolled. Click on the 3 dots and then **enroll** to enroll the HSM and make it available

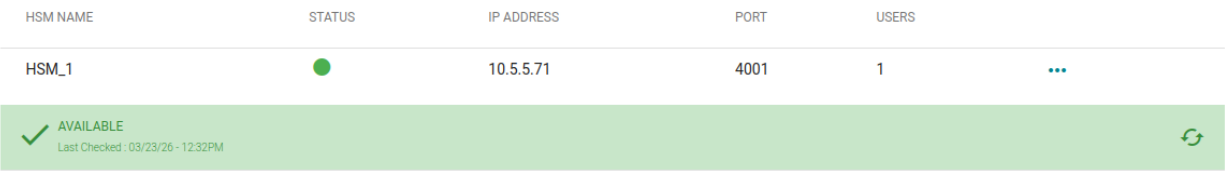

Figure 10 : HSM Added and Available

The new HSM is now sucessfully added.

Please refer to the “CryptoServer” documentation to create the HSM users.

It is recommended to enroll 2 HSMs for redundancy. An ESKM supports maximum number of 4 HSMs.

5.2 Configuration on VMWare vCenter

The steps below illustrate the configurations using a VMware vSphere Web Client.

This section is not a substitute for VMware documentation. Should this section offer different instructions than VMware's documentation, follow the instructions issued by VMware.

1. Open a web browser and enter the vSphere Web Client URL.
2. Go to Configure > Key Providers.

The screenshots used in the following sections, are captured from vSphere version 9.

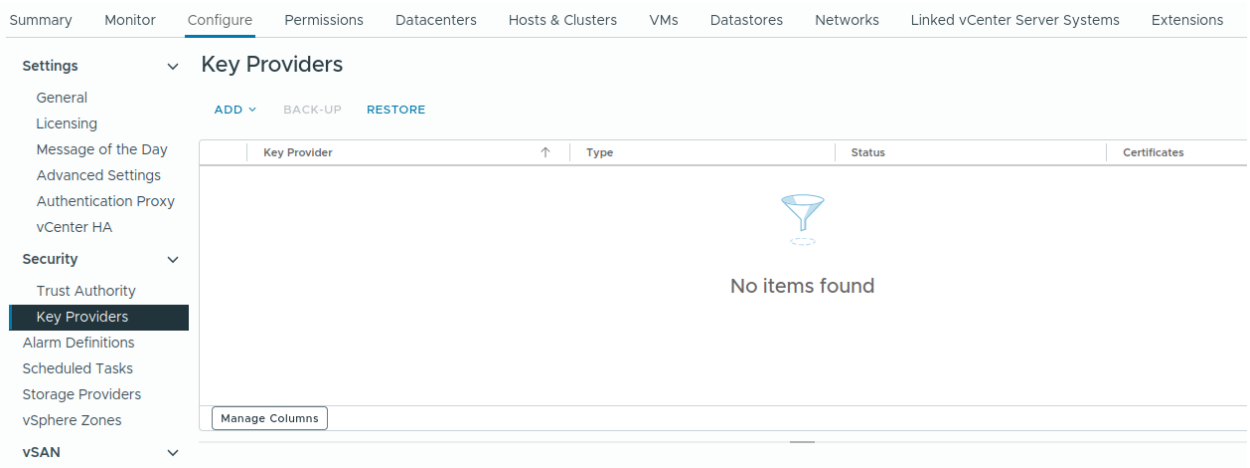

Figure 11 : Configure

3. Click on **ADD**.
4. Enter the following details to add a new Key Management Server (KMS).

Filed Name	Details
Name	Enter a name for the key provider configuration in vCenter. This is an internal identifier used to reference the KMS instance.
KMS	Enter a name or alias for the Key Management Server. This value is used to identify the KMS within the key provider configuration.
address	Enter the IP address of the configured ESKM.
port	KMIP port number 5696.
Proxy server	Do not enter anything.
Proxy port	
User name	
Password	

Table 5: New ESKM

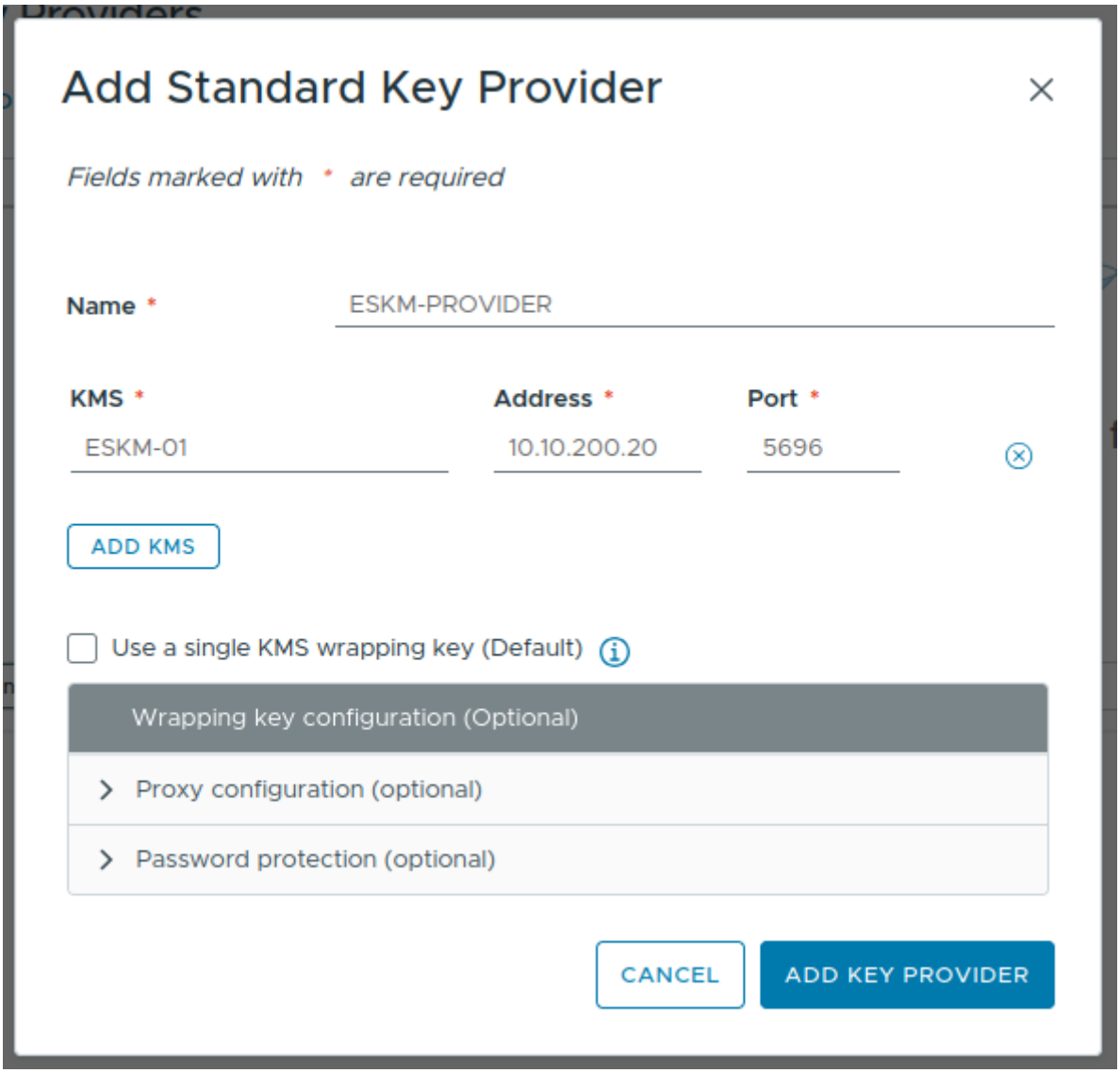

Figure 12 : Add KMS

5. Review the input information and click **ADD**.

vCenter Server provides an optional configuration to **use a single KMS wrapping key**. When this option is enabled, vCenter retrieves a single key from the KMS and uses it to wrap internally generated data encryption keys. This approach reduces the number of KMIP operations and minimizes key management overhead on the KMS.

While this mode can improve performance and scalability in environments with a large number of encrypted workloads, it also reduces the visibility of individual key lifecycle operations at the KMIP level. In contrast, when this option is not enabled, vCenter requests a unique key from the KMS for each encryption operation, allowing full traceability and management of keys within the KMS.

