MySQL

Enterprise Edition 8.0.28

Integration Guide

ESKM

Version 8.2.0 or later

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	2026-03-24
Status	PUBLISHED
Document No.	IG-2026-0019

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. All Utimaco ESKM product documentation is available from Utimaco's web site at https://utimaco.com/.

1.1 About This Guide

This guide provides an integration guide explaining how to integrate MySQL with UTIMACO ESKM.

1.1.1 Target Audience for This Guide

This guide is intended for administrators of MySQL and of ESKM.

1.1.2 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 the OK button.
Monospaced	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file example.conf in the /exmp/demo/ directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or Error! Reference source not found..

Table 1: Document conventions

Special icons are used to highlight the most important notes and information.

Here you find important safety information that should be followed.

Here you find additional notes or supplementary information.

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

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AES	Advanced Encryption Standard
CA	Certificate Authority
CD	Compact Disc
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
ESKM	Enterprise Secure Key Manager
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface

Abbreviation	Meaning
HTTPS	Hypertext Transfer Protocol Secure
KMIP	Key Management Interoperability Protocol
KMS	Key Management System
MSI	Microsoft Installer
RDBMS	Relational Database Management System
RSA	Rivest-Shamir-Adleman
SCP	Secure Copy
SSH	Secure Shell
SSL	Secure Socket Layer
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
XML	Extensible Markup Language

Table 2: Abbreviations

2 Overview

2.1 MySQL

MySQL is an open-source relational database management system (RDBMS). MySQL is the world's most popular open-source database. As we are using MySQL Enterprise Edition for this integration so let us see some information about it.

MySQL Enterprise Edition includes the most comprehensive set of advanced features, management tools and technical support to achieve the highest levels of MySQL scalability, security, reliability, and uptime. It reduces the risk, cost, and complexity in developing, deploying, and managing business-critical MySQL applications.

MySQL software delivers a very fast, multithreaded, multi-user, and robust SQL (Structured Query Language) database server. MySQL Server is intended for mission-critical, heavy-load production systems as well as for embedding into mass-deployed software.

2.2 ESKM

The ESKM is a complete solution for generating, storing, serving, controlling and auditing access to encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys, either locally or remotely.

ESKM is the first industry-certified Key Management Interoperability Protocol (KMIP) v2.1 offering with market leading support for partner applications and pre-qualified solutions, integrating out-of-the-box with varied deployments, as well as custom integrations.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using, meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured required Software.

3.1 Tested Versions

The integrations that have been successfully tested with Utimaco ESKM product are shown in the following configurations below:

Operating System	MySQL Version	Utimaco ESKM Version
Windows Server 2019 Windows Server 2016 CentOS 7.9	MySQL Enterprise Edition 8.0.28	Version 8.2.0 or later

Table 3: List of Tested Versions

3.2 Software Requirements

Software	Software Requirements
OpenSSL	Version 1.1.1
MySQL	Enterprise Edition 8.0.28

Table 4: List of Software Requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
ESKM	Version 8.2.0 or later

Table 5: List of Hardware Requirements

Setup an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com

3.4 Prerequisites

Before you begin, please ensure that you have installed/setup:

- Operating system listed in Tested Versions.
- MySQL Server listed in Tested Versions.
- ESKM listed in Tested Versions.
- Uploaded the MySQL enterprise edition packages/installer to the server.
- Port 3306, 5696 should be open on the firewall.

4 Software Installation – MySQL

Installing the Oracle MySQL Enterprise Edition depends on the operating system on which you are installing it. See the Oracle documentation for details on how to install Oracle MySQL Enterprise Edition in your environment.

If you have already installed and configured MySQL, please ensure that it meets the requirements as stated in **Integration Requirements and Prerequisites**, then proceed to **ESKM Server Configuration**.

4.1 On Linux:

The below high-level steps were used to install and configure MySQL on a CentOS 7.9 Linux server.

1. Login to the server with root credentials.
2. (Optional) Update the server prior to the install.

›_ Console

```
# yum update
```

3. Go to the directory where MySQL Zip file is copied and unzip it.
4. Install MySQL using the following command:

›_ Console

```
# yum localinstall ./*.rpm
```

During the installation, you might be prompted to enter the password for the root user for your MySQL installation.

5. When installing MySQL on CentOS 7.9, a temporary root password is generated and available in mysqld.log file under /var/log.
6. Log in to the MySQL client.

›_ Console

```
# mysql -h 127.0.0.1 -uroot -p
```

7. Enter the Temporary password created for the root user.
8. Change the root password.

›_ Console

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY '<NEW_PASSWORD>'; mysql>
FLUSH PRIVILEGES;
mysql> exit;
```

9. Test the new password.

›_ Console

```
# mysql -u root -p<new_password>
```

4.2 On Windows:

The steps below were used to install and configure MySQL on a Windows 2016 server.

1. Log in to the Windows Server with Administrator privileges.
2. Unzip the MySQL file and double click the MSI installer.exe file.
3. In the installation wizard, choose the appropriate Setup type as per your requirement. Here, we are going to select the Full option and click on the Next button.

4. Follow the installation wizard and complete the MySQL installation.

5 ESKM Server Configuration

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.

If you have already setup the ESKM, then skip Setting up local CA.

5.1 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 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 large, the ESKM displays the key fingerprint on the console, as shown below.

›_ Console

```
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 display.

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 8.2.0 User Guide.

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

5.2 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.

