HPE

ProLiant

iLO DL380 Gen10, Gen10+,Gen11

Integration Guide

ESKM

8.54.0

utimaco®

Imprint

Copyright 2025	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	2025-12-09
Status	PUBLISHED
Document No.	IG-2025-0063

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco to facilitate secure server-side encryption practices. It outlines the integration of HPE ProLiant servers with Utimaco's Enterprise Secure Key Manager (ESKM), enabling robust key lifecycle management and enhanced protection of encryption keys used for securing data at rest on physical drives.

1.1 About this guide

This guide describes how to integrate HPE ProLiant with Utimaco's Enterprise Secure Key Manager (ESKM) to enable secure key management for encrypted storage operations. The integration allows HPE Smart Array controllers to retrieve encryption keys from ESKM, ensuring centralized control over key generation, distribution, and lifecycle management. By binding encrypted volumes and boot drives to keys managed by ESKM, organizations can enhance data-at-rest protection, meet compliance requirements, and maintain operational continuity through secure key retrieval and auditing features.

1.2 Target Audience

This guide is intended for HPE ProLiant administrators and Utimaco ESKM administrators.

1.3 Purpose of the Integration

The integration of HPE ProLiant with Utimaco ESKM establishes a secure, centralized key management infrastructure for safeguarding sensitive cryptographic keys used across enterprise applications and data storage systems. This setup ensures that encryption keys are generated, stored, and managed within a certified, hardware-based key management environment, significantly reducing the risk of unauthorized access, key compromise, or data breaches. By leveraging Utimaco ESKM's robust key lifecycle controls and HPE ProLiant's enterprise-grade performance, organizations can enforce consistent security policies, meet compliance requirements, and enhance the overall resilience of their IT infrastructure.

1.4 Abbreviations

Abbreviations	Meaning
ESKM	Enterprise Secure Key Manager
HPE	Hewlett-Packard Enterprise
iLO	Integrated Lights-Out
KMIP	Key Management Interoperability Protocol
KMS	Key Management Server
CA	Certificate Authority
SSL	Secure Sockets Layer
TLS	Transport Layer Security
FIPS	Federal Information Processing Standards
IP	Internet Protocol

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	Click on **ADD**
`Monospaced`	Code that is given for explanation or as an example, file paths	Enter `y`
Italic	References and important terms	HPE ProLiant version listed in *Tested Versions*

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 HPE ProLiant

HPE ProLiant is a high-performance server platform built for reliability, scalability, and security in enterprise environments. It supports diverse workloads—from virtualization to data analytics—and includes features like HPE iLO for remote management and Silicon Root of Trust for firmware protection. With modular design and advanced RAID, ProLiant ensures efficient operations and strong data protection across hybrid infrastructures.

2.2 Overview of Utimaco ESKM (Enterprise Secure Key Manager)

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

2.3 Joint Value Proposition

Integrating HPE ProLiant with Utimaco ESKM delivers a secure and centralized solution for enterprise key management. HPE ProLiant provides a reliable and scalable server platform for hosting critical workloads, while Utimaco ESKM ensures that cryptographic keys are securely generated, stored, and managed within a certified hardware-based environment. This integration strengthens data protection across applications and storage systems, supports regulatory compliance, and reduces the risk of key compromise or unauthorized access.

3 Integration Requirements and Prerequisites

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

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

3.1 Tested Versions

HPE ProLiant iLO Version	Utimaco ESKM Version
iLO DL380 G10, iLO DL380 G10+, iLO DL380 G11	8.54.0

Table 2: Tested Versions

3.2 Software Requirements

Software	Software Requirements
HPE ProLiant	iLO DL380 G10, iLO DL380 G10+, iLO DL380 G11
Utimaco ESKM	8.54.0

Table 3: Software Requirements

3.3 Prerequisites

Before you begin, please ensure that you have:

- Installed and set up HPE ProLiant version listed in *Tested Versions*.
- ESKM listed in *Tested Versions*.
- The required Secure Encryption license for the Proliant server from HPE.
- The required iLO Advance license for the Proliant server from HPE.
- The required minimum HPE ProLiant Gen8/9/10/11 (iLO v4).
- Retrieved and installed HPE SSA (Smart Storage Administrator) software.

- Installed and configured a Smart Array Controller compatible with Secure Encryption (typically Px3x and Px4x).

4 Installation and Configuration

The following section outlines the procedures required to configure both Utimaco ESKM and HPE ProLiant components for seamless integration.

4.1 Installing and Configuring Utimaco ESKM Server

4.1.1 First Run

The 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.

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 set up 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:
    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.
    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 to 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 the 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.

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.

Press Enter to accept the default.

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

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 that 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 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.

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 8.54.0 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.

4.1.2 Setting Up the 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 the information required by the Create Local Certificate Authority section of the window to create your local CA.
    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**.
    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.

e. Click **Create**.

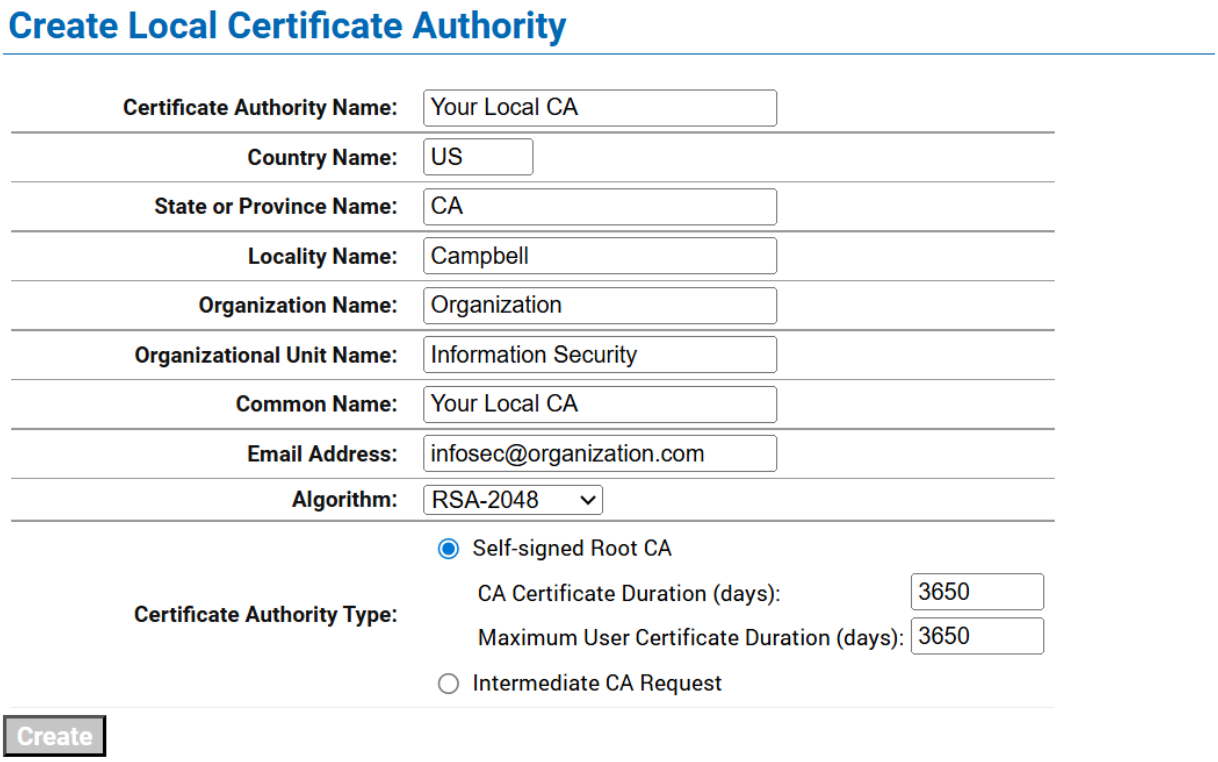

Figure 1 : Create Local CA

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/Re-certify operations.

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 I**nstall 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**.

4.1.3 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 who 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 & CAs**, select **Certificates**.
3. Scroll down to the **Create Certificate** section.
    a. Enter **Certificate Name**, **Country Name**, **State or Province Name**, **Locality Name**, **Organization Name** and **Organization Unit Name**.
    b. Select **RSA-2408** from the **Algorithm** dropdown list.
    c. Select the previously created CA certificate name from the **Local CA** drop-down list.
    d. Select **Server** from the **Certificate Purpose** dropdown list.
4. Click on Create.

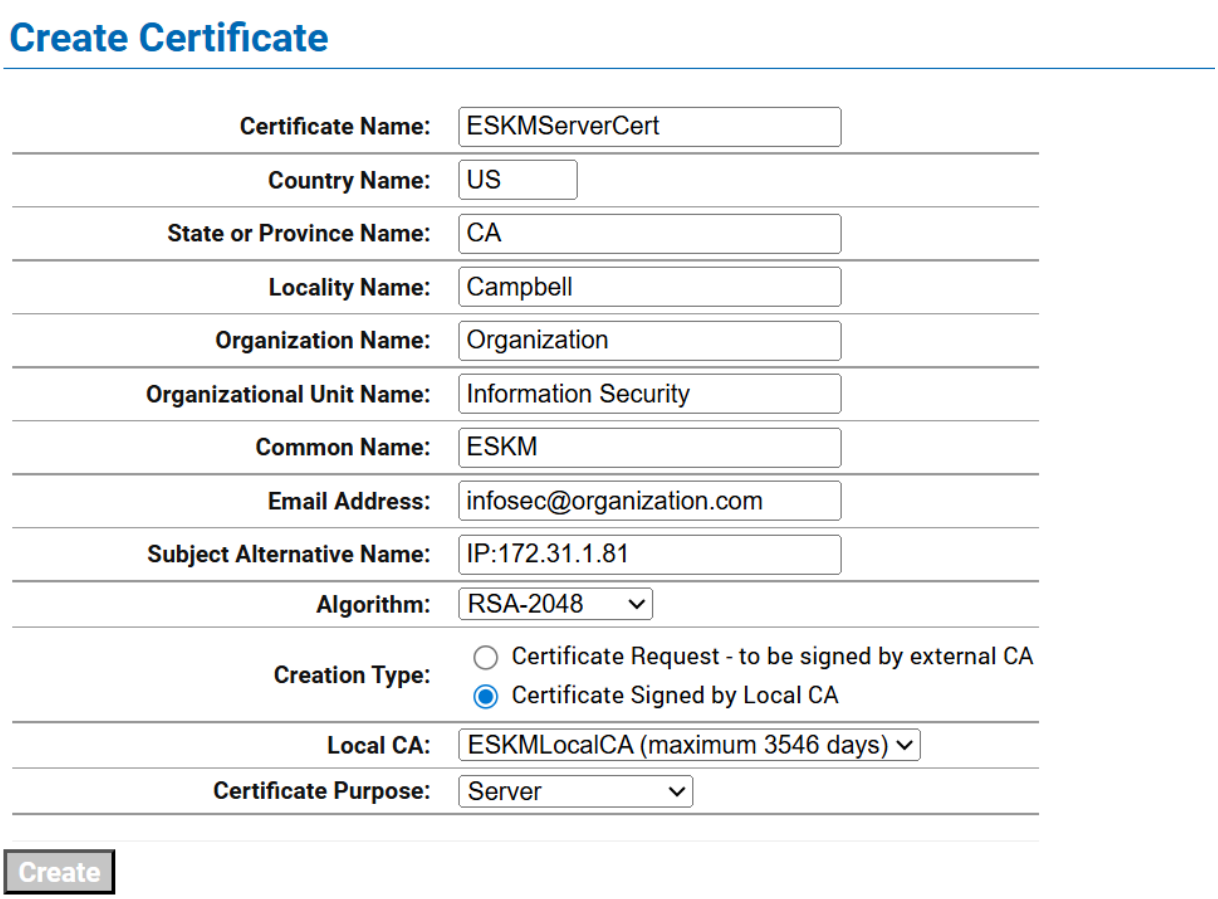

Figure 2 : Create Certificate

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

4.1.4 Set Up 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.

4.1.4.1 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**.

