VMware vCenter/ESXi

9.0

Integration Guide

Utimaco ESKM

8.54

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	2.0.0
Date	2026-03-30
Status	PUBLISHED
Document No.	IG-2026-0025

Table of Contents

1 Introduction

This guide is part of the documentation provided by Utimaco to support the integration of Utimaco Enterprise Secure Key Manager (ESKM) with VMware vCenter Server. It provides the necessary information to configure ESKM, establish the integration, and validate the solution in a secure and reproducible manner.

Additional documentation related to Utimaco products can be found on the Utimaco website at https://utimaco.com/.

1.1 About this Guide

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

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 system and security administrators with knowledge of:

- Data security administration
- Network configuration

1.3 Purpose of the Integration

The integration of VMware vCenter Server with Utimaco Enterprise Secure Key Manager (ESKM) is designed to provide centralized, secure, and standards-based key management for VMware environments.

VMware vSphere supports encryption of virtual machines, virtual disks, and other sensitive data through the use of an external Key Management Server (KMS). In this architecture, cryptographic keys are not stored within vCenter itself but are managed externally, improving the overall security posture and enabling compliance with enterprise security requirements.

Utimaco ESKM acts as an external KMS by implementing the OASIS Key Management Interoperability Protocol (KMIP), a standardized interface for key lifecycle management. Through KMIP, vCenter can securely request, store, and manage encryption keys without direct exposure to key material.

This integration enables organizations to:

- Centralize cryptographic key management in a dedicated and secure platform
- Enforce strong access control and key lifecycle policies
- Separate key management from application and infrastructure layers
- Leverage a standards-based protocol (KMIP) for interoperability and scalability

By combining VMware's encryption capabilities with Utimaco's secure key management platform, this integration ensures that sensitive data within virtualized environments is protected using enterprise-grade cryptographic controls while maintaining operational flexibility and compliance with security best practices.

1.4 Abbreviations

Abbreviation	Meaning
CA	Certificate Authority
CSR	Certificate Signing Request
CN	Common Name
SAN	Subject Alternative Name
IP	Internet Protocol
KMIP	Key Management Interoperability Protocol

Abbreviation	Meaning
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	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

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 VMware vCenter/ESXI

VMware vCenter Server is the centralized management platform for VMware vSphere environments, enabling the administration of ESXi hosts, virtual machines, and associated resources. It provides features such as workload management, high availability, and lifecycle operations across virtualized infrastructure.

VMware ESXi is the hypervisor that runs directly on physical hardware and hosts virtual machines. Together with vCenter, it supports advanced capabilities including virtual machine encryption, which relies on external Key Management Servers (KMS) for secure key handling.

Through its support for the OASIS Key Management Interoperability Protocol (KMIP), vCenter can integrate with external key management solutions to enable secure encryption and key lifecycle management.

2.2 Overview of ESKM

Utimaco Enterprise Secure Key Manager (ESKM) is a centralized key management platform designed to securely generate, store, and manage cryptographic keys across enterprise environments. It provides comprehensive key lifecycle management, including key creation, distribution, rotation, and deletion.

ESKM supports industry standards such as KMIP, enabling interoperability with third-party systems and applications. It also integrates with Hardware Security Modules (HSMs) to provide hardware-backed key protection and secure cryptographic operations.

By separating key management from application infrastructure, ESKM enhances security, simplifies compliance, and enables centralized control over cryptographic assets.

2.3 Joint Value Proposition

The integration of VMware vCenter with Utimaco ESKM enables secure and centralized key management for encrypted virtualized environments. By leveraging the KMIP protocol, vCenter can delegate key management operations to ESKM while maintaining seamless integration with existing workflows.

This approach ensures that cryptographic keys are stored and managed outside of the virtualization platform, reducing exposure and improving security. Additionally, when combined

with HSM integration, the solution provides hardware-backed protection for sensitive key material.

Together, VMware and Utimaco deliver a standards-based, scalable, and secure solution for managing encryption in virtual infrastructures, supporting enterprise security requirements and regulatory compliance.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

These integrations have been successfully tested with the Utimaco HSM and OpenSSL.

VMWare ESXi	VMWare vCenter	Utimaco ESKM Version	Utimaco HSM
ESXi v8.0.3	VCenter v8.0.3g	ESKM v8.54	ESKM Embedded HSM
ESXi v9.0.2	VCenter v9.0.2	ESKM v8.54.5	EKSM Embedded HSM
ESXi v8.0.3	vCenter v8.0.3g	ESKM v8.54	u.trust Anchor Se-Series
ESXi v9.0.2	vCenter v9.0.2	ESKM v8.54.5	u.trust Anchor Se-Series

Table 3: List of tested versions

3.2 Hardware and Software Requirements

- Requires minimum VMWare ESXi version 9.0, or later.
- Requires minimum vCenter version 9.0, or later.
- Requires minimum Enterprise Secure Key Manager v8.54.5, or later.

For more information about VMware's documentation, refer to www.vmware.com/support/pubs.

3.3 Prerequisites

- Administrative access to the ESKM Management Console.
- VMware vCenter Server access with sufficient privileges to configure a Key Management Server (KMS).
- A properly initialized and network-accessible Hardware Security Module (HSM).

- A **Crypto User** created on the HSM with the required permissions.
- Availability of the corresponding **key material**, including key file and password for the Crypto User.

For more information about HSM setup and user provisioning, refer to the Utimaco documentation available on the support portal https://utimaco.com/.

4 Installation and Configuration

4.1 Setting Up ESKM

ESKM server must be configured with specific values such as time zone, IP address, netmask, gateway, host name, and port number used for the ESKM Management Console interface.

This section includes procedures on the following topics:

- First Run
- Setting Up Local CA
- Setting Up ESKM Certificate
- Set Up Cluster
- Set Up KMIP Server
- Set Up KMS Server

4.1.1 Accessing Serial Console via PuTTY

Use the following steps to set up PuTTY and access serial console.

1. Navigate to device manager and figure out the COM port that you'll be using.

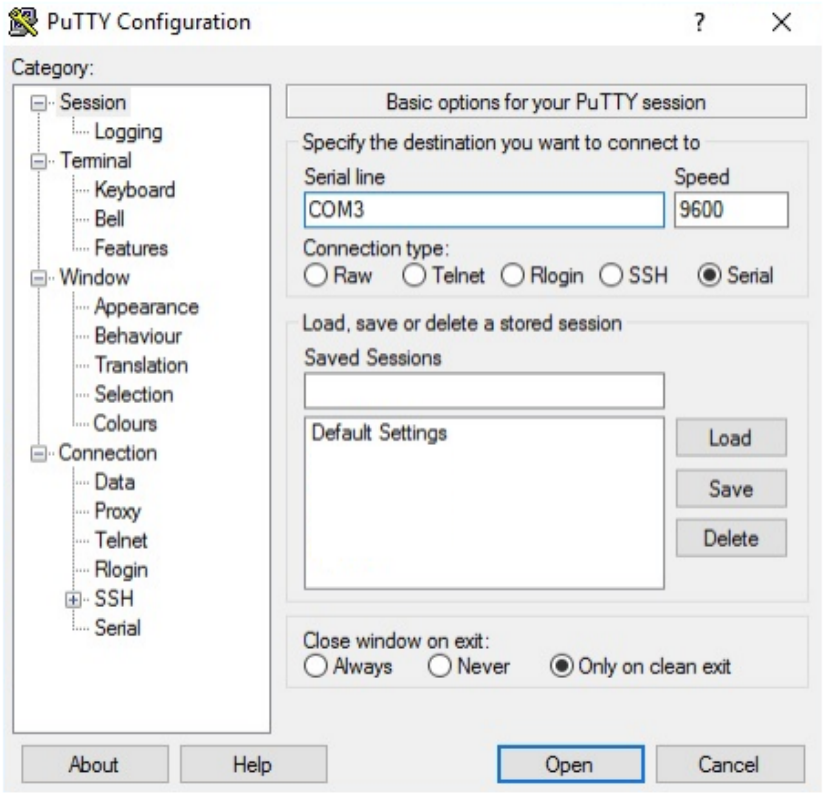

Figure 1 : PuTTY Configuration

2. Run PuTTY.
3. Switch the Connection Type to Serial.
4. Edit the Serial Line to match the COM port you want to use.

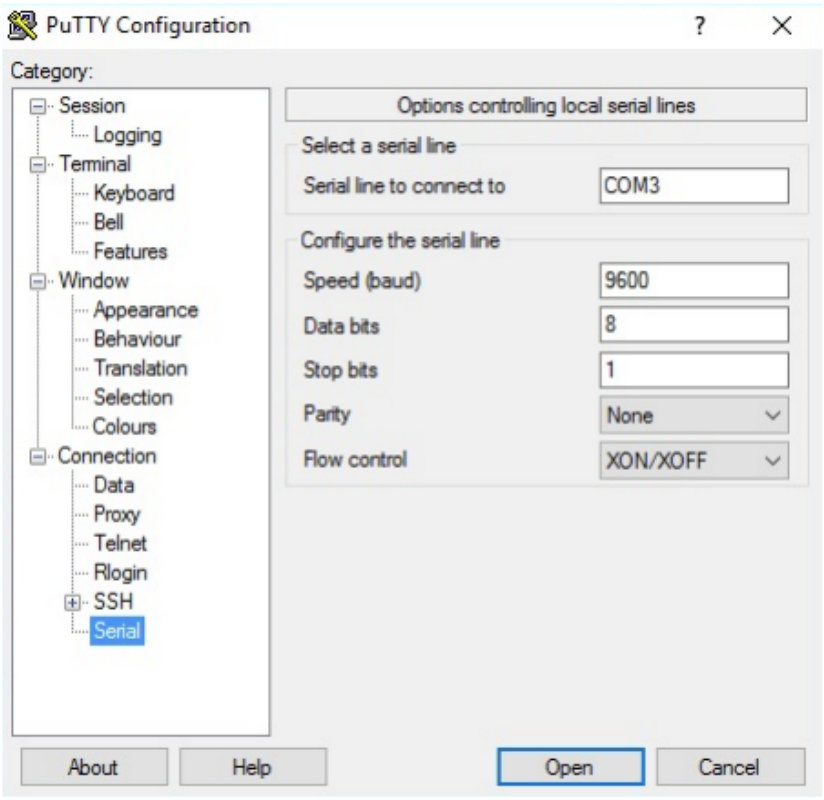

Figure 2 : Serial line

5. Make sure all of the settings are correct.
6. Click **Open** to start the session.

4.1.2 First Run

To configure the time zone, IP address, netmask, gateway, host name, and port number used for the ESKM Management Console interface, the following procedure must be performed once for each ESKM server. Ensure that the ESKM server is powered off before starting this procedure.

1. Power on the ESKM server by pressing the Power On/Standby button located behind the front bezel door.
2. When the startup sequence completes, the following prompt displays on the PC or laptop that is running the terminal emulator program (such as PuTTY):

To setup and configure PuTTY, please refer to Accessing Serial Console via PuTTY.

Are you ready to begin setup? (y/halt):

Enter **y**.

3. Follow the prompts to enter the necessary information:

Press **Enter** to accept the default.

a. Admin account password. Be sure to record this value and store it in a safe place. The Security Officer will use the admin account to configure the ESKM servers.

Utimaco has no ability to assist or recover access if administrator credentials (username, password) are lost.

b. Time zone.

c. Date.

d. Time. The time is based on a 24–hour clock; there is no a.m. or p.m. designation. For example, 1:20 p.m. is 13:20:00.

e. The static IPv4 address of the ESKM server. The ESKM server cannot obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server.

f. Subnet mask.

g. Default gateway.

h. Hostname, including the domain. For example, eskm.example.com. The screen displays the information you entered and the message:

"Is this correct? (y/n):"

If the information displayed is correct, enter y; if not, enter n and make the necessary corrections.

i. Enable IPv6. If the ESKM server will be installed in an IPv6 network, enter **y** to the prompt and also the confirmation prompt. If the ESKM server will not be installed in an IPv6 network, or you wish to enable IPv6 later, enter **n**. If you entered **y**, you will be prompted to specify the IPv6 address. If you know the IPv6 address enter y, and then at the next prompt enter the IPv6 address with prefix in this format.

IPv6 address/prefix. The default prefix is /64.

If you do not know the IPv6 address, enter n. You can enter IPv6 addresses later using either the ESKM Management Console or Command Line Interface.

Only enable IPv6 if you are certain that the ESKM server is required to operate on an IPv6 network. Once enabled it cannot be disabled via the ESKM Management Console or the Command Line Interface.

Client systems can use IPv4 addresses to connect to the KMS and KMIP services running on the ESKM system. ESKM supports IPv6 addresses for clients that use either the KMIP or ESKM XML protocols, and are on the same subnet as the ESKM server. The following ESKM features, which utilize SCP to move files, support IPv6 addresses:

- backup, restore, scheduled backup, transfer logs, and software upgrade/ install.

In addition, you can also use a server which has an IPv6 address to perform the following functions:

- remotely administer the ESKM server via the ESKM Management Console or the command line interface.
- perform network diagnostics (ping and netstat).

If you decide later, after completing the setup process, that you need to enable IPv6 support, you can use the Command Line Interface command **ipv6 enable**, to enable IPv6. You can then use the **ipv6 address** command or the ESKM Management Console interface to specify the IPv6 address.

j. Web interface port number.

k. Press **Enter** to complete and save the configuration settings.

