Dell

PowerEdge Servers

Integration Guide

Utimaco ESKM

utimaco®

Imprint

Copyright 2020	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 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	06/10/2025
Status	**PUBLISHED**
Document No.	IG-2025-0016

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 website at https://utimaco.com/

1.1 About This Guide

This guide provides an integration guide explaining how to integrate an Utimaco ESKM with Dell PowerEdge Servers. Utimaco ESKM securely generates and manages keys that can then be used by iDRAC to lock and unlock storage devices on a Dell PowerEdge server. iDRAC requests the ESKM to create a key for each storage controller, and then fetches and provides that key to the storage controller on every host boot so that the storage controller can then unlock the Self-Encrypting Drives.

1.1.1 Target Audience for This Guide

This guide is intended for administrators of Dell PowerEdge Servers and of Utimaco ESKM.

1.1.2 Contents of This Guide

After the introduction this guide is divided up as follows:

Chapter 2 Overview

Chapter 3 Integration Requirements and Prerequisites

Chapter 4 Installing and Configuring Utimaco ESKM Server

Chapter 5 Integrating Dell PowerEdge Servers with Utimaco ESKM

Chapter 6 Troubleshooting

Chapter 7 Further Information

1.1.3 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 [ESKMIRG].

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

1.1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning

BMC	Baseboard Management Controller
CA	Certificate Authority
CN	Common Name
CSADM	CryptoServer Command-line Administration Tool
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
ESKM	Enterprise Secure Key Manager
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
iDRAC	Integrated Dell Remote Access Controller
IP	Internet Protocol
KMIP	Key Management Interoperability Protocol
KMS	Key Management System
OU	Organizational Unit

PEM	Privacy Enhanced Mail
SED	Self-Encrypting Drive
SEKM	Secure Enterprise Key Manager
URL	Uniform Resource Locator
VT	Virtualization Technology
XML	Extensible Markup Language

Table 2: List of Abbreviations

2 Overview

2.1 Dell PowerEdge Servers

Dell provides the OpenManage Secure Enterprise Key Manager (SEKM) that assists iDRAC (the Dell PowerEdge server BMC) in securing storage devices on a PowerEdge server. OpenManage SEKM enables you to use an external Key Management Server (KMS) to manage keys that can then be used by iDRAC to lock and unlock storage devices on a Dell PowerEdge server. iDRAC requests the KMS to create a key based on iDRAC Key Policy, and then fetches and provides that key to the storage controller on every host boot so that the storage controller can then unlock the SEDs.

2.2 Utimaco 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 businesscritical, 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 the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco ESKM with following Storage Controllers.

Storage controller	Minimum firmware version required	Utimaco ESKM Version
PERC H965i Front	8.0.0.0.18-81	ESKM 8.4.0 or later
PERC H965i Adapter	8.0.0.0.18-81	ESKM 8.4.0 or later
PERC H755 Front	52.16.1-4074	ESKM 8.4.0 or later
PERC H755N Front	52.16.1-4074	ESKM 8.4.0 or later
PERC H755 Adapter	52.16.1-4074	ESKM 8.4.0 or later
PERC H750 Adapter	52.16.1-4074	ESKM 8.4.0 or later
PERC H740P Mini	51.13.2-3714	ESKM 8.4.0 or later
PERC H740P Adapter	51.13.2-3714	ESKM 8.4.0 or later
BOSS-N1 Monolithic	2.1.13.2017	ESKM 8.4.0 or later
BOSS-N1 Modular	2.1.13.2017	ESKM 8.4.0 or later

HBA 355i Adapter (VxRail platforms only)	17.15.08.00	ESKM 8.4.0 or later
HBA 355i Front (VxRail platforms only)	17.15.08.00	ESKM 8.4.0 or later

Table 3: List of Tested Versions

3.2 Hardware Requirements

Hardware	Hardware Requirements
ESKM	8.4.0 or later
RAM	6 GB of RAM for one instance of the simulator
RAM	12 GB of RAM for two instances of the simulator
Disk Space	40 GB of free disk space for each instance of the simulator
VT	VT support for Intel system

Table 4: 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/

3.3 Prerequisites

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

- Storage Controller listed in Tested Versions

- ESKM listed in Tested Versions
- PowerEdge Server Prerequisites:
  - iDRAC SEKM license installed.
  - iDRAC Data Center or iDRAC Enterprise license
  - iDRAC updated to the firmware version which supports SEKM.
  - Supported storage devices updated to the firmware version which supports SEKM.

4 Installing and Configuring Utimaco ESKM Server

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 Section Setting up Local CA

4.1 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 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

j) **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.

k) Web interface port number.

l) 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 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.

4.2 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
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

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.

4.2.1 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

4.3 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 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