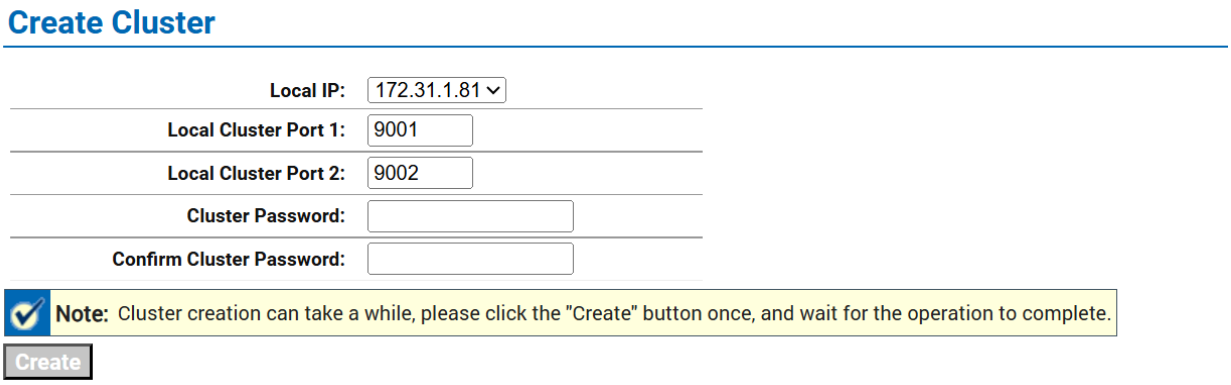

Figure 3 : Create Cluster

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 Cluster Port 1** value and **Local Cluster Port 2** value. These values default to 9001 and 9002, respectively.

Local Cluster Port 1 defines the port on which the ESKM appliance "listens" for cluster administration requests, Local Cluster Port 2 defines the port on which the ESKM appliance "listens" for "database" based cluster administration requests.

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.

4.1.4.2 Adding ESKM Servers to the Cluster

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

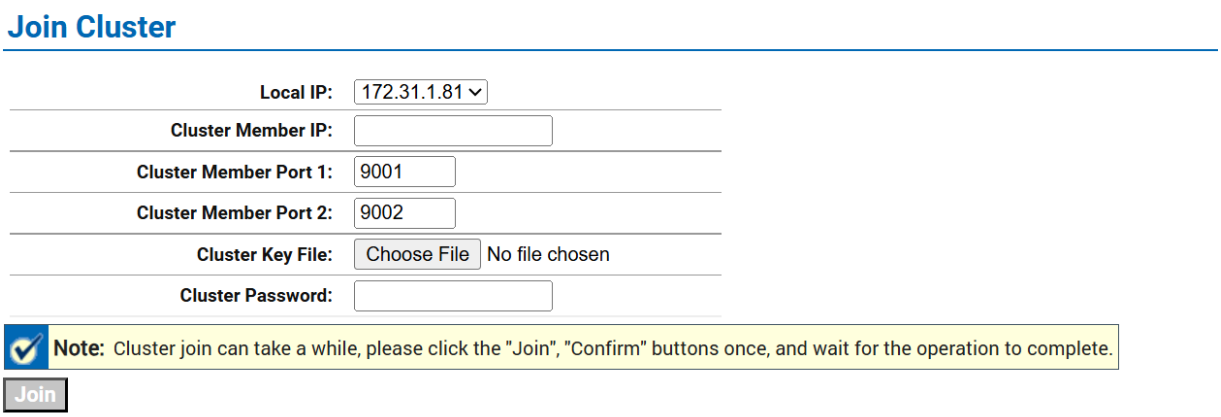

Figure 4 : Join Cluster

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. Alternatively, 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 values for the **Cluster Member Port 1** and **Cluster Member Port 2.**
    d. Type the original cluster member's IP into **Cluster Member IP**.
    e. Type the original cluster member's port into **Cluster Member Port 1**. The default value of this port is 9001. If this value was changed while creating the cluster, use that value.
    f. **Cluster Member Port 2** is the port number used by the ESKM appliance, defined in the existing Cluster Member IP field for replication of data.
    g. Click **Browse** and select the **Cluster Key File** you saved while creating the cluster.
    h. Type the cluster password into **Cluster Password**.
    i. Click **Join**.
    j. 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.

4.1.5 Set Up 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 an 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 be 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.

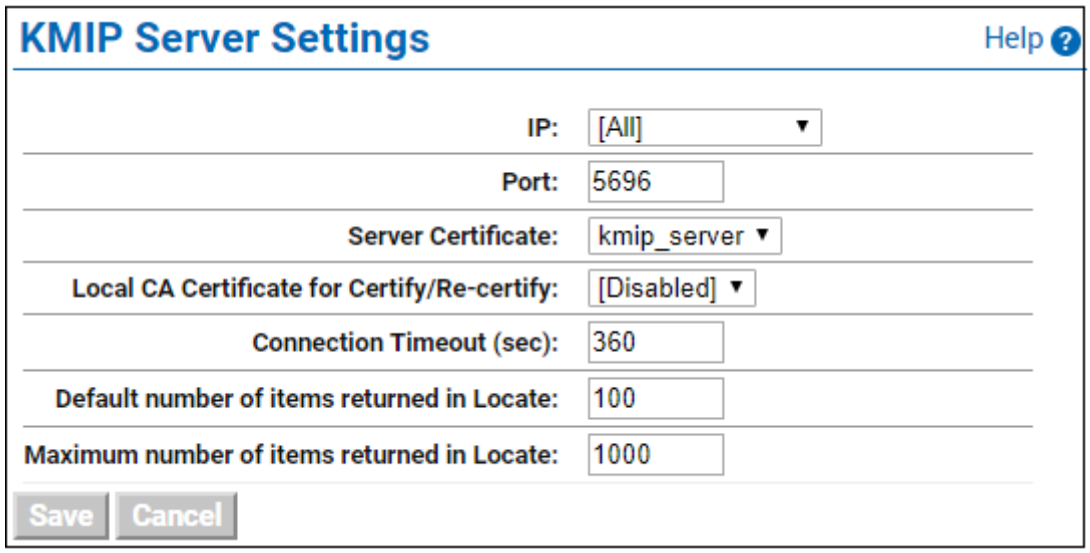

Figure 5 : KMIP Server Settings

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.

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

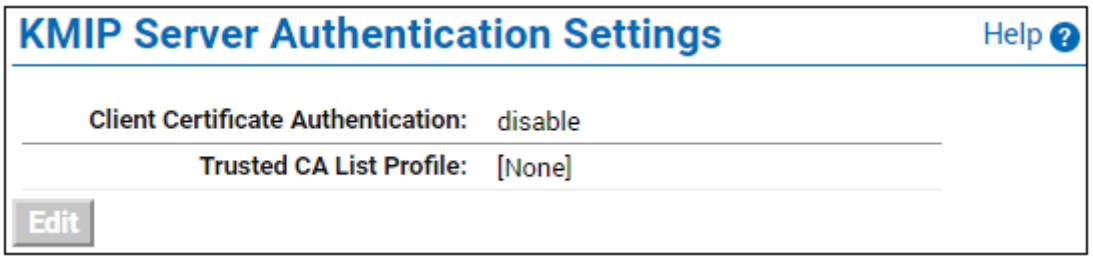

Figure 6 : KMIP Server Authentication Settings

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

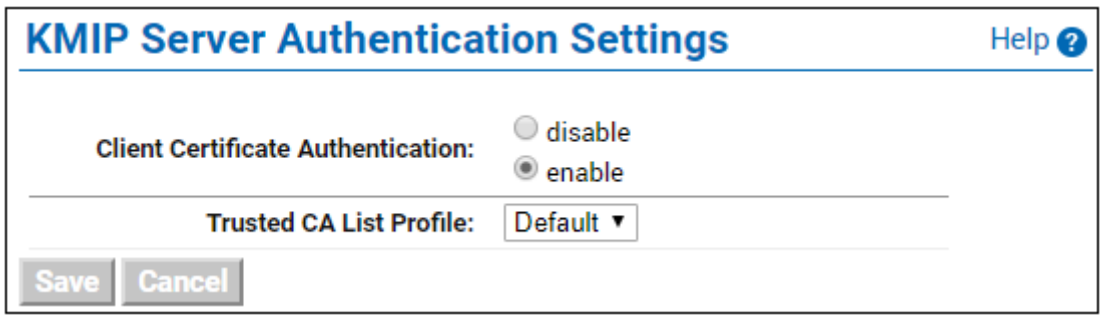

Figure 7 : KMIP Server Authentication Settings - Enable Authentication

4.1.6 Set Up 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.
    a. The IP address can be an IPv4 address or an IPv6 address. If support for IPv6 has been enabled, see *First run*.
    b. 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**.
    c. For **Server Certificate**, select the name of the certificate you created in *Setting up ESKM certificate*. For example, ESKM KMS Server.
    d. Enable **Allow Key and Policy Configuration Operations**.
    e. Enable **Allow Key Export**.

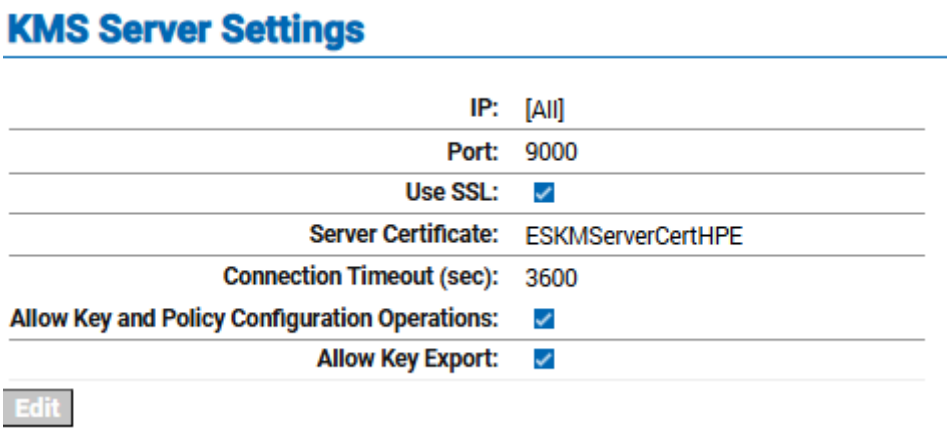

Figure 8 : KMS Server Settings

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 the KMIP client certificate, perform the following steps.