At this point, you have given the setup program everything it needs. The ESKM creates SSH keys and also a self-signed Web Admin server certificate. They are used to authenticate the ESKM to users making SSH and Web Admin connections to the ESKM. Because the actual key is fairly large, the ESKM displays the key fingerprint on the console, as shown below.

```
Creating certificate for Web administration server...

Creating certificate for signing logs...

Creating SSH host keys...

SSH RSA key fingerprint:

2048 SHA256:aTp6A447vp8dOj43FTT5B/aux6V7zddPzNXxZB0C1SE

SSH ECDSA key fingerprint:

521 SHA256:BKO/EfVUKSFpIzVn/WiJ4fS+8CqLyGJSawoQAsvmUoM

SSH ed25519 key fingerprint:

256 SHA256:/hWJGM+7hzDRWPsyCP6/gKqWR99cgMh9/TV5WLTFIrs

Webadmin certificate fingerprint (SHA-1):

2048

64:50:e2:01:fb:2a:28:54:1a:3b:30:94:3b:25:b7:ff:97:73:13:70

Initializing key store. This could take several minutes. Performing KMIP setup

Starting services...

The Web-based Management Console will now be available at this URL:

<https://xxx.xxx.xxx.xxx:9443> This device has now been configured. Press Enter to
continue.
```

A log-in prompt displays.

To prevent a "man-in-the-middle" attack when connecting to the ESKM, Utimaco recommends that you write down these fingerprints and compare them with what is presented when you connect to the ESKM via SSH or HTTPS.

If necessary, you can install and specify a different server certificate for remote Web Administration. See the sub-section **Configuring the web admin server certificate**, which is located in section 4 of the Enterprise Secure Key Manager 5.1 User Guide.

4. Unplug the null modem cable from the laptop or PC and from the ESKM server. All additional configuration will be done from the ESKM Management Console.

4.1.3 Setting Up Local CA

The local CA is used to sign and verify the server certificate and may also be used to sign client certificate requests. To create and install a local CA, perform the following steps:

1. Log in to the ESKM Management Console using the admin username and the password you supplied in First run, step 3a.
2. Select the **Security** tab.
3. In **Certificates & CAs**, click **Local CAs**.
4. Enter information required by the Create Local Certificate Authority section of the window to create your local CA.

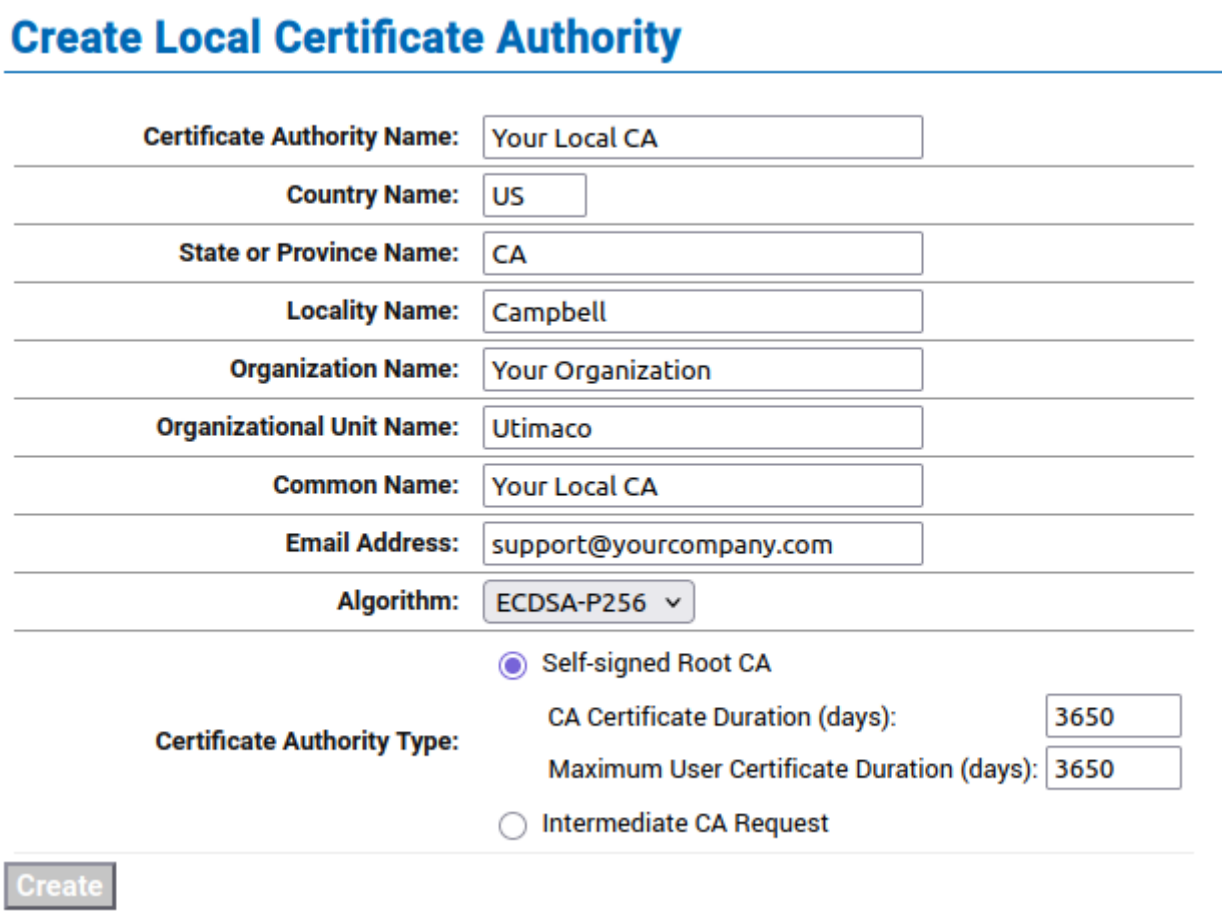

Figure 3 : Create Local Certificate Authority

a. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example **ESKM Local CA**.

b. Enter your organizational information.

c. Select the **Algorithm**. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

d. Click **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.

5. Click **Create**.
6. If the local CA will be used to sign ESKM client certificate requests, add the CA to the Trusted CA list.

a. In **Certificates & CAs**, click **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.

b. Click on the **Default** Profile Name (not the radio button).

c. In the **Trusted Certificate Authority List**, click **Edit**..

d. From the list of Available CAs in the right panel, select the CA you created in step 4. For example, **ESKM Local CA**.

e. Click **Add**.

f. Click **Save**.

Repeat the steps above any time another local CA is needed. For example, you may want to create a KMIP Local CA to support the KMIP Certify/Recertify operations.

Add a third-party CA certificate

If your client certificates were signed by a third-party CA, you must install the third-party CA certificate, and then add it to the Trusted CA list.

To install a third-party CA certificate, perform the following steps:

1. In **Certificates & CA**s, click **Known CAs** to display the **Install CA Certificate section**.
2. Enter a value for the Certificate Name and paste the CA certificate text in the **Certificate** field.
3. Click **Install**. The CA certificate will be added to the Known CAs list.

To add the third-party CA certificate to the Trusted CAs list, perform the following steps:

1. In **Certificates & CAs**, click **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.
2. Click on the **Default** Profile Name.
3. In the **Trusted Certificate Authority List**, click **Edit**.
4. From the list of Available CAs in the right panel, select the third-party CA you require.
5. Click **Add.**
6. Click **Save**.

4.1.4 Setting Up ESKM Certificate

ESKM server certificates are used by the client to authenticate the ESKM server during the TLS/SSL handshake. ESKM supports two types of clients. Clients that use the ESKM protocol are referred to as ESKM clients. Clients that use the KMIP protocol are referred to as KMIP-enabled clients. The ESKM clients communicate with the KMS server and KMIP-enabled clients communicate with the KMIP server.

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your ESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to these server certificates should clearly indicate their purpose. For example:

ESKM KMS Server and ESKM KMIP Server.

KMIP requires mutual authentication. After configuring the KMIP server, **enable** KMIP client certificate authentication. The KMIP client certificate authentication status is **disabled** by default.

If you will be using a third-party CA, and wish to use an existing server certificate, see Import a Third-Party Server Certificate.

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

1. Click the **Security** tab.
2. In **Certificates and CAs**, select **Certificates**.
3. Enter information required by the **Create Certificate Request** section of the window to create the ESKM server certificate.

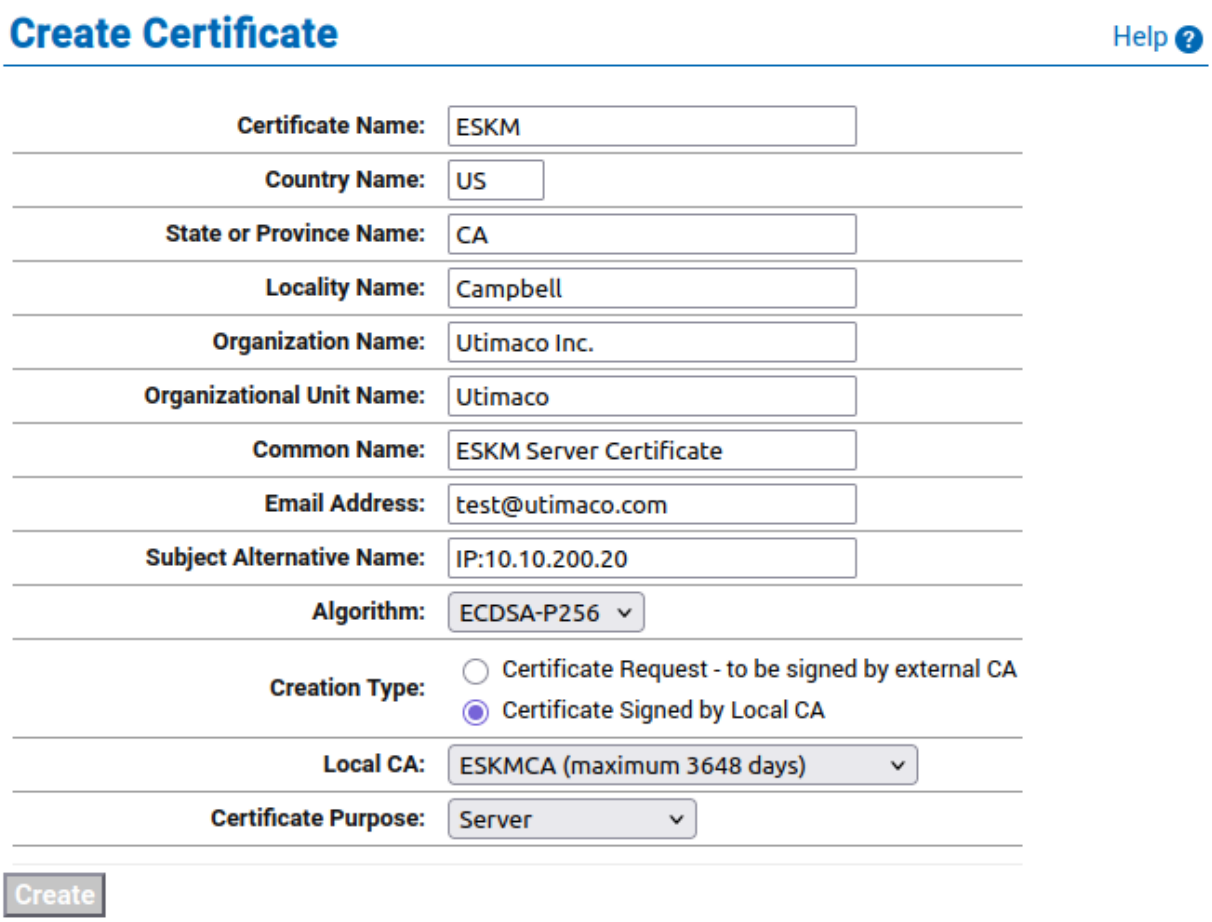

Figure 4 : Create Certificate Request

a. Enter a Certificate Name and Common Name, for example ESKM KMS Server.

b. Enter your Organizational information.

c. Enter the **Subject Alternative Name**, and **Algorithm**. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

d. Select the **Local Certificate Authority (CA)** to be used for signing the certiifcate.

e. Select the **Certificate Purpose** (e.g., Server or Client).

4. Click **Create Certificate Request.**

The certificate is automatically signed by the selected Local CA and becomes active immediately. No manual CSR export, signing, or certificate installation steps are required.

Repeat all of the steps above for the KMIP server certificate. You must perform these steps on each ESKM server after joining the cluster.

The “certificate name” must remain same on all ESKM servers across the cluster.