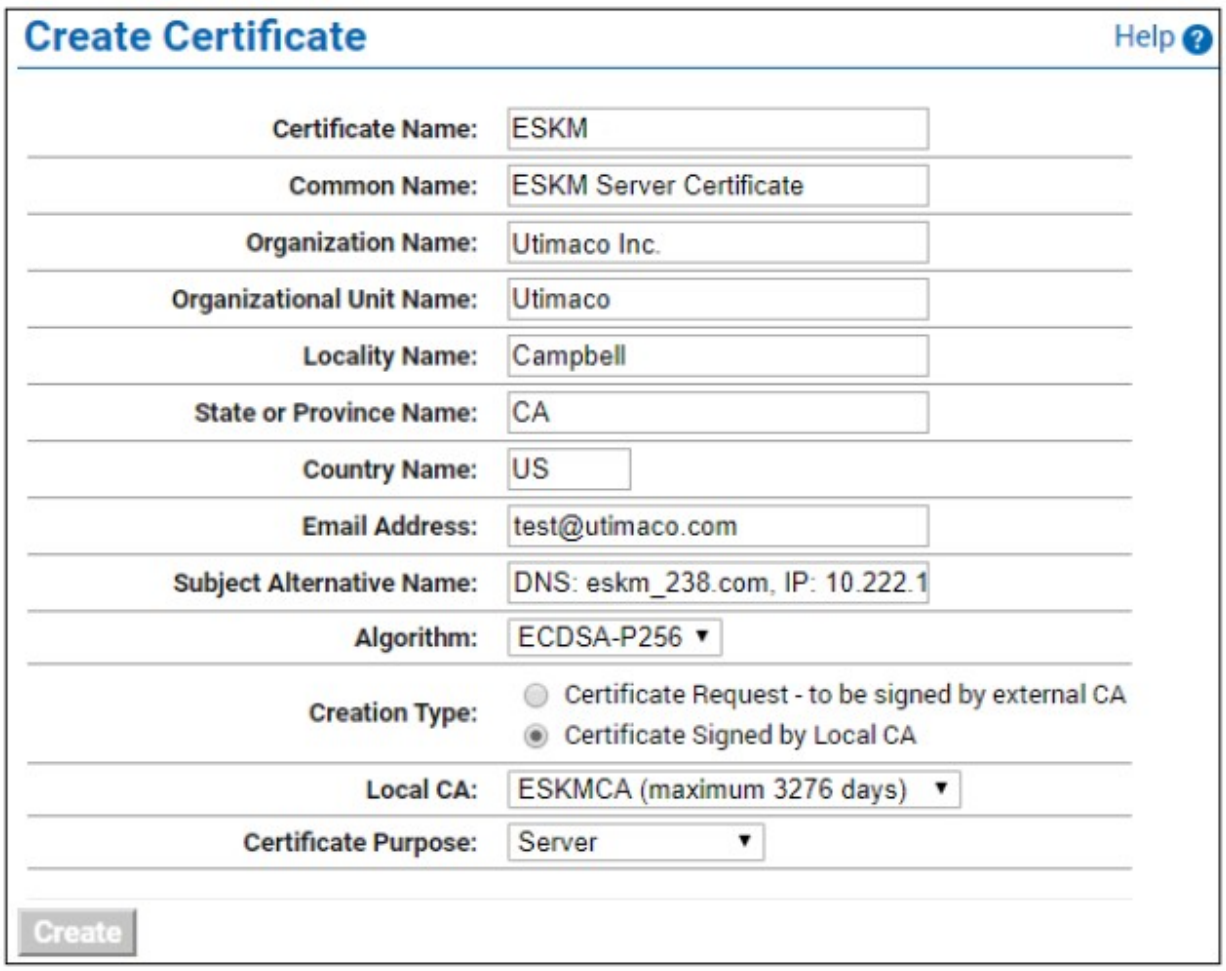


Figure 2: Create Certificate window

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

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 Server Certificate

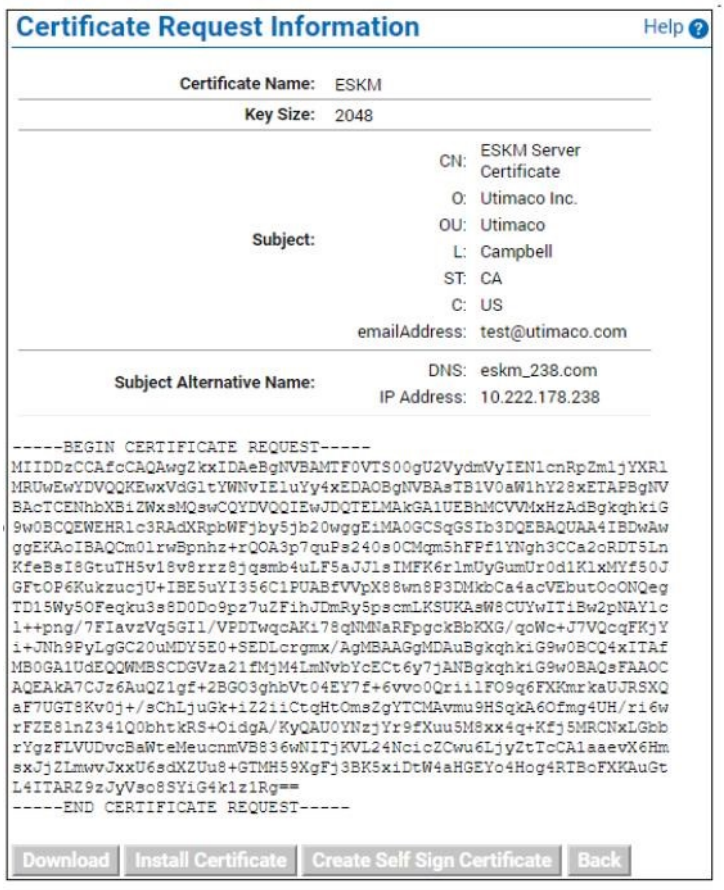


Figure 3: Certificate Request Information window

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

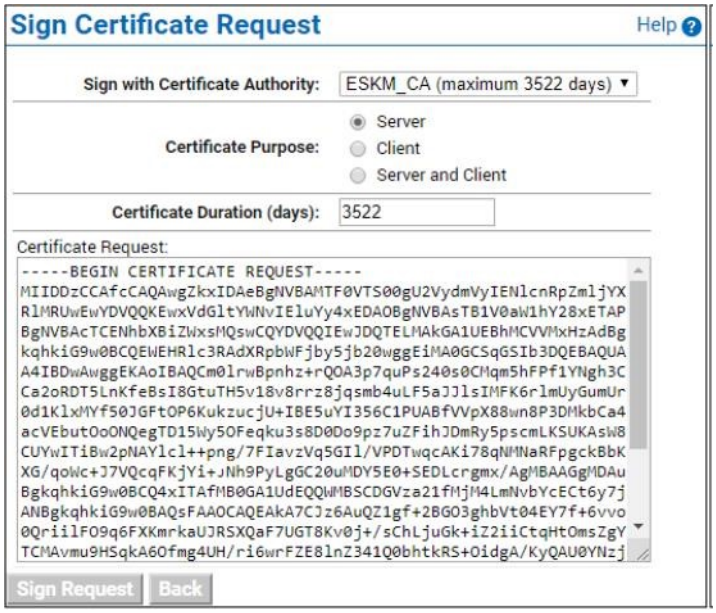


Figure 4: Sign Certificate Request window

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 Server Certificate
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 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.

4.3.1 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

4.4 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 4.5 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.