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

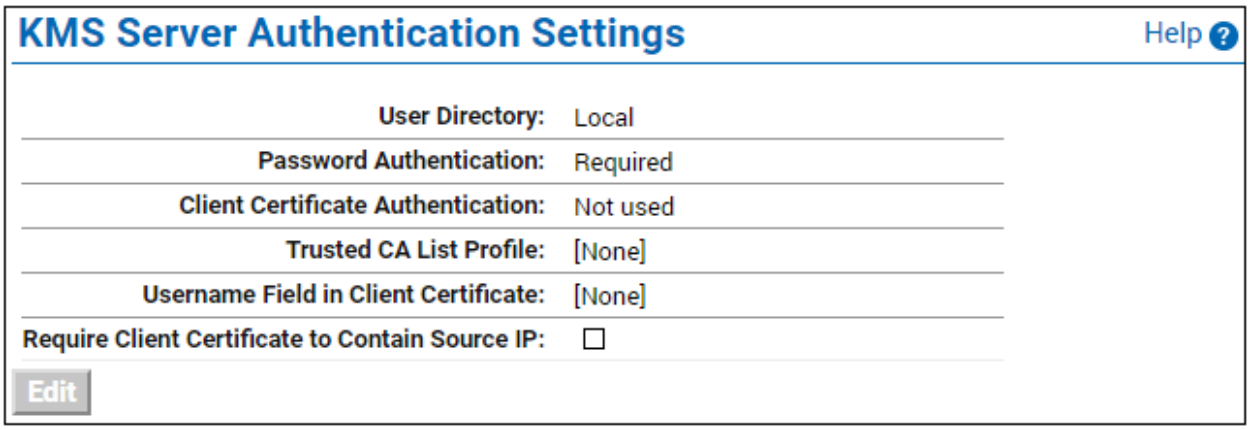

Figure 9 : KMS Server Authentication Settings - Edit

8. Click the 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**.

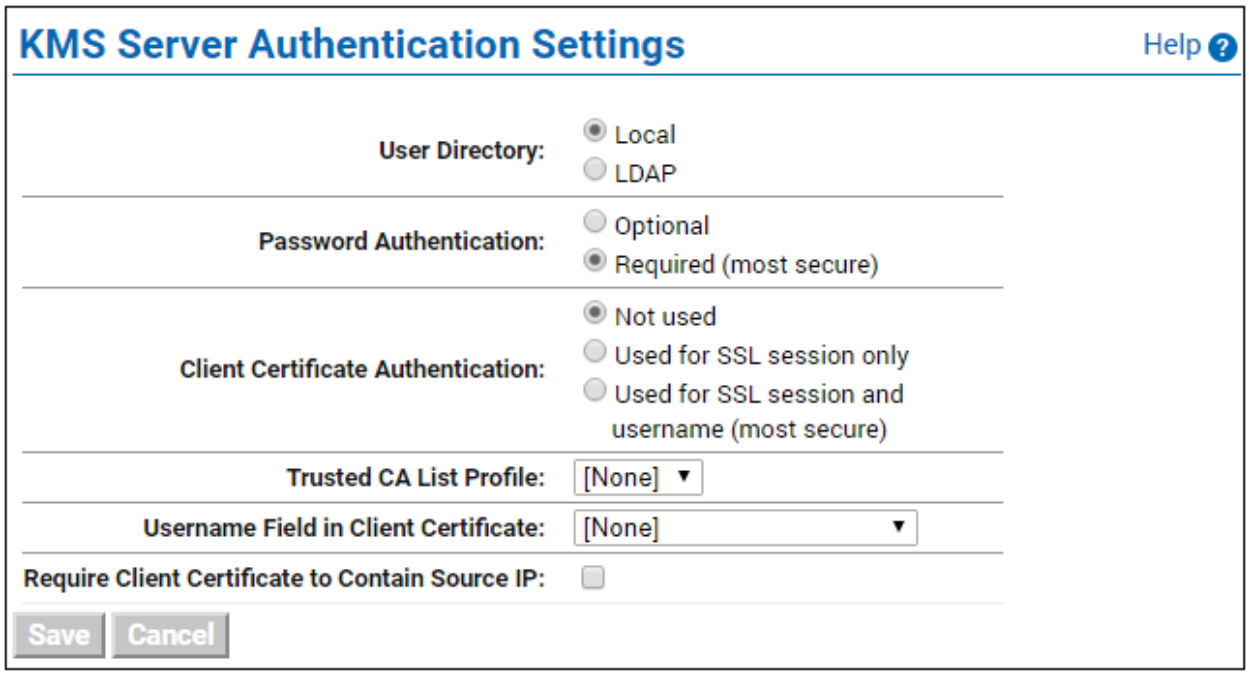

Figure 10 : KMS Server Authentication Settings - Authentication

4.1.7 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**.

5 Integration Steps

This section provides the step-by-step procedure for integrating ESKM with HPE ProLiant Server.

Utimaco ESKM integrates with HPE ProLiant Server to manage the encryption using a high-assurance scalable key manager in a security hardened appliance.

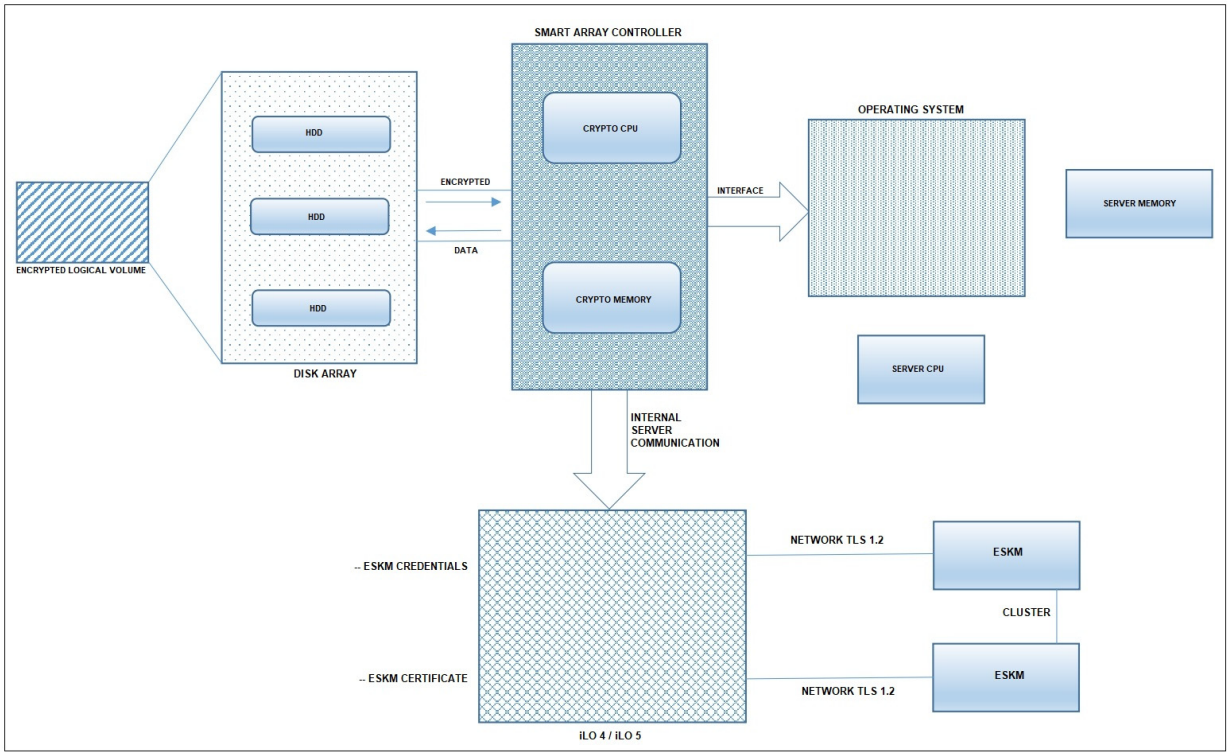

Figure 11 : Integration architecture

When integrating "HPE Secure Encryption" with "ESKM", we will be using the iLO port to set up the initial configuration and perform the enrollment with the ESKM. The iLO must be configured in such a way that it can access the ESKM over the network.

5.1 Configuration on Utimaco ESKM

We must create “temporary credentials” on the ESKM for the iLO to authenticate and execute the enrollment steps.

1. Log in to the ESKM Management Console using the admin username and the password.
2. Go to **Security > Users & Groups > Local Users.**

3. Click on **ADD**.
4. Create a local user with the username “ilo_reg_user”
    a. Enable “User Administration Permission” to allow this user to create other client users.
    b. Enable “Change Password Permission” to allow this user to change client user passwords.
    c. Uncheck “Enable KMIP” and leave this field blank.

Do not assign this user to any User group. It must remain stand-alone.

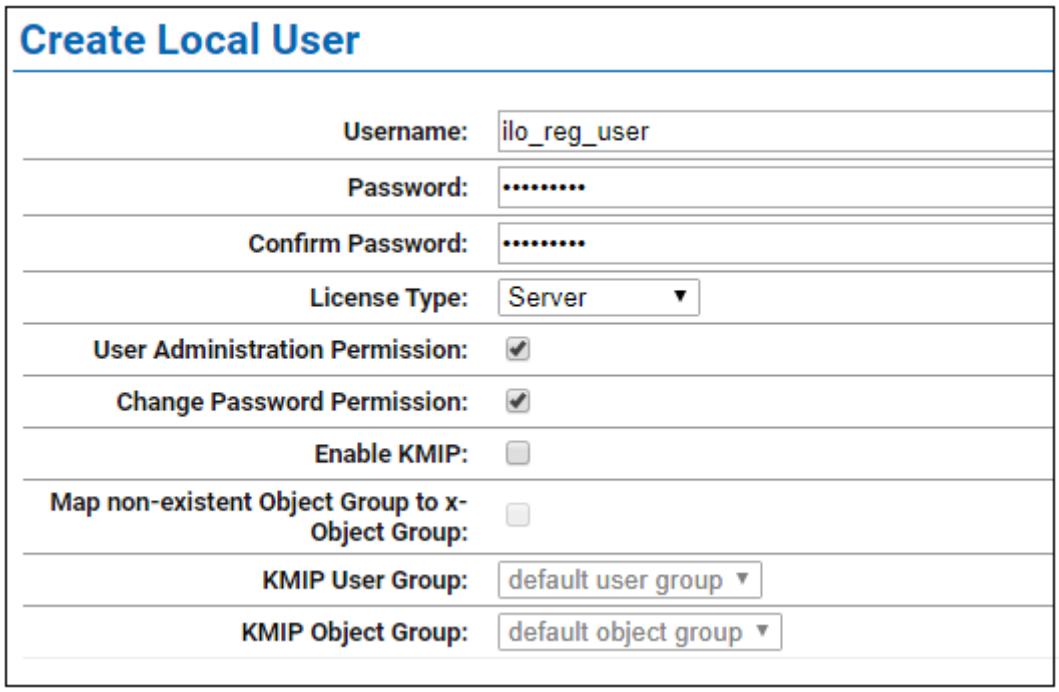

Figure 12 : Create Local User

5. Go to **Security > Users & Groups > Local Groups**.
6. Click on **ADD**.
7. Create a user group that lists all servers under the “Group” that serves the same applications or function.
    a. Group: “FinanceGroup”, for the servers used by Finance applications, for example
    b. Group Type: ESKM.

Utimaco recommends grouping ProLiant Servers based on organizational unit/ department.

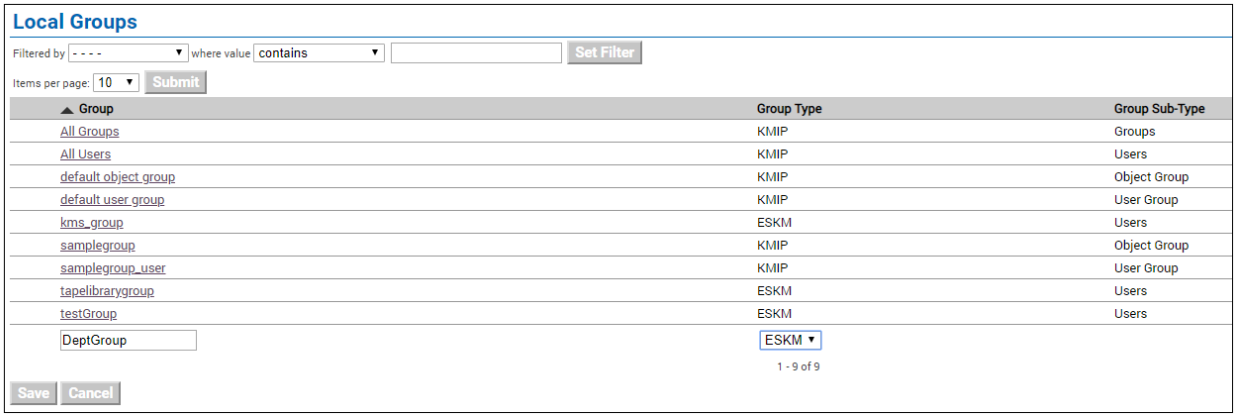

Figure 13 : Local Groups

8. Click on **Save**.
9. Go to **Security > Keys & KMIP Objects > Create Keys**.
10. Create a Key that will be used as a “master key” to encrypt “drive keys”.
    a. Key Name: “FinanceMasterKey”, for example, or some preferred name.
    b. Owner Username: ilo_reg_user.
    c. Key Type: ESKM.
    d. Algorithm: AES-256.
    e. Exportable: Enable.

Owner Username is the master user created earlier.