5.2.1 Establish trust between vCenter and ESKM

1. Click **TRUST** in the "Make vCenter Trust KMS" window and click on "MAKE KMS TRUST VCENTER".

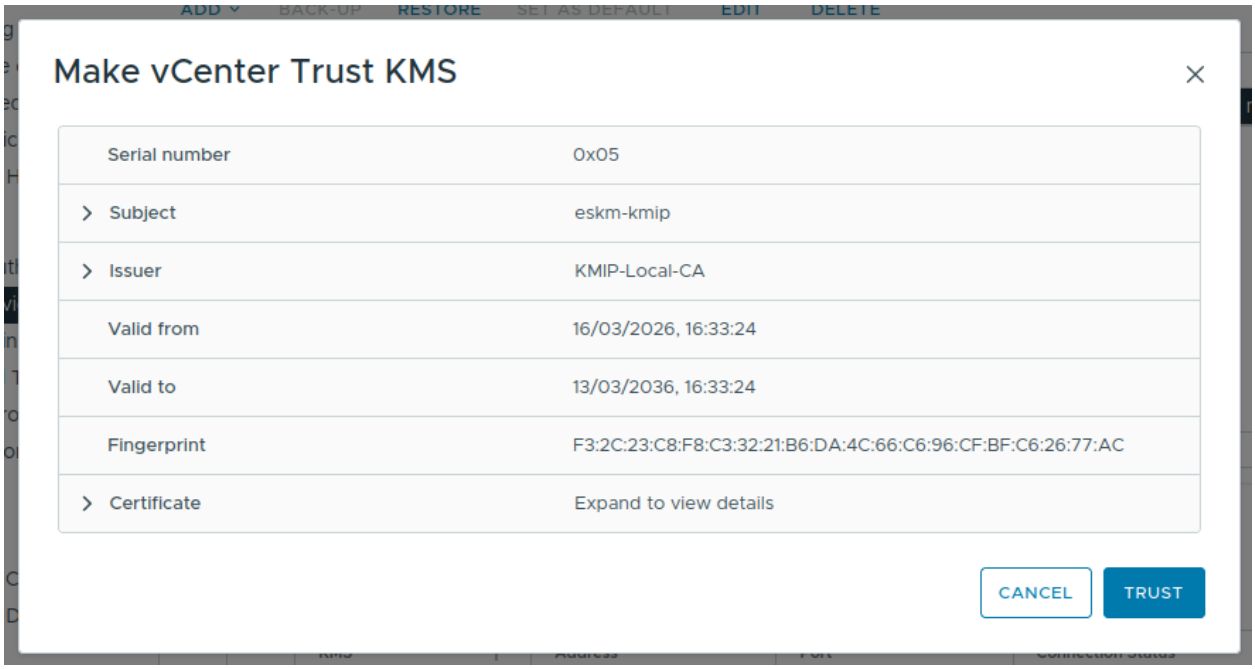

Figure 13 : Make vCenter Trust KMS Dialog window

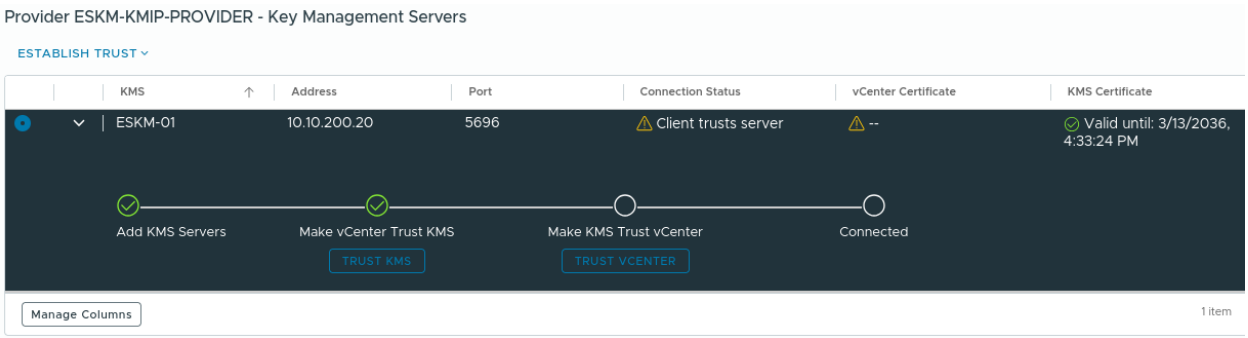

Figure 14 : Steps to stablish trust between vCenter and ESKM

2. Navigate to Choose a method, Select “New Certificate Signing Request (CSR)” and click **NEXT**.

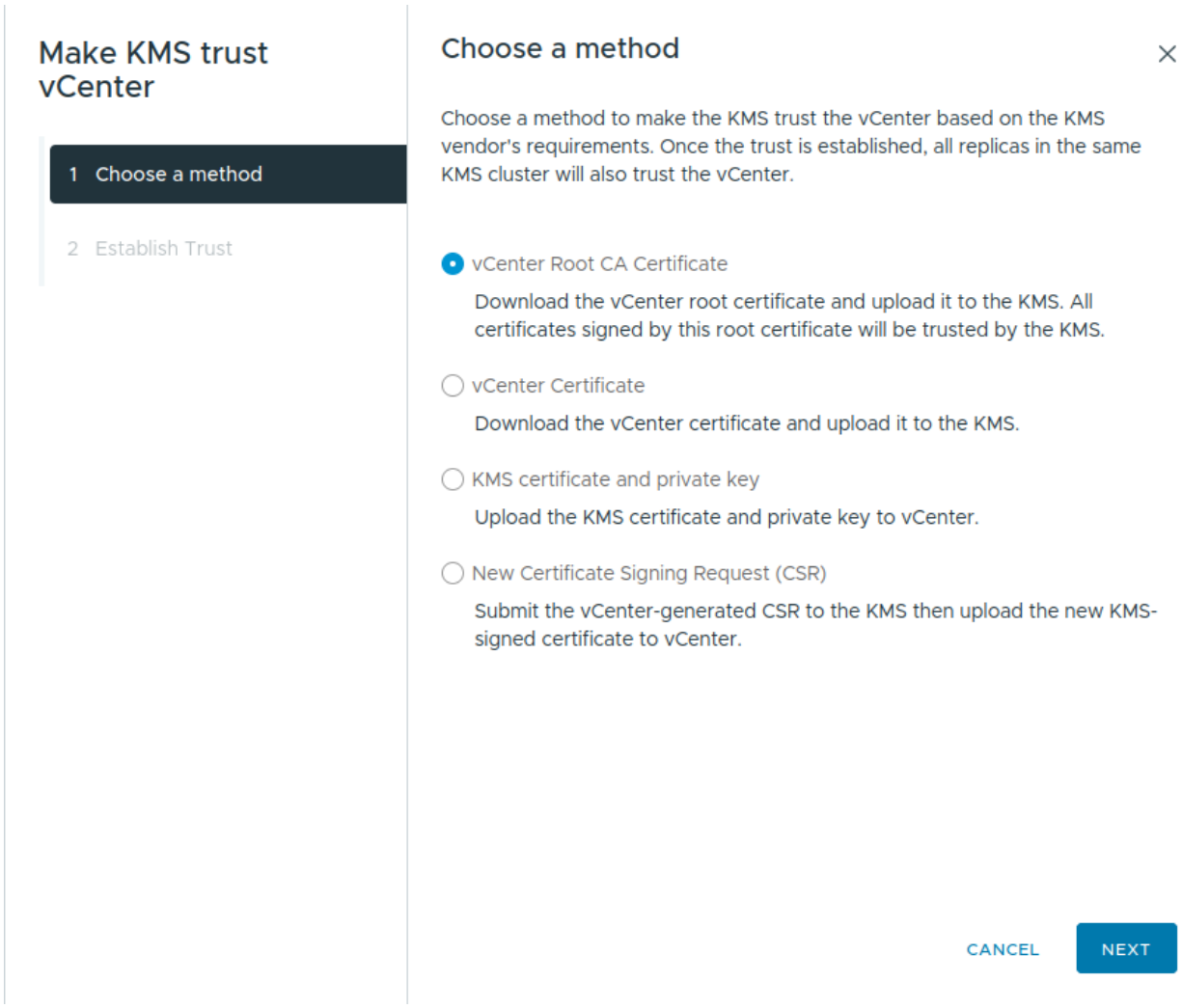

Figure 15 : Method selection for trust stablishment

3. In “Submit CSR to KMS”, click on **COPY** to copy the certificate request. Alternatively, click on **DOWNLOAD** to download the certificate request.

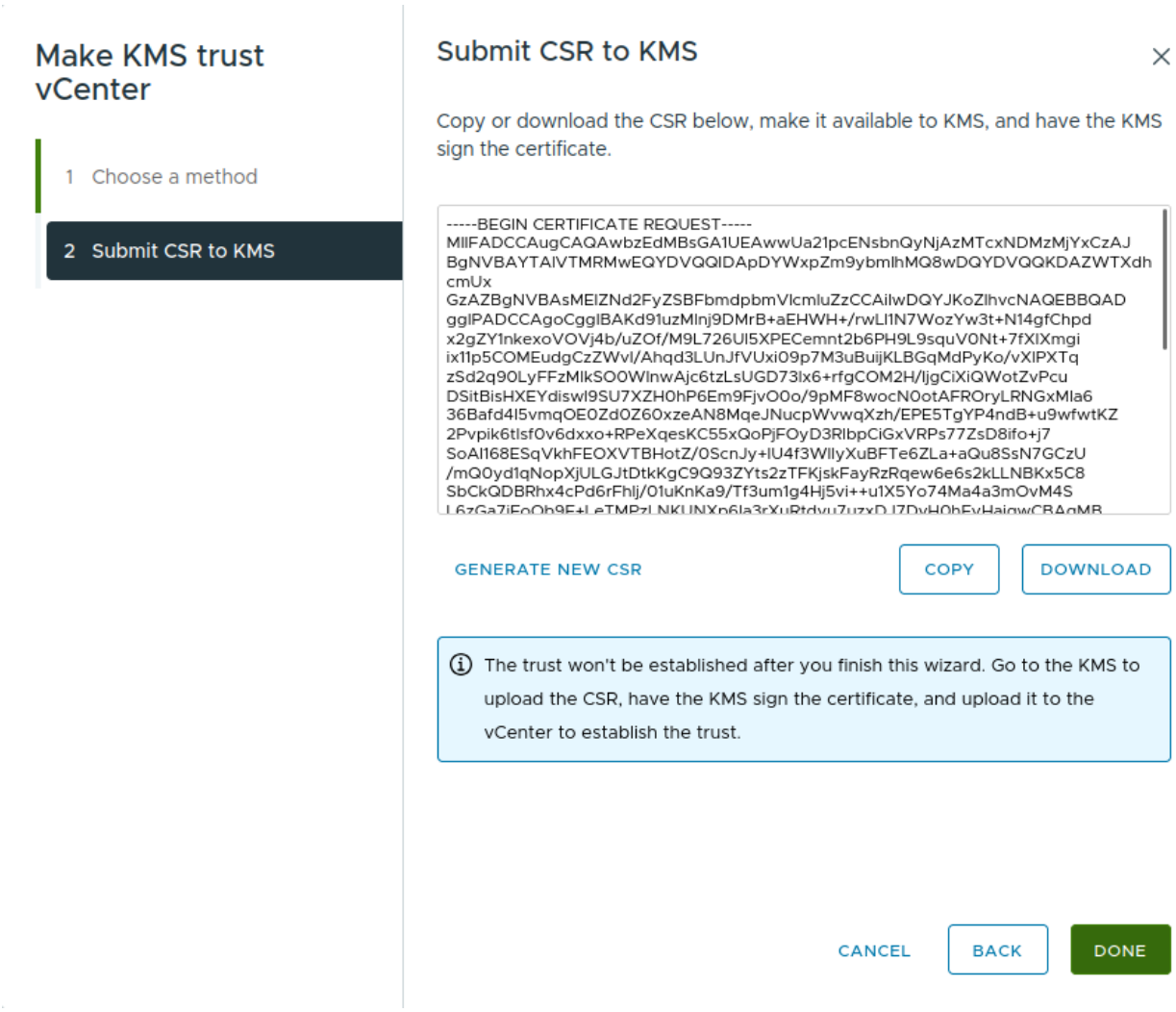

Figure 16 : Submit CSR to KMS dialog window

4. Click on **DONE**.

5. Go to ESKM and click on **Security > Certificates & CAs > Local CAs.**

6. Select the CA, and then click **Sign Request**.

Figure 17 : Local Certificate Authority List window

7. Set "Certificate Purpose" to **Client**.
8. Paste the certificate request generated by the client application into the certificate request field.
9. Click **Sign Request**.

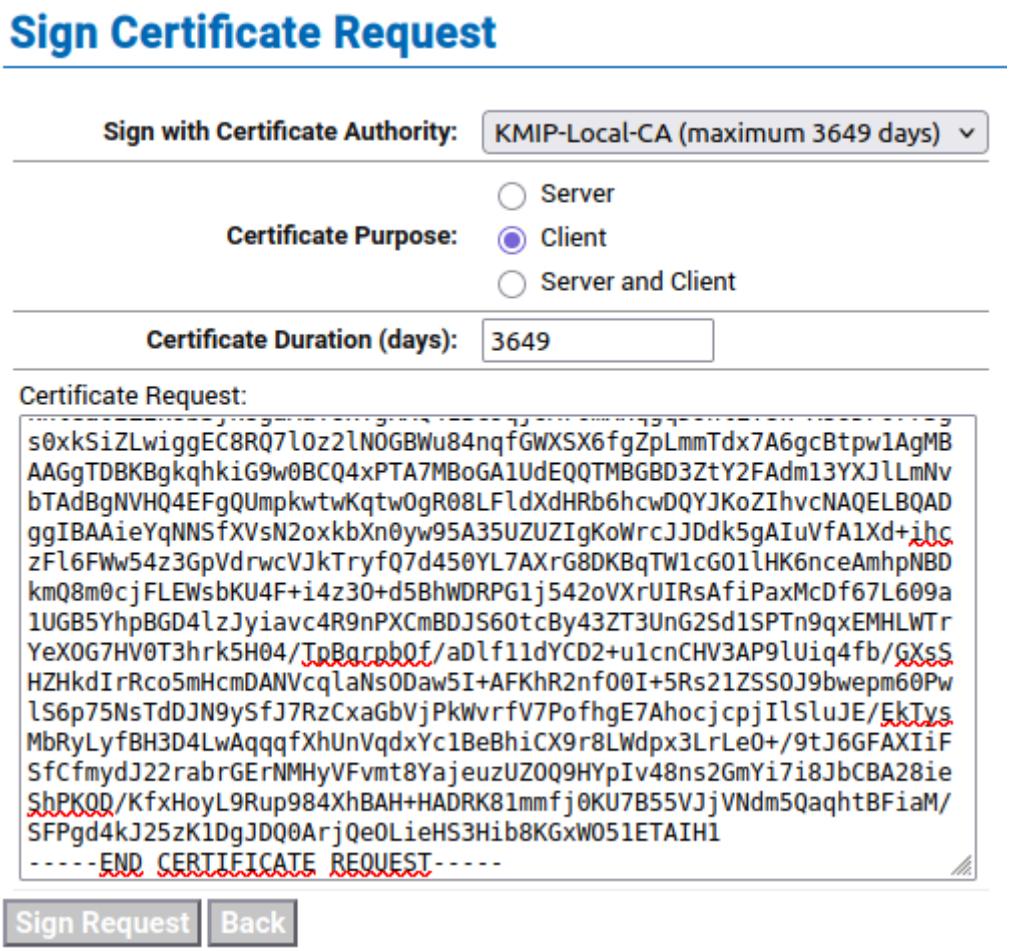

Figure 18 : Sign Certificate Request window

CA Certificate Information

Key Size:	4096
Start Date:	Mar 16 15:40:32 2026 GMT
Expiration:	Mar 13 15:40:32 2036 GMT
Issuer:	C: US ST: CA L: Campbell O: Utimaco Inc. OU: Utimaco CN: KMIP-Local-CA emailAddress: test@utimaco.com
Subject:	C: US ST: California O: VMware OU: VMware Engineering CN: kmipClnt260317153915

```
-----BEGIN CERTIFICATE-----
MIIENDCCA9ugAwIBAgIBBjAKBggqhkjOPQQDAjCBjzELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMVXRpbWFjbyBJ
bmMuMRAwDgYDVQQLEwdVdGltYWNvMRYwFAYDVQQDEw1LTUlQLUxvY2FsLUNBMR8w
HQYJKoZIhvcNAQkBFhB0ZXN0QHV0aW1hY28uY29tMB4XDTI2MDMxNjE1NDAzMloX
DTM2MDMxMzE1NDAzMlowbzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
aWExDzANBgNVBAoMBlZNd2FyZTEbMBkGA1UECwwSVk13YXJlIEVuZ2luZWVyaW5n
MR0wGwYDVQQDDBRrbWlwQ2xudDI2MDMxNzE1MzkxNTCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAIqdHvvZXZqMJNd5+4tWOXFIC2vHE4KjgqQoRqm1m2r3
+HCwmnWuT2nnc4CkpV2oFrLRofUnVx7tC1gKubjNwOu412Le2lZQDp6hCunOajvz
```

Figure 19 : CA Certificate Information window

10. Please note down the Common Name (CN) from the certificate information page and download the certificate.
11. Open the Management Console of the ESKM and navigate to **Security > Local Users & Groups > Local Users**.
12. At the bottom of the list, click **Add**.
13. The **Create Local User** window appears.
14. Create a KMIP local user in ESKM and provide the signed certificate content.

The “Username” must match with the noted “Common Name (CN)”.