Import a third-party server certificate

An externally generated public/private key pair can be imported into the ESKM system for use as a server certificate. The encrypted private key data and the public key certificate must be present in the third-party server certificate file. For example:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAB.........vvbKI=
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDhjCCA.........MKH9Fk
-----END CERTIFICATE-----
```

In addition, the password for the private key file must be known.

To import a third-party server certificate, perform the following steps:

1. In **Certificates & CAs**, click **Certificates** to display the **Import Certificate section**.
2. Provide the source location of the certificate file.
3. Enter the Certificate Name and private key password.
4. Click **Import Certificate**.

4.1.5 Setup Cluster

The procedures in this section will establish a cluster configuration on one ESKM server and then transfer that configuration to the remaining ESKM servers.

If you only have one ESKM server, skip this section.

- In Creating the Cluster, the cluster is created on one ESKM server.

Skip this section if you already have an ESKM cluster.

- In Adding ESKM Servers to the Cluster, each of the additional ESKM servers will be added to the cluster.

4.1.5.1 Creating the Cluster

To create the cluster, perform the following steps on one of the ESKM servers to be clustered:

1. From the ESKM Management Console, click the **Device** tab.
2. In the **Device Configuration** menu, click **Cluster**.

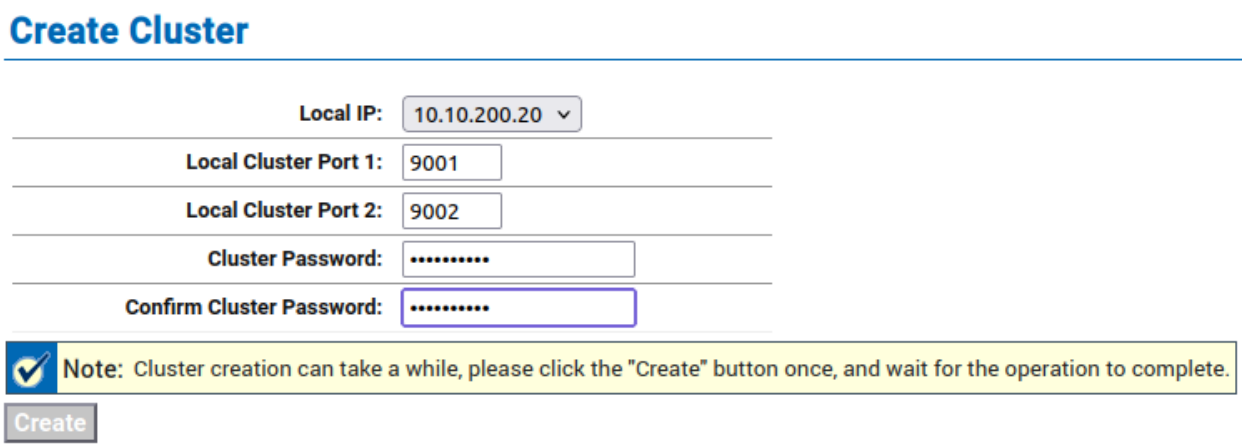

Figure 5 : Create Cluster

3. If required, change the **Local IP** value. If you have enabled Ethernet#2 you can use its IP address for clustering.

All ESKM servers in a cluster must use an IPv4 address for the cluster.

4. If required, change the **Local Port** value. Utimaco recommends using the default value of 9001.
5. Choose a cluster password and enter it into the Cluster Password field. Enter the password a second time into the Confirm Cluster Password field.
6. Click the **Create** button.
7. In the **Cluster Settings** section of the window, click **Download Cluster Key** and save the key to a convenient location, such as your computer's desktop.

The cluster key is a text file and is only required temporarily. It may be deleted from your computer's desktop after all ESKM servers have been added to the cluster.

4.1.5.2 Adding ESKM Servers to the Cluster