11. Click on **Create**.

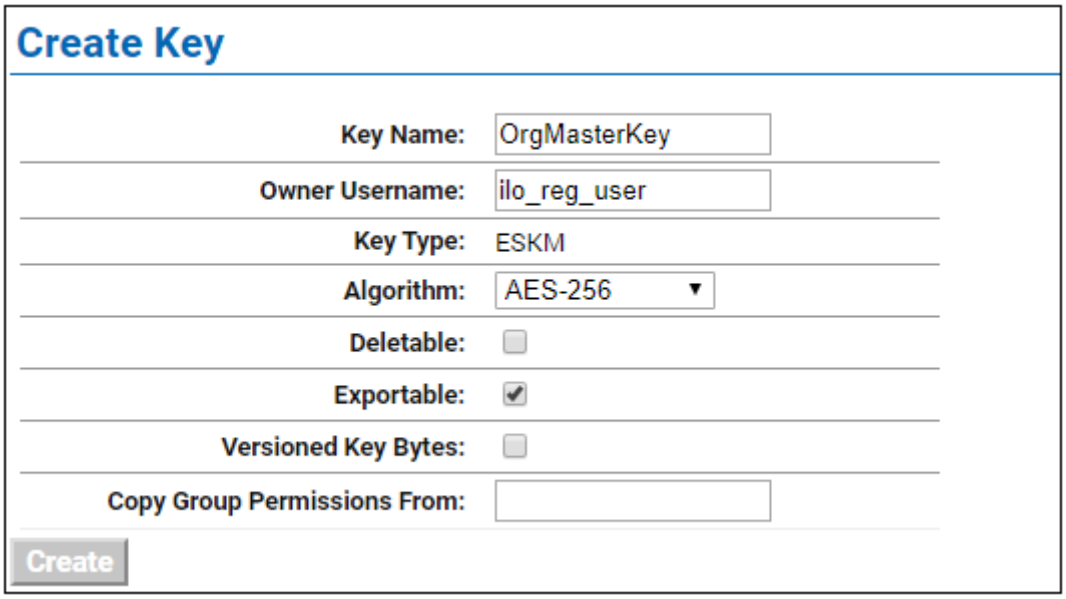

Figure 14 : Create Key

12. Assign the master key to the group that was previously created.
13. Run a Key Query in the ESKM.
14. Find the key that you created in step 10.
15. Click on the key to view its properties.
16. Under “Group Permissions”, add the group to which this key is going to be a part of.
    a. Export: select “Always”
    b. Full: select “Always”

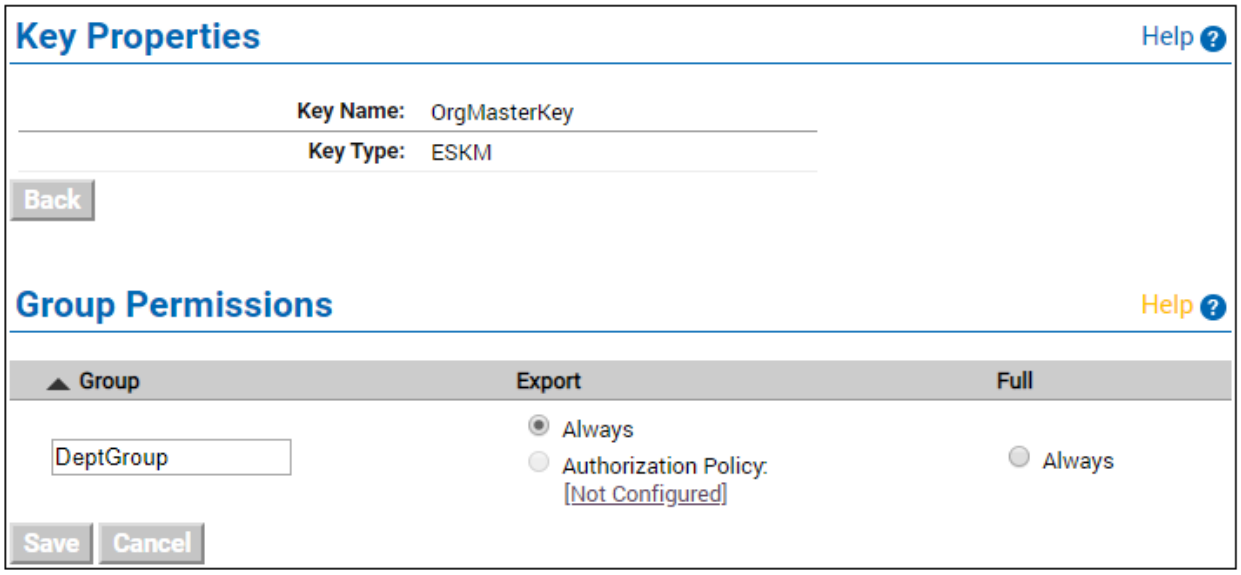

Figure 15 : Group Permissions

17. Click on **Save**.

5.2 Configuration on HPE ProLiant

5.2.1 Configuring iLO for Enrollment with ESKM

Please perform the following steps to configure the iLO to get enrolled with ESKM.

1. Log in to the iLO interface with “Local login name” and “Password”.

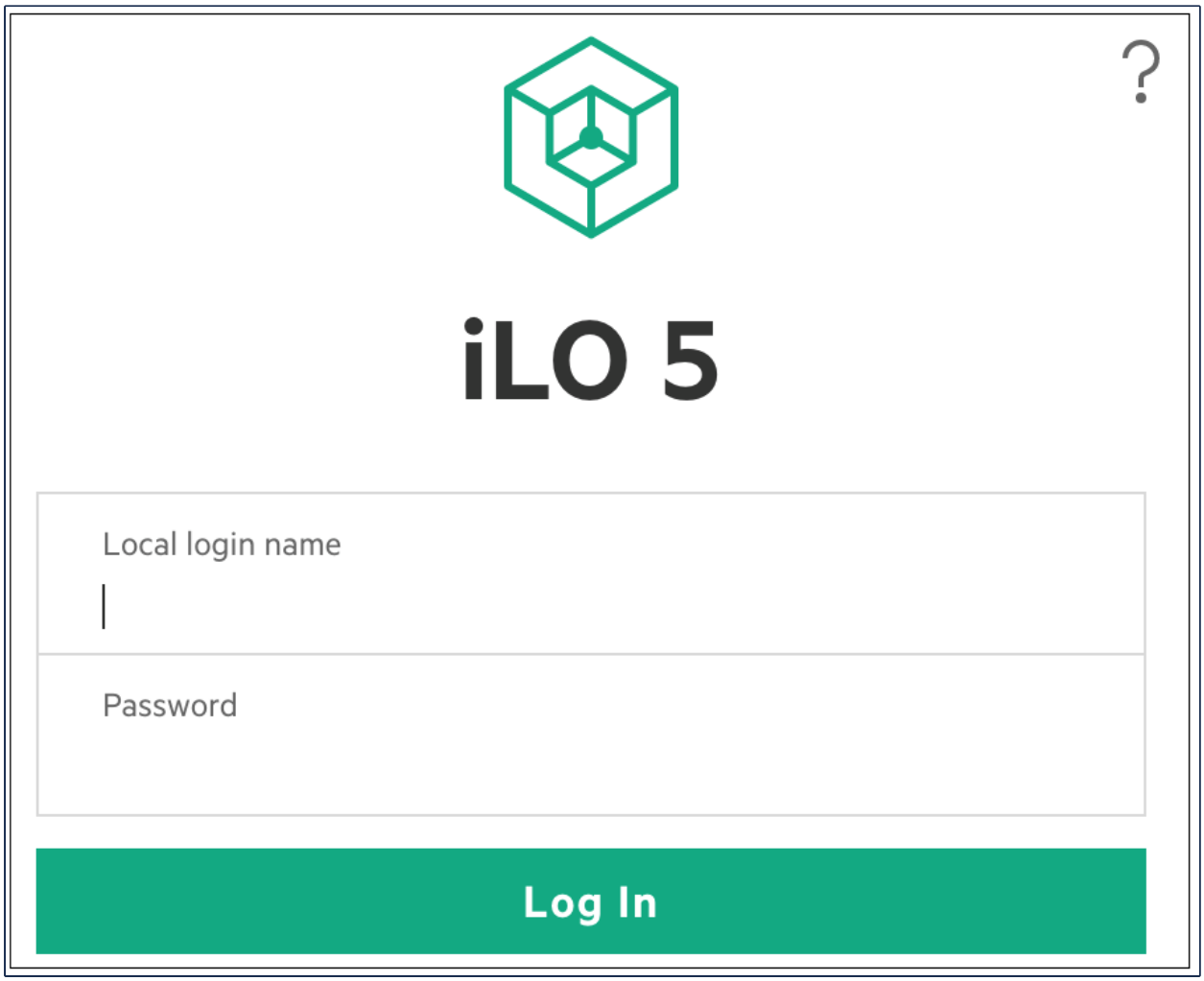

Figure 16 : iLO Login Page

2. Click on the "Administration" menu and click on “Licensing” to verify if an iLO Advanced license is already installed.

Please contact HPE Support to request and install an iLO Advanced license using the following link:

https://buy.hpe.com/us/en/software/server-management-software/server-ilo-management/ilo-licenses/hpe-ilo-advanced/p/332279

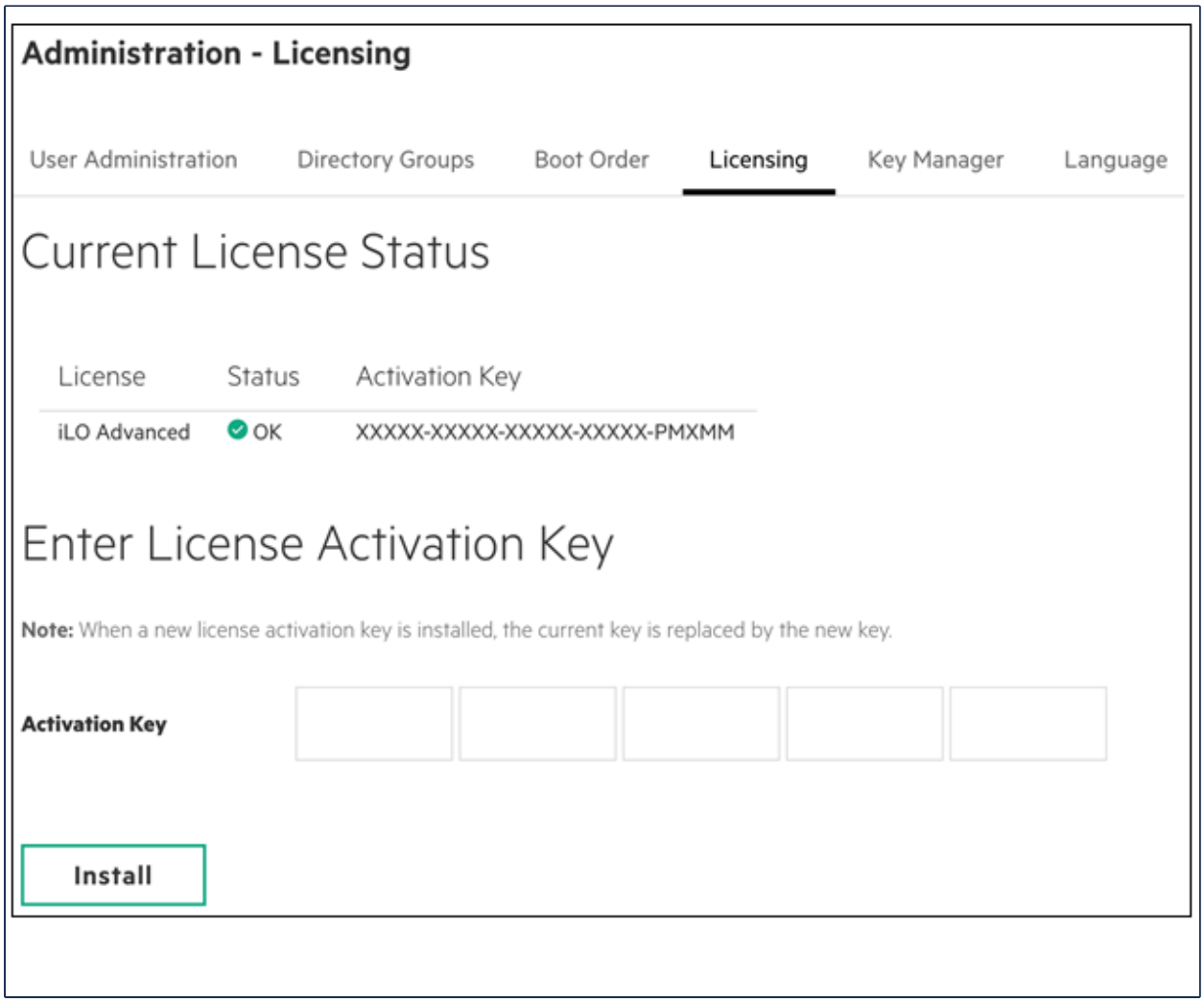

Figure 17 : Licensing window

Click on the “Administration” menu and click on the “Key Manager” tab.