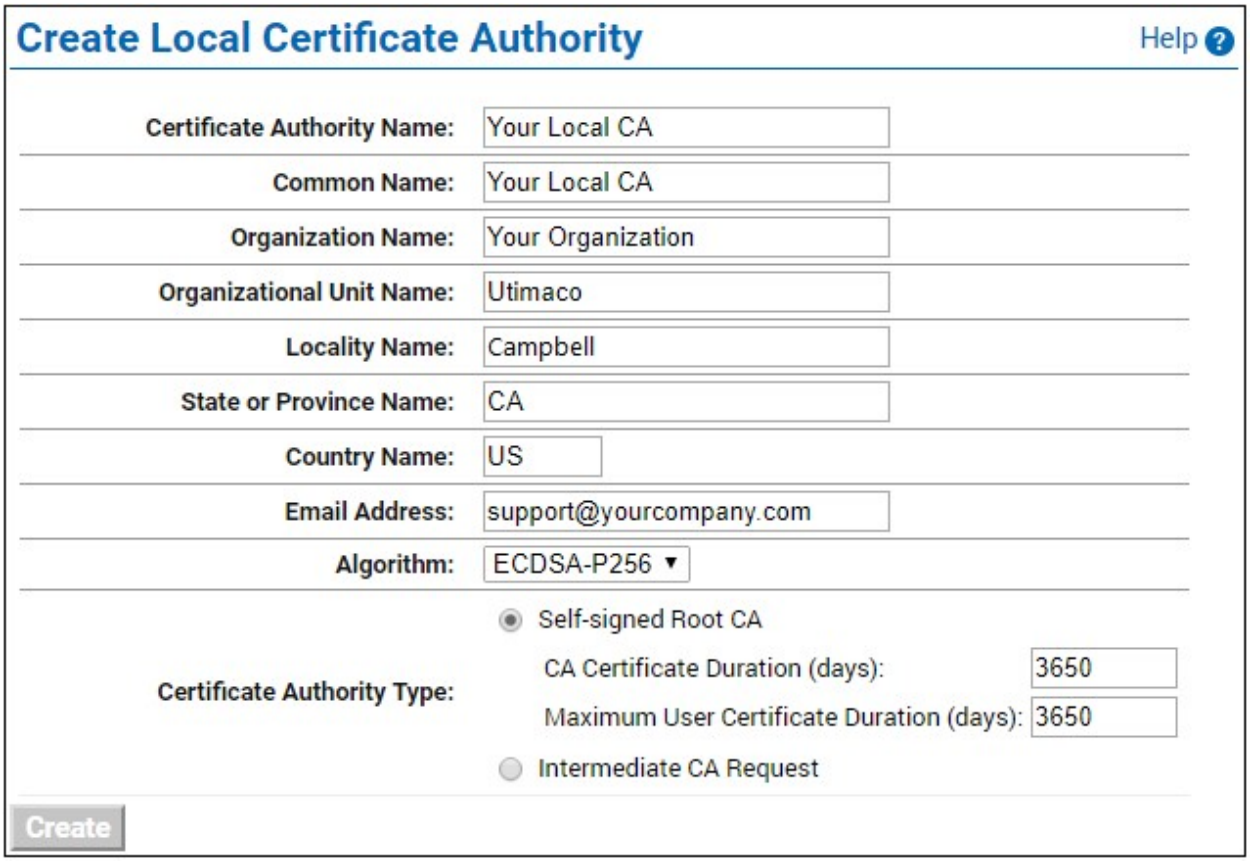

Figure 1 : Create Local CA window

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 when another local CA is needed. For example, you may want to create a KMIP Local CA to support the KMIP Certify/Re-certify 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 & CAs, 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.

5.3 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 KMIPenabled 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.

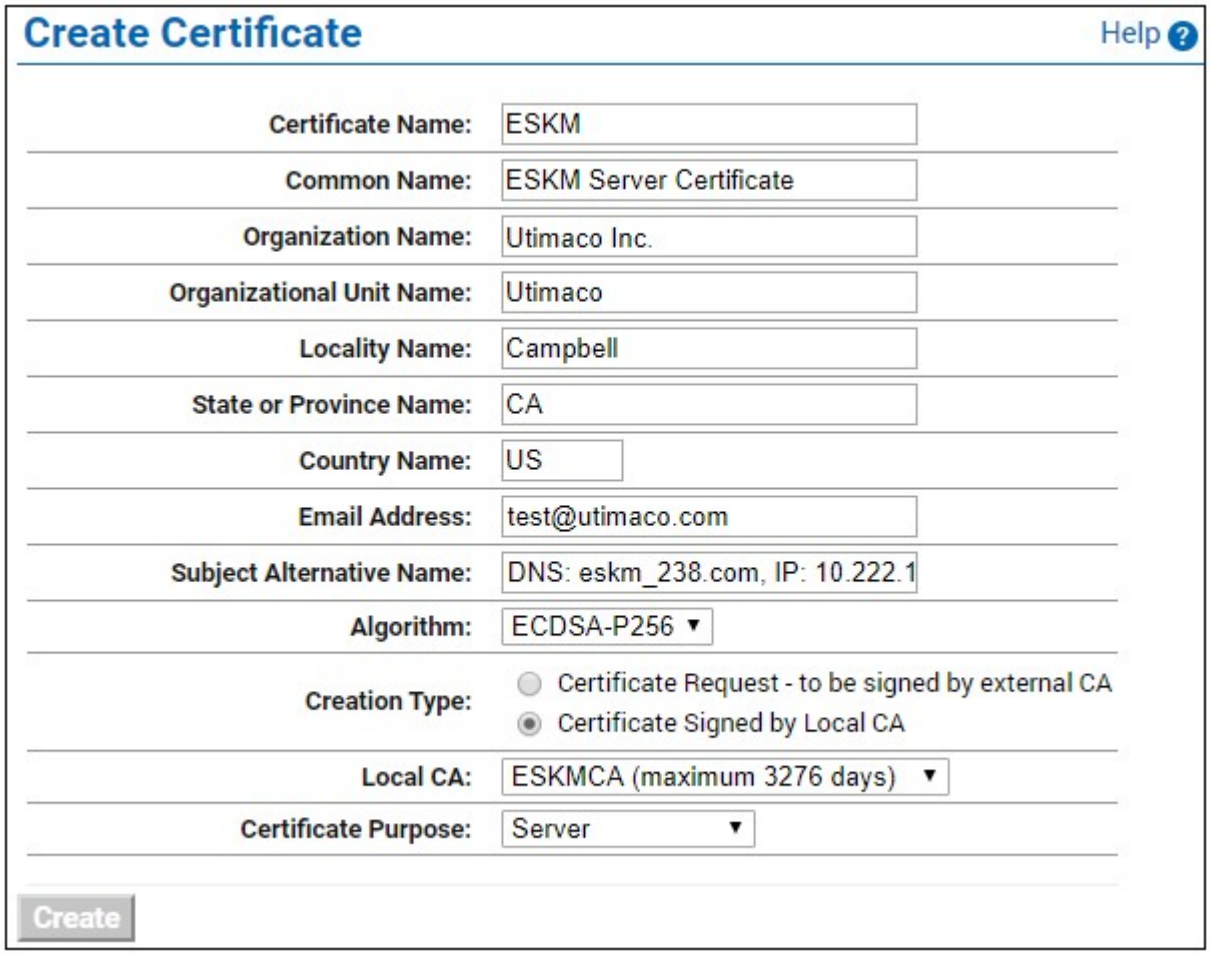

Figure 2 : Create Certificate window

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

b) Enter your Organizational information.

c) Enter/Select the Subject Alternative Name, Algorithm, Creation Type, Local CA, and Certificate Purpose. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

4. Click Create.

5. The Certificate List will include the newly created certificate, its status will be Request Pending. Click on the certificate name. For example, ESKM KMS Server.