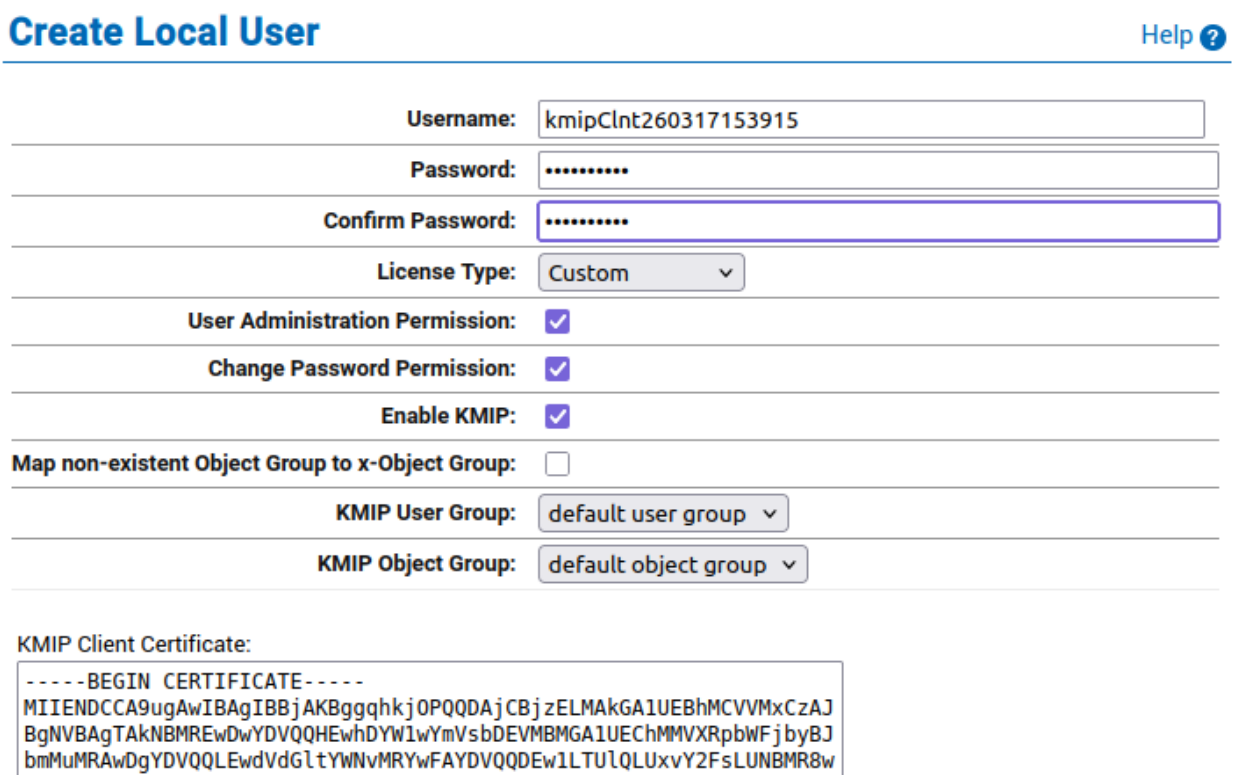

Figure 20 : Create Local User dialog window

Selected Local User

Username:	kmipClnt260317153915
Password:	********
License Type:	Custom
User Administration Permission:	☑
Change Password Permission:	☑
Enable KMIP:	☑
Default KMIP Object Group:	default object group
Client Certificate:	Subject: C: US ST: California L: O: VMware emailAddress: Common Name: kmipClnt260317153915 Not Valid Before: Mar 16 15:40:32 2026 GMT Not Valid After: Mar 13 15:40:32 2036 GMT
Date Created:	2026-03-17 16:44:22
Date Last Modified:	2026-03-17 16:44:22
Last Access Time:	

KMIP Client Certificate Contents:

```
-----BEGIN CERTIFICATE-----
MIIENDCCA9ugAwIBAgIBBjAKBggqhkjOPQQDAjCBjzELMAkGA1UEBhMCVVMxCzAJ
```

Figure 21 : Selected Local User

15. Go to vCenter and click on **Establish Trust** > **“Upload Signed CSR Certificate”**.

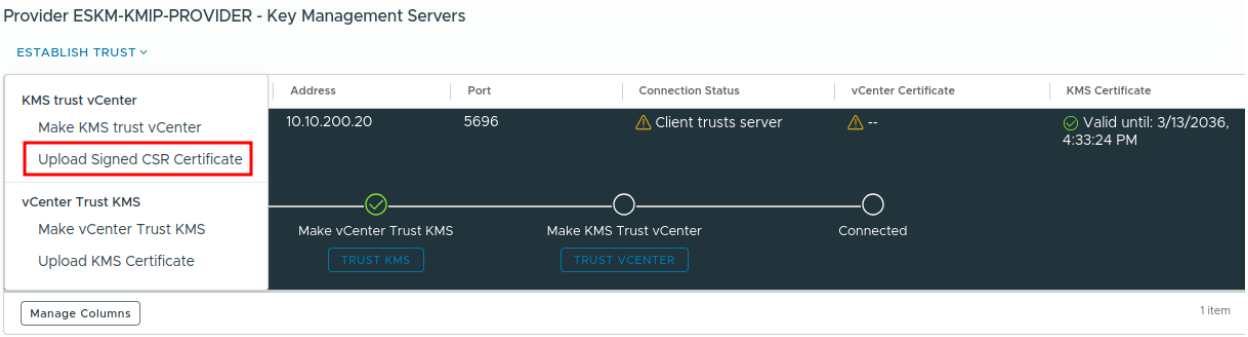

Figure 22 : Upload Signed Certificate Menu

16. Click **UPLOAD A FILE** and select the downloaded certificate from ESKM.

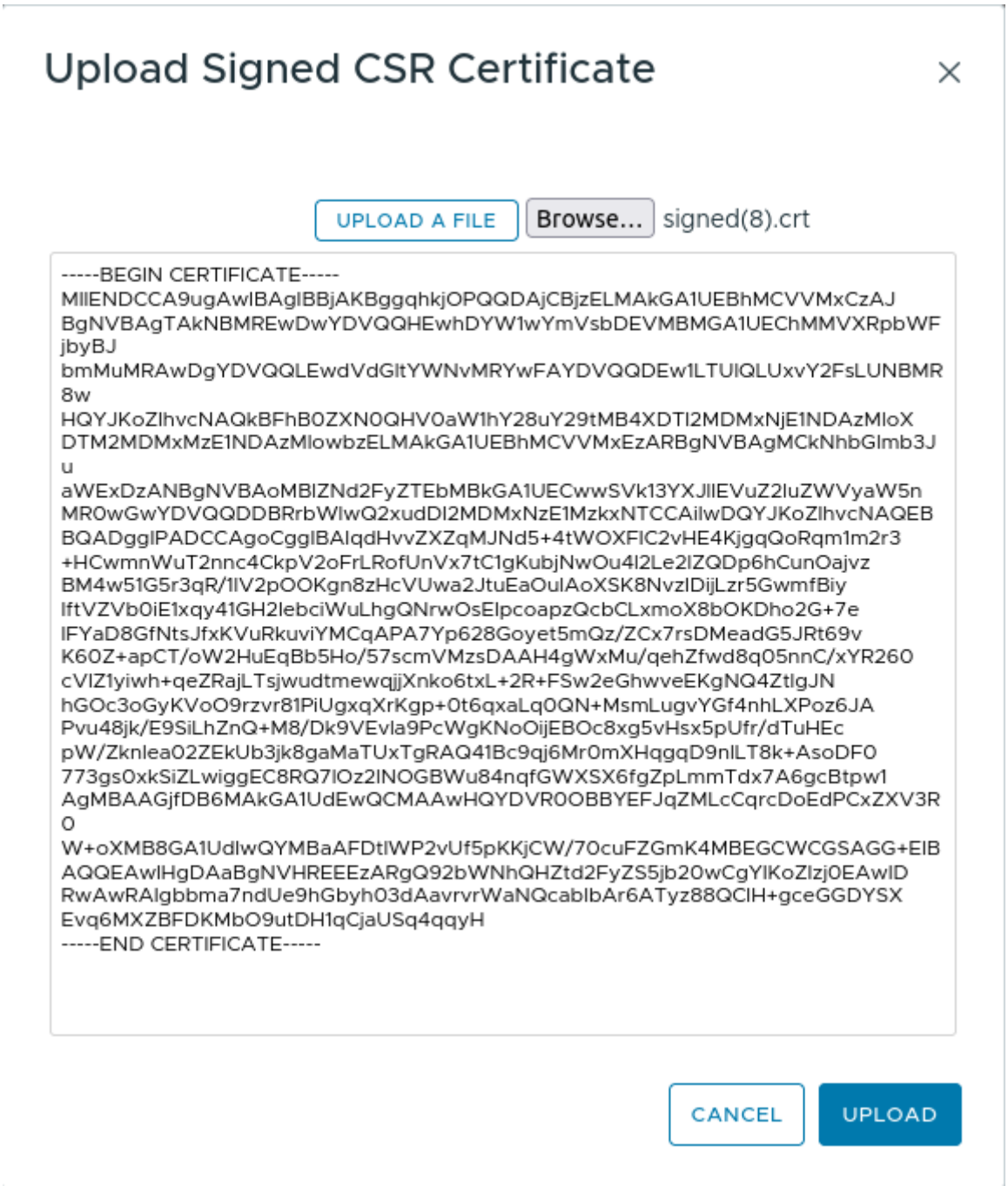

Figure 23 : Upload Signed CSR Certificate

17. Click on **UPLOAD** to confirm trust.
18. Confirm that the ESKM server is accessible and connected.

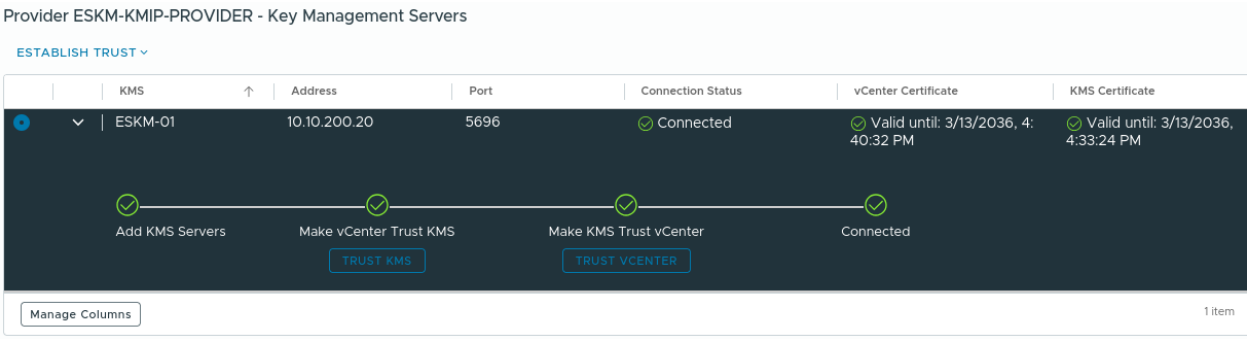

Figure 24 : Cpmpleted trust stablishment process

19. Click on **EDIT** in the key Provider then **ADD KMS** to add another ESKM server to the existing cluster and allow failover.