4.4.1 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

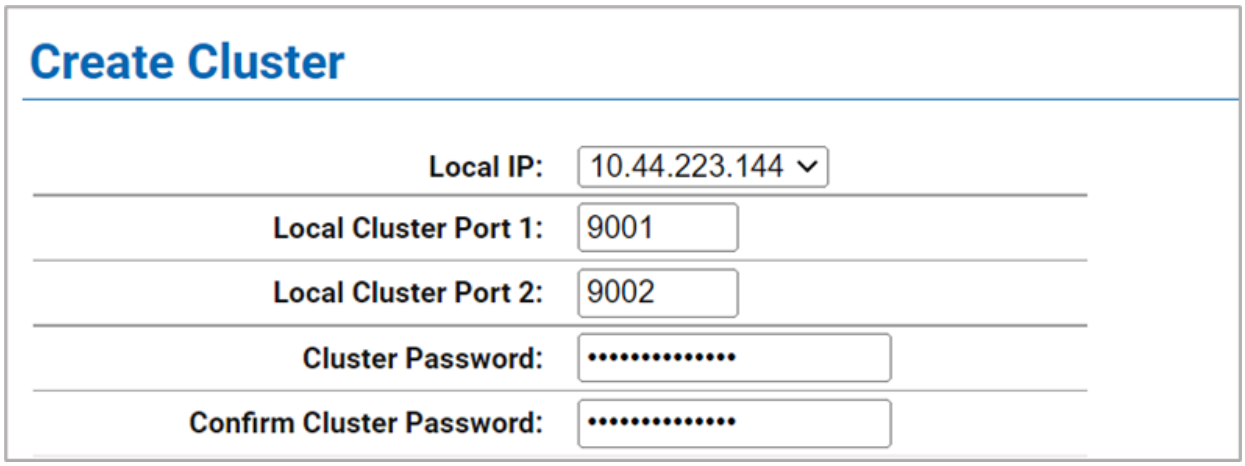


Figure 5: Create Cluster window

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

4.4.2 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.

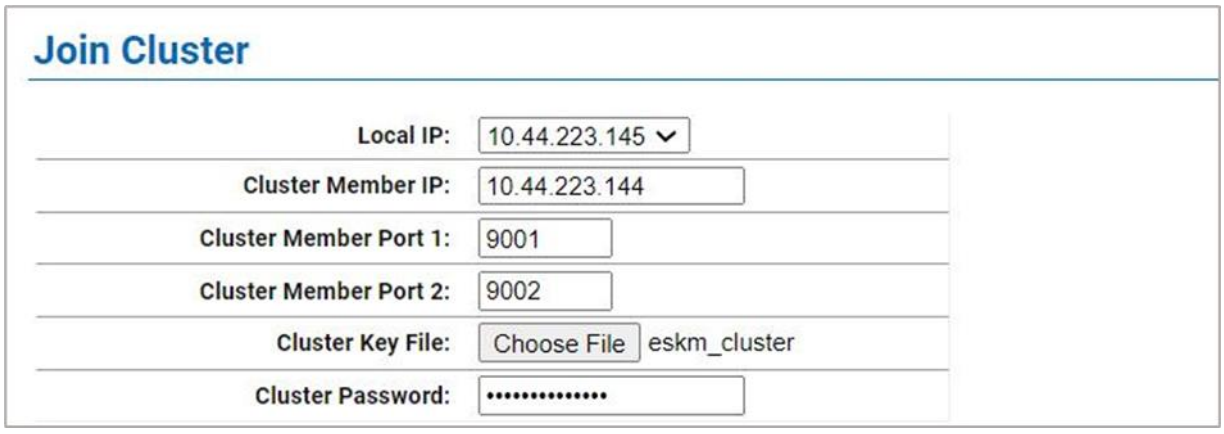


Figure 6: Join Cluster window

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

4.5 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.

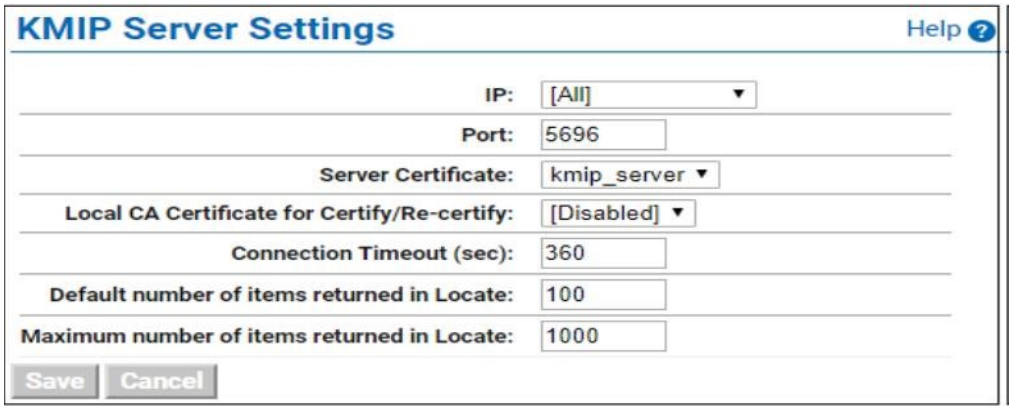


Figure 7: KMIP Server Setting window

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

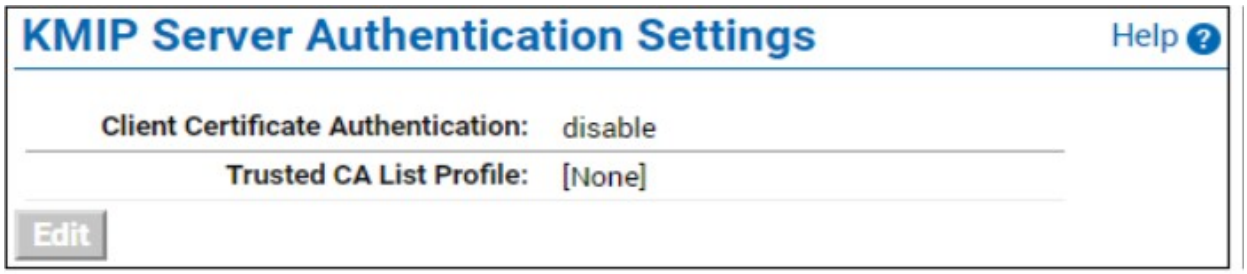


Figure 8: KMIP Server Authentication Setting window

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

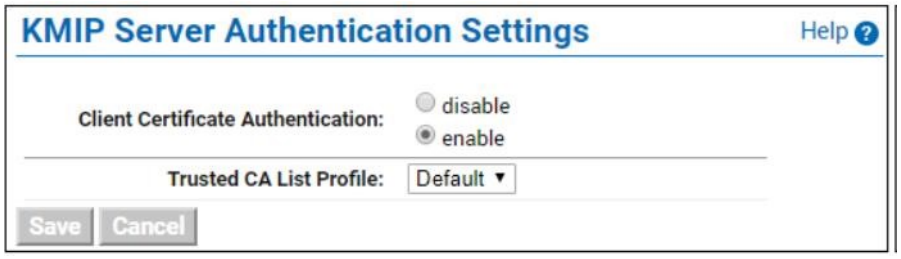


Figure 9: KMIP Server Authentication Setting window

5 Integrating Dell PowerEdge Servers with Utimaco ESKM

You need to complete the following steps to integrate Dell PowerEdge Servers with Utimaco ESKM.