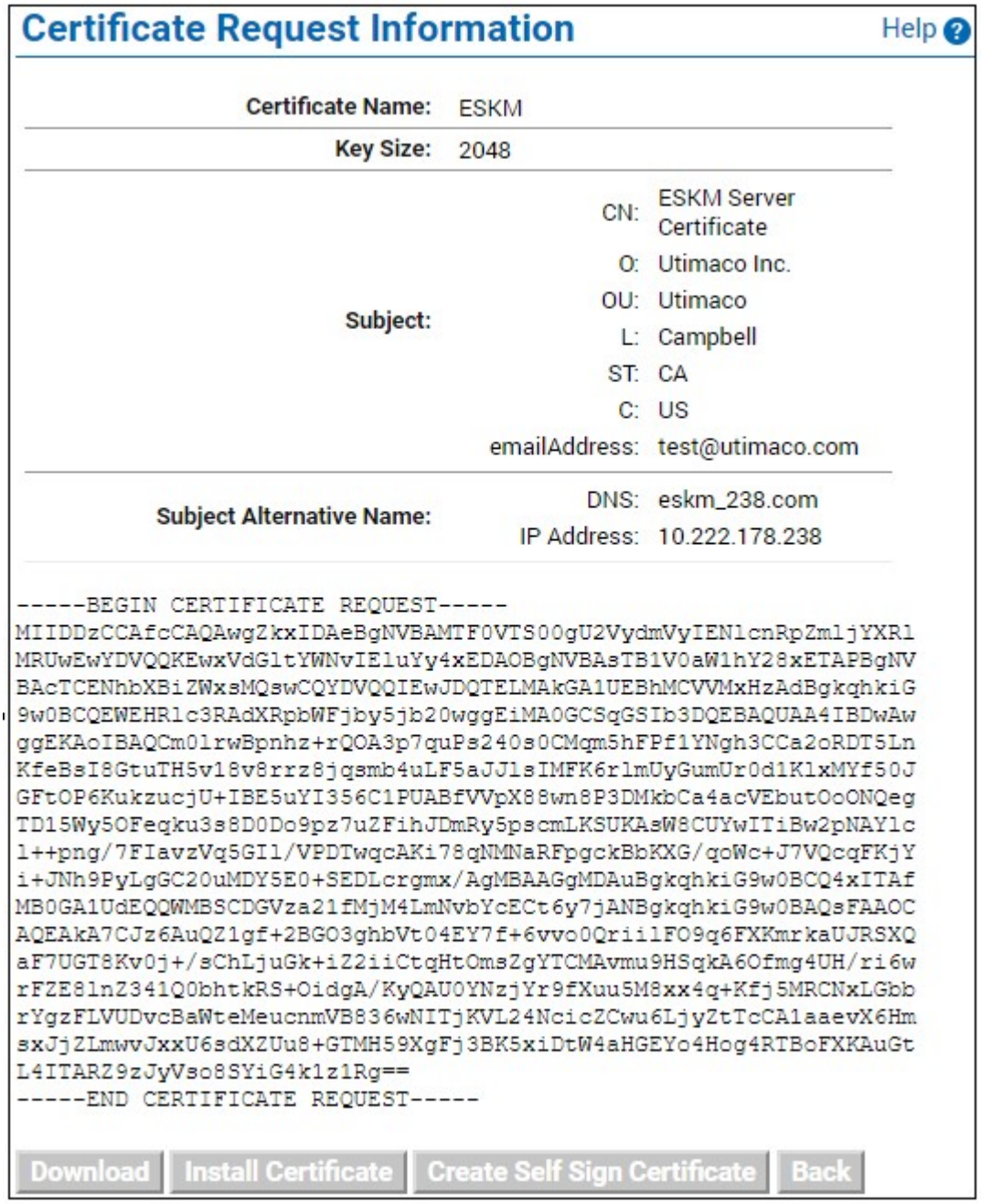

Figure 3 : Certificate Request Information window

Key Size refers to the size of the key or elliptic curve associated with this certificate.

6. In the Certificates & CAs menu, click Local Cas.

7. Click on the CA name you created in Setting up local CA for example ESKM Local CA.
8. Click Sign Request.
9. Enter data required by the Sign Certificate Request section of the window.

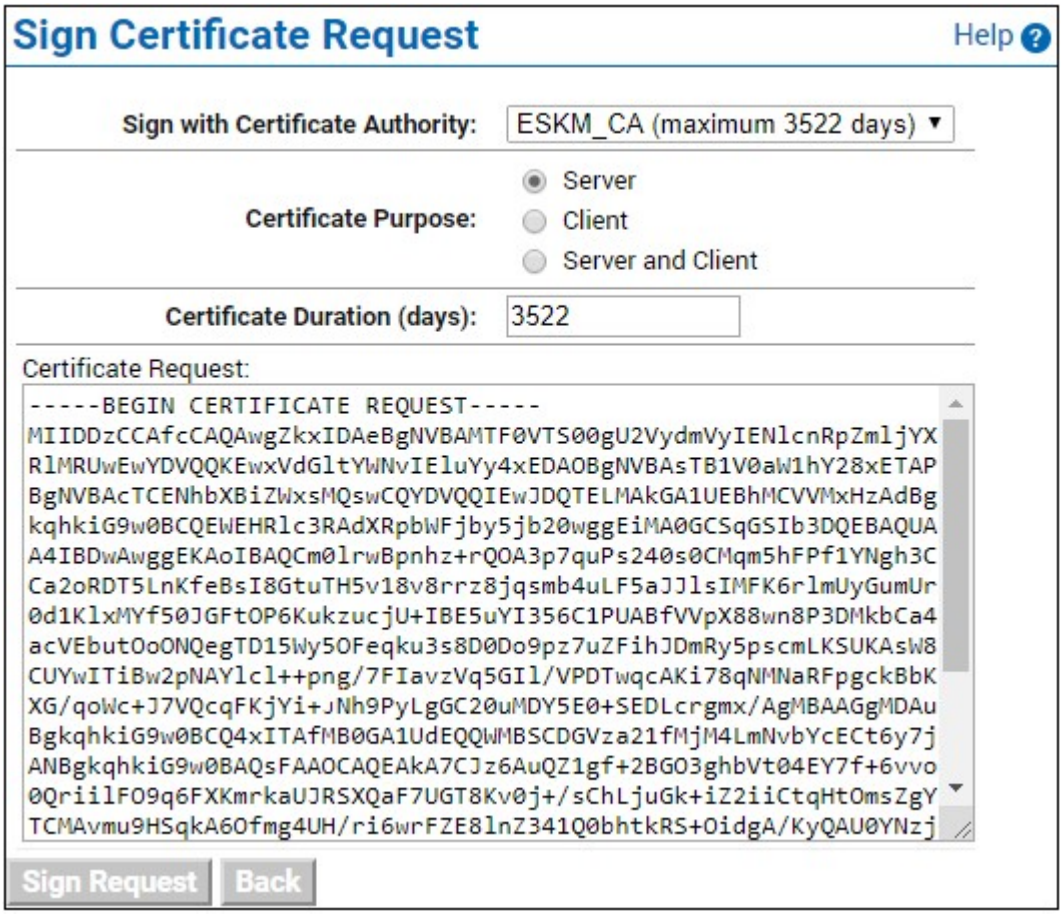

Figure 4 : Sign Certificate Request window

a) Select the CA name from the Sign with Certificate Authority drop down box. For example, ESKM Local CA.

b) Select Server as the Certificate Purpose.

c) Enter the number of days before the certificate must be renewed based on your site's security policies. The default value is 3649 days (10 years).