20. Enter the details to add a Key Management Server (ESKM).

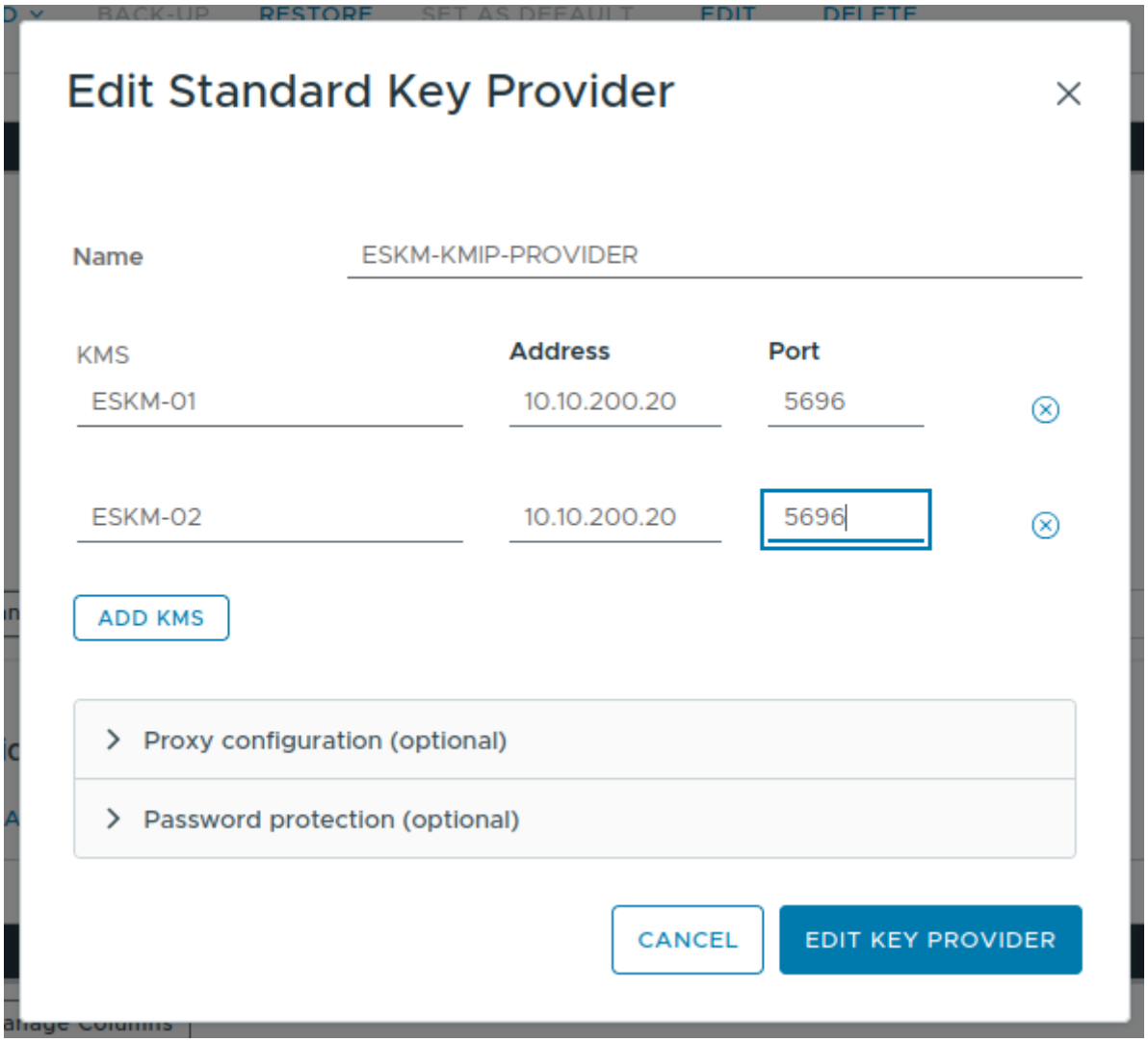

Figure 25 : Add Standard Key Provider for second ESKM

21. Review the input information and click **ADD**.
22. Click **TRUST** to make the vCenter trust KMS.

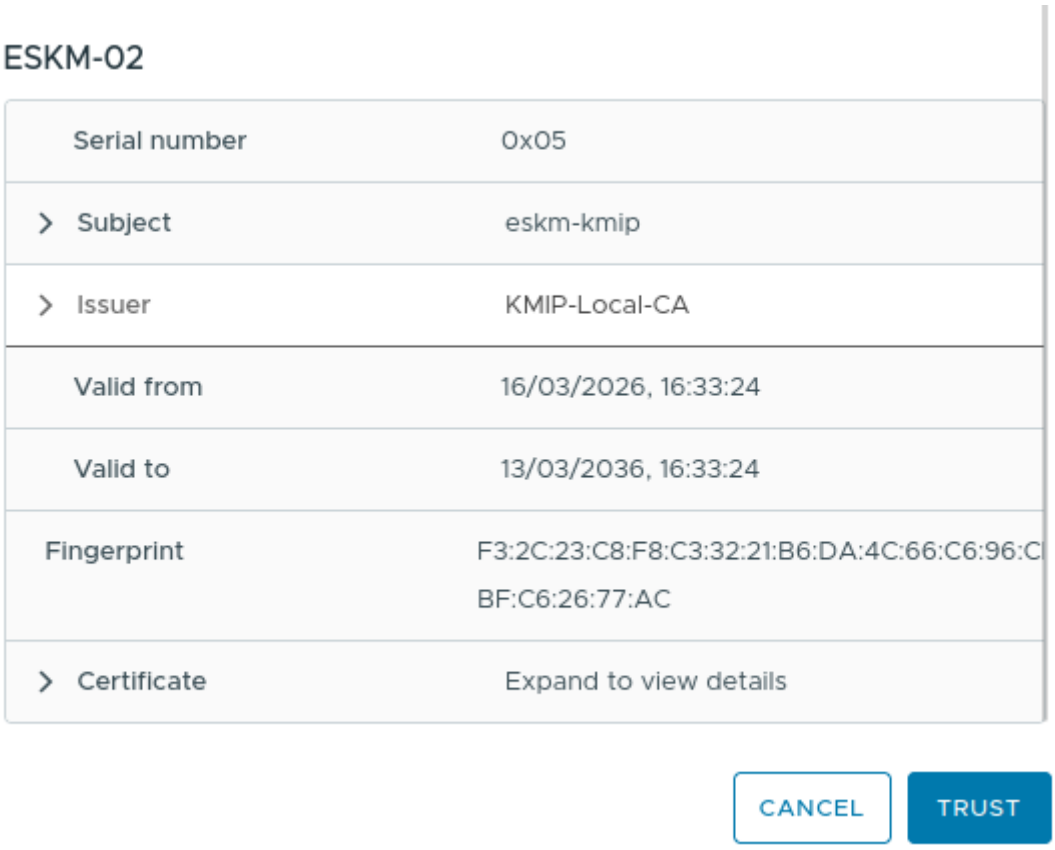

Figure 26 : Make vCenter Trust KMS on second ESKM

23. Confirm both the ESKM servers are accessible.

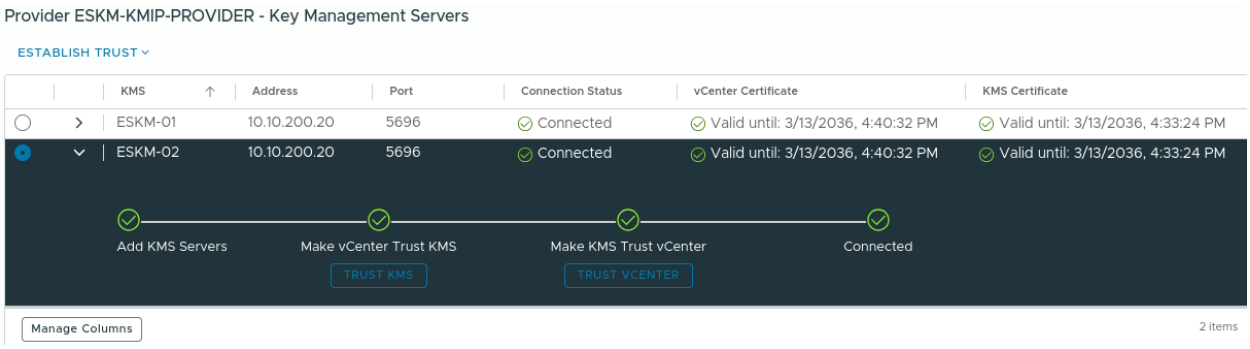

Figure 27 : Completed trust stablishment process on second ESKM

ESKM will be successfully integrated with VMware by following the procedure described above. Please follow the VMware policy guidelines to encrypt the VMs/ VSAN.

5.3 Configuration on VMWare Cloud Director

Before starting this section, ensure that VMware vCenter Server is already configured with ESKM as a Key Management Server (KMS), and that trust between both components has been successfully established as explained in the Installation and Configuration.

5.3.1 Adding vCenter Server

Cloud Director relies on vCenter Server to provide compute, storage, and encryption capabilities. Therefore, the vCenter Server must be added before proceeding.

1. Log in to the VMware Cloud Director provider portal.
2. Navigate to **Resources → Infrastructure Resources → vCenters.**

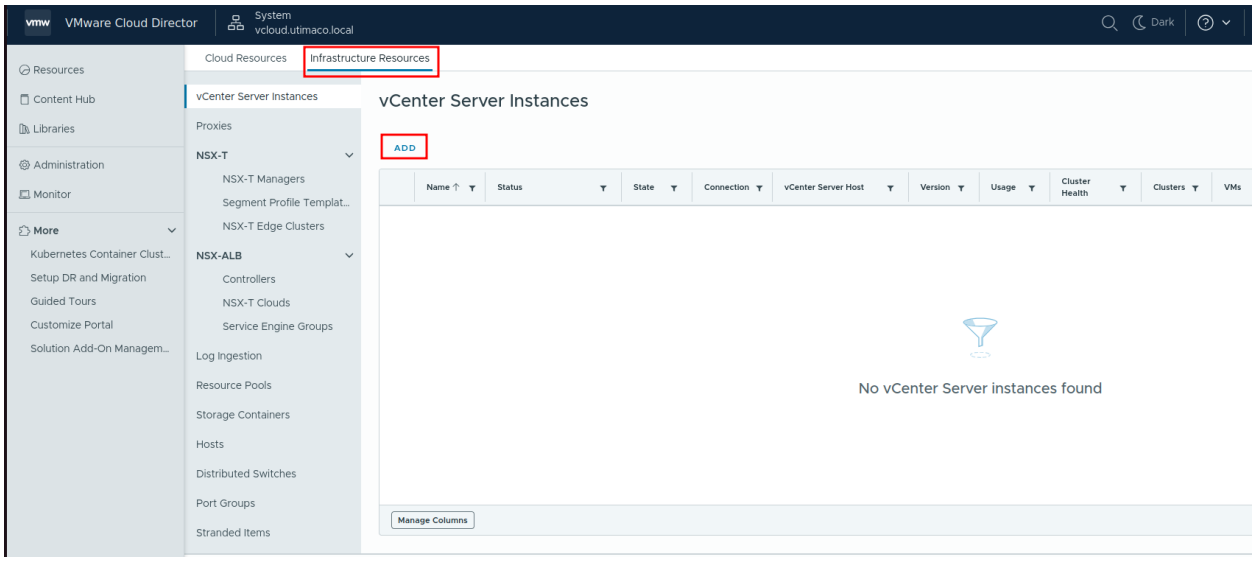

Figure 28 : Add vCenter Server Instance

3. Click **ADD.**

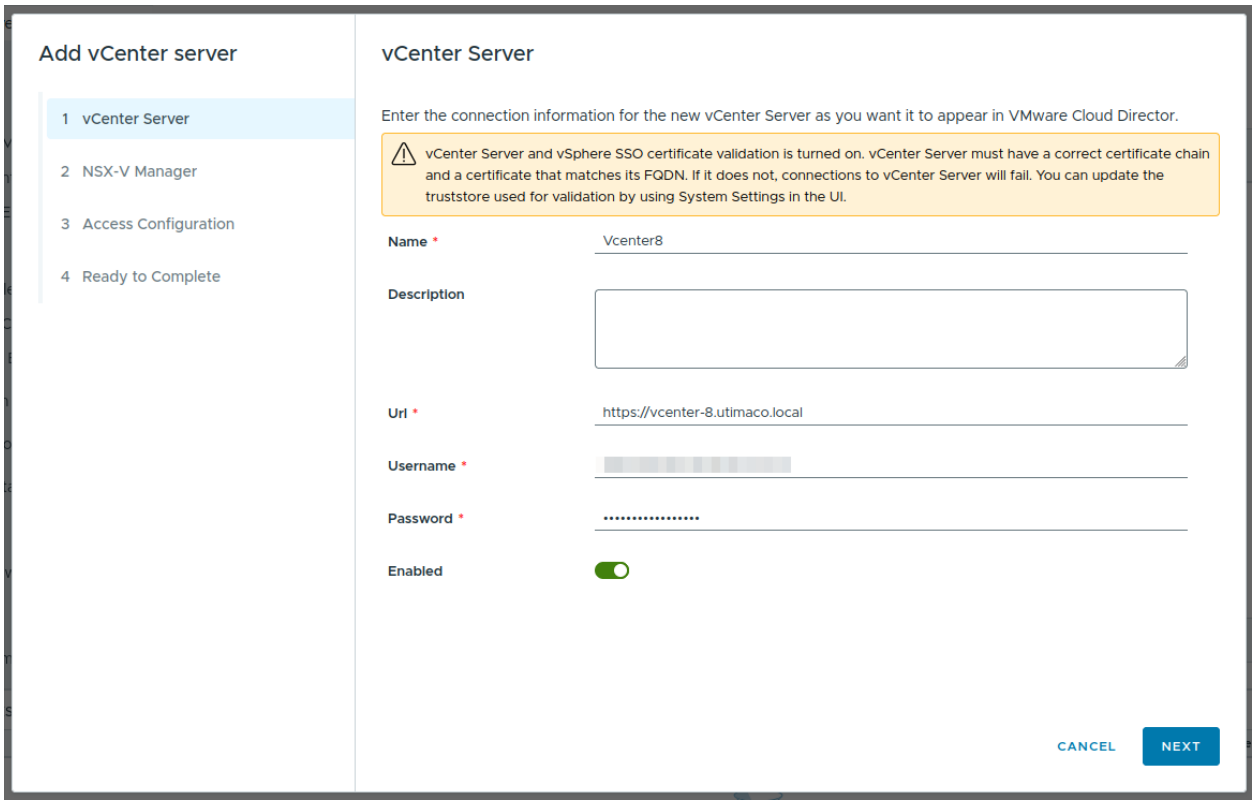

Figure 29 : vCenter Server Form

4. Provide:

- **Name**: Logical identifier
- URL: `https://<vcenter-hostname>`
- **Username**: Corresponding vCenter username (e.g., `administrator@vsphere.local`)
- **Password**: Corresponding password

5. Accept the certificate when prompted and complete the wizard.

Figure 30 : Trust vSphere Certificate

6. Enable the vSphere instance created.

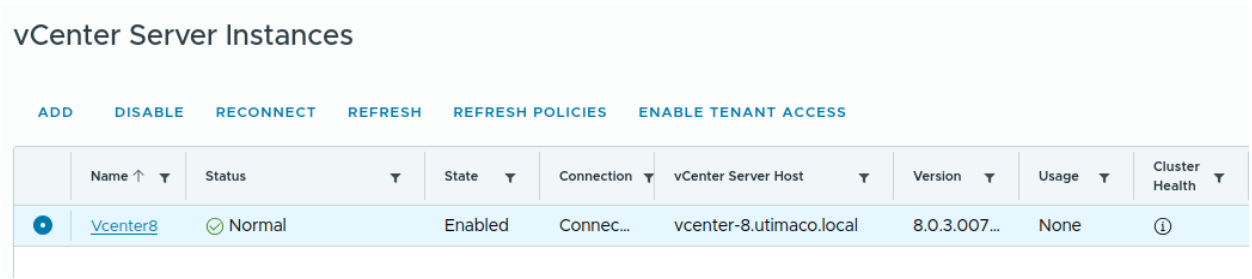

Figure 31 : vCenter Server Instance enabled

5.3.2 Creating a Provider VDC

The Provider Virtual Data Center (Provider VDC) exposes vCenter resources to VMware Cloud Director.