To setup ESKM servers to the cluster, perform the following steps in the **Join Cluster** section on each additional ESKM server.

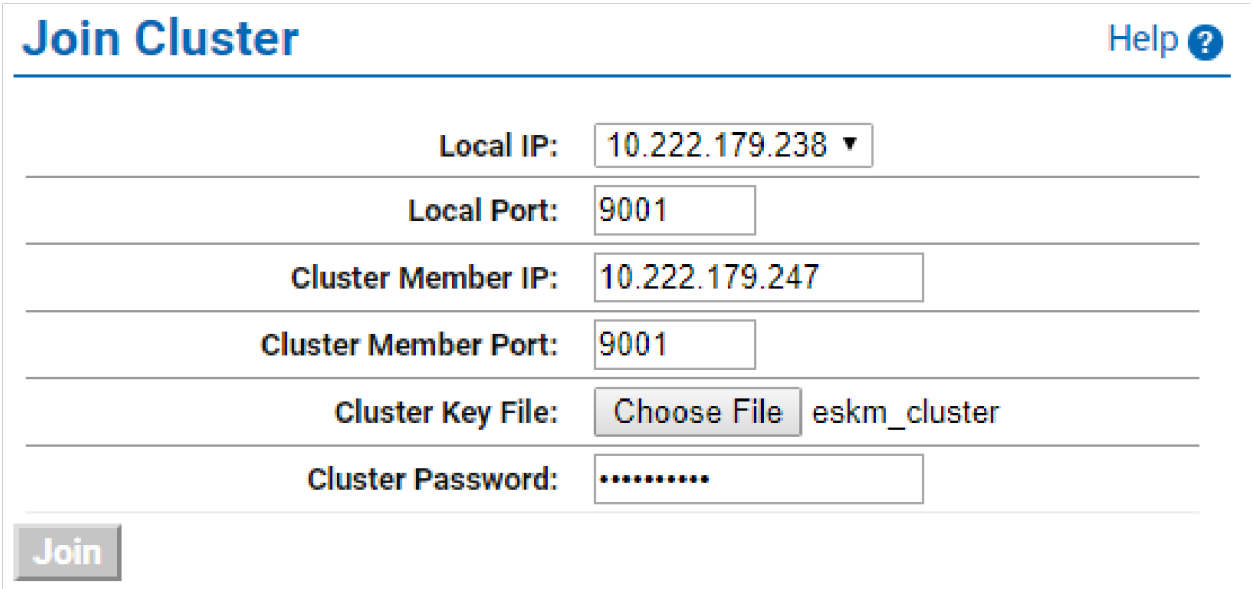

Figure 6 : Join Cluster

Adding multiple ESKM servers to the cluster is a serial process. Add the first ESKM server and then monitor the system log for the status of the synchronization process. Wait until the "**Cluster synchronization succeeded.**" message appears in the system log before attempting to add the next ESKM server to the cluster. The amount of time required to complete the synchronization process is a function of the number of keys in the cluster.

If the new ESKM server is a replacement and is configured with the same IP address as the failed ESKM server, make sure the client does not send any key generation requests until the new ESKM server has successfully completed the cluster synchronization process. Alternately, you can stop the KMS and KMIP servers and then start them once the cluster synchronization process is complete. Use the system log to monitor the progress of the cluster synchronization process.

1. Join the ESKM server to the cluster.

    a. Select the **Device** tab.

    b. In the **Device Configuration** menu, click on **Cluster**.

    c. In the **Join Cluster** section of the window, select the appropriate **Local IP** value and then input the appropriate value for the **Local Port.**

All ESKM servers in a cluster must use an IPv4 address for the cluster.

d. Type the original cluster member's IP into **Cluster Member IP**.

e. Type the original cluster member's port into **Cluster Member Port.** The default value of this port is 9001. If this value was changed in while creating the cluster, use that value.

f. Click **Browse** and select the **Cluster Key File** you saved in while creating the cluster.

g. Type the cluster password into **Cluster Password**.

h. Click **Join**.

i. Click **Confirm** to synchronize with the cluster.

If the ESKM server joining the cluster is SSL enabled, this step will cause the WebAdmin service and the KMS and KMIP servers to restart, resulting in a temporary connection loss. To restore the connection, refresh the browser.

2. After adding all members to the cluster, you can then delete the cluster key file from the desktop.
3. After clustering the ESKM servers, follow the steps in Setting up ESKM Certificate to create and install the server certificates on each ESKM server that has joined the cluster. Depending on the KMS and KMIP configuration, two server certificates may need to be created for each ESKM server in the cluster. **Be sure to use the same server certificate name** as specified under KMS Server Settings and KMIP Server Settings.