5.1 Set up SEKM on iDRAC

Licensing and firmware update

SEKM is a licensed feature with the iDRAC Enterprise license as a pre-requisite. To avoid an additional iDRAC firmware update, it is recommended that the SEKM license is installed first and then the iDRAC firmware is updated to a version that supports SEKM. This is because an iDRAC firmware update is always required after the SEKM license is installed irrespective of whether the existing firmware version supports SEKM or not. The existing interface methods for installing license and firmware update can be used for SEKM.

Set up SSL certificate

The SEKM solution mandates two-way authentication between the iDRAC and the ESKM. iDRAC authentication requires generating a CSR on the iDRAC and then getting it signed by a CA on the ESKM and uploading the signed certificate to iDRAC. For ESKM authentication, the ESKM CA certificate must be uploaded to iDRAC.

Generate iDRAC CSR

Though most of the CSR properties are standard and self-explanatory, here are a few important guidelines:

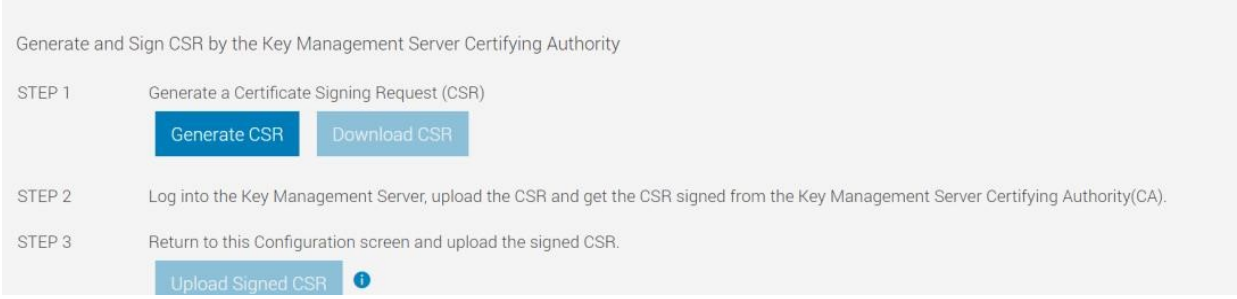
If the “Username Field in Client Certificate” option on the ESKM is enabled, then ensure that the iDRAC account username on the ESKM is entered in the correct field (CN or OU or ESKM User ID) that matches the value selected in the ESKM.

If the **Require Client Certificate to Contain Source IP** field is enabled on the KMS then enable the “iDRAC IP Address in CSR” field during the CSR generation.

5.2 Configure SEKM by using the iDRAC GUI

1. Start iDRAC by using any supported browser
2. From iDRAC **Dashboard** -> **Storage** -> **SEKM**

3. Click **Generate CSR**



Download CSR option will become available after generating a CSR.

4. In the **Generate Certificate Signing Request (CSR)** dialog box, select or enter data
5. Click **Generate**. The CSR file is generated. Save it to your system

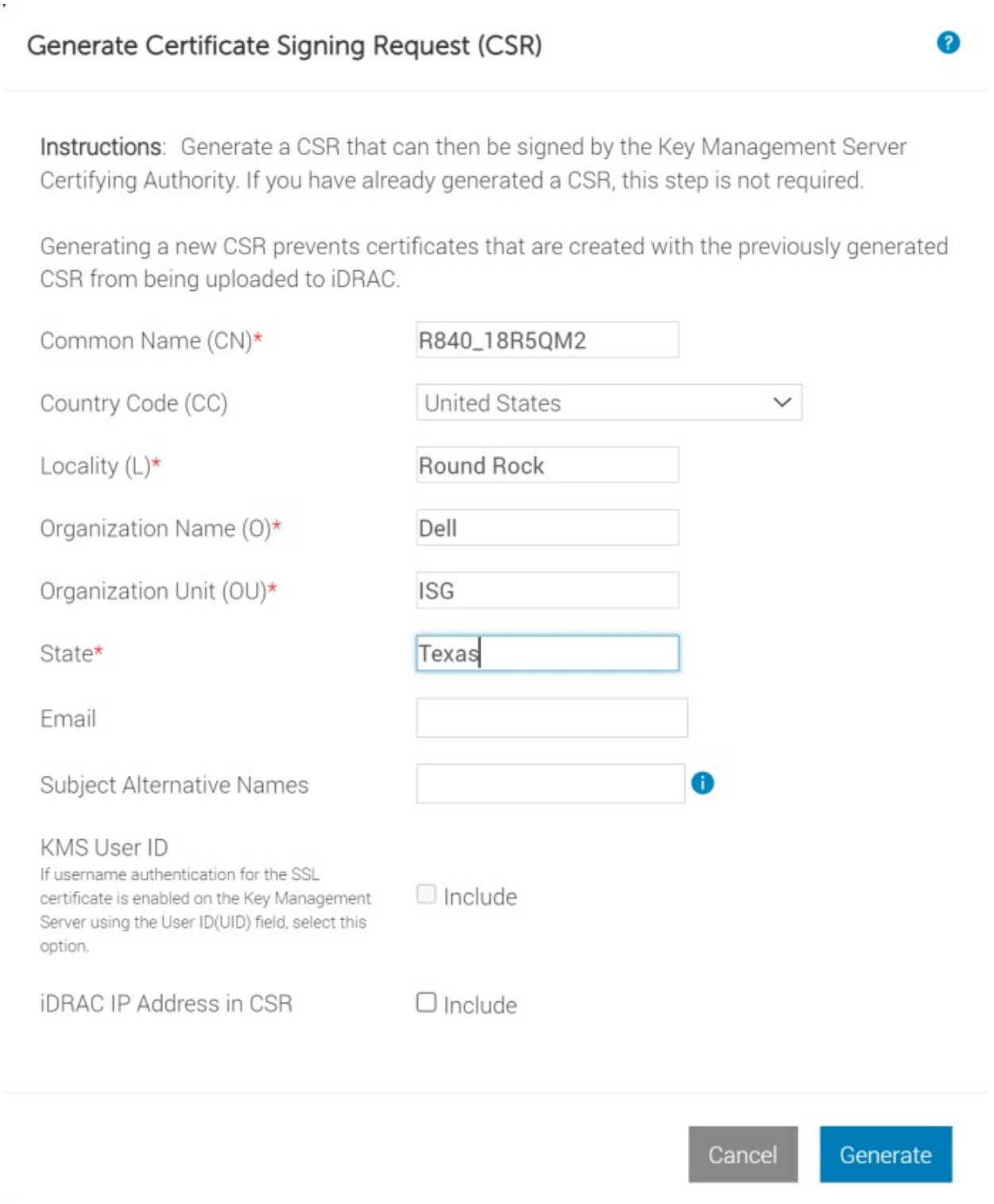


Figure 11: Supplying details for CSR

5.3 Signing the CSR file on Utimaco ESKM

1. Copy the CSR file to Utimaco ESKM

›_ Console

-----BEGIN CERTIFICATE REQUEST-----

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV i/
OyLyeJ7l1SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae LPXSqhw/
kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z