1. Navigate to **Resources → Cloud Resources → Provider VDCs**.

2. Click **New**.

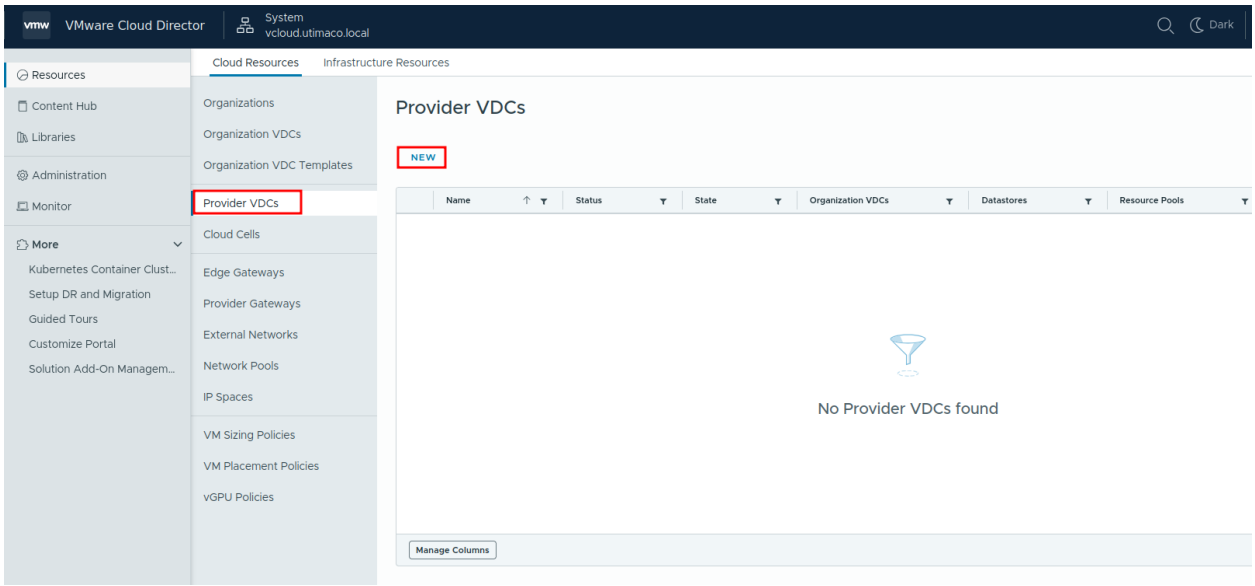

Figure 32 : New Provider VDCs

3. Select:

- The added vCenter Server
- The target cluster
- The VM Encryption Policy

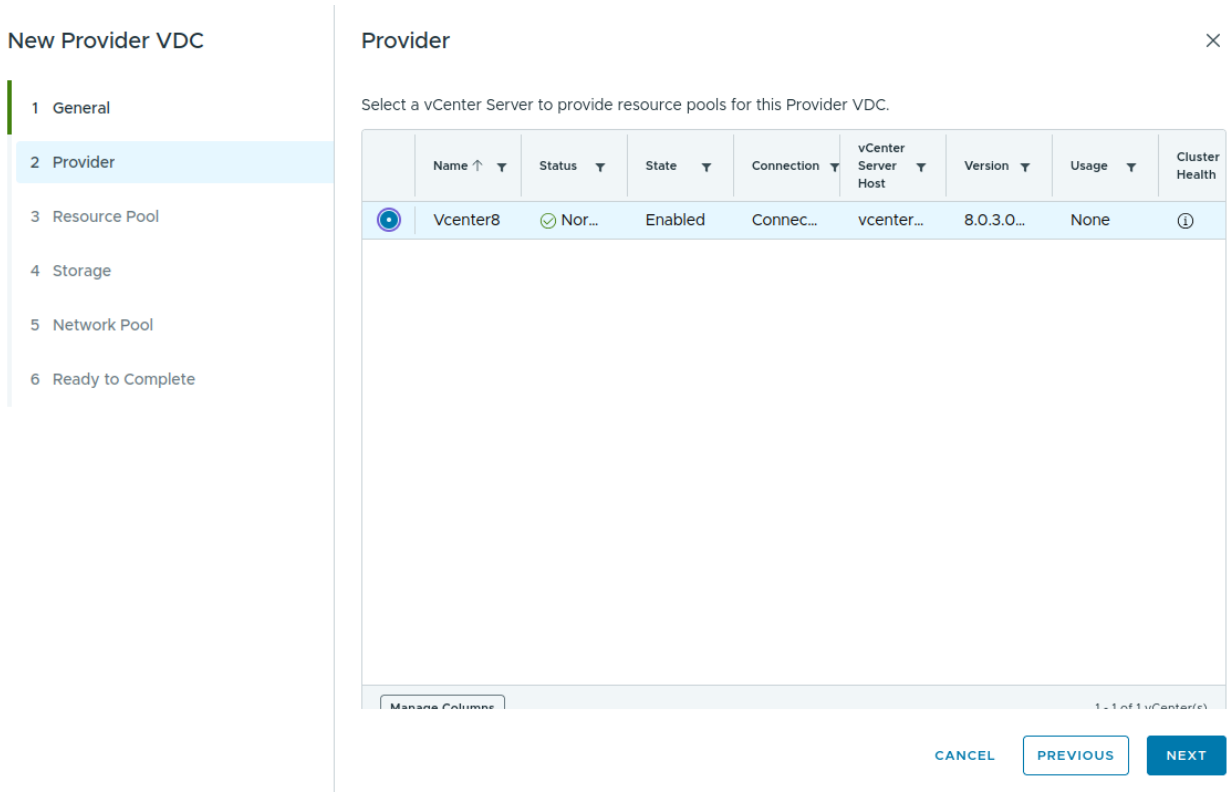

Figure 33 : Vcenter Provider Selection

VMware Cloud Director requires the selected vCenter resources to be provided from a cluster with vSphere Distributed Resource Scheduler (DRS) enabled. If DRS is disabled or the ESXi host is not part of a cluster, no resource pools will be available for selection during Provider VDC creation.

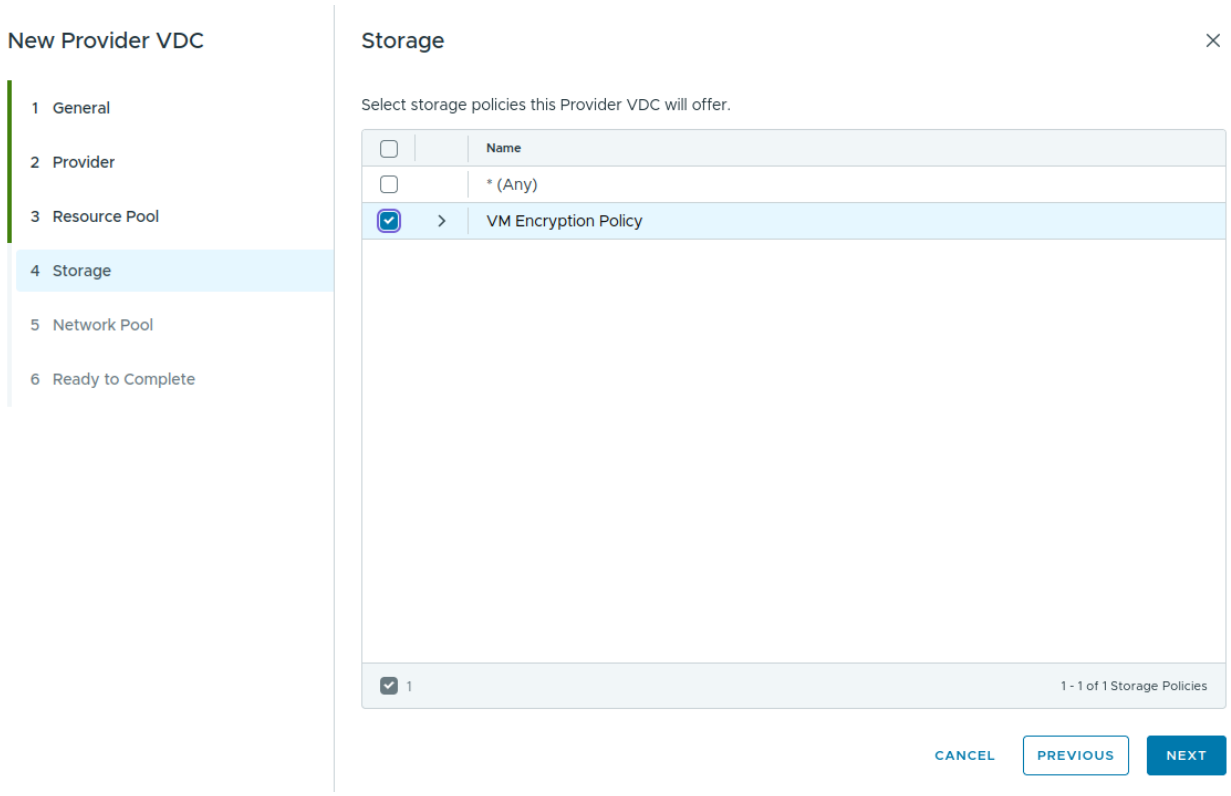

Figure 34 : Storage Policy Selection

4. Complete the wizard using default settings where applicable.
5. Verify that the Provider Virtual Data Center status is **Normal** and the state is **Enabled**.

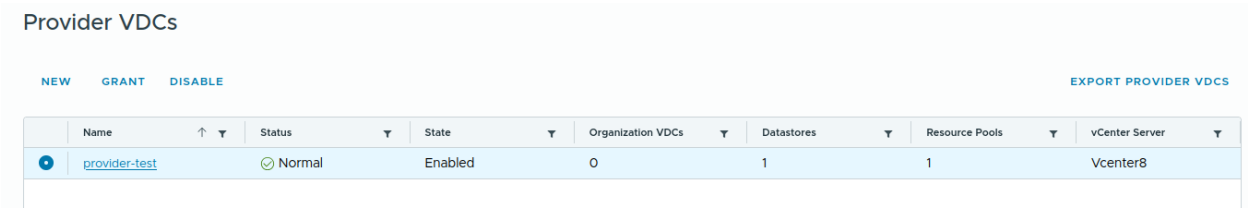

Figure 35 : Provider VDCs Created

5.3.3 Creating an Organization VDC

An Organization Virtual Data Center (Org VDC) is required to deploy virtual machines.

1. Navigate to **Resources** → **Cloud Resources** → **Organizations**.
2. Click **New** to Create a new organization.

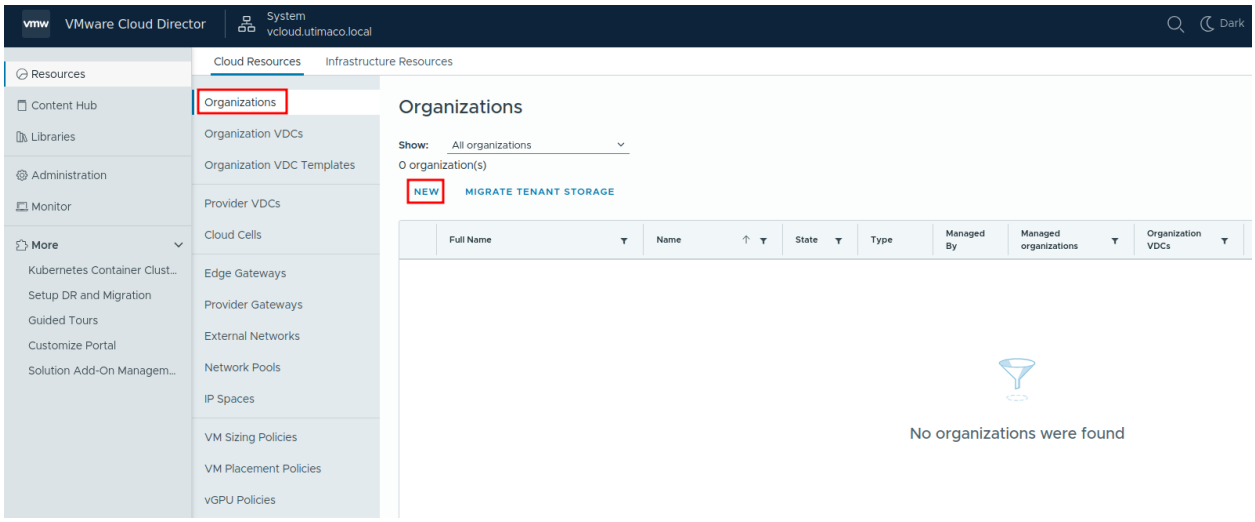

Figure 36 : Create New Organization

3. Provide the required organization details and complete the wizard.
4. Navigate to **Resources → Cloud Resources → Organizations VDCs**.
5. Click **New** to create a new Organization VDC.
6. In the creation wizard:
    - Select the previously created **Provider VDC**.
    - Configure compute allocation as required.