4. After creating the KMIP server certificate you must manually restart the KMIP server. Go to the Services List section of the Services Configuration page (**Device -> Maintenance -> Services -> KMIP Server**).
5. Go to the Services List section (**Device > Services**) and start the KMIP server.

4.1.6 Setup KMIP Server

Skip this section if your ESKM system will not be communicating with KMIP-enabled clients.

The KMIP server provides the interface to clients that use the KMIP protocol. Transport Layer Security (TLS) is required, therefore you must specify the name of the server certificate.

To configure the KMIP server, perform the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMIP Server** to display the **KMIP Server Configuration** window.
3. In the **KMIP Server Settings** section of the window, click **Edit**.
4. Configure the KMIP Server Settings. The IP address can be an IPv4 address, or IPv6 address. If support for IPv6 has been enabled, see First run. If necessary, change the Port and Connection Timeout values. Utimaco recommends the default values of 5696 for the Port and 3600 for the Connection Timeout. For **Server Certificate**, select the name of the certificate you created in Setting up ESKM certificate. For example, ESKM KMIP Server.

If your ESKM server is operating in FIPS compliant mode, you must specify a KMIP server certificate that complies with the FIPS requirements.

If your ESKM servers are in a cluster and you are selecting a new KMIP server certificate from the "Server Certificate:" field, you must make sure that all of the ESKM servers in the cluster already have a KMIP server certificate installed with this same name.

If your ESKM server will support the KMIP Certify or Re-certify operations you must specify the name of a Local CA that will be used to create the certificate. In addition, you must set the KMIP user group permissions for these operations to enabled. For more information on setting KMIP user group permissions, see the KMIP Permission model description, which is located in section 3 of the *Enterprise Secure Key Manager User Guide*.

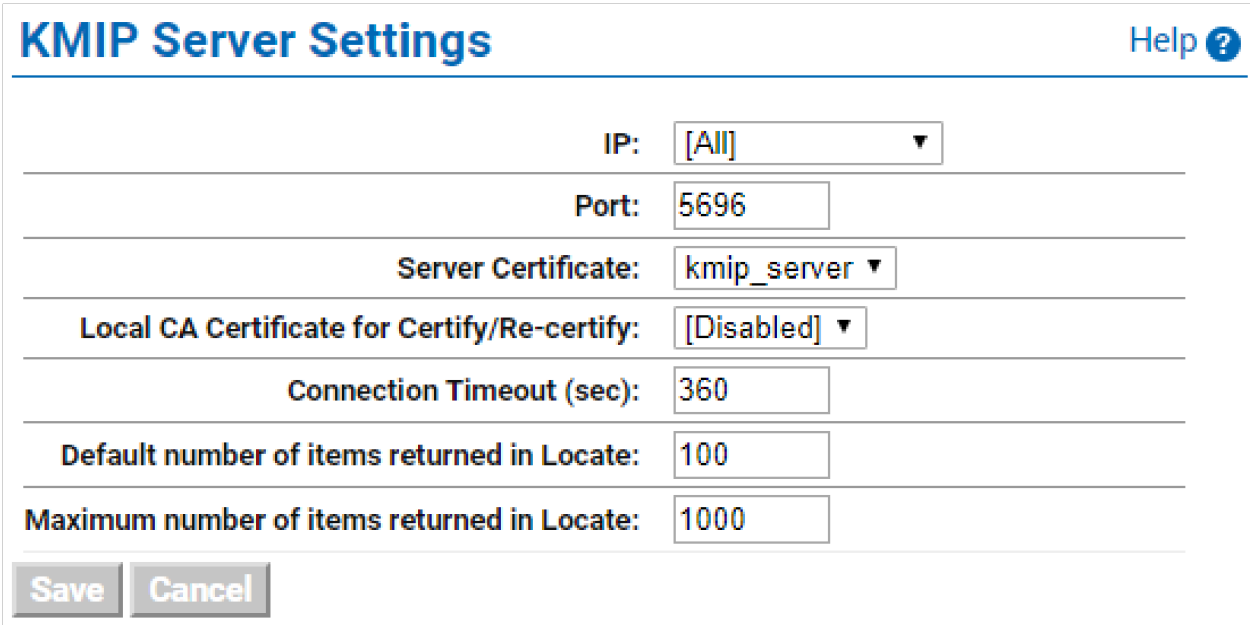

Figure 7 : KMIP Server Settings

5. Click **Save**.

Changing the KMIP server setting causes the KMIP server to restart.

6. Confirm that the KMIP server is started.

   a. Go to the Services List section of the Services Configuration page (**Device -> Maintenance -> Services -> KMIP Server**).