10. Click Sign Request.
11. In the Certificates & CAs menu, click on Certificates.

12. Click on the certificate name created in step 3 of this section. For example, ESKM KMS Server.
13. Click Install Certificate.
14. Paste the signed certificate data from step 12, and then click Save. Note that the Certificate status is now Active.

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.

5.3.1 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:

›_ Console

```
-----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.

5.4 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 cluster is already setup, then skip Section **5.5 Setup KMIP Server**.

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

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

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

5.4.1 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.

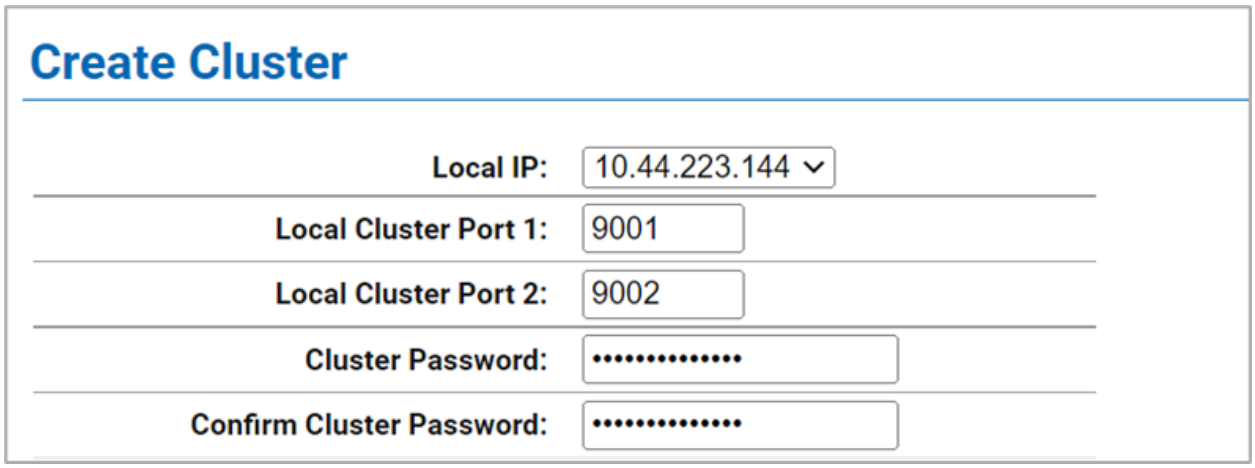

Figure 5 : Create Cluster window

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.

5.4.2 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.

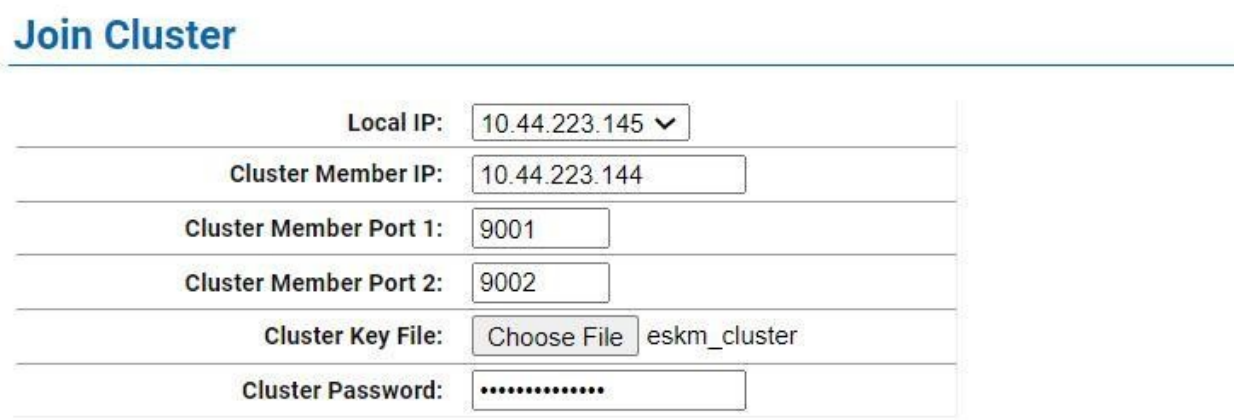

Figure 6 : Join Cluster window

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.

5.5 Setup KMIP Server

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.

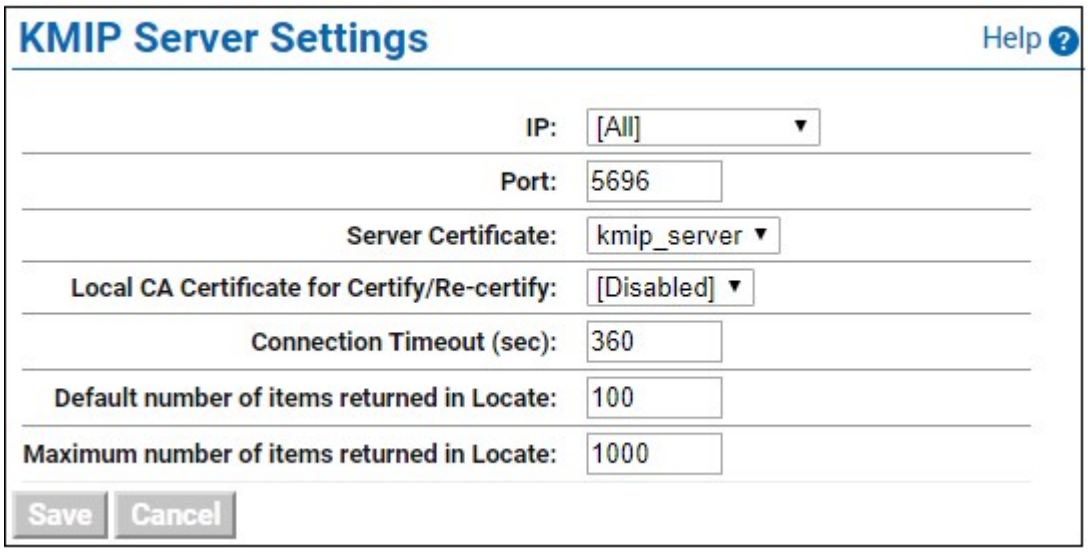

Figure 7 : KMIP Server Setting window

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.

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

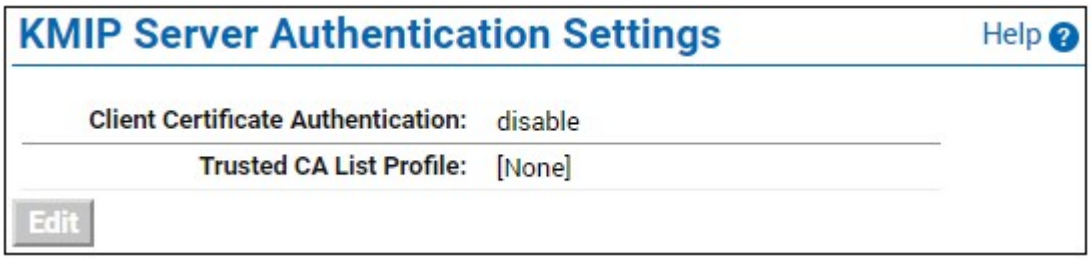

Figure 8 : KMIP Server Authentication Setting window

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

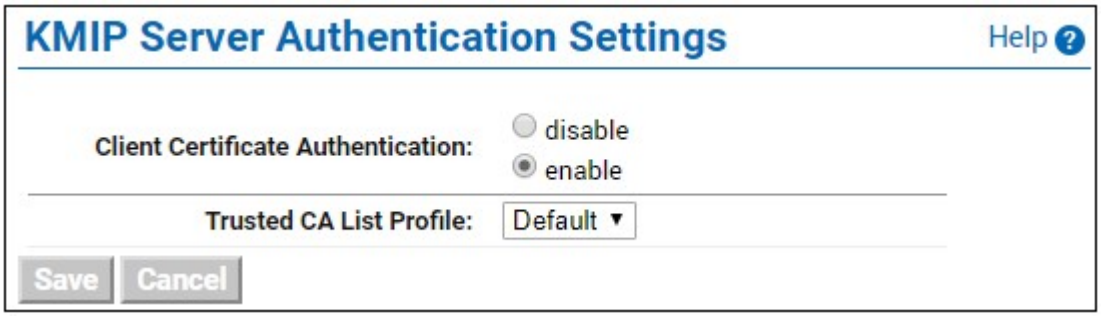

Figure 9 : KMIP Server Authentication Setting window

6 Client Certificate for MySQL

This section provides the step-by-step procedure for creating a client certificate for integrating ESKM with MySQL server.

The following steps provide a high-level overview of the process to configure communication between MySQL and the ESKM system.

1. Configure the ESKM server, including:
    a. Configure the KMIP server settings.
2. Create KMIP user and password.
3. Connect MySQL to the ESKM server.