3. Fill out the “Key Manager Servers” form.

    a. Primary Key Server Address: ESKM server IP Address

    b. Primary Key Server Port: ESKM KMS Server Port (9000)

    c. Require Redundancy: Enable

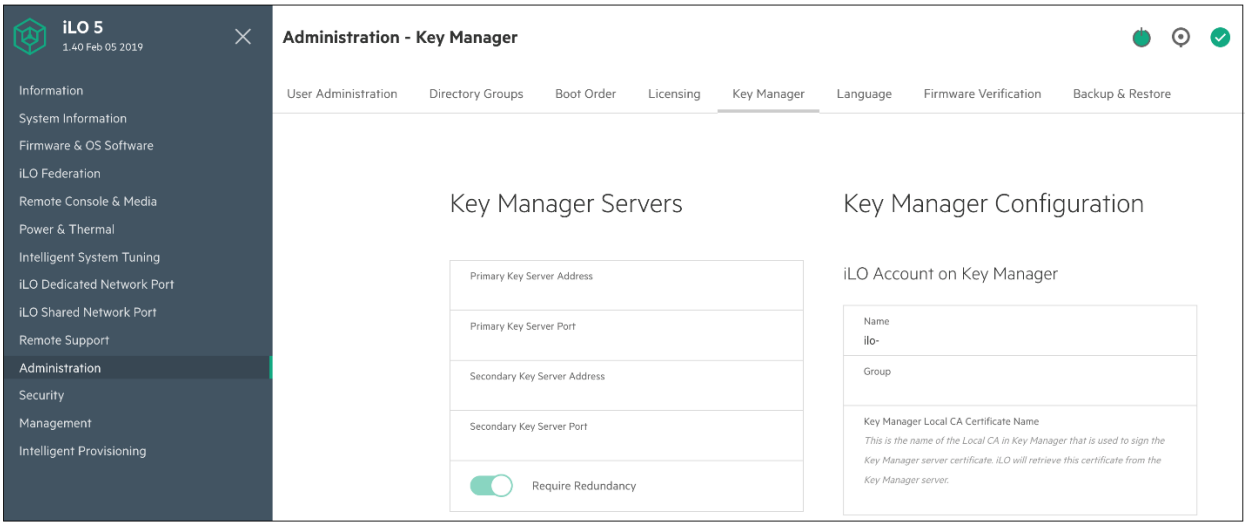

Figure 18 : Key Manager Form

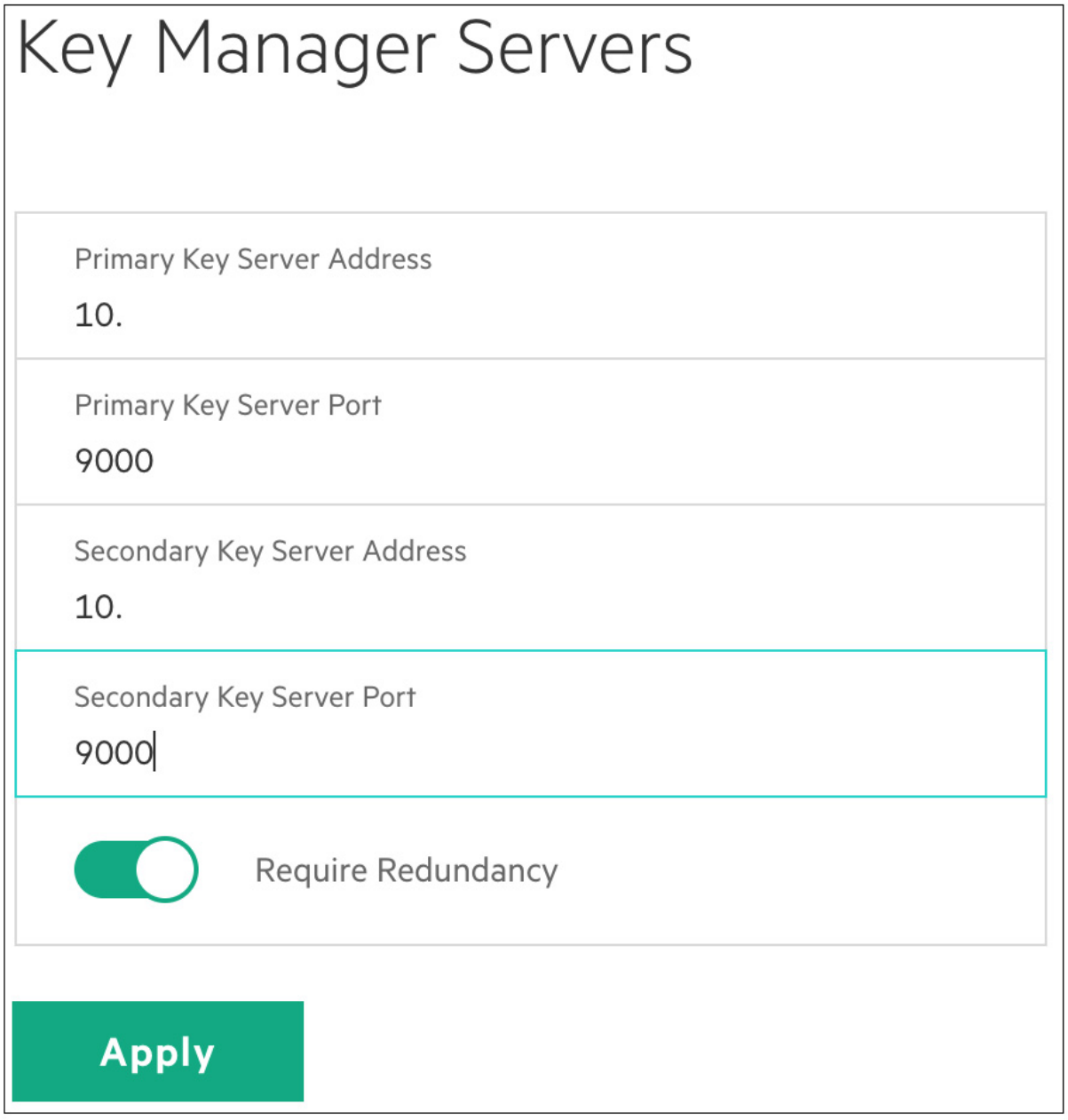

Figure 19 : Key Manager Servers

5. Click on **Apply** after filling out the “Key Manager Servers” form, and “Key Manager settings saved successfully” will be displayed.

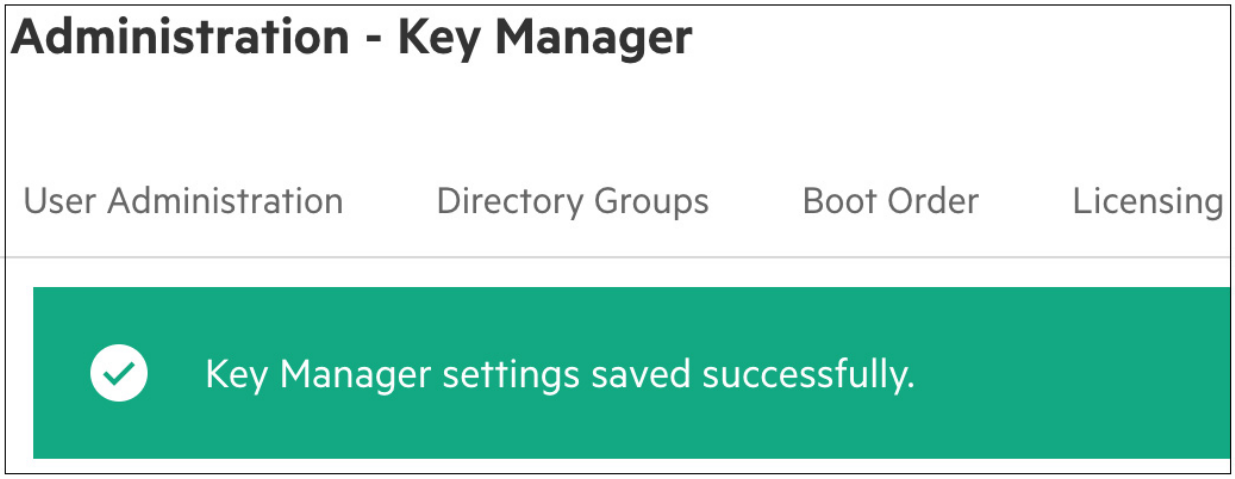

Figure 20 : Key Manager settings successful

6. Again, click on the “Administration” menu and click on the “Key Manager” tab.
7. Fill out the “iLO Account on Key Manager” form under “Key Manager Configuration”.
    a. Name: This will already be populated.
    b. Group: The user group we created in the ESKM.
    c. Key Manager Local CA Certificate Name: The name of the Local CA created on the ESKMs.

Name is the username for the iLO of this particular ProLiant server.

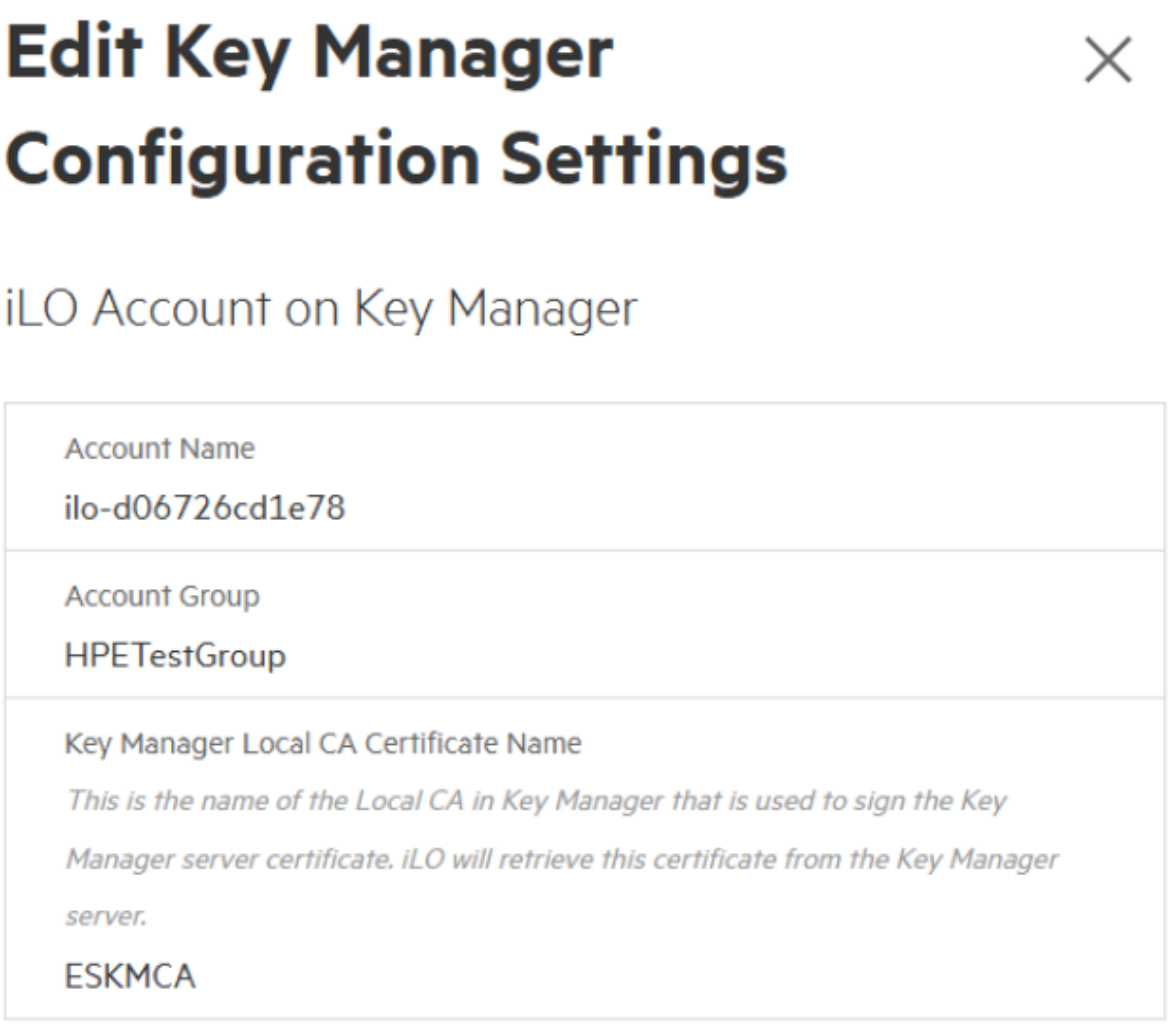

Figure 21 : iLO Account on Key Manager form

8. Fill out the “Key Manager Administrator Account” form under “Key Manager Configuration”.
    a. Login Name: ilo_reg_user (The user created on ESKM).
    b. Password: The password created on ESKM.