   b. The status of the KMIP server should be Started. If the status is Stopped, select the KMIP Server, and then click **Start**.

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your ESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to these server certificates should clearly indicate their purpose. For example:

ESKM KMS Server and ESKM KMIP Server.

KMIP requires mutual authentication. After configuring the KMIP server, **enable** KMIP client certificate authentication. The KMIP client certificate authentication status is **disabled** by default.

To enable KMIP client certificate, perform the following steps.

1. In the **KMIP Server Authentication Settings** section of the window, click **Edit**.

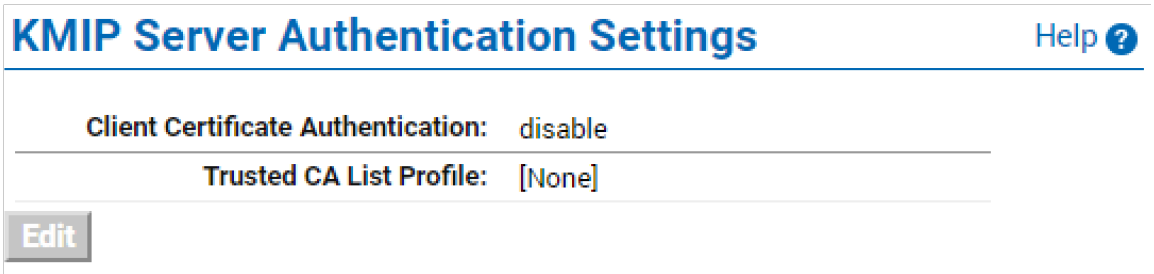

Figure 8 : KMIP Server Authentication Settings

2. Click **enable**, select the appropriate Trusted CA list and click **Save**.

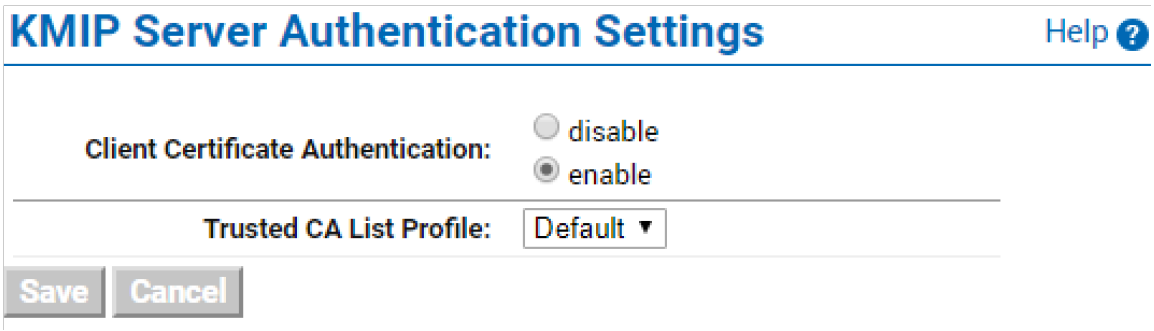

Figure 9 : KMIP Server Authentication Settings - enable

4.1.7 Setup KMS Server

The KMS server provides the interface to clients that use the KMS protocol. Secure Sockets Layer (SSL) is required, therefore you must specify the name of the server certificate.

To configure the KMS server, perform the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMS Server** to display the **KMS Server Configuration** window.
3. In the **KMS Server Settings** section of the window, click **Edit**.
4. Configure the KMIP Server Settings. The IP address can be an IPv4 address, or IPv6 address. If support for IPv6 has been enabled, see First run. If necessary, change the Port and Connection Timeout values. Utimaco recommends the default values of 9000 for the Port and 3600 for the Connection Timeout. For **Server Certificate**, select the name of the certificate you created in Setting up ESKM certificate. For example, ESKM KMS Server.

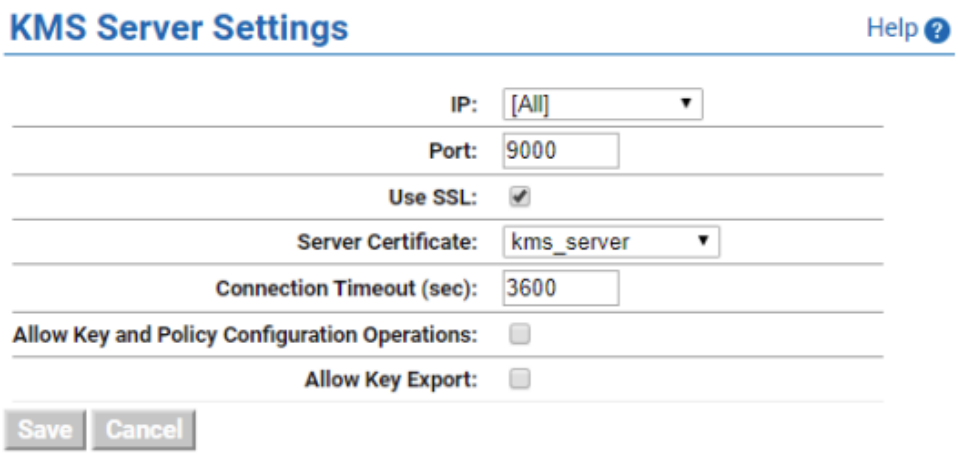

Figure 10 : KMS Server Settings

5. Click **Save**.
6. Confirm that the KMS server is started.
    a. Go to the Services List section of the Services Configuration page (**Device -> Maintenance -> Services -> KMS Server**).
    b. The status of the KMS server should be Started. If the status is Stopped, select the KMS Server, and then click **Start**.

To enable KMIP client certificate, perform the following steps.

1. In the **KMS Server Authentication Settings** section of the window, click **Edit**.

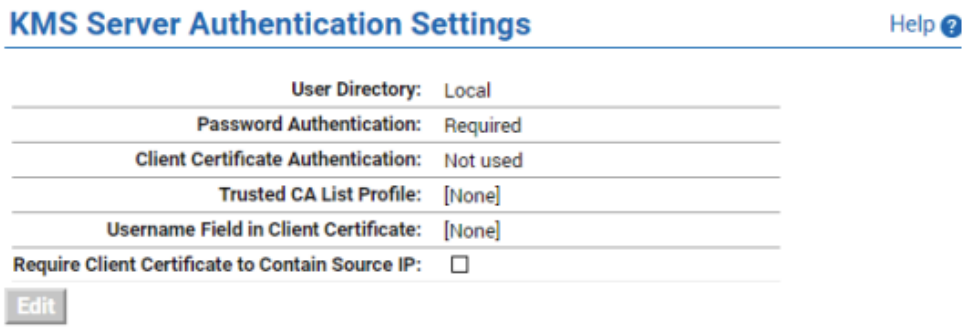

Figure 11 : KMS Server Authentication Settings