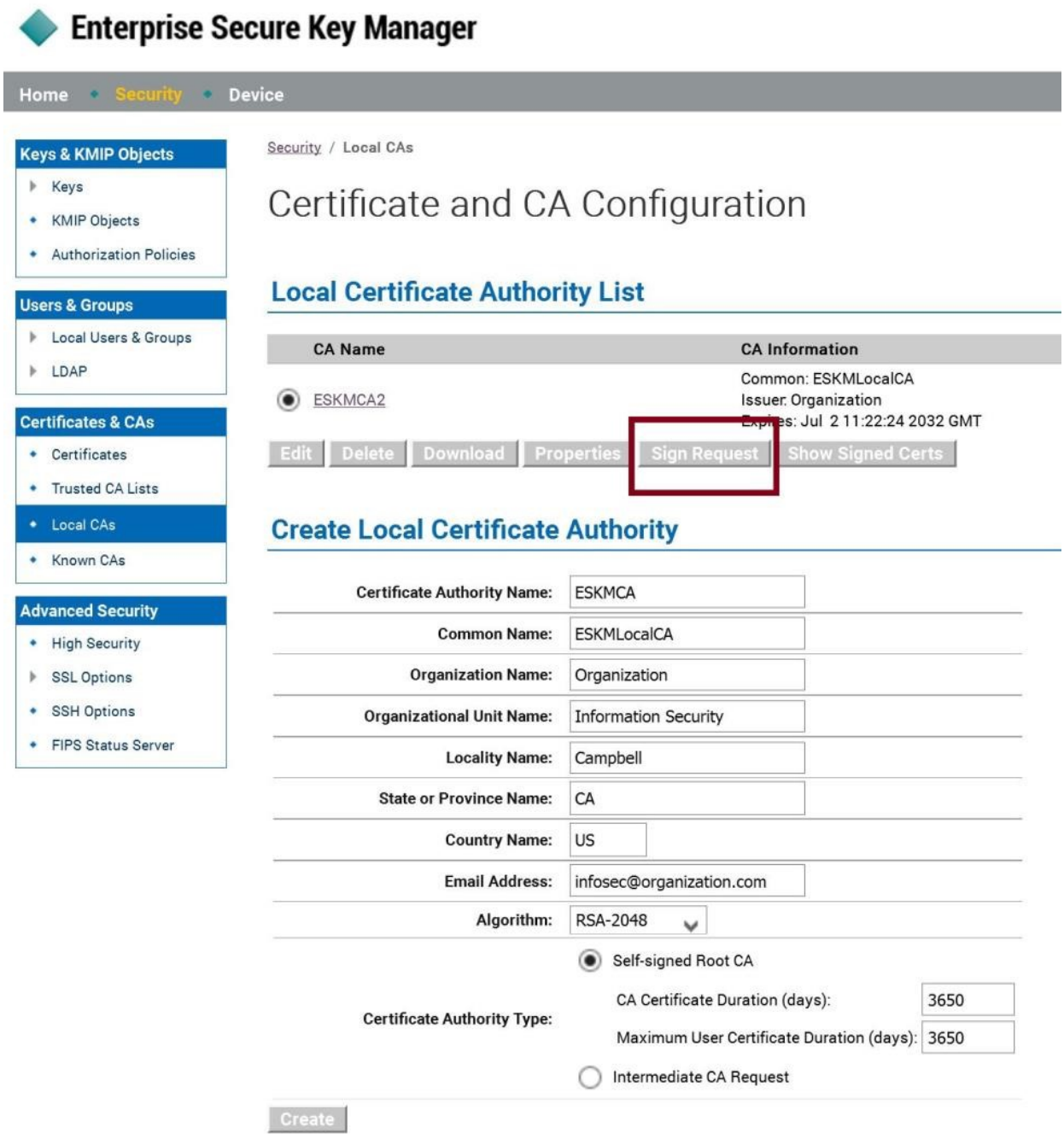
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg