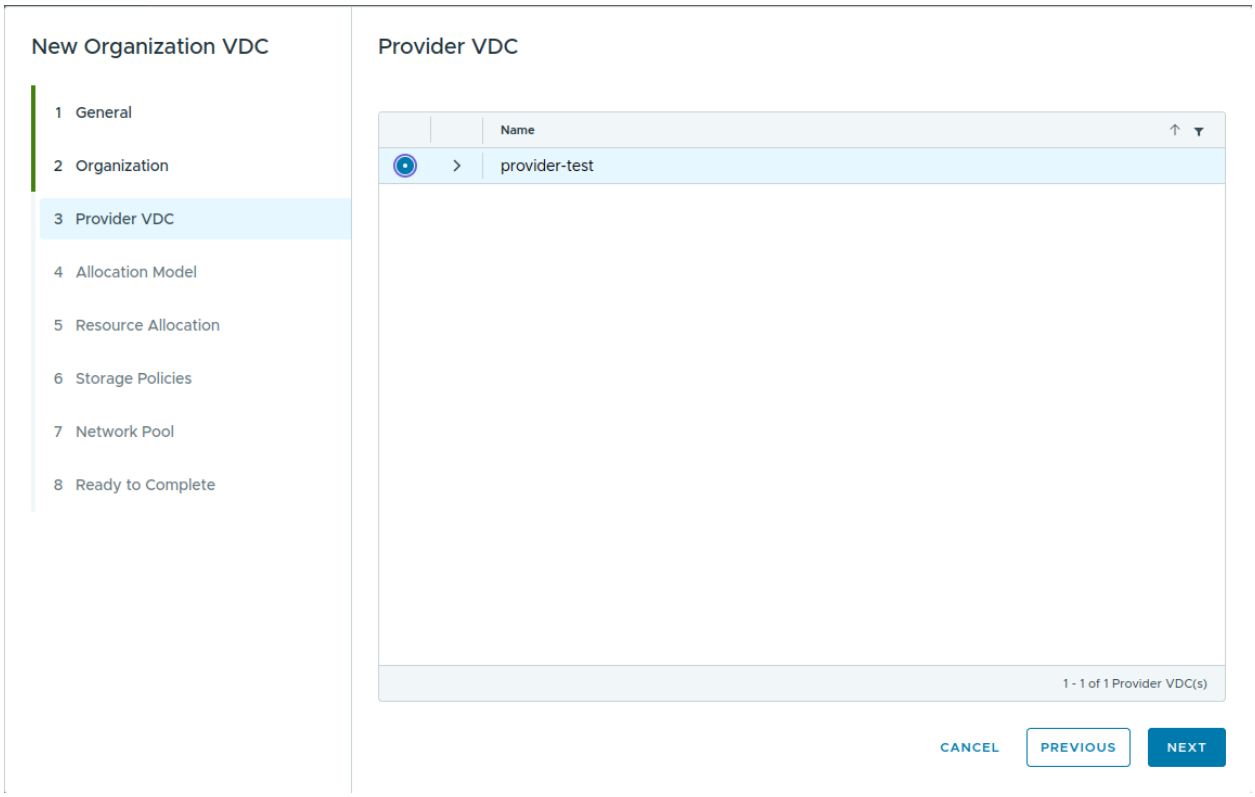

Figure 37 : Provider VDC Selection

7. In the **Storage Policies** section, select a storage policy with **VM Encryption** capability.

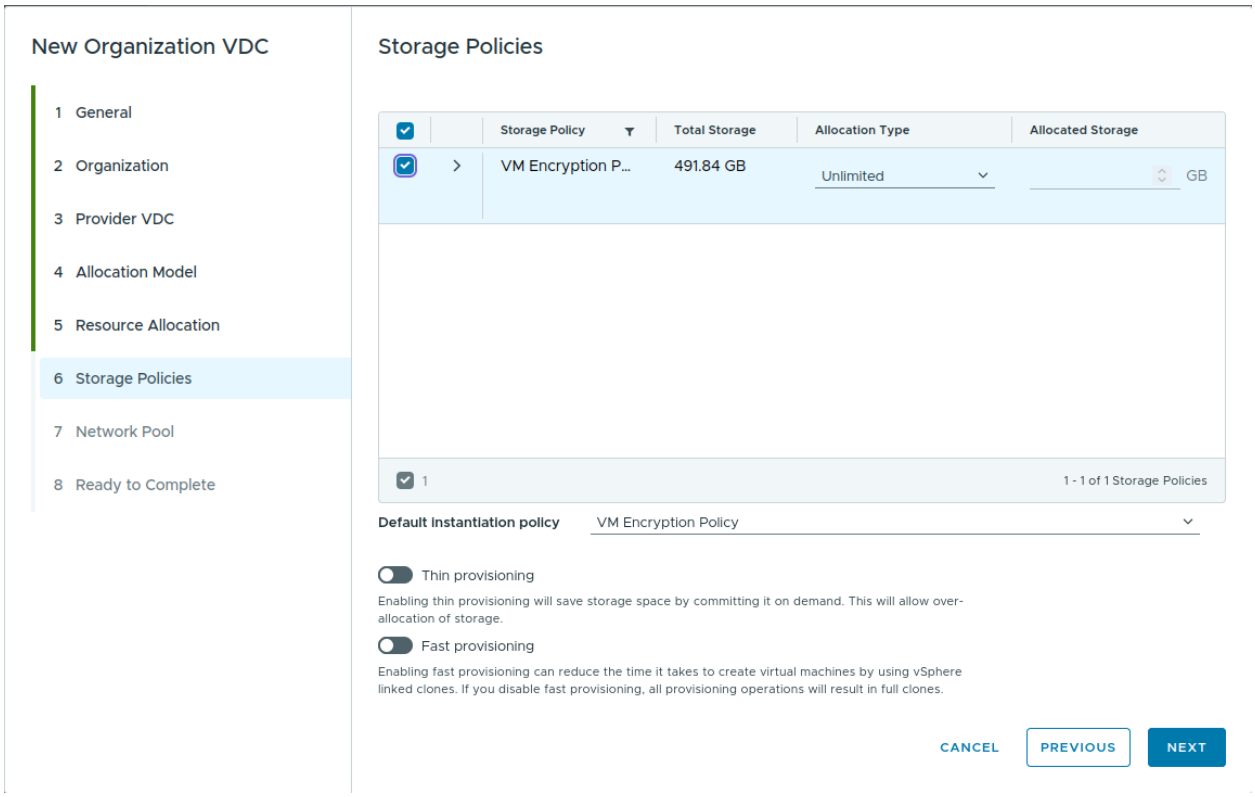

Figure 38 : Storage Policy Selection

8. Complete the remaining steps using default settings where applicable.
9. Verify that the Organization VDC status is **Normal** and the state is **Enabled**.

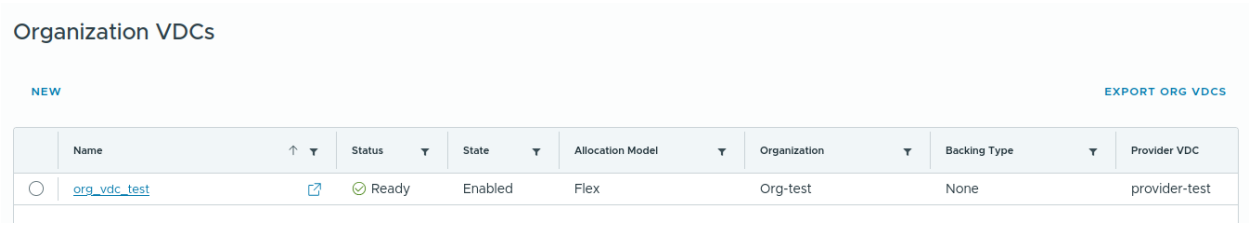

Figure 39 : Organization VDC Created

5.3.4 Deploying an Encrypted VM

To validate the integration, deploy a virtual machine using an encryption-enabled storage policy.

1. Log in as an organization user.
2. Navigate to **Virtual Machines**.

3. Click **New VM**.

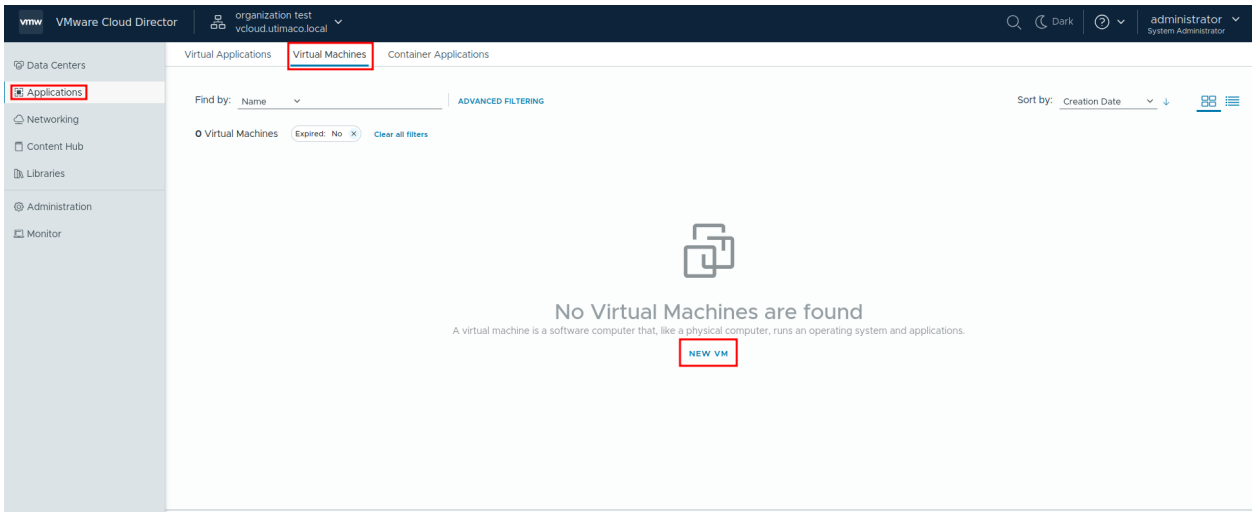

Figure 40 : New Virtual Machine

4. Select a template or ISO.
5. In the storage policy selection, Choose a policy that includes **VM Encryption**.

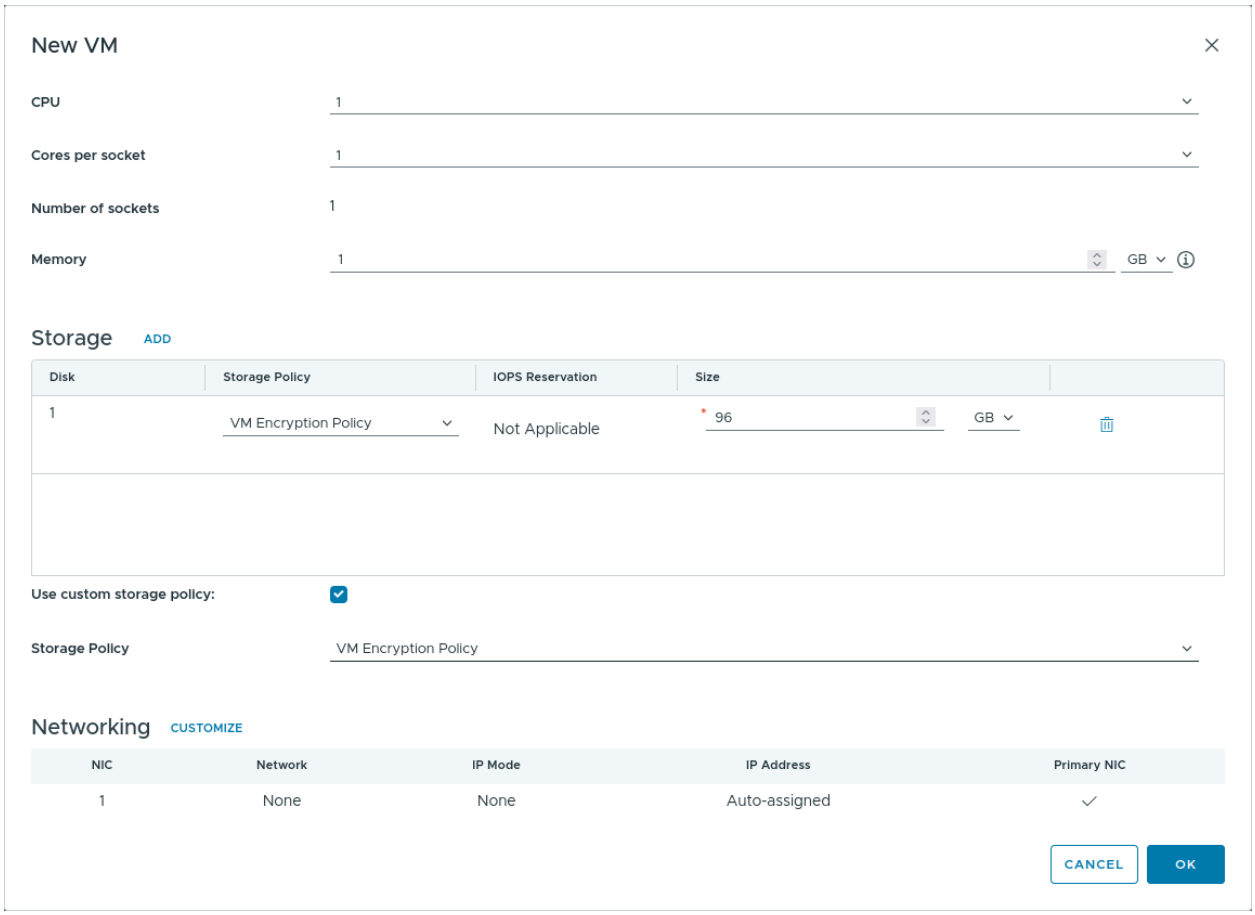

Figure 41 : Storage Policy Selection

6. Complete the deployment.
7. Verify that the virtual machine is marked as **Encrypted** in VMware Cloud Director or VMware vCenter Server.