6.1 Configure the ESKM Server

This process begins with ensuring that Utimaco's Enterprise Secure Key Manager (ESKM) appliance is set up and configured correctly.

6.2 Configure the KMIP Server Settings

For more information about configuring the KMIP server settings, refer to Setup KMIP server.

For "Server Certificate", under the Server Certificate drop-down, it shall be ESKM_server_cert in this case.

The KMIP server is now configured to use the server certificate.

6.3 Create Client Certificate Using ESKM

6.3.1 Client Certificate On Linux

1. Login to the Management Console, and navigate to Security > Certificates and CAs > LocalCA.
2. Select certificate.

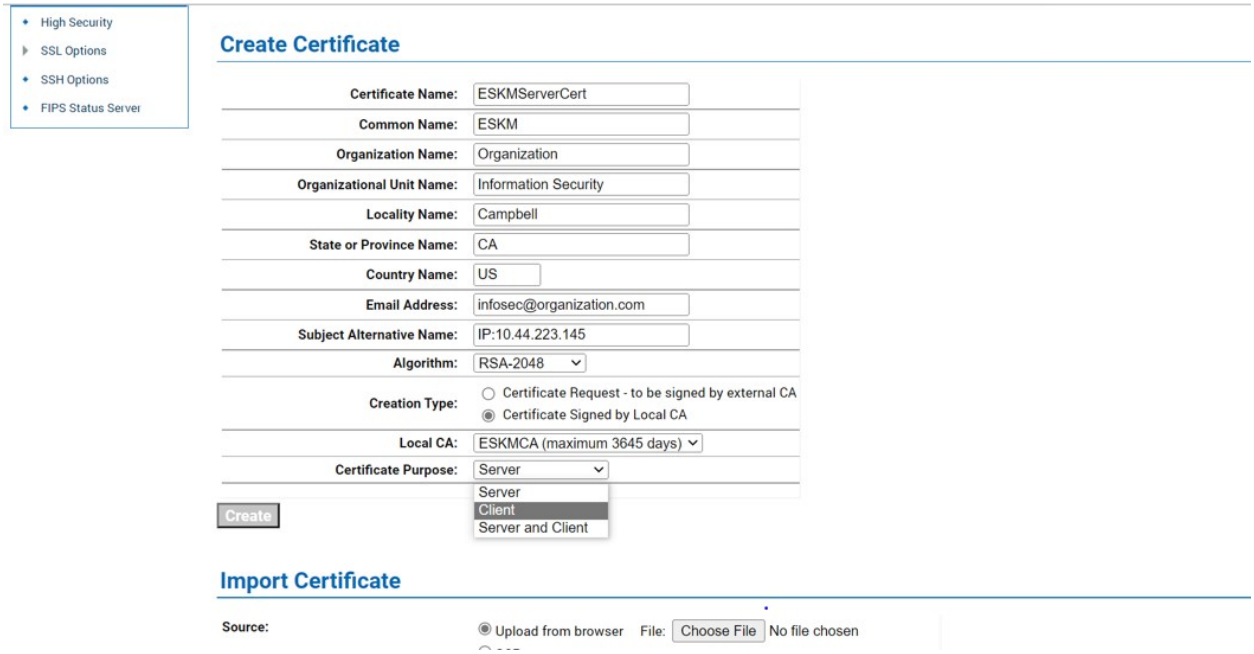

Figure 10 : Create Certificate window

The Common Name must match the name of the KMIP user (in these examples, this is KMIP_client).

3. After crating the certificate with a local CA, click on Download to download the file.
4. Save as the correct name; in this case, /home/user/cert.pem.

6.3.2 Client Certificate On Windows

For the windows, execute the same steps from 1 to 3 from On Linux section and then follow the below steps.

Create mysql-keyring-okv folder in following location C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv folder and allow following permission to the folder.

1. After creating the mysql-keyring-okv folder in C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv right-click, then Properties -> Security, then Edit -> Add etc.
2. Once the user is added check "Modify" in addition to Read & execute, List folder contents, Read and Write.
3. Also, Grant modify access to MySQL folder inside Program Files and restart the MySQL services.

4. Save the CA, which was downloaded in step 3, as CA.pem on C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv\ssl location.

6.3.3 Export Certificate with Private Key from ESKM

This topic is similar for both Linux and windows operating systems.

1. Enter the password to export the key.

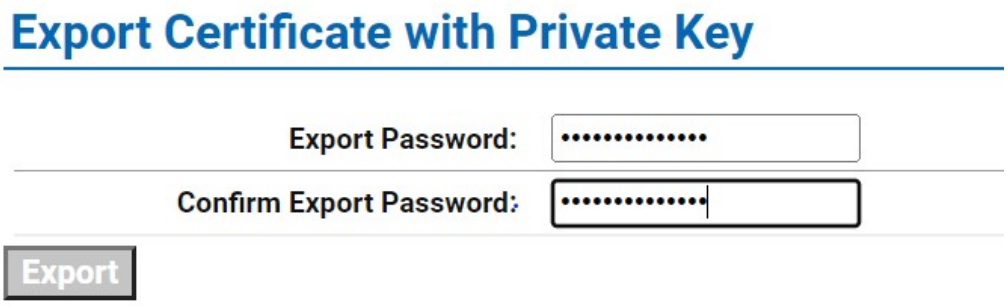

Figure 11 : Export Certificate with Private Key window

2. Converting PKCS#12 key into PEM using OpenSSL.

›_ Console