5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw

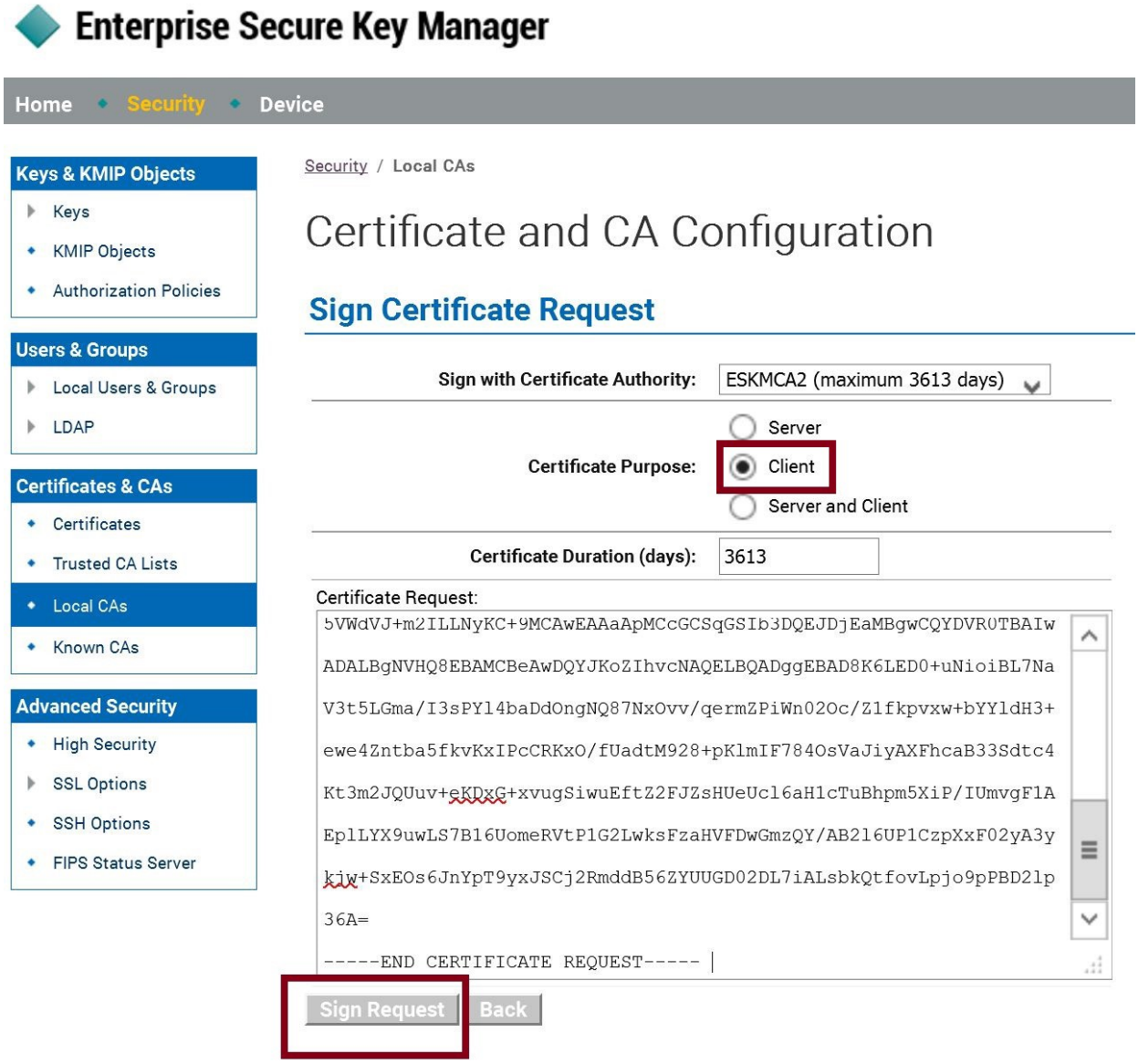
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB2l6UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp 36A=

-----END CERTIFICATE REQUEST-----

2. Click **Security Tab → Local CAs.** Click **Sign Request**



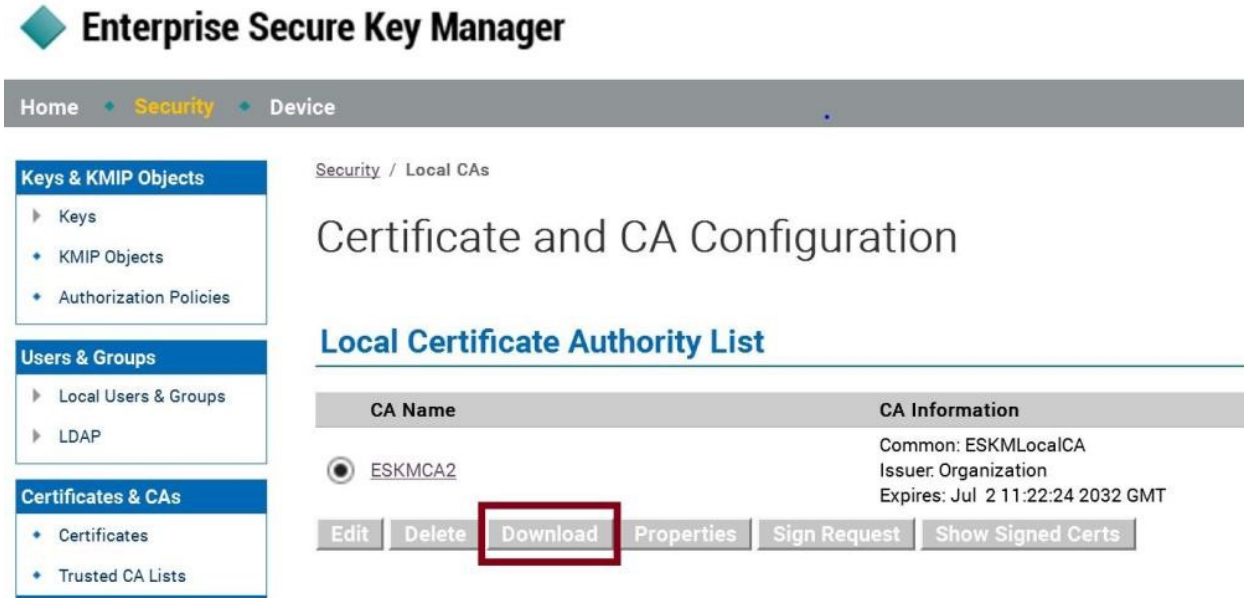
3. Select **Client** as the purpose of generating the certificate
4. Paste the complete CSR content in the **Certificate Request** box
5. Click **Sign Request**



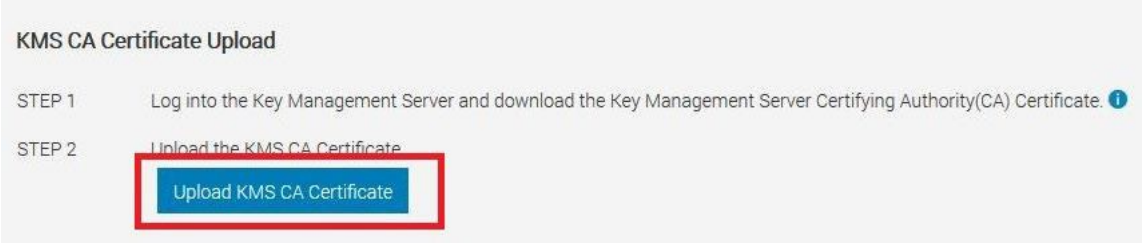
6. After the request is signed, click **Download**, to save the signed CSR file to your system
7. To upload the file that you just got signed on Utimaco ESKM access the iDRAC GUI
8. Go to the **SEKM Certificate** page and click **Upload Signed CSR**. A message is displayed to indicate the successful upload

5.4 Download the server CA file from Utimaco and upload to iDRAC

1. On the Utimaco GUI, click **Security Tab → Local CAs**
2. Select the Server CA you are using and click **Download**. The file is saved to your local system



3. On the iDRAC GUI, in the **KMS CA Certificate** section, click **Upload KMS CA Certificate**
4. Upload the Server CA you just downloaded from Utimaco. A message is displayed to indicate the successful upload.