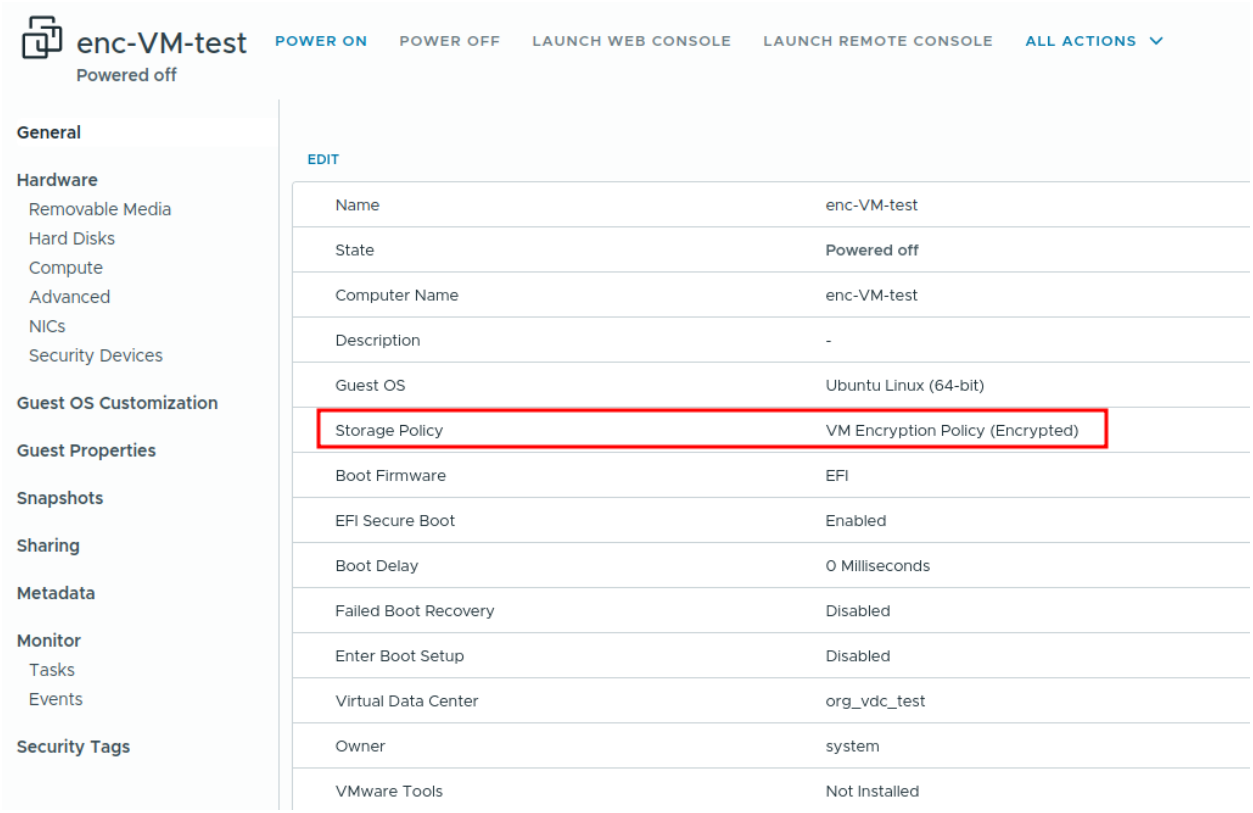

Figure 42 : Proper Storage Policy

8. In ESKM, navigate to **Security → KMIP Objects**.
9. Verify that new **AES-256 SymmetricKey** objects have been created, with a creation timestamp corresponding to the virtual machine deployment time.

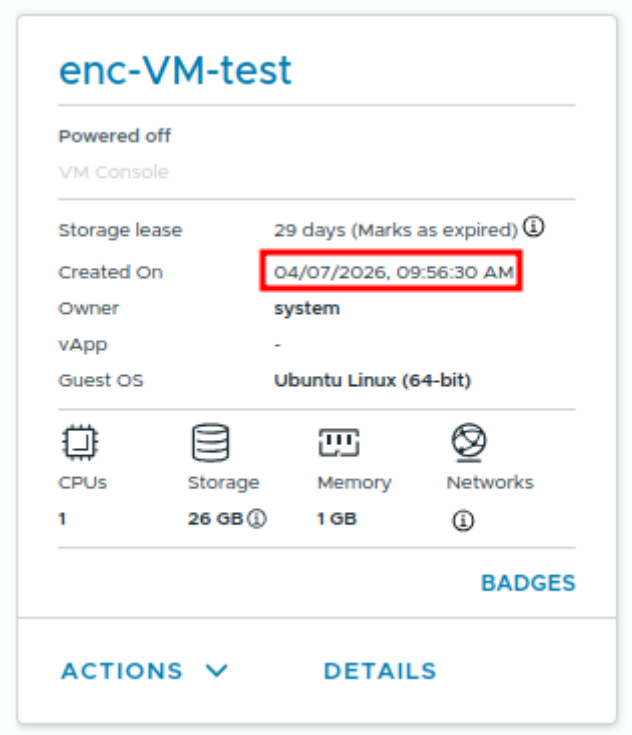

Figure 43 : VM Creation Time

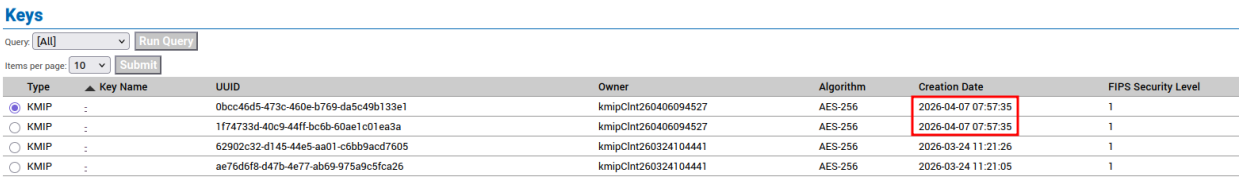

Figure 44 : KMIP Objects Creation Time

6 Verification and Testing

6.1 Functional Testing (encryption/decryption, signing, etc.)

To validate the integration between VMware Cloud Director, VMware vCenter Server, and ESKM, perform the following steps:

1. Deploy a virtual machine as described in Deploying an Encrypted VM .
2. In VMware vCenter Server, navigate to the cluster associated with the Organization VDC and locate the deployed virtual machine.
3. Verify that the virtual machine is marked as **Encrypted**, that the encryption is provided by the configured ESKM Key Provider, and that it is compliant with the assigned VM storage policy.

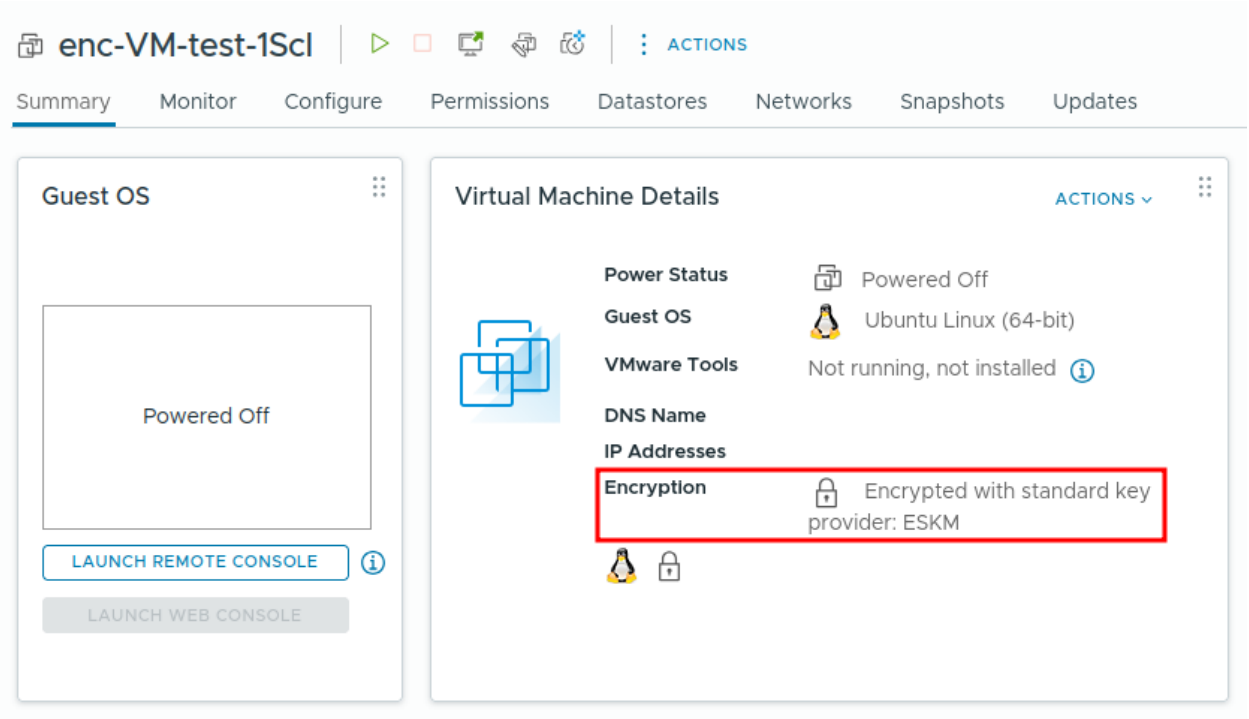

Figure 45 : VMware Cloud Director VM Encrypted

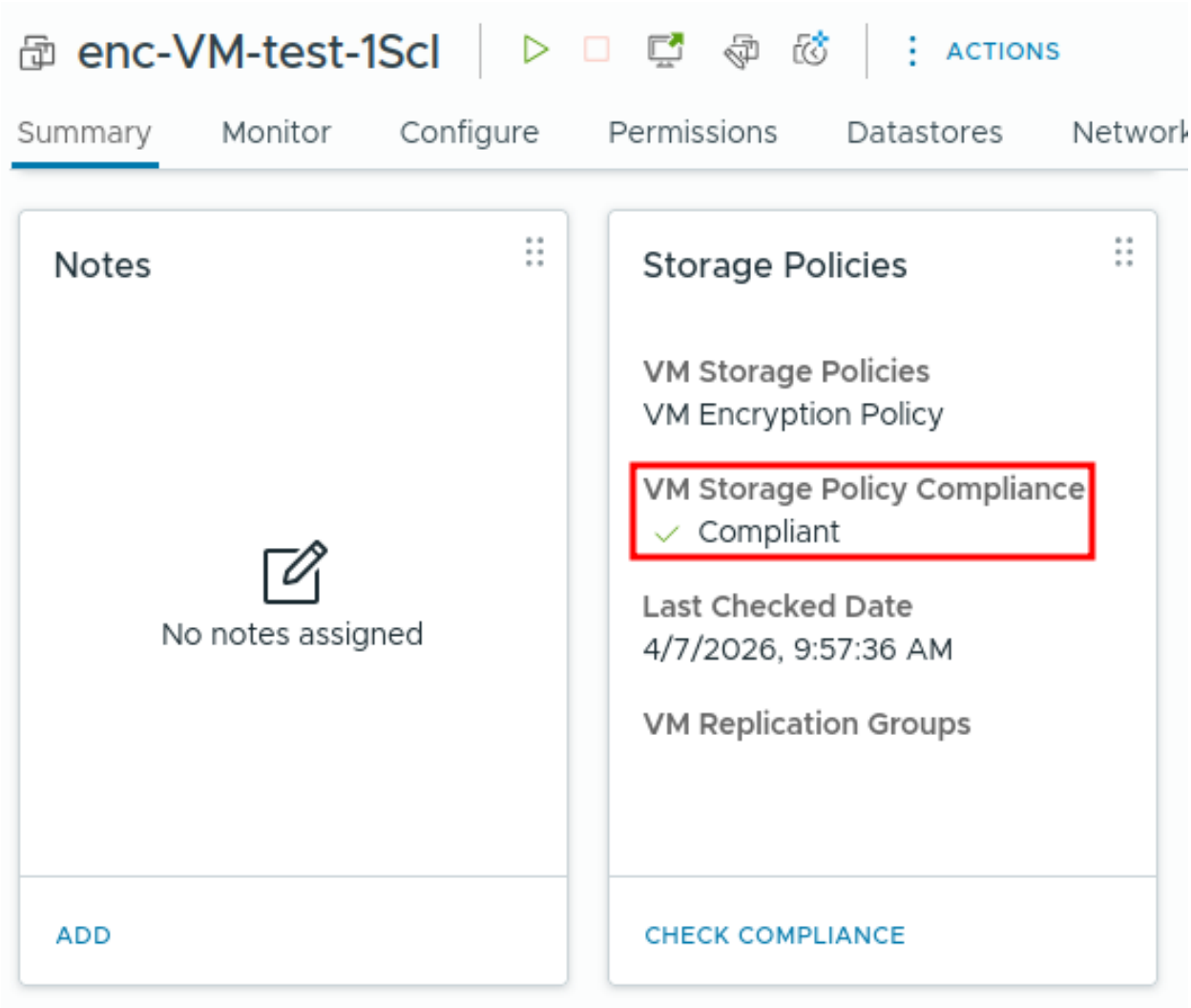

Figure 46 : VMware Cloud Director VM Policy Compliant

To validate the integration between VMware vCenter and ESKM, perform the following steps to encrypt a virtual machine:

1. Log in to the vCenter Server.
2. Navigate to **Menu → VMs and Templates**.
3. Select an existing virtual machine.
4. Right-click the virtual machine and select **VM Policies → Edit VM Storage Policies**
5. In the **VM Storage Policy** section:
    - Select a policy that includes **VM Encryption**.
    - Ensure the policy is associated with the configured key provider (ESKM).

- It can be configured for the whole VM or per disk.