```
openssl pkcs12 -in <key name.p12> -nodes -nocerts | openssl rsa -out key.pem
```

6.4 Create a Client Certificate and Key (Using openssl)

6.4.1 Create a CSR on the Client

1. The certificate signing request (CSR) is created on the machine running the client.

Before performing this step, ensure that OpenSSL is already installed on your system.

2. Using OpenSSL, create a private key, using the commands and syntax shown below. This example shows the creation of a 2048-bit RSA key.

›_ Console

```
#openssl genrsa -out KMIP_client.key 2048
```

The following output appears:

›_ Console

```
Generating RSA private key, 2048 bit long modulus

.........................+++

.........................+++

e is 65537 (0x10001)
```

3. Generate a certificate signing request (CSR) using the private key.

›_ Console

```
openssl req -config "<path>openssl.cnf" -new -key KMIP_client.key >

KMIP_client.csr
```

The following output appears:

›_ Console

```
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields, there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
...
```

4. Enter the information in the fields as prompted.

Field	Example
Country Name	USA
State Name	CA
Locality Name	Campbell
Organization Name	Organization
Organization Unit Name	Information Security
Common Name	ESKM
Email Address	infosec@organization.com

Table 6: Certification Information

The Common Name must match the name of the KMIP user.

5. You are then prompted to add other parameters, such as a “challenge password” or

“optional company name”. To skip those parameters, press Enter.

This process creates a certificate request file called KMIP_client.csr. It also creates a private key file called KMIP_client.key.

6. Download `KMIP_client.key` file to client system with correct name; in this case,

`/var/lib/mysql/mysql-keyring-okv/ssl/key.pem`.

For Windows, execute the steps 1 to 5 from **Create a CSR on the client** section and then follow step 7.

7. Download and save `KMIP_client.key` file in C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv\ssl location as `key.pem`.

6.4.2 Use the Local CA to Sign CSR

The CSR now needs to be signed by the local CA.

1. Using a text editor (or using the more <filename> command), open the KMIP_client.csr file.
2. Select the entire text and copy to your clipboard.
3. Now, login to the Management Console and navigate to Security > Certificates & CAs > Local Cas

Be sure to include the first and last lines (-----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST----).

4. Select the CA used by your ESKM (in this case, LocalCA), and click Sign Request. The Sign Request window appears.

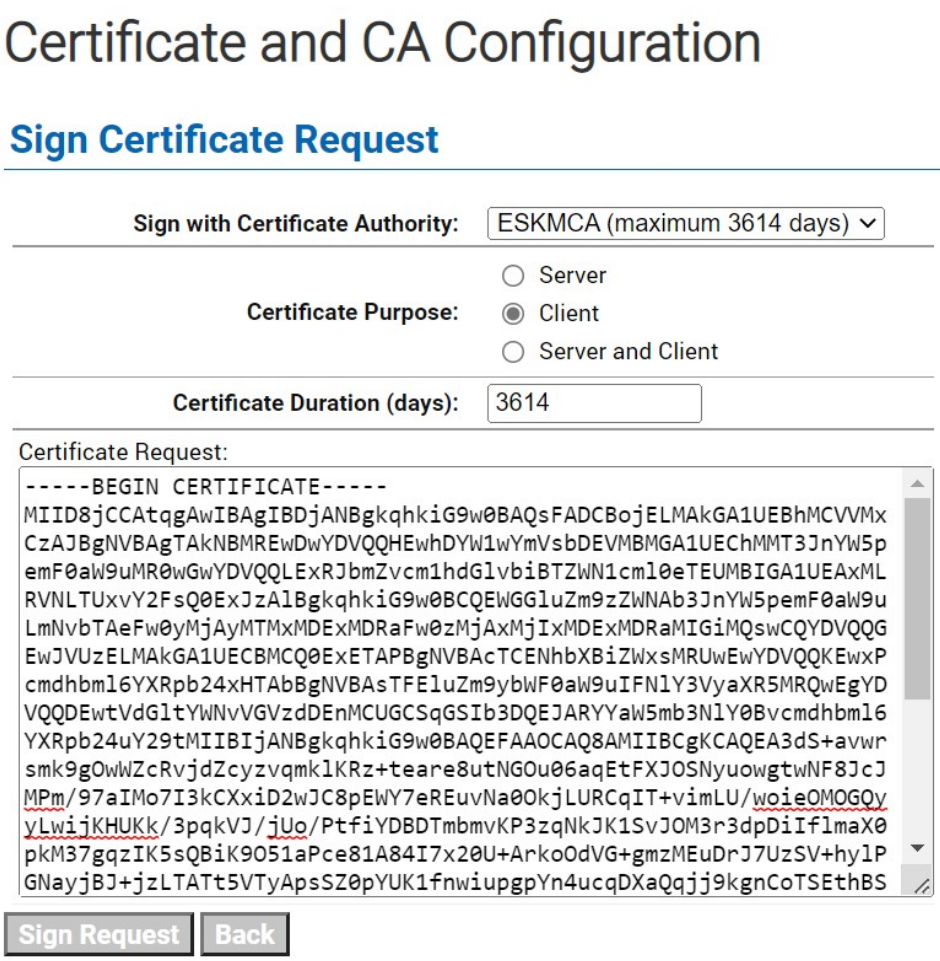

Figure 12 : Sign Certificate Request window

5. For Certificate Purpose, select Client.
6. Paste the CSR text that you have copied to your clipboard (Step 2 above) into the Certificate Request window.
7. Click Sign Request. The signed client certificate now appears.