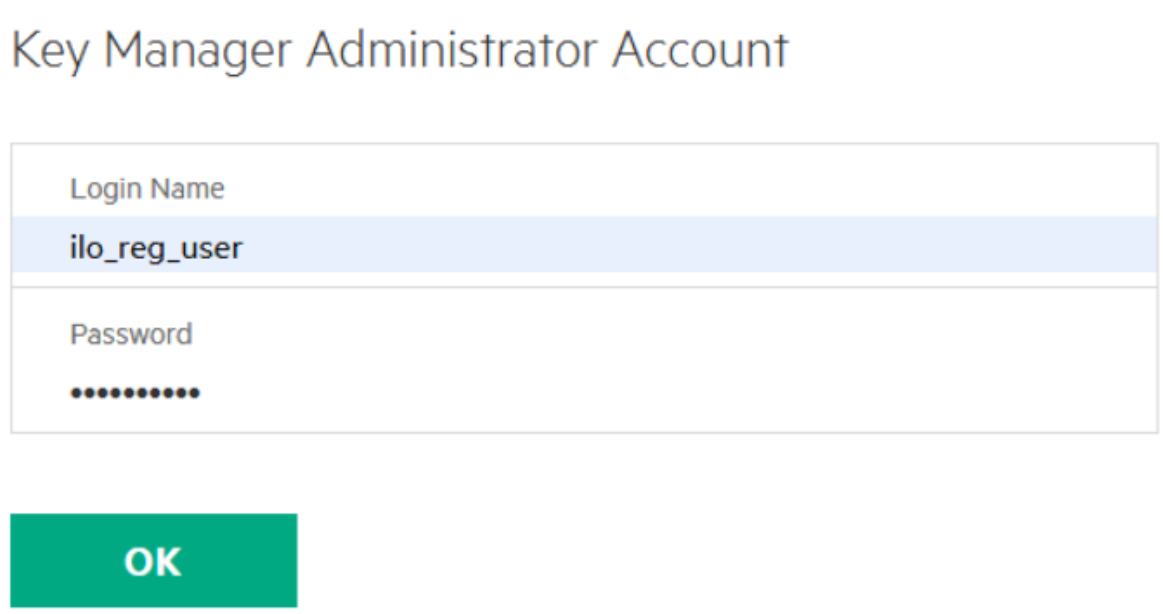

Figure 22 : Key Manager Administrator Account form

9. Click on Update Key Manager, and again, the “Key Manager settings saved successfully” will be displayed.

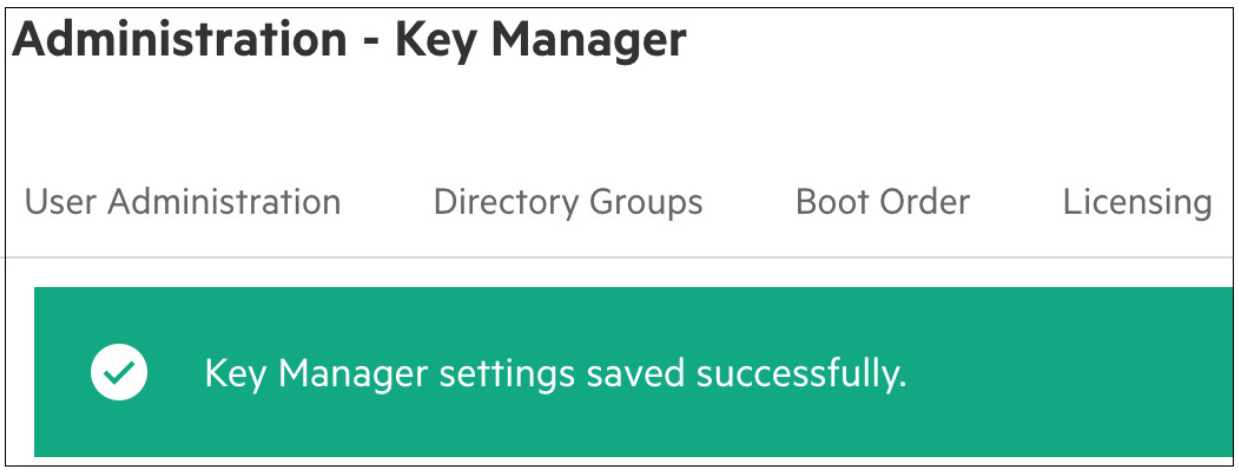

Figure 23 : Key Manger settings successfull

10. Click on “Test Key Manager Connections” to test the connectivity to the key managers and to view the details of the “Key Manager Events”.

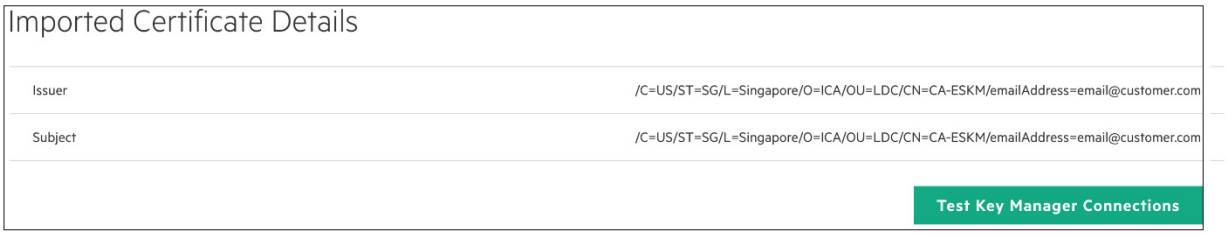

Figure 24 : Imported Certificate Details window

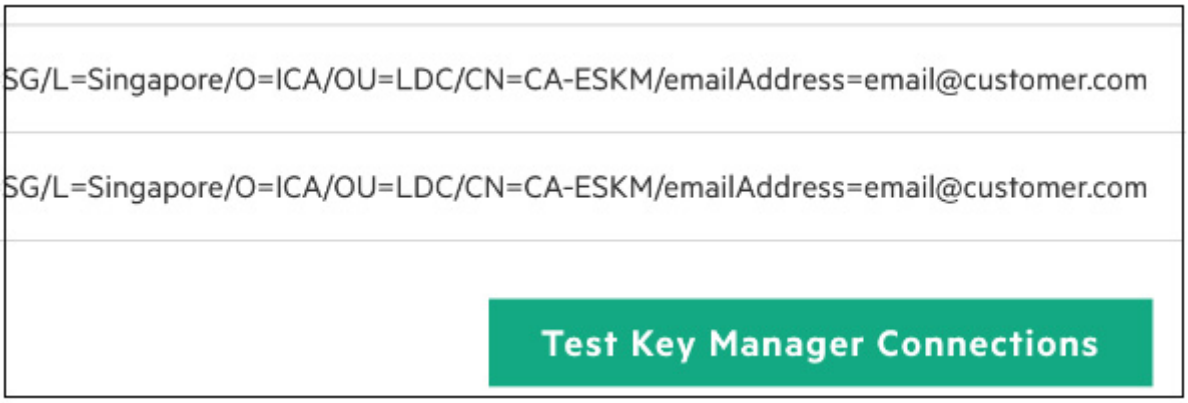

Figure 25 : Test Key Manager Connections

Figure 26 : Key Manager Events

5.2.2 Configure the HPE Smart Array Controller

Please perform the following steps to configure the HPE Smart Array Controller.

1. Boot the server and continuously press F10 to enter Intelligent provisioning.

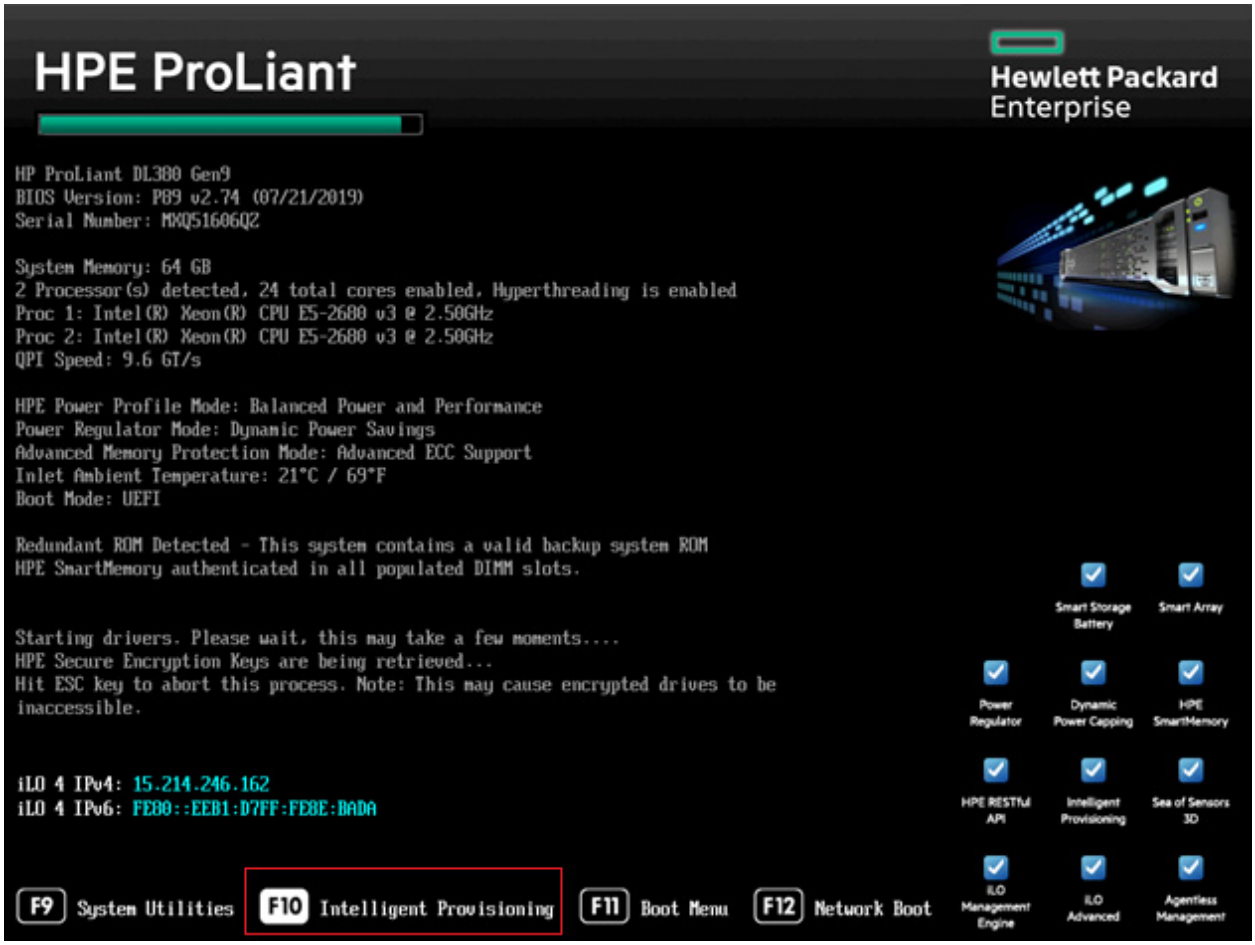

Figure 27 : HPE ProLiant Boot Menu

2. Open the HPE Smart Array Controller.

Please refer to the “HPE Smart Storage Administrator guide” for more details using the following link:

https://support.hpe.com/hpsc/doc/public/display?docId=c03909334

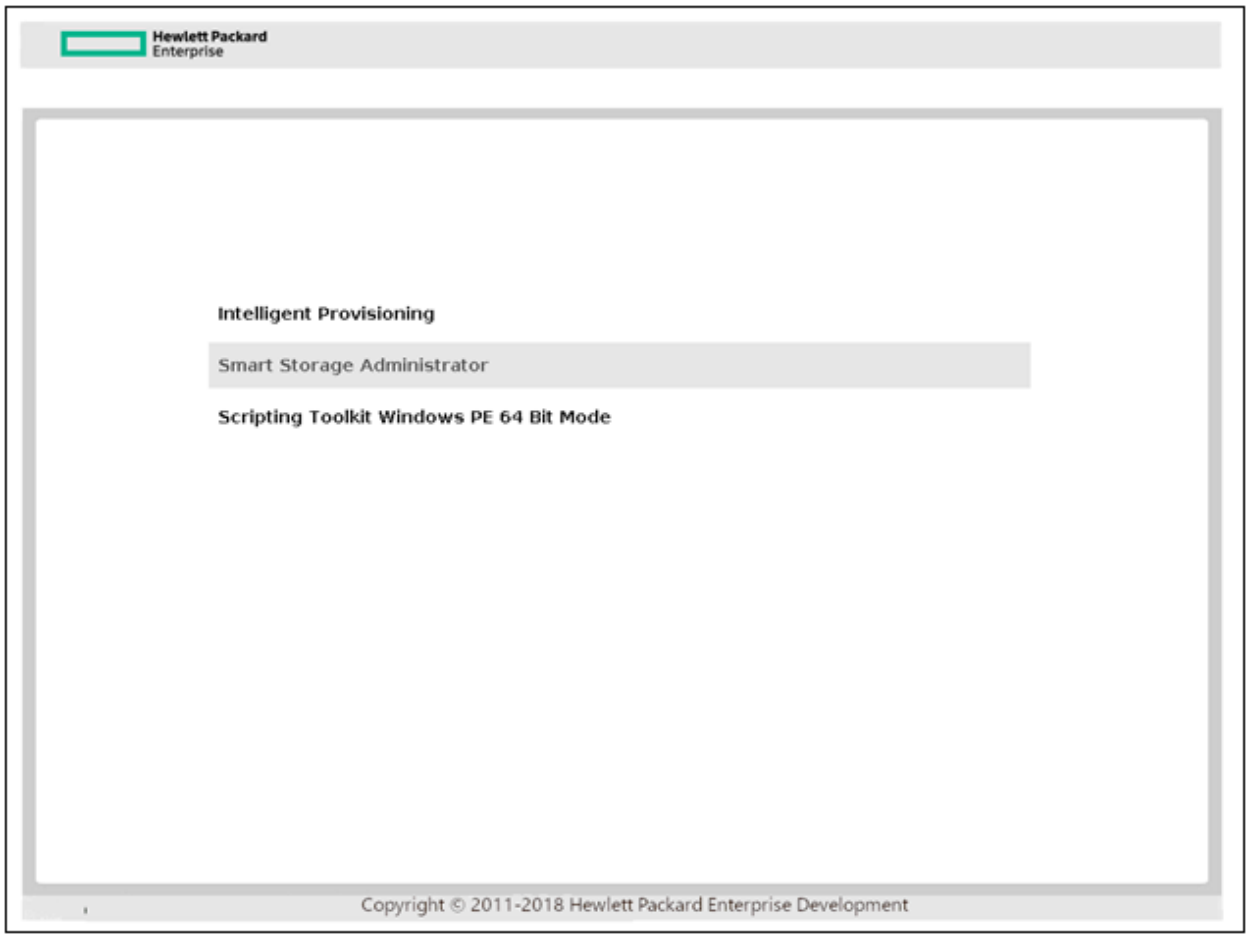

Figure 28 : HPE Smart Array Controller

3. Select a controller that is compatible with secure encryption.

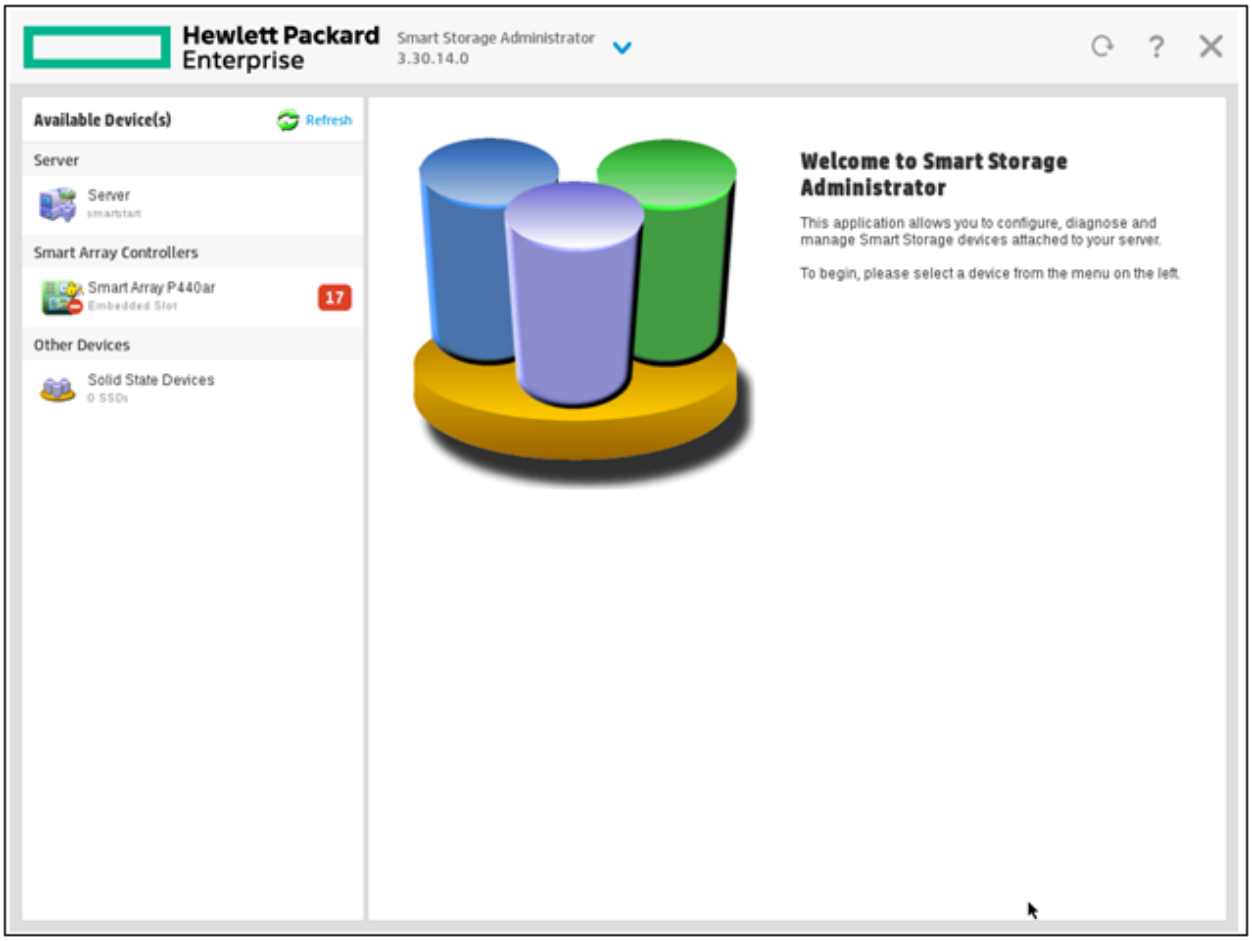

Figure 29 : Smart Storage Administrator

4. Click on **Configure**.

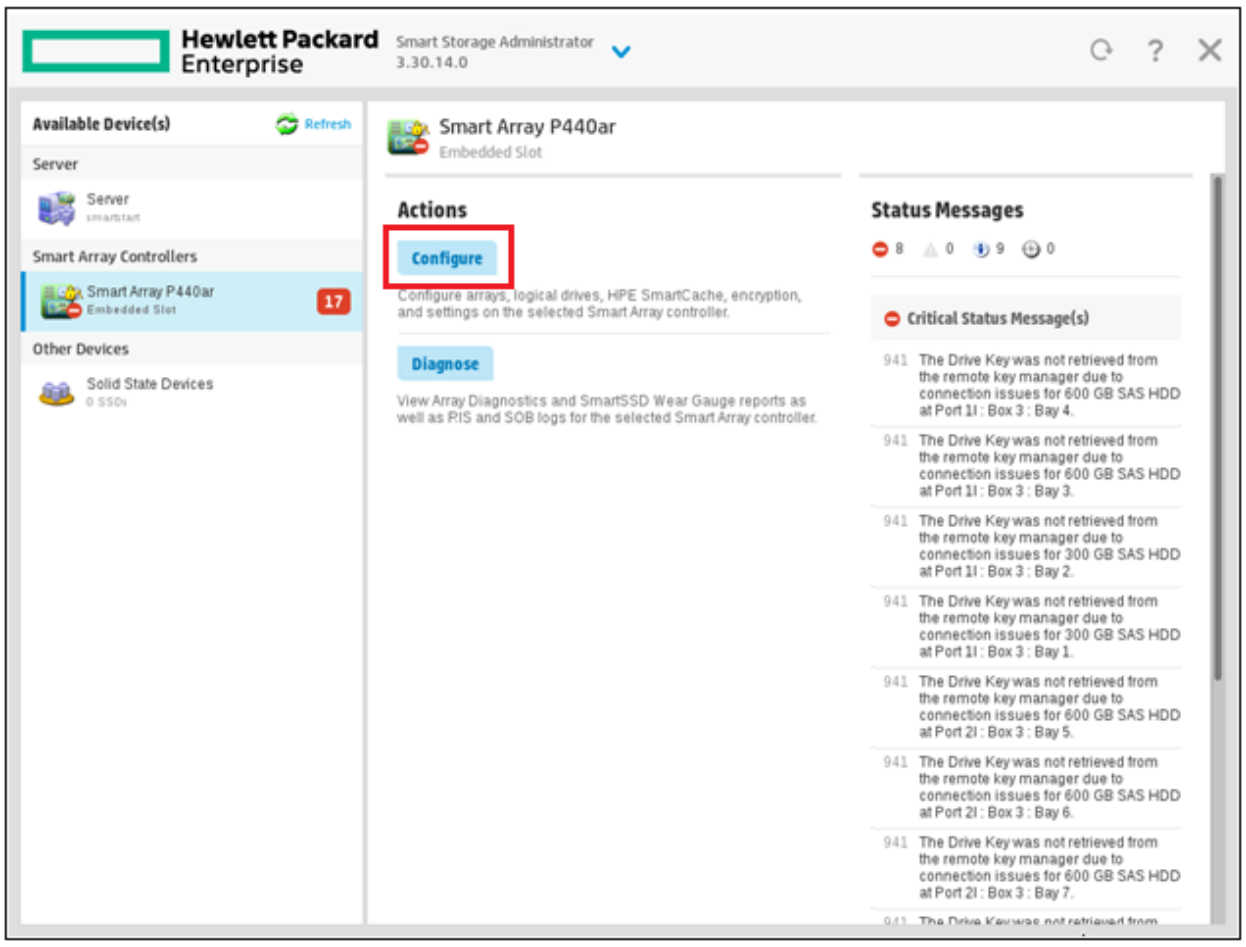

Figure 30 : Smart Array Administrator

5. Go to “Tools” and click on “Encryption Manager” to open it.
    a. Create a new crypto officer password.
    b. Perform the initial setup.
    c. Perform the full setup.
    d. Enter a crypto/security officer password.
    e. Enable and disallow future plaintext volumes (Recommended).