5.5 Creating KMIP User and Password on ESKM

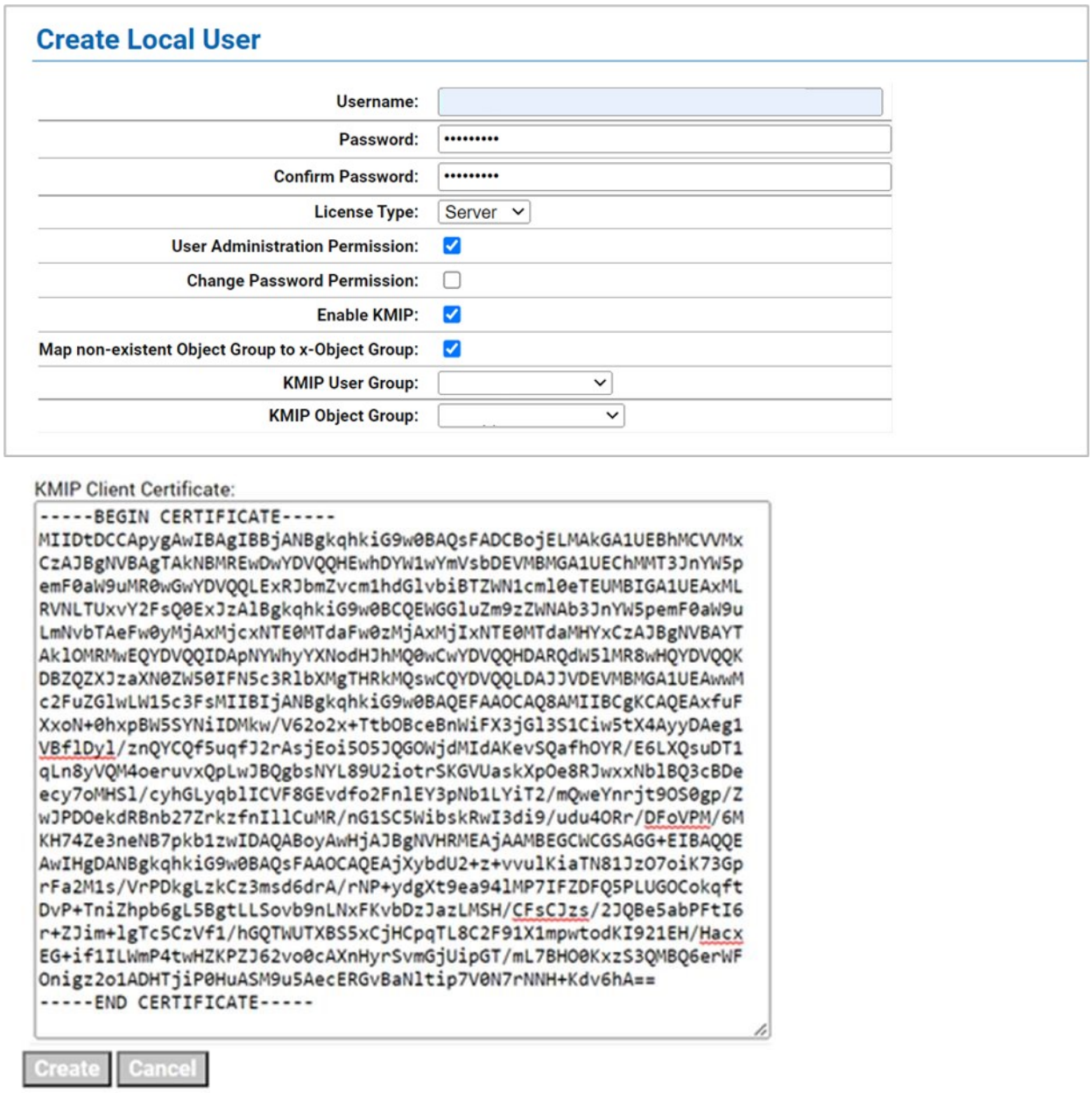
To create a user — an individual (client) on the ESKM server follow the below steps:

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.



8. Click Create

The user R840_18R5QM2 now appears on the list of Local Users.

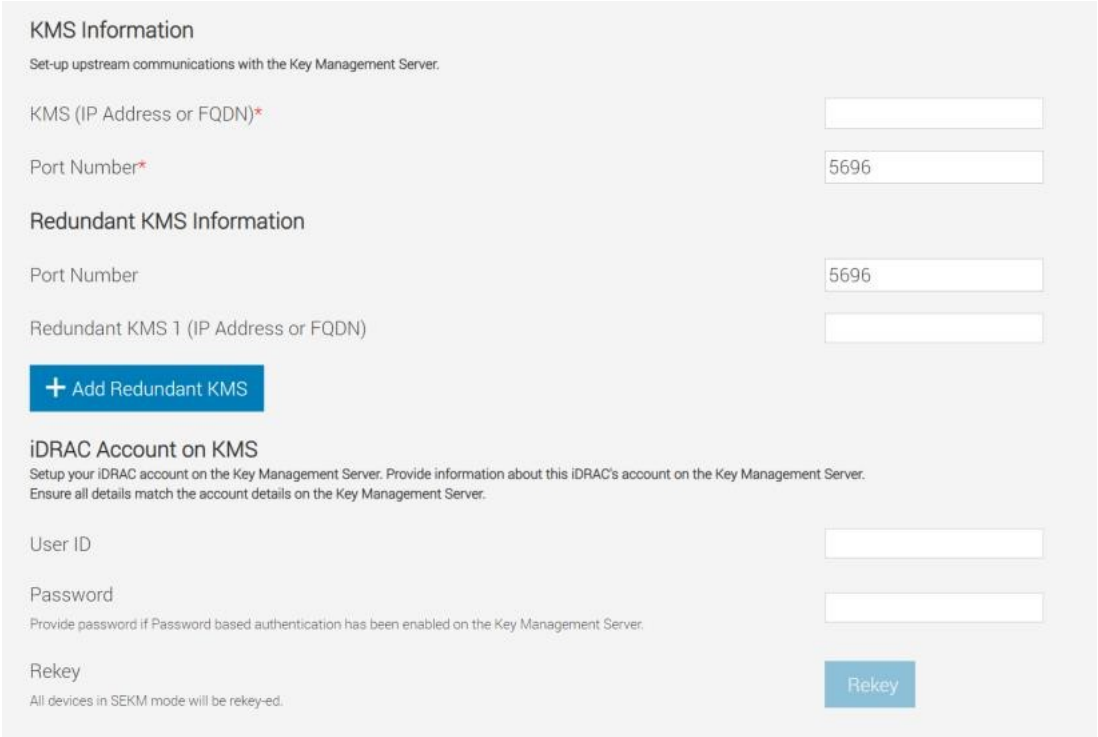
5.6 Configure the Key Management Server (KMS) settings on iDRAC

1. Enter or select data in the fields, and then click Apply

Make sure you already have a user created on the KMS you will be using for key exchange with the iDRAC. For the username, ensure it matches the exact value in the CSR certificate property you selected for the ESKM KMIP Username field in client certificate Authentication Settings.