2. Click appropriate option under **User Directory**, **Password Authentication**, and **Client Certificate Authentication.** Select the appropriate Trusted CA list, and Username in Client Certificate and click **Save**.

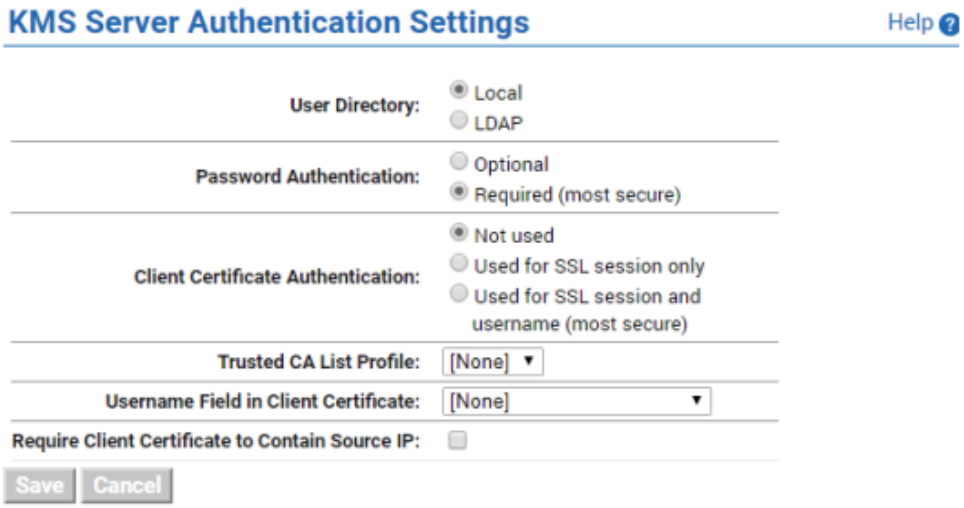

Figure 12 : KMS Server Authentication Settings

5 Integration Steps

This section provides the step-by-step procedure of integrating ESKM with VMware.

5.1 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.

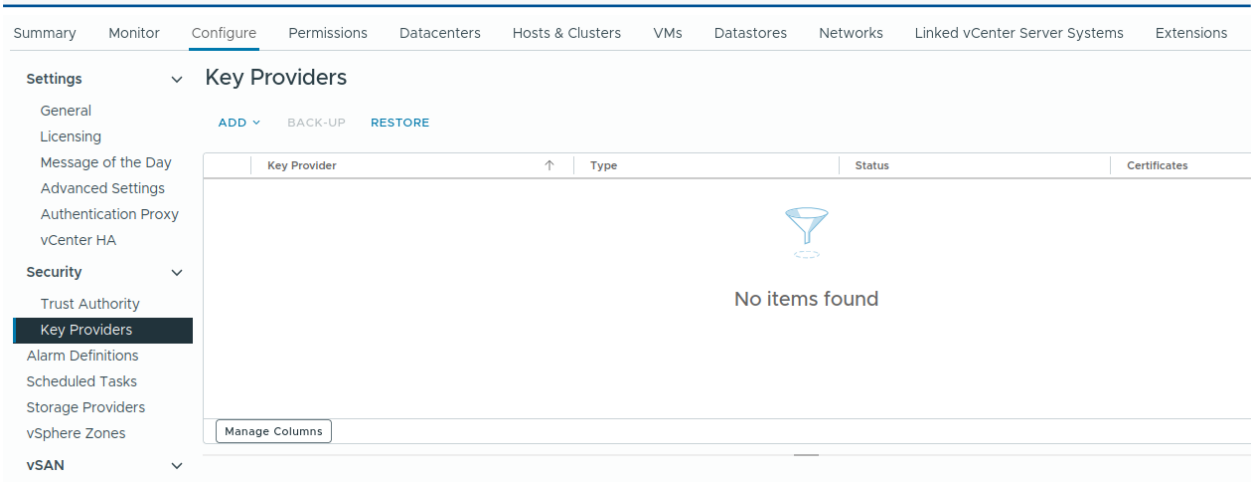

Figure 13 : Configure

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 4: New ESKM

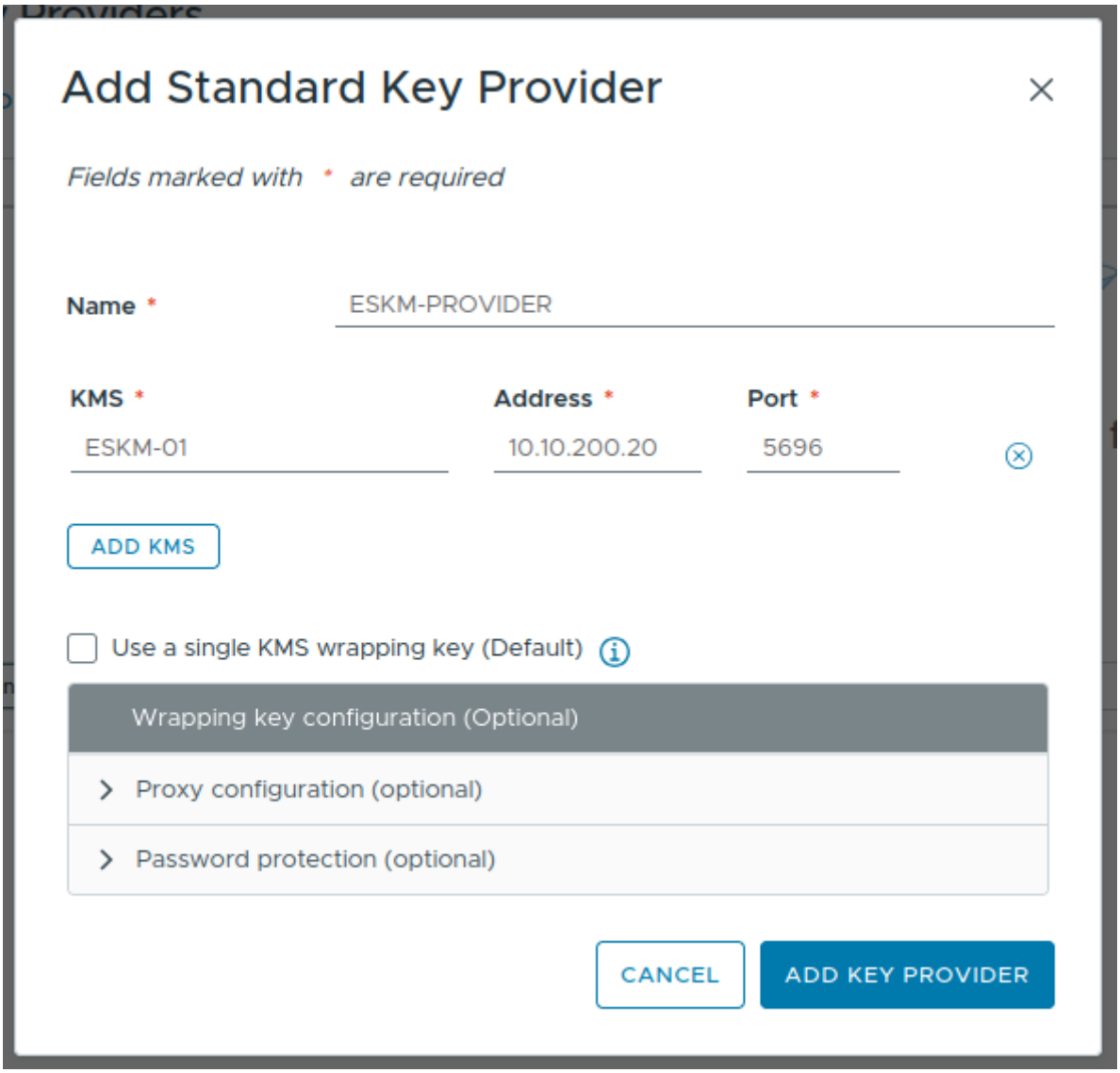

Figure 14 : Add KMS

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.

5.1.1 Establish trust between vCenter and ESKM

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

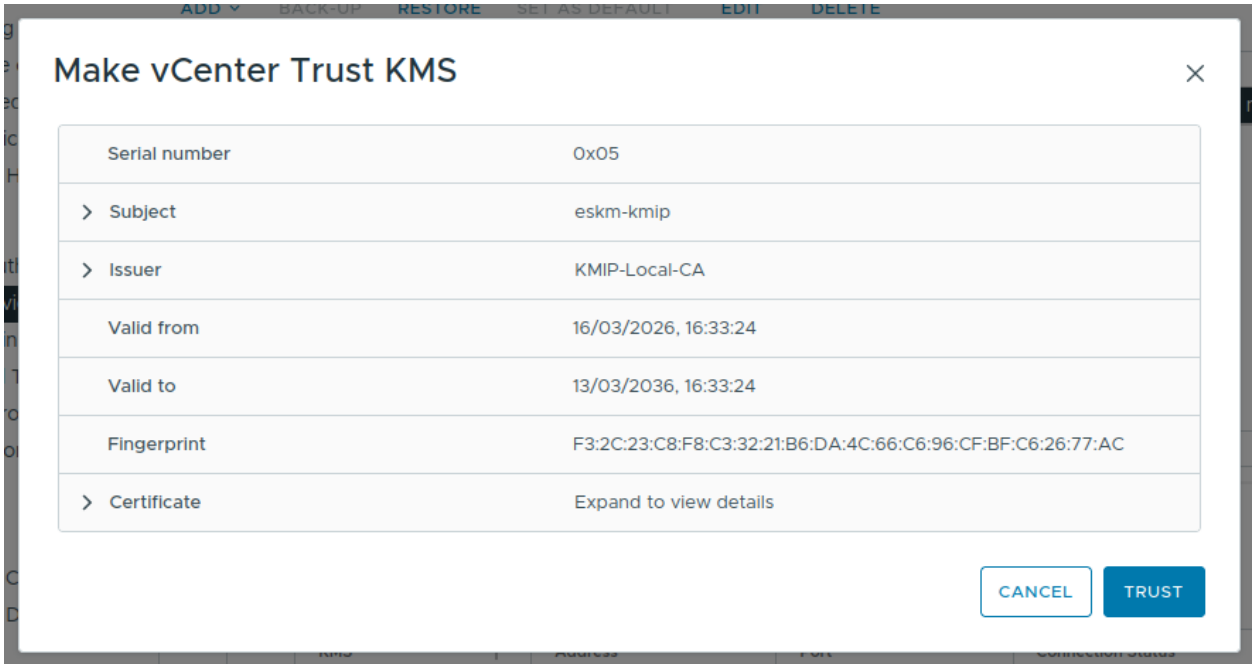

Figure 15 : Make vCenter Trust KMS Dialog window

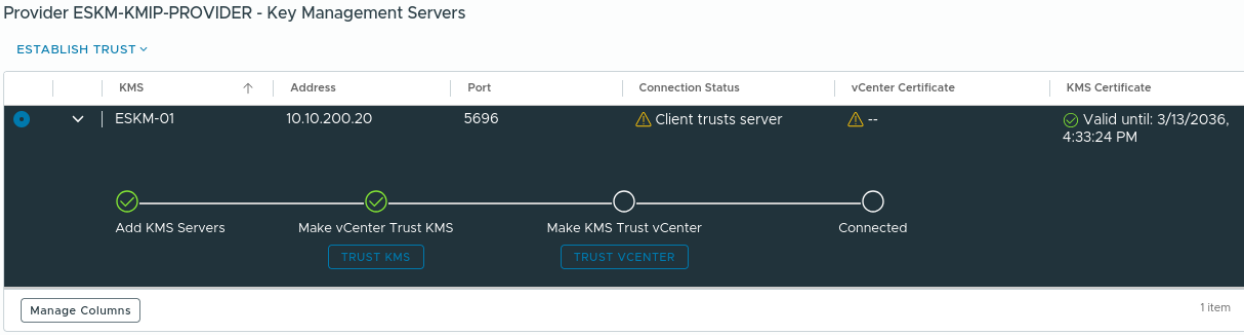

Figure 16 : Steps to stablish trust between vCenter and ESKM

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

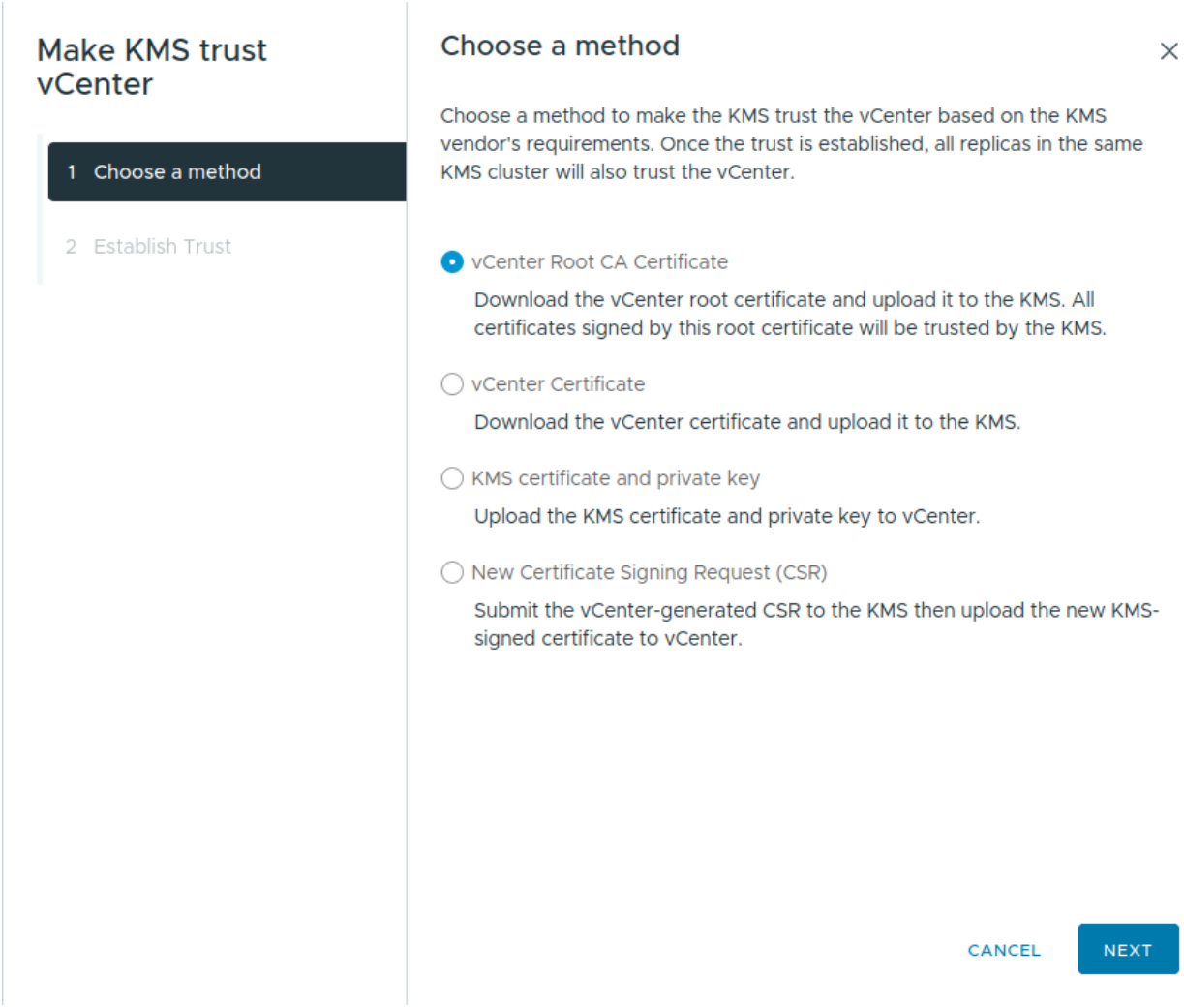

Figure 17 : Method selection for trust stablishment

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

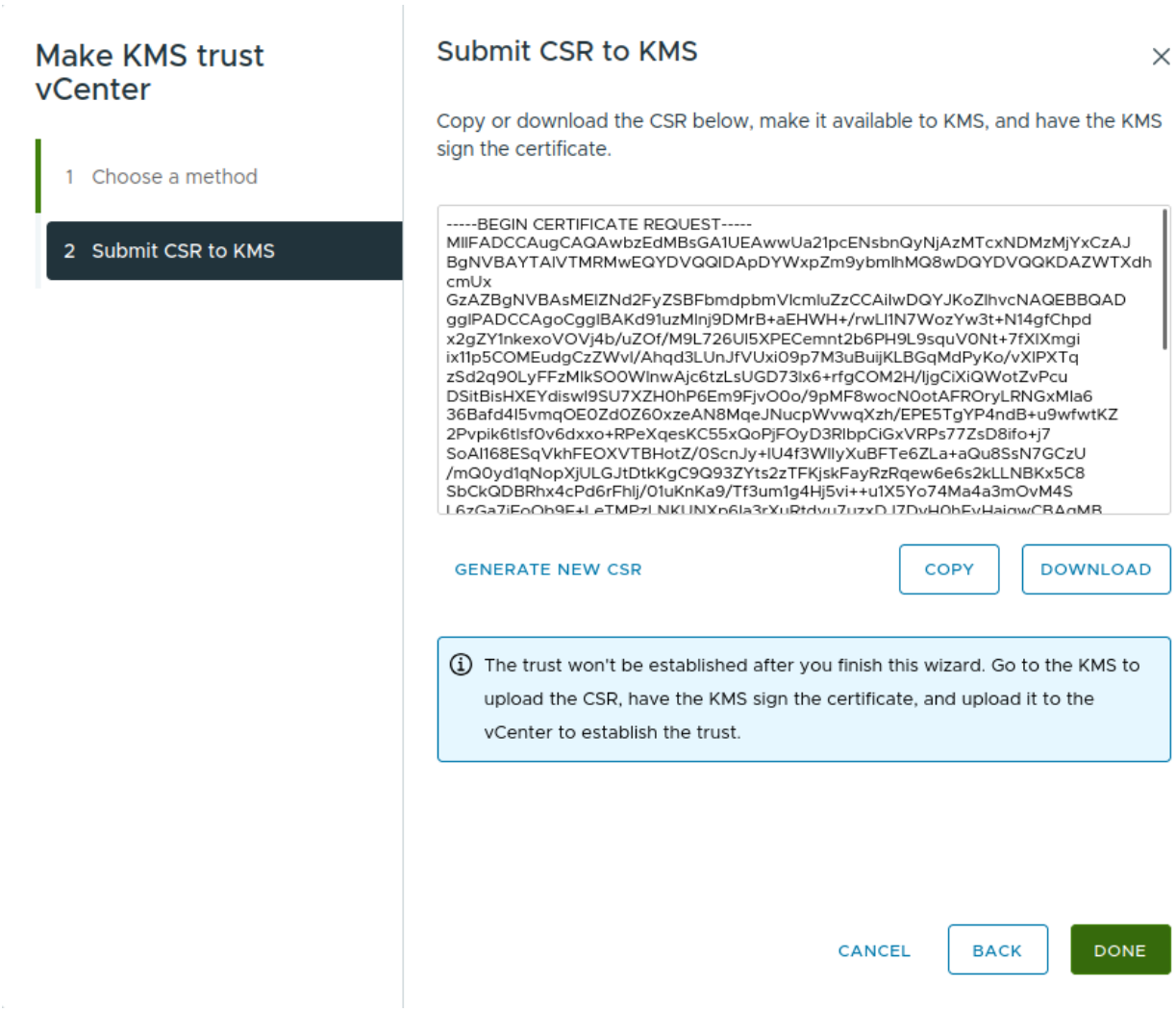

Figure 18 : Submit CSR to KMS dialog window

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 19 : 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**.

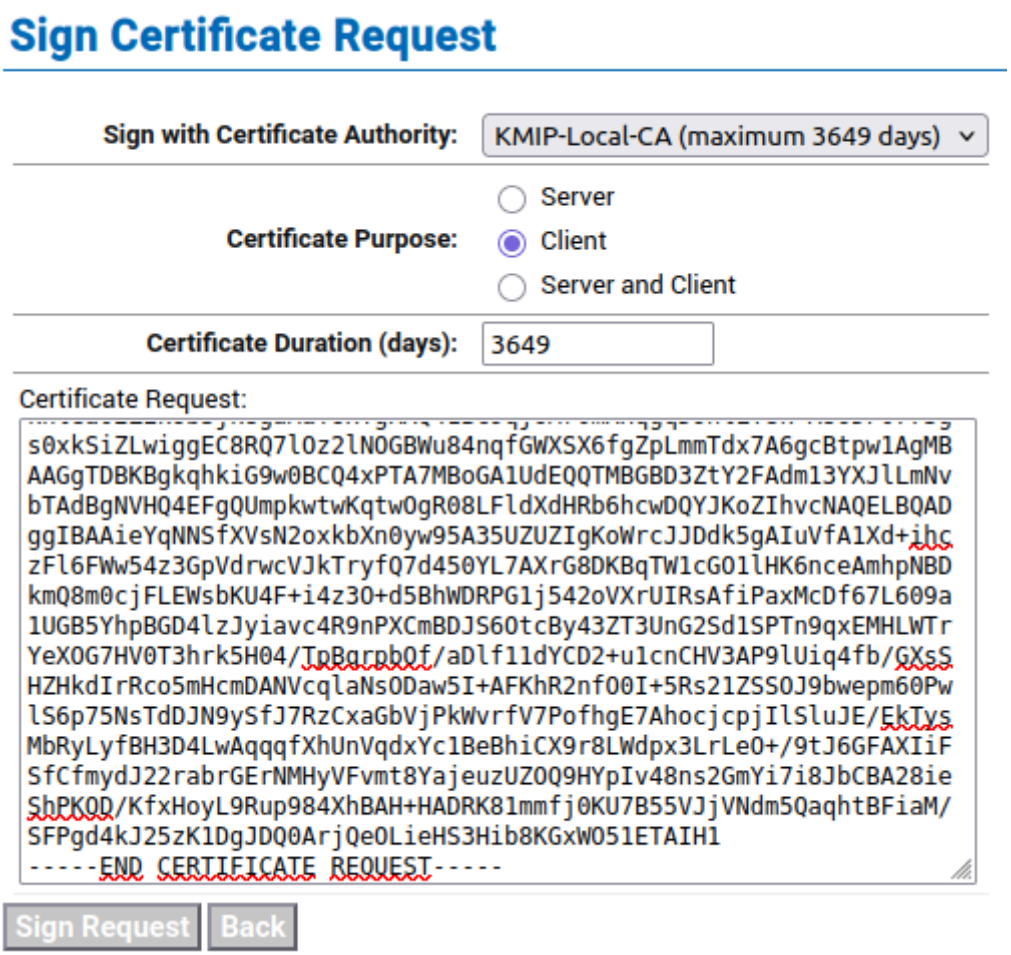

Figure 20 : Sign Certificate Request window

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 21 : 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)”.

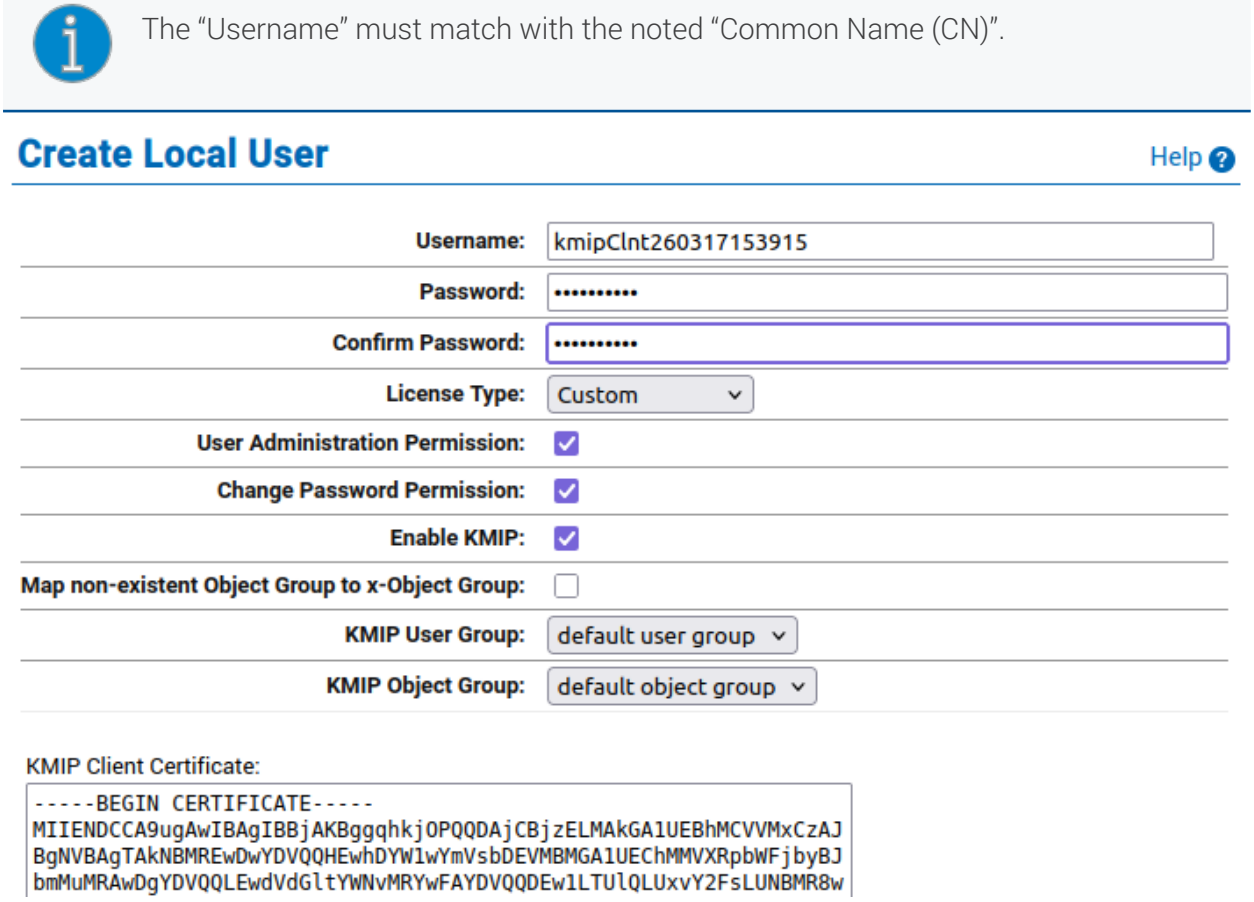

Figure 22 : Create Local User dialog window

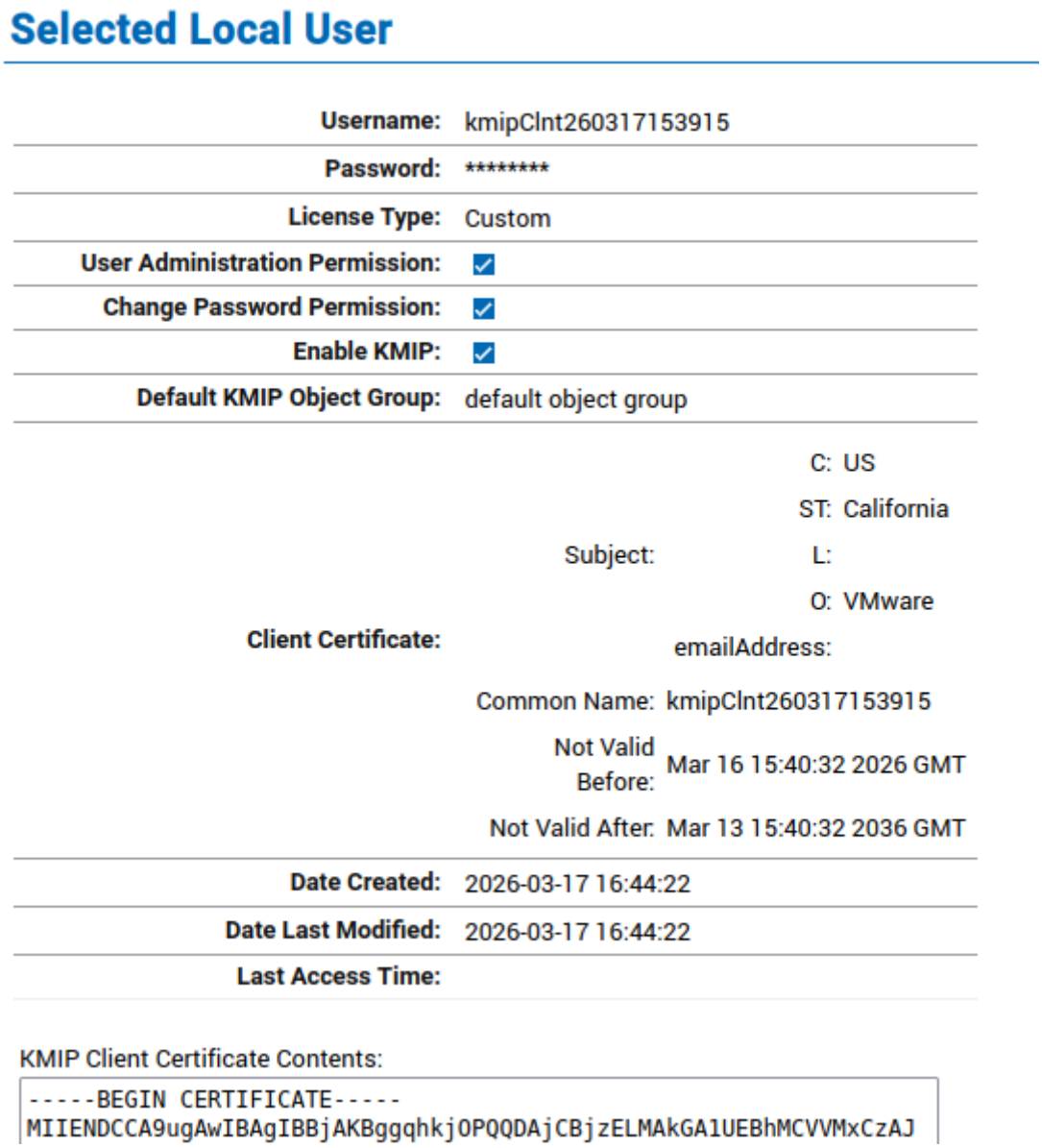

Figure 23 : Selected Local User

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

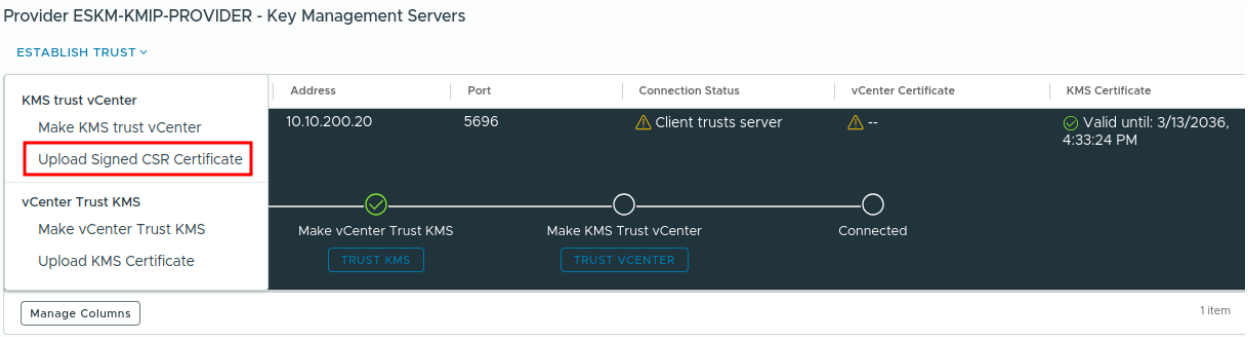

Figure 24 : Upload Signed Certificate Menu

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

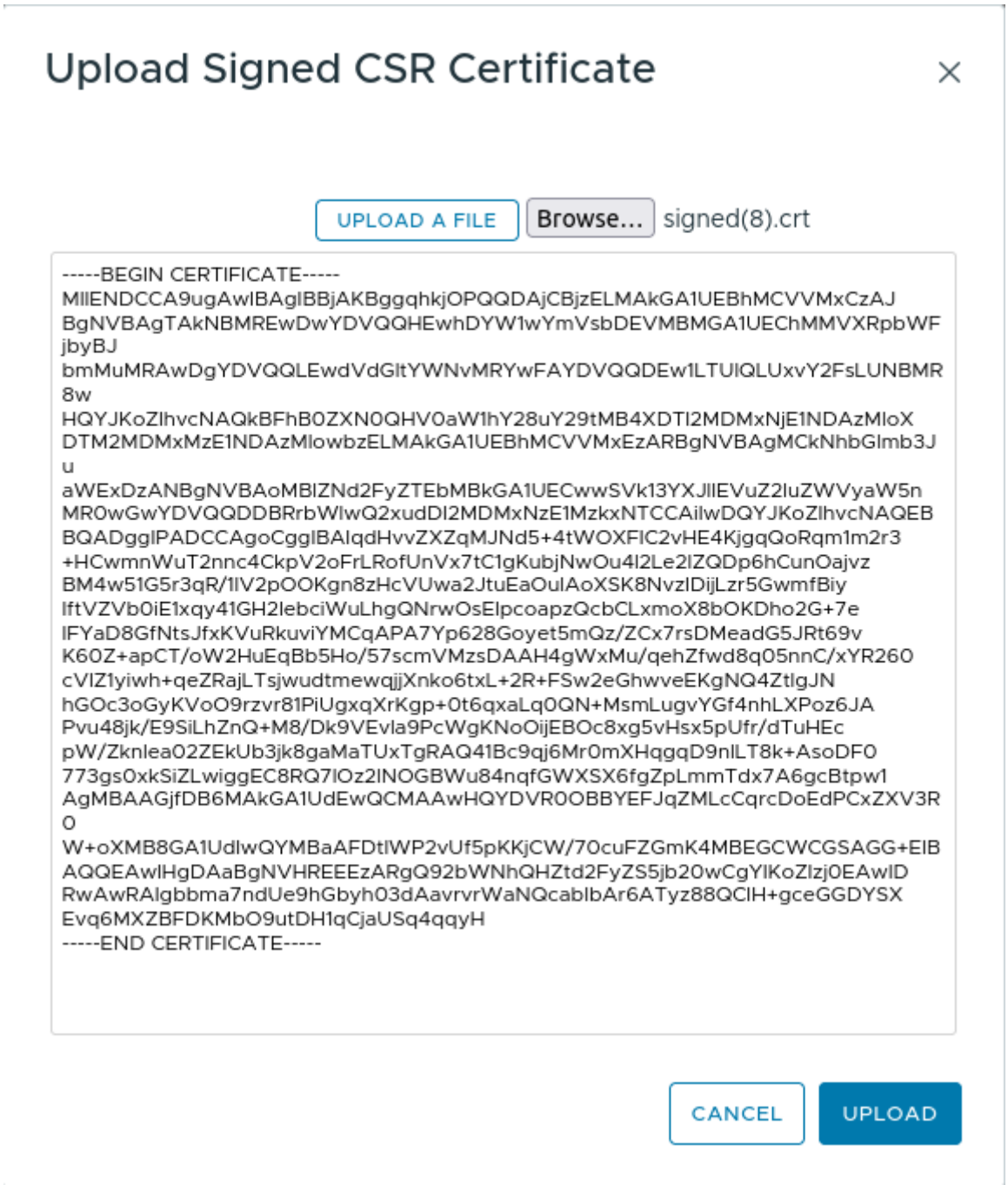

Figure 25 : Upload Signed CSR Certificate

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

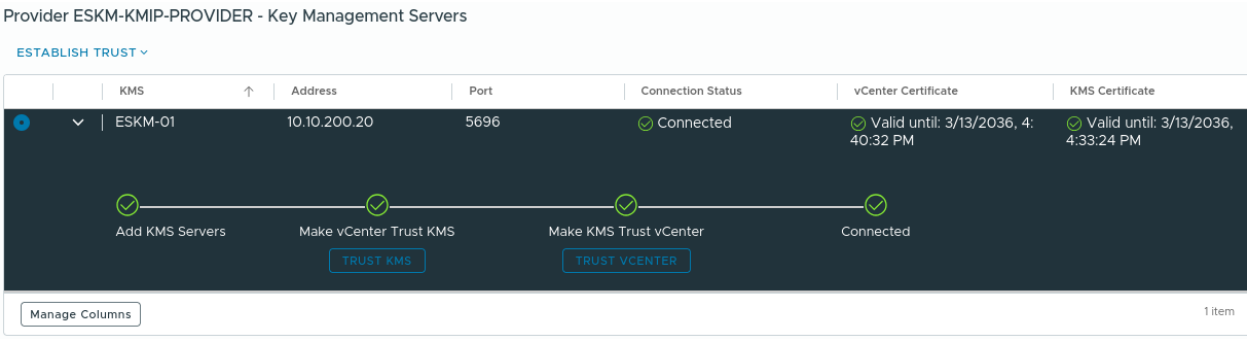

Figure 26 : Cpmpleted trust stablishment process

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).

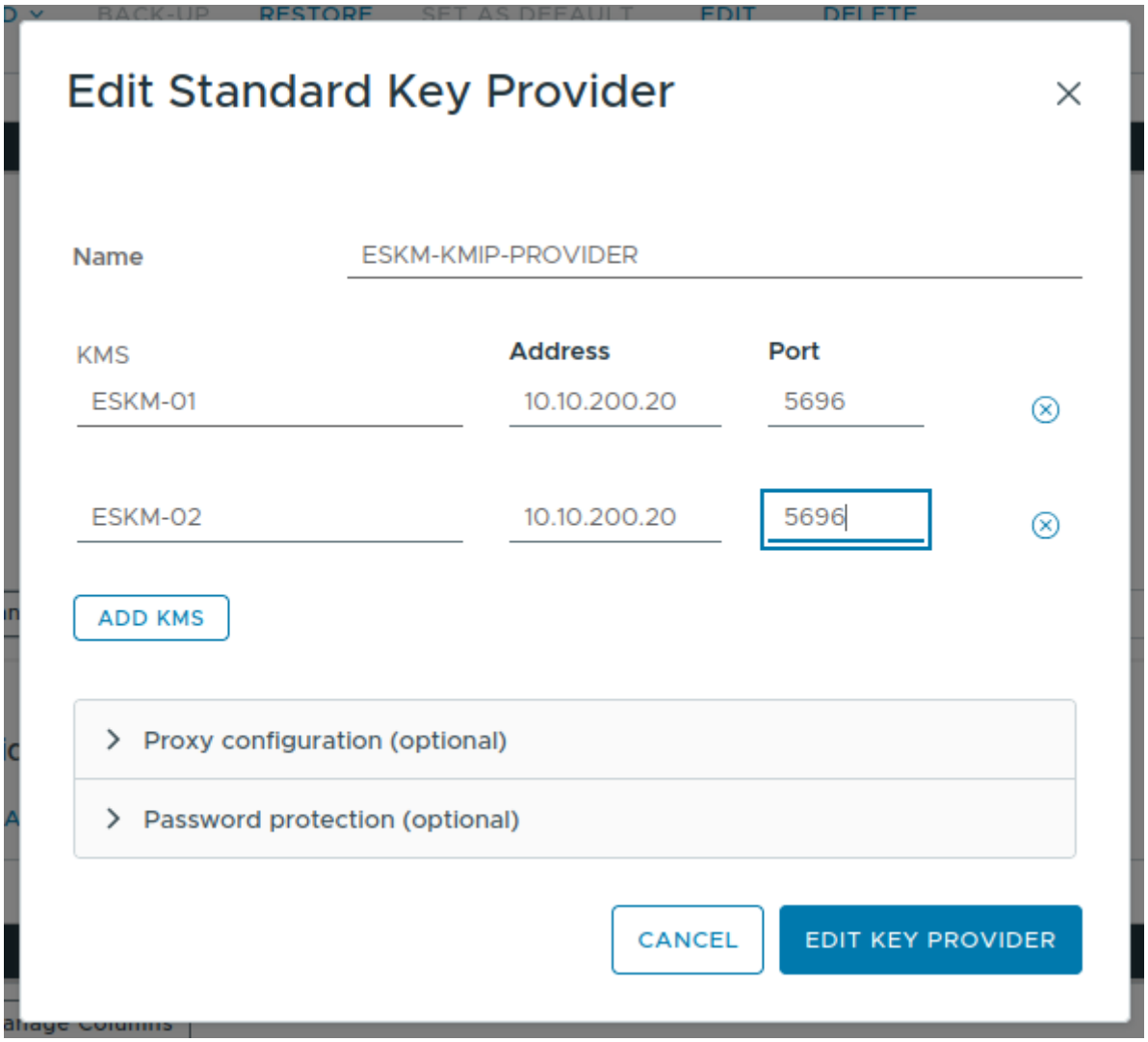

Figure 27 : Add Standard Key Provider for second ESKM

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

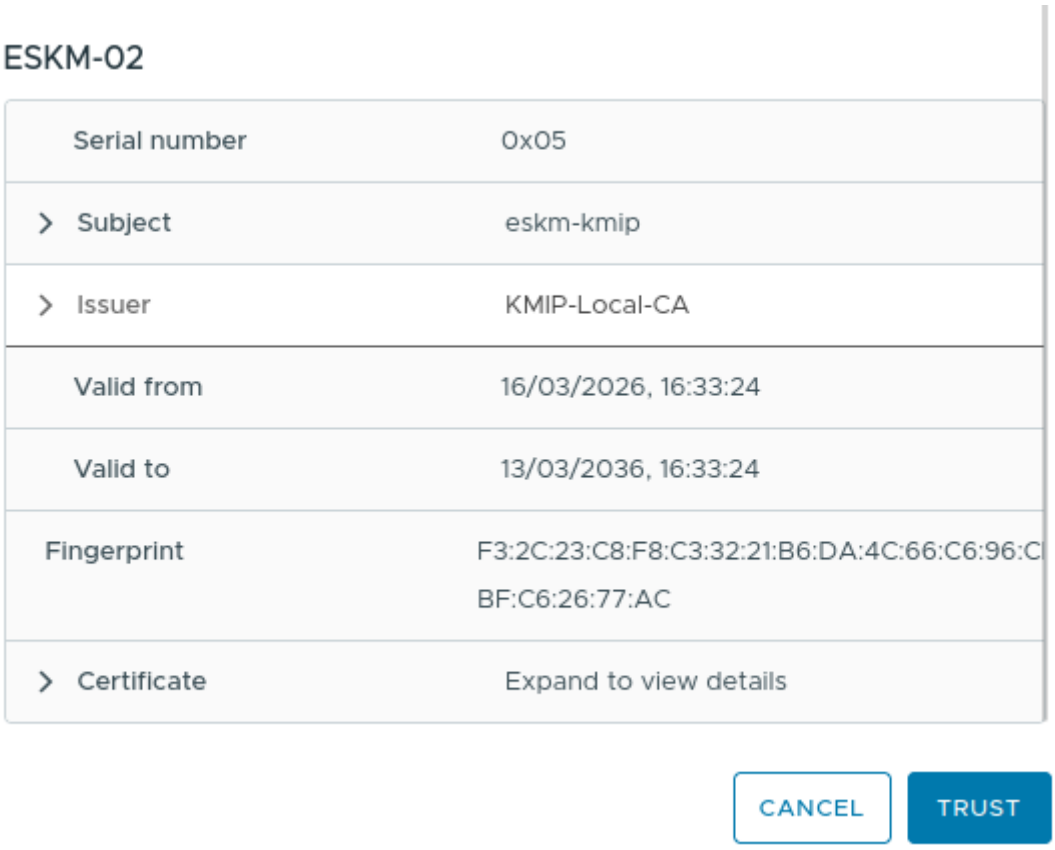

Figure 28 : Make vCenter Trust KMS on second ESKM