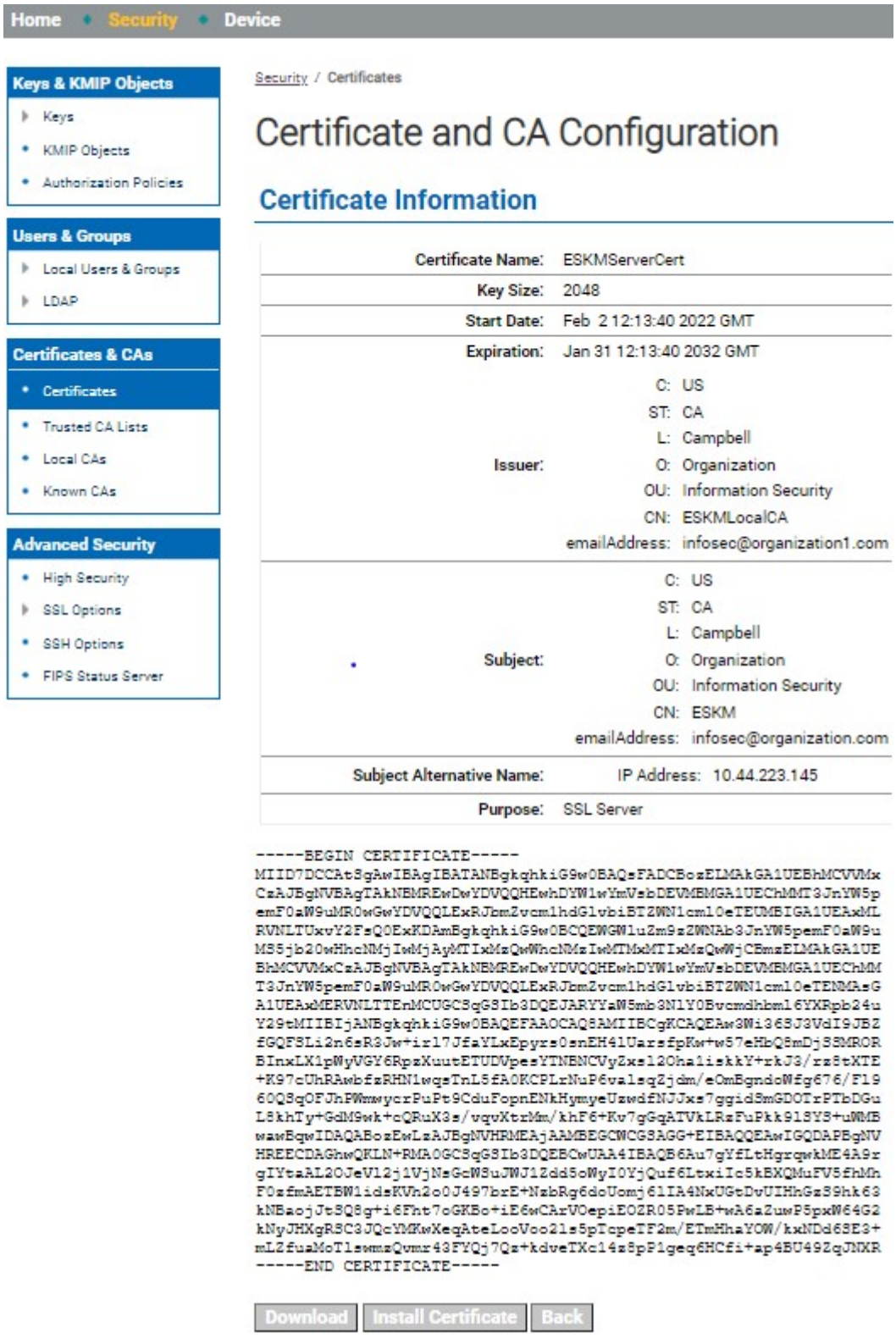

Figure 13 : Certificate Information window

8. After signing the certificate request with a local CA, click on Download to download the file.

9. Save as the correct name; in this case, `/var/lib/mysql/mysql-keyringokv/ssl/cert.pem`

For Windows, execute the steps 1 to 8 from **Use the local CA to sign CSR** section and then follow step 10.

10. Save as the correct name; in this case, C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv\ssl - > `cert.pem`

7 KMIP User and Password

Create the user — an individual (client) on the ESKM server, in this case, KMIP_client.

A client license is required for each user created on the ESKM server. Refer to the ESKM Installation and Replacement Guide for information about how to request and install the license pack.

1. Login to the Management Console, and navigate to Security > Local Users & Groups > Local Users.
2. At the bottom of the list, click Add. The Create Local User window appears.
3. Create a “username” and “password” for the KMIP user.

The “Username” must match with the “Common Name (CN)” provided during the client certificate creation.

4. Select “permissions” for this user.
5. Click the Enable KMIP option.
6. If required, from the drop-down lists, select the User and Object group to which the user belongs. In this case, Company-group_user and Company-group.
7. Paste the signed client certificate request, still on your clipboard from Step 8 above, into the KMIP Client Certificate field. (If it isn’t on your clipboard, open KMIP_client.pem and recopy it).

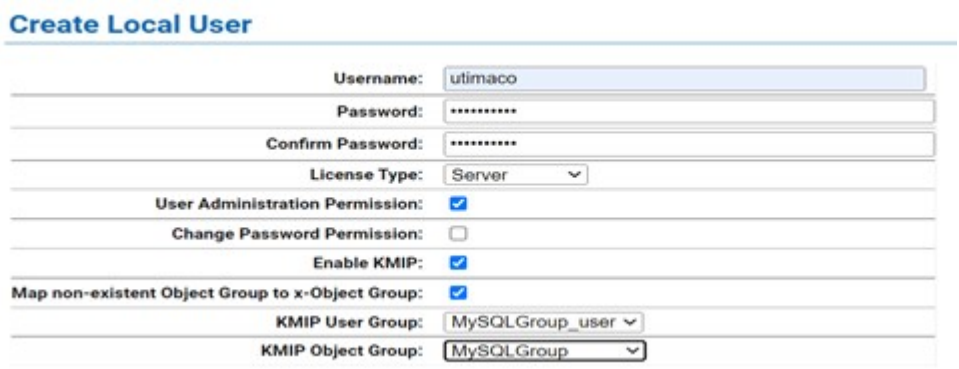

Figure 14 : Create Local User window

8. Click Create.

The user KMIP_client now appears on the list of Local Users.

The configuration of the ESKM server is now complete.

8 Installation keyring_okv Plugin

8.1 About keyring_okv Plugin

The keyring_okv plugin is a KMIP 1.1 plugin for KMIP-compatible back-end keyring storage products, such as ESKM KeyStore. It is available in MySQL Enterprise Edition distributions.

8.1.1 keyring_okv Plugin On Linux

The configuration directory used by keyring_okv as the location for its support files should have a restrictive mode and be accessible only to the account used to run the MySQL server. For example, on Unix and Unix-like systems, to use the /var/lib/mysql/mysql-keyringokv directory, the following commands, executed as root,

1. Create the directory and set its mode and ownership.

›_ Console

```
cd /var/lib
# mkdir -p mysql/mysql-keyring-okv/ssl
# chmod -R 750 mysql
# chown -R mysql mysql
# chgrp -R mysql mysql
```

2. To be usable during the server startup process, keyring_okv must be loaded using the -early-plugin-load option. Also, set the keyring_okv_conf_dir system variable to tell keyring_okv where to find its configuration directory. Edit the /etc/my.cnf file and add the plugin into the mysqld section.

›_ Console