Please make sure that crypto/security officer are admins for Secure Encryption and must be trusted employees.

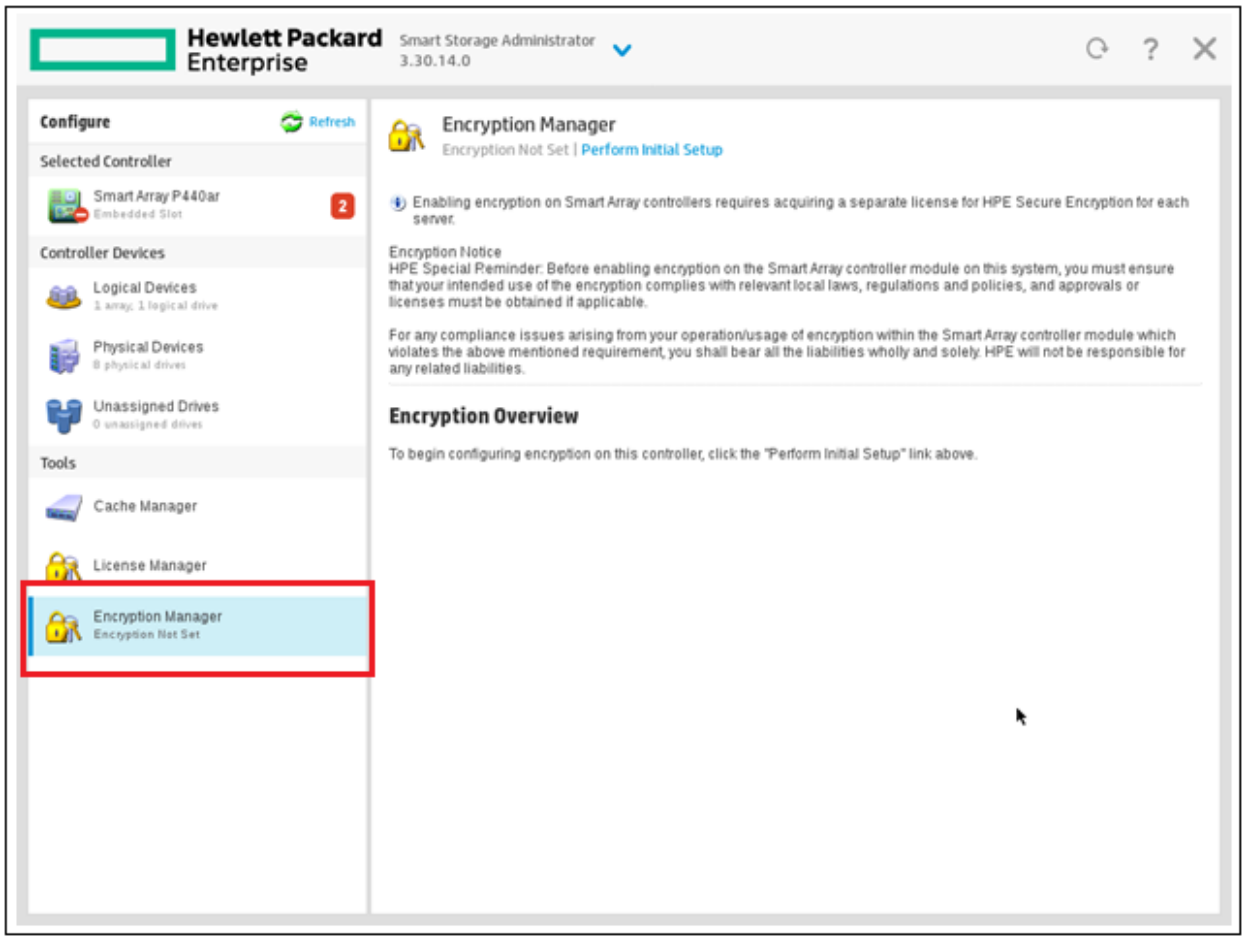

Figure 31 : Encryption Manager

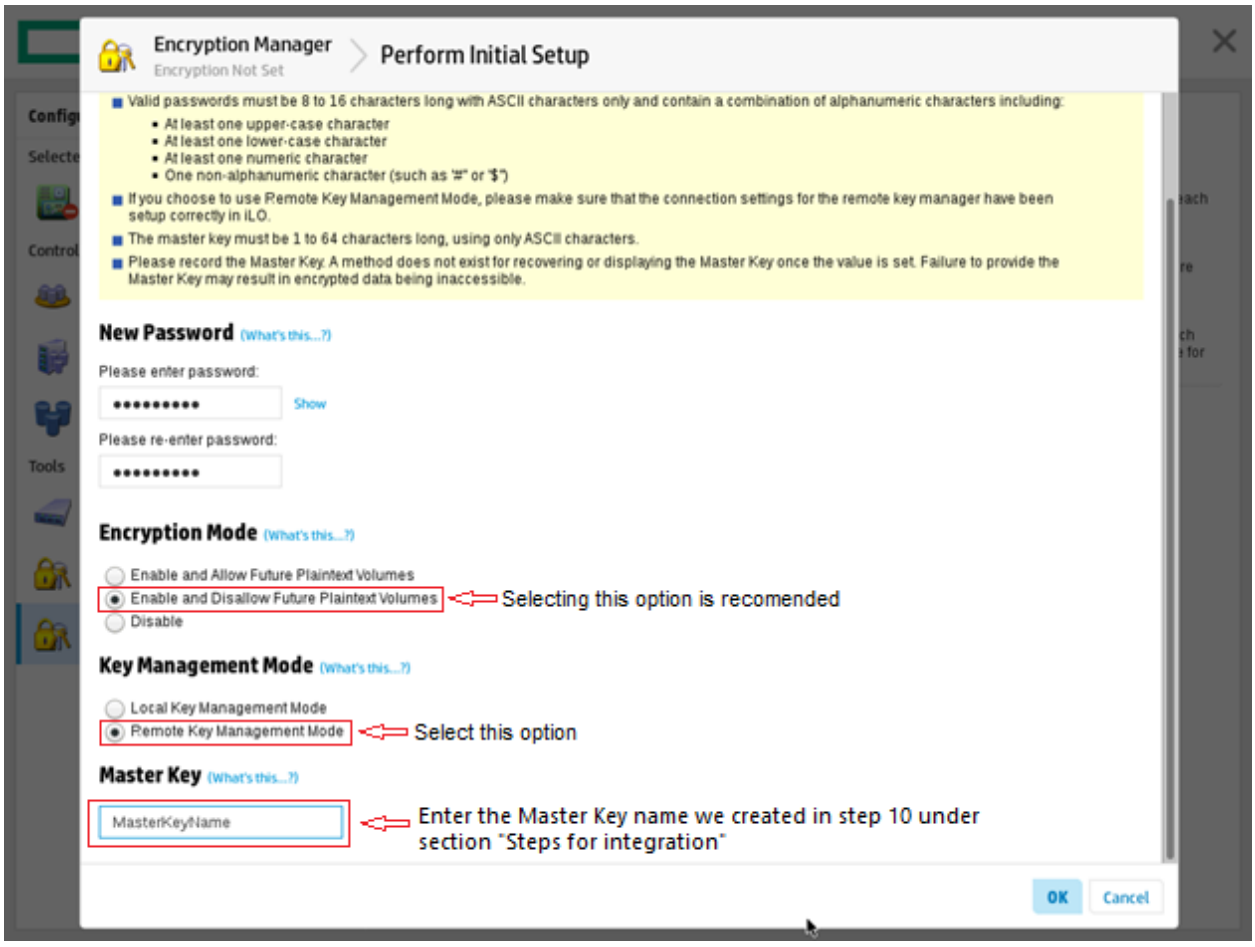

Figure 32 : Encryption Manager - Initial Setup

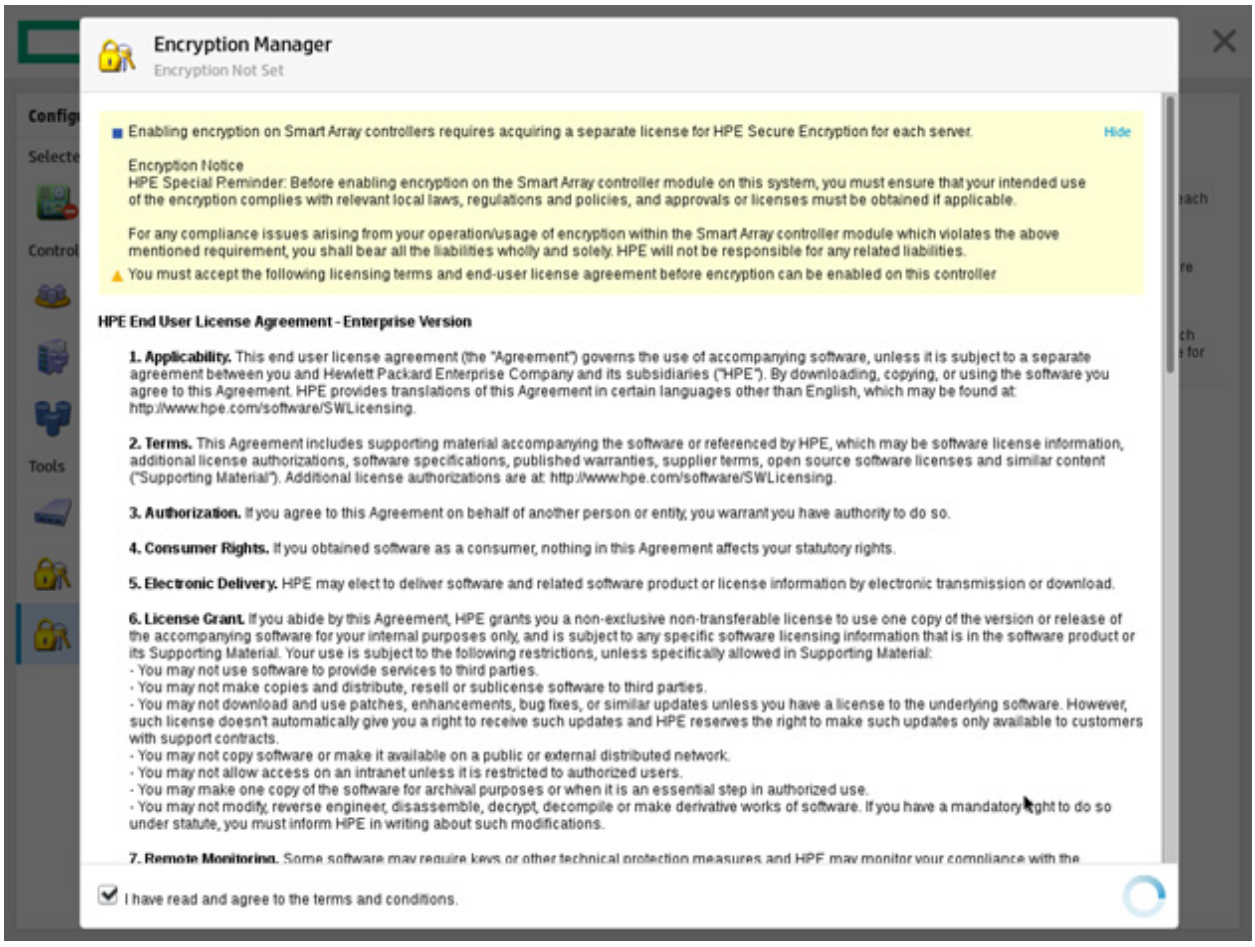

Figure 33 : Encryption Manager - End User License Agreement