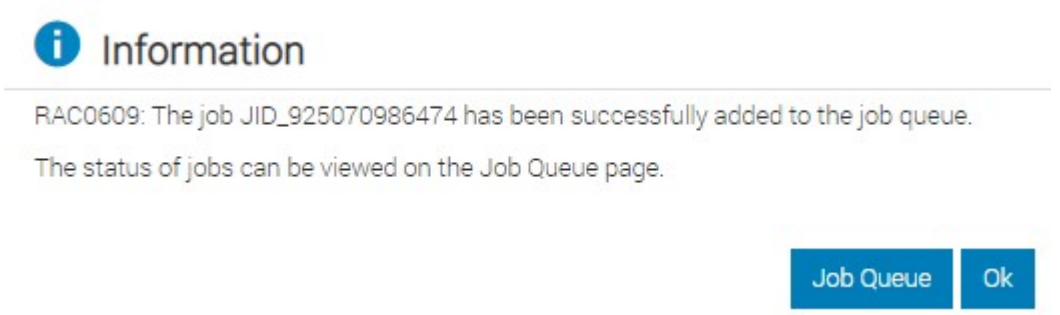
For example, in the signed CSR Certificate on iDRAC used in this experiment, the Common Name property is set to “R840_18R5QM2”. On the ESKM server, in the KMIP Authentication Settings, the “Username field in client certificate” field is set to “Common Name”. For creating a username on ESKM, you must create a user with the name “R840_18R5QM2”. This is the user which iDRAC will be using for key exchange.

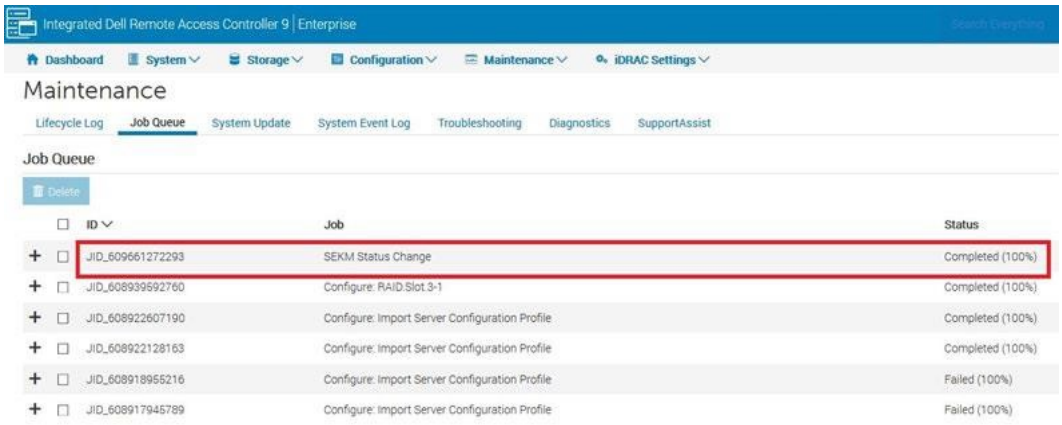
2. Provide the username and password which you created on ESKM in the User ID and Password fields below



A message is displayed indicating that a job ID has been created

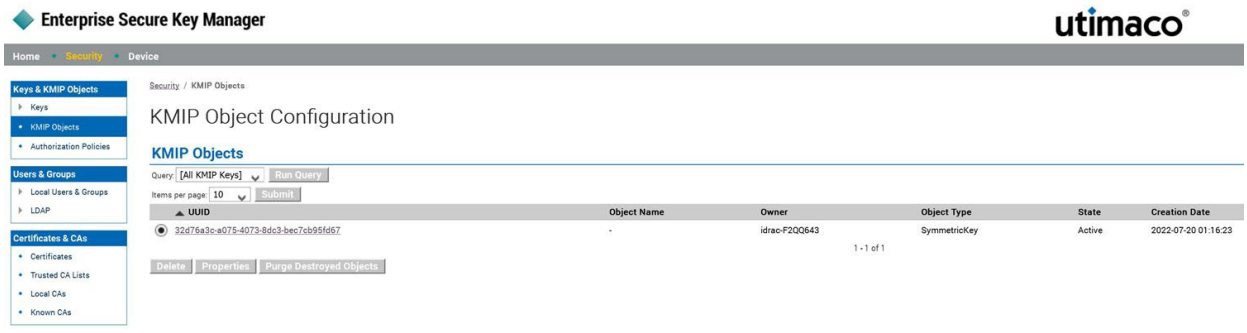
3. Go to the **Job Queue** page and ensure that the job ID is marked as successfully completed. If you see any job status failures, view Lifecycle Logs for more information about the failure. iDRAC SEKM configuration with Utimaco is now complete





5.7 Viewing iDRAC key ID on Utimaco

1. Log in to Utimaco GUI. Click **Security Tab → KMIP Objects**



This completes integration of Dell PowerEdge Servers with Utimaco ESKM.

6 Troubleshooting

Error	Diagnosis
installed the SEKM license, but I cannot enable the SEKM on iDRAC	Make sure you update the iDRAC firmware after you install the SEKM license. This is required even if you had a SEKM supported iDRAC firmware version prior to installing the SEKM license.
iDRAC SEKM status has changed to “Failed” after changing the KMIP authentication settings on the ESKM	If you changed the username or password of the iDRAC account on the KMS then make sure you change the corresponding properties on the iDRAC as well and enable SEKM. If you changed the value of the “Username field in the Client Certificate” option on the KMS, then you need to generate a new CSR from iDRAC by setting the appropriate CSR property to the username, get the CSR signed by the KMS CA and then upload it to iDRAC. For example, if you change the value of the “Username field in the Client Certificate” option on the KMS from “Common Name” to “Organizational Unit” then generate a new CSR by setting the OU property to the iDRAC KMS username, sign it using the KMS CA and then upload it to iDRAC. If you enabled the “Require Client Certificate to contain Source IP” property on the KMS then generate a new CSR by selecting the “Include iDRAC IP Address in CSR”, sign it using the KMS CA and then upload it to iDRAC

Table 5: List of Error and its Diagnosis

7 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/

8 References

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