23. Confirm both the ESKM servers are accessible.

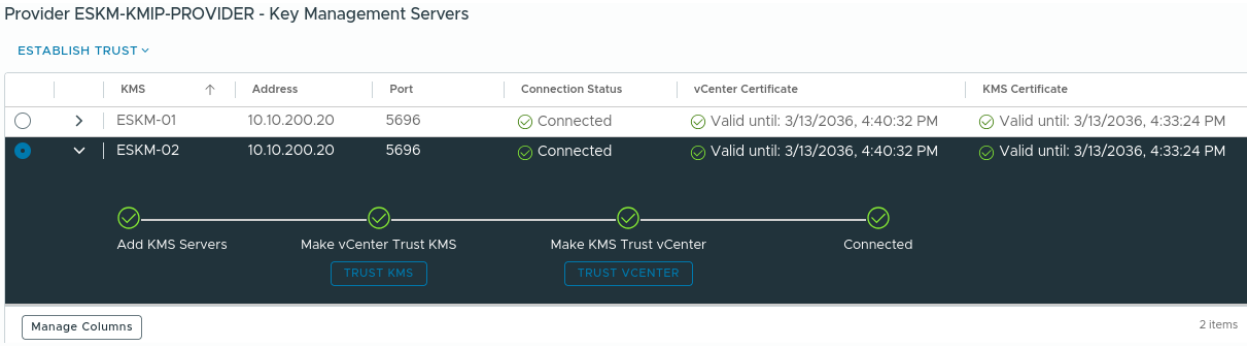

Figure 29 : Completed trust stablishment process on second ESKM

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

5.2 Configuration on Utimaco ESKM

5.2.1 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.

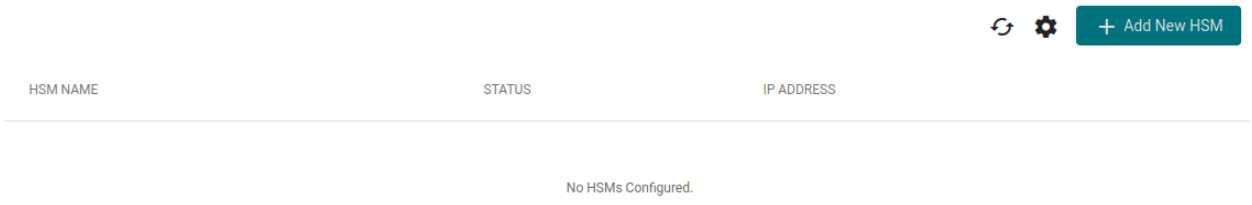

Figure 30 : HSM Integration Dashboard

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

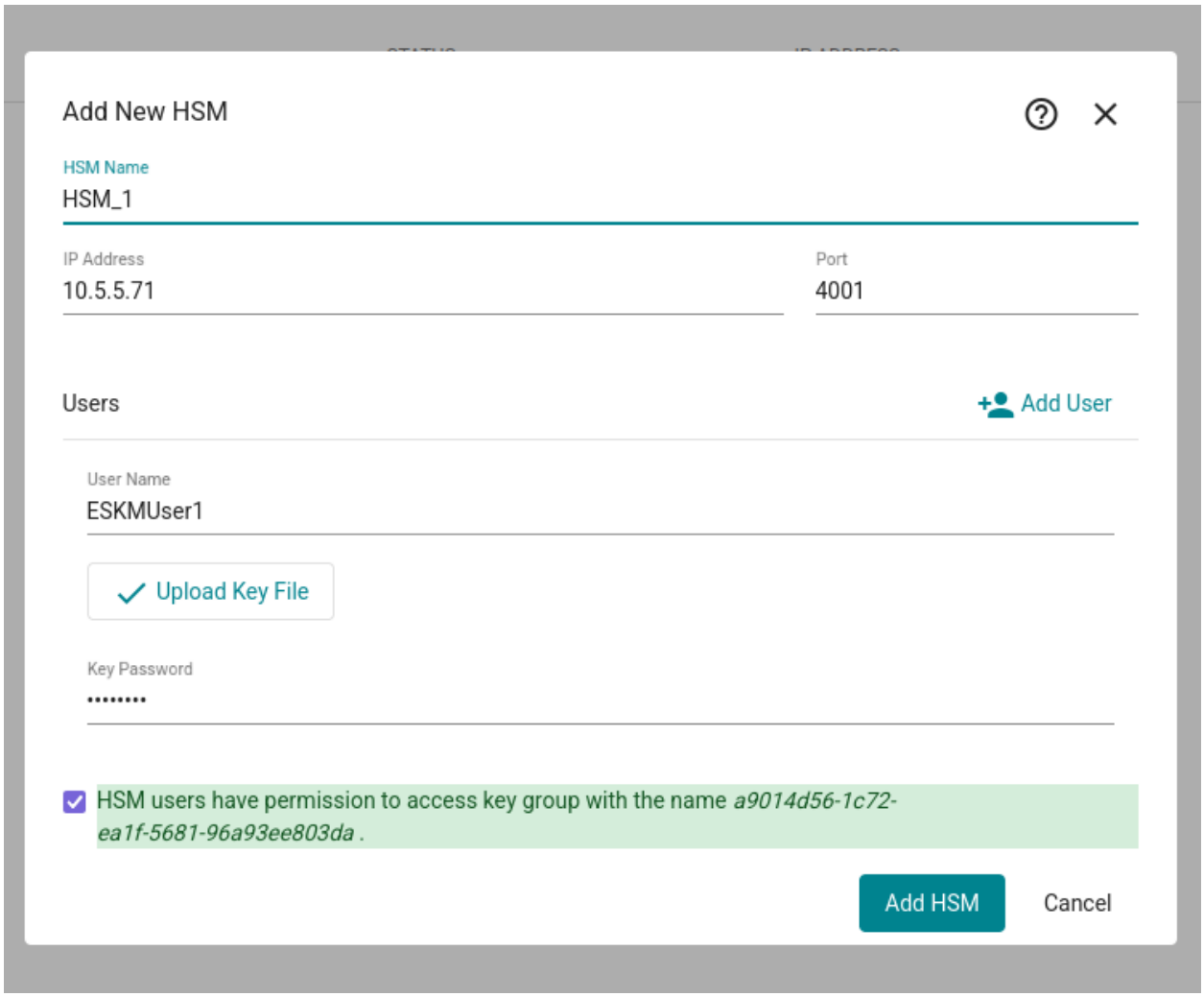

Figure 31 : Add New HSM

- 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.

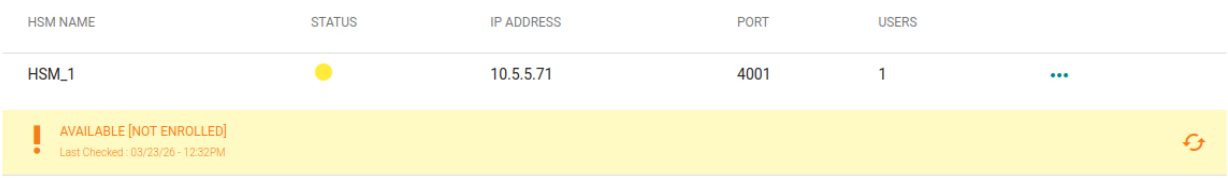

Figure 32 : HSM Added (Not Enrolled)

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 33 : 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.

6 Verification and Testing

6.1 Functional Testing

This section describes common procedures for testing the integration between the VMWare vCenter and the Utimaco ESKM.

6.1.1 Encrypting a Virtual Machine

To validate the integration between VMware vCenter and Utimaco 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.

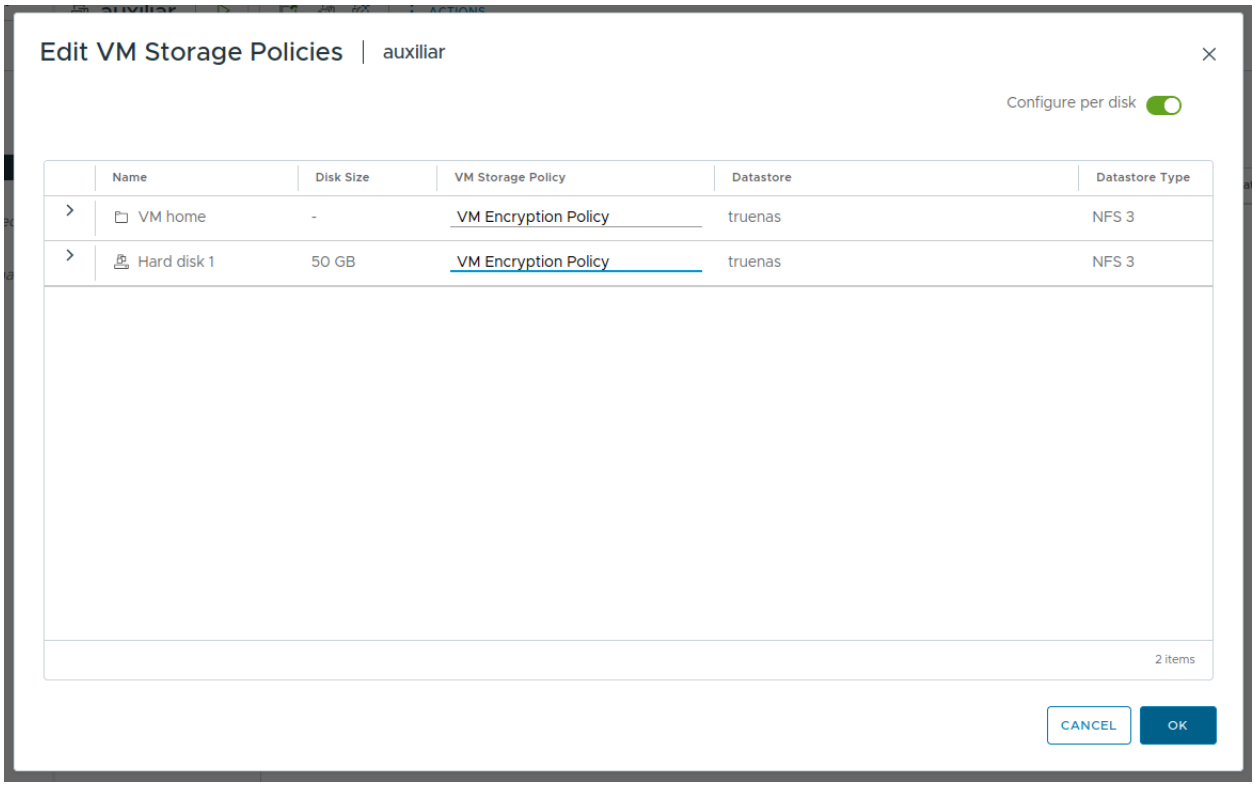

Figure 34 : Edit VM Storage Policies

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

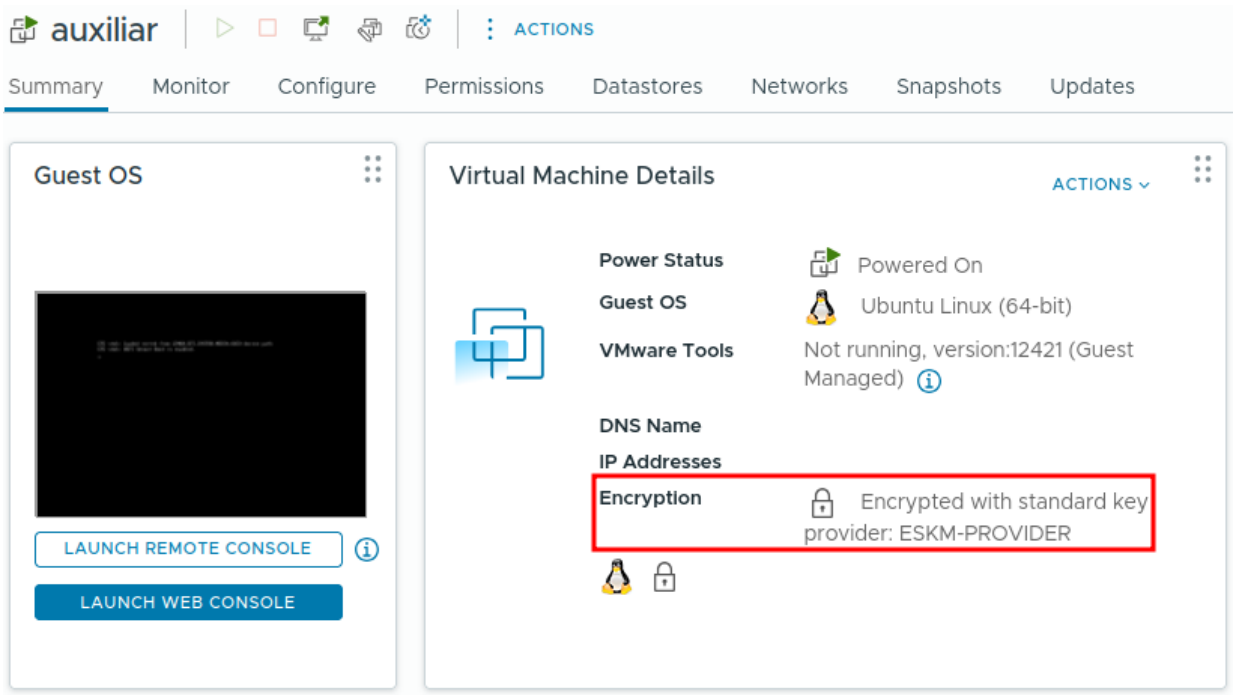

Figure 35 : Encrypted VM

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.

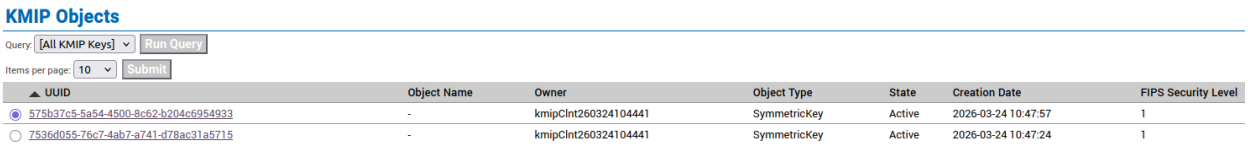

Figure 36 : KMIP Objects created

- 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 37 : Successful Key Retrieval

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.

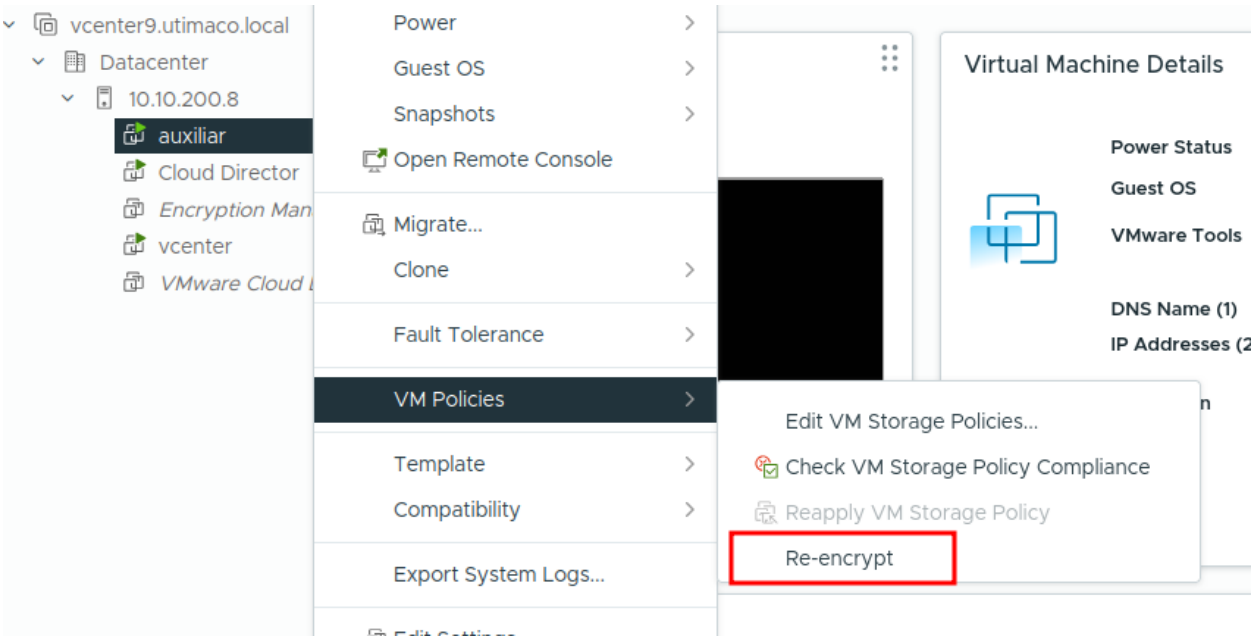

Figure 38 : VM Re-encryption

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.

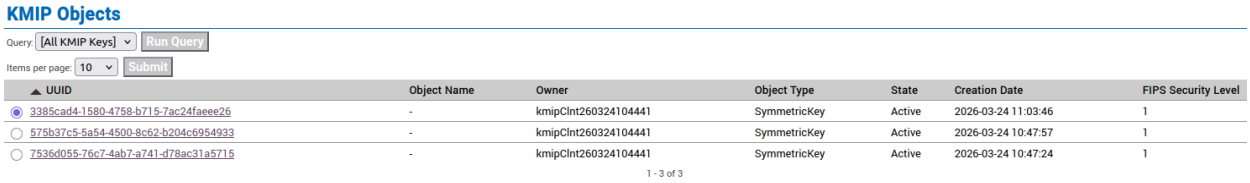

Figure 39 : New Key Created

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

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.
Lost the “admin” account password and no other users exist.	Contact Utimaco Technical Support .

Table 5: Troubleshooting

8 Contact and Support Information

8.1 Utimaco Technical Support

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

8.2 24-hour support

24-hour emergency support is available to those customers who have valid service contracts. Use this service for product and system emergencies that occur after normal working hours or on weekends and U.S. holidays. Questions about product installation and setup are supported during normal working hours.

For 24-hour emergency support call: 800-500-7858 (U.S.A.) +1-916-414-0216 (International).