```
[mysqld]
early-plugin-load=keyring_okv.so
keyring_okv_conf_dir=/var/lib/mysql/mysql-keyring-okv
```

3. Make sure you have Downloaded the CA.pem, cert.pem, and key.pem to our MySQL client under the SSL directory and give permission with mysql.

›_ Console

```
#chown mysql:mysql ssl -R
#chmod 755 ssl -R
```

4. In the configuration directory, create a file named okvclient.ora. It should have following format:

›_ Console

```
SERVER=xxx.xxx.xxx.xxx:5696
STANDBY_SERVER=xxx.xxx.xxx.xxx:5696
STANDBY_SERVER is optional.
Example:
SERVER=10.44.223.144:5696
STANDBY_SERVER=10.44.223.145:5696
```

5. Set the permissions on these files.

›_ Console

```
cd /var/lib/mysql/mysql-keyring-okv/okvclient.ora
chmod -R 750 okvclient.ora
chown -R mysql:mysql okvclient.ora
```

6. After completing the preceding procedure, restart the MySQL server. It loads the keyring_okv plugin and keyring_okv uses the files in its configuration directory to communicate with ESKM.

7. Verify that the keyring_okv plugin is working.

mysql›

```
mysql> SELECT PLUGIN_NAME, PLUGIN_STATUS FROM INFORMATION_SCHEMA.PLUGINS WHERE
PLUGIN_NAME LIKE 'keyring%';
```

8.1.2 keyring_okv Plugin On Windows

The configuration directory used by keyring_okv as the location for its support files should have a restrictive mode and be accessible only to the account used to run the MySQL server. For example, on Windows-like systems, to use the

Create mysql-keyring-okv folder in following location C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv folder and allow following permission to the folder.

1. After creating the mysql-keyring-okv folder in C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv right-click, then Properties -> Security, then Edit -> Add etc.
2. Once the user is added check "Modify" in addition to Read & execute, List folder contents, Read and Write.
3. Also, Grant modify access to MySQL folder inside Program Files.
4. Restart the MySQL server after making above changes.
5. To be usable during the server startup process, keyring_okv must be loaded using the -early-plugin-load option. Also, set the keyring_okv_conf_dir system variable to tell keyring_okv where to find its configuration directory.

›_ Console

```
[mysqld]
early-plugin-load=keyring_okv.dll
keyring_okv_conf_dir=" C:\Program Files\MySQL\MySQL Server 8.0\mysql
keyring-okv”
```

Edit the C:\ProgramData\MySQL\MySQL Server 8.0\my.ini file and add the plugin into the mysqld section.

6. Download the CA.pem, cert.pem to our MySQL server under the SSL folder.

7. In the configuration directory, create a file named okvclient.ora. It should have following format:

›_ Console

```
SERVER=xxx.xxx.xxx.xxx:5696
STANDBY_SERVER=xxx.xxx.xxx.xxx:5696 STANDBY_SERVER is optional.
Example:
SERVER=10.44.223.144:5696
STANDBY_SERVER=10.44.223.145:5696
```

8. Set the mysql permissions on the file.

C:\Program Files\MySQL\MySQL Server 8.0\mysql-keyring-okv\okvclient.ora

9. After completing the preceding procedure, restart the MySQL server. It loads the keyring_okv plugin and keyring_okv uses the files in its configuration folder to communicate with ESKM.

10. Verify that the keyring_okv plugin is working.

mysql›

```
mysql> SELECT PLUGIN_NAME, PLUGIN_STATUS FROM INFORMATION_SCHEMA.PLUGINS WHERE
PLUGIN_NAME LIKE 'keyring%';
```

9 KMIP Object Verification

Verify that the new object, a symmetric key with the owner KMIP_client was created.

1. Use keyring_okv plugin to create encrypted tables. When you create the first encrypted table, InnoDB will ask keyring_okv to generate primary key (AES-256) in ESKM. You can check this in the ESKM Web UI in KMIP Objects. This primary key is used to encrypt tablespace keys. InnoDB also asks ESKM to generate a key (AES-256) for encrypting table. The tablespace key is wrapped using the primary key and stored alongside the encrypted table. For subsequent encrypted tables, only the tablespace key is generated, and the same primary key is used to wrap the tablespace key.

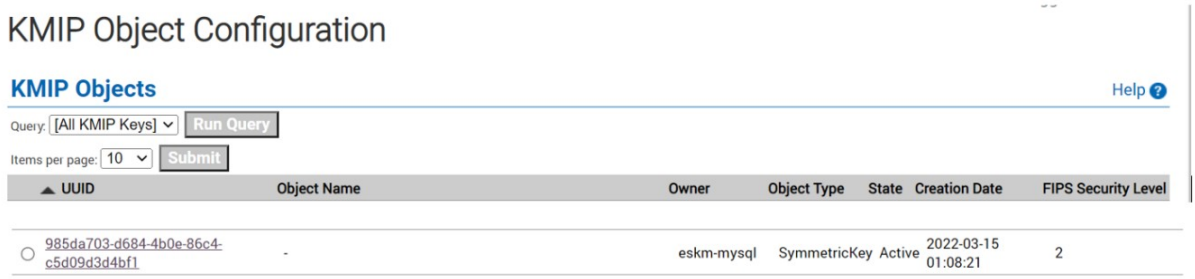

Figure 15 : KMIP Object Configuration window

2. Here is an example of how you create an encrypted table.

mysql›

```
SQL> CREATE DATABASE MySQL_TDE_Test;
USE MySQL_TDE_Test;
CREATE TABLE `test_encryption` (
`id` int(10) unsigned NOT NULL AUTO_INCREMENT,
`name` varchar(15) NOT NULL,
PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=1 DEFAULT CHARSET=latin1 ENCRYPTION = 'Y';
```

10 Troubleshooting

Error	Diagnosis
Unable to encrypt the tables and there is not any action under ESKM. Also, we have checked the error logs of mysql and found below logs. [ERROR] [MY-012657] [InnoDB] Encryption can't find master key, please check the keyring is loaded. [ERROR] [MY-012226] [InnoDB] Encryption information in datafile: . \mysql_tde_test\test_encryption.ibd can't be decrypted, please confirm that keyring is loaded.	▪ We must take care that during the server startup process, keyring_okv must be loaded using the--early-plugin-load option. ▪ Also, set the keyring_okv_conf_dir system variable to tell keyring_okv where to find its configuration directory. Edit the /C:\Program Data\MySQL\MySQL Server 8.0/my.ini file and add the plugin into the mysqld section. ▪ Restarted the MySQL services. Hence issue got resolved.

Table 7: List of Errors and their Diagnoses

11 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All ESKM product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

12 References

Reference	Title/Company
[ESKMIRG]	ESKM_Installation and Replacement_Guide.pdf
[ESKMUG]	ESKM_User_Guide.pdf

Table 8: References

13 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.