6. Click **OK** to apply the policy.

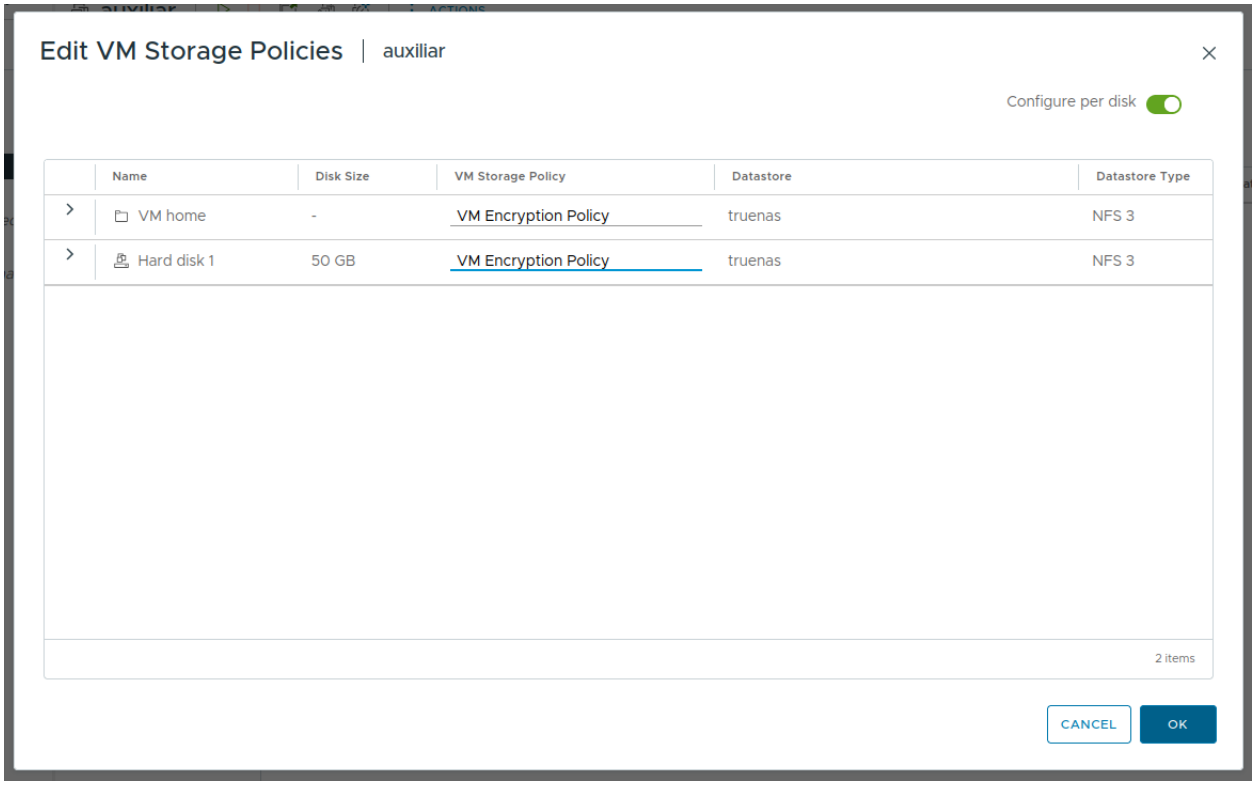

Figure 47 : Edit VM Storage Policies

7. Monitor the task progress in the **Recent Tasks** panel until completion.

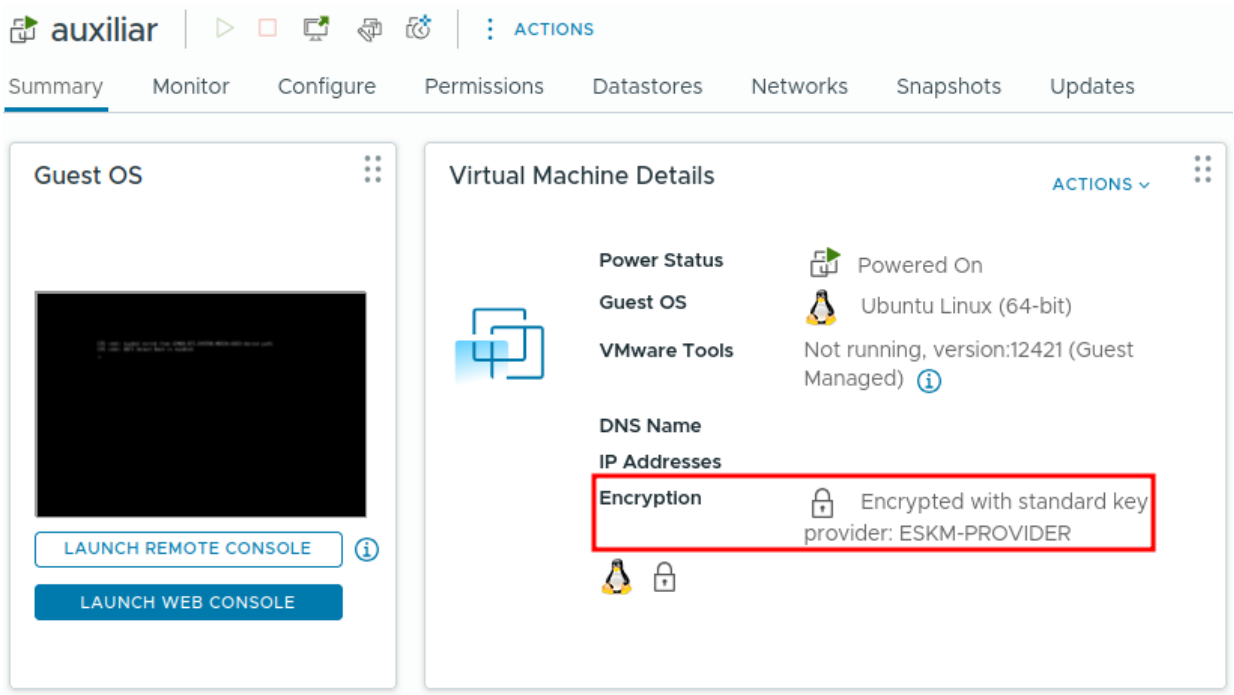

Figure 48 : Encrypted VM

The virtual machine should display as **Encrypted** in its summary.

- In ESKM, navigate to **Security** → **KMIP Objects**
- Verify that a new **Symmetric Key (AES-256)** has been created.

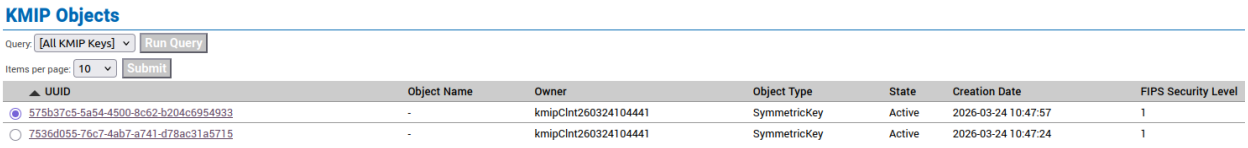

Figure 49 : KMIP Objects created

- Navigate to **Device** → **Log Viewer** → **KMIP** to verify the logs

```
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[GET_ATTRIBUTES] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[GET_ATTRIBUTES] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[GET_ATTRIBUTES] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[ADD_ATTRIBUTE] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[ADD_ATTRIBUTE] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[575b37c5-5a54-4500-8c62-b204c6954933] Operation:[ADD_ATTRIBUTE] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
[KMIP Server] [Authentication Success] User:[kmipClnt260324104441] From IP: 10.10.200.10
[KMIP Server] [ClientOperation] User:[kmipClnt260324104441] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
```

Figure 50 : Successful Key Retrieval

6.1.1 Encrypting a Virtual Machine

6.1.2 Key Rotation (Re-encryption)

If during the vCenter configuration, the Key Provider is configured to use a **single KMS wrapping key option**, the re-encryption operation may not result in the creation of a new KMIP object in ESKM. In this mode, vCenter uses a single key obtained from the KMS to wrap internally generated encryption keys, reducing the number of KMIP key creation operations.

As a result, key rotation at the KMIP level may not be visible, and the same KMS key may continue to be used for multiple encryption operations.

To validate key rotation, perform a re-encryption of the virtual machine:

1. In vCenter, select the encrypted virtual machine.
2. Right-click the virtual machine and select **VM Policies → Re-encrypt.**
3. Confirm the operation when prompted.

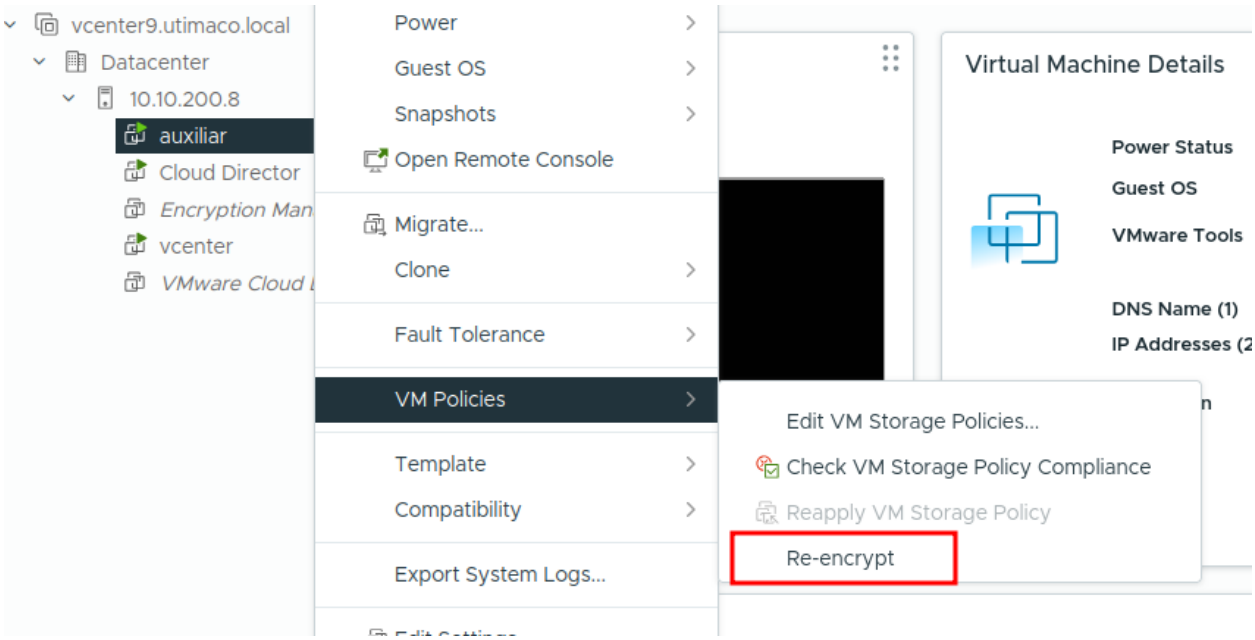

Figure 51 : VM Re-encryption

4. Monitor the task progress until completion.
5. In ESKM:
    - A new KMIP object is created.
    - The new object has a **different Unique Identifier (UUID)** than the previous key.

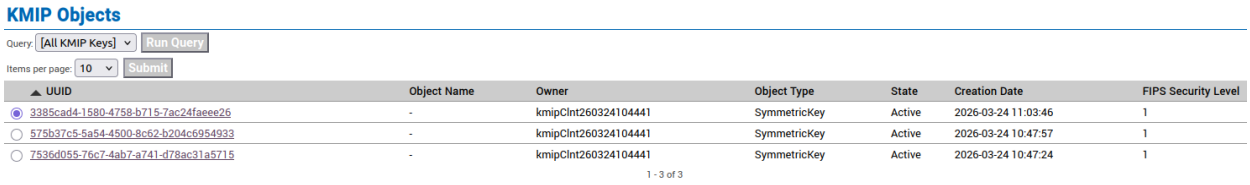

Figure 52 : New Key Created

6.1.3 Key Lifecycle Behaviour

To validate key lifecycle behavior, remove encryption from the virtual machine:

1. In vCenter, select the encrypted virtual machine.
2. Right-click the virtual machine and select **VM Policies → Edit VM Storage Policies.**
3. In the **VM Storage Policy** section:
    - Select a **non-encrypted (default) policy**.

4. Click **OK** to apply the changes.
5. Monitor the task progress until completion.

- The virtual machine is no longer marked as encrypted.
- In ESKM:
  - The previously created KMIP keys remain present.
  - The keys remain in **Active** state.

7 Troubleshooting

7.1 Common Issues and How to Resolve Them

Problem	Possible solution
Unable to connect to the Management Console	▪ Ensure that the browser version you're using supports TLS 1.1 and above. ▪ Ensure that the URL you are using to connect to the ESKM appliance begins with "HTTPS" (not simply "HTTP") and that the port number is correct. The default web administration port is 9443.
Unable to log into the Management Console	▪ Ensure that cookies are enabled on the browser. ▪ Ensure that the user account was granted the "Web Admin Access" privilege. ▪ Ensure that the "Web Administration" service is running.
Unable to log in via SSH	▪ Ensure that the user account was granted the "SSH Admin Access" privilege. ▪ Ensure that the "SSH Administration" service is running.
Unable to create certificate	▪ Ensure that the Country Name is the two letter country code. For example, the country code for the United States is the two letters "US".
ESKM is unable to trust Vcenter	▪ Update the ESKM to the latest version ▪ Use an alternative trust establishment method, such as importing the vCenter Root CA certificate into ESKM and configuring it as a trusted Certificate Authority.

Problem	Possible solution
Encrypted virtual machine cannot be powered on due to key access failure.	▪ Ensure that the KMIP service on ESKM is running and reachable from vCenter. ▪ Ensure network connectivity between vCenter/ESXi hosts and the ESKM (correct IP, port 5696, no firewall blocking). ▪ Confirm that the Key Provider is correctly configured and in a **Connected/Trusted** state in vCenter.
No clusters or resource pools are available during Provider VDC creation in VMWare Cloud Director.	▪ Ensure that the ESXi host is part of a vSphere cluster with Distributed Resource Scheduler (DRS) enabled. VMware Cloud Director requires DRS-enabled clusters to expose resource pools for Provider VDC configuration.
Cannot add vCenter instance to VMWare Cloud Director	▪ Ensure the vCenter version is compatible with the Cloud Director version in the official Broadcom Product Interoperability Matrix ▪ Ensure Cloud Director has connectivity with vCenter. ▪ Ensure the credentials to vCenter are correct (by default the user is administrator@vsphere.local)

Problem	Possible solution
Lost the “admin” account password and no other users exist.	For technical questions, contact Utimaco Technical Support: ▪ E-mail: support-atalla@utimaco.com ▪ Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International). ▪ Website: https://support.utimaco.com/ Before contacting Utimaco with your questions, collect the following information: ▪ Product model names and numbers. ▪ Technical support registration number or NonStop system number (if applicable). ▪ Service Agreement ID number (SAID). ▪ Product serial numbers. ▪ Error messages. ▪ Software version number.

Table 6: Troubleshooting

7.2 Log Locations and Interpretation

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

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **KMIP**.
2. Review the logs for operations based on the Partner Product.

8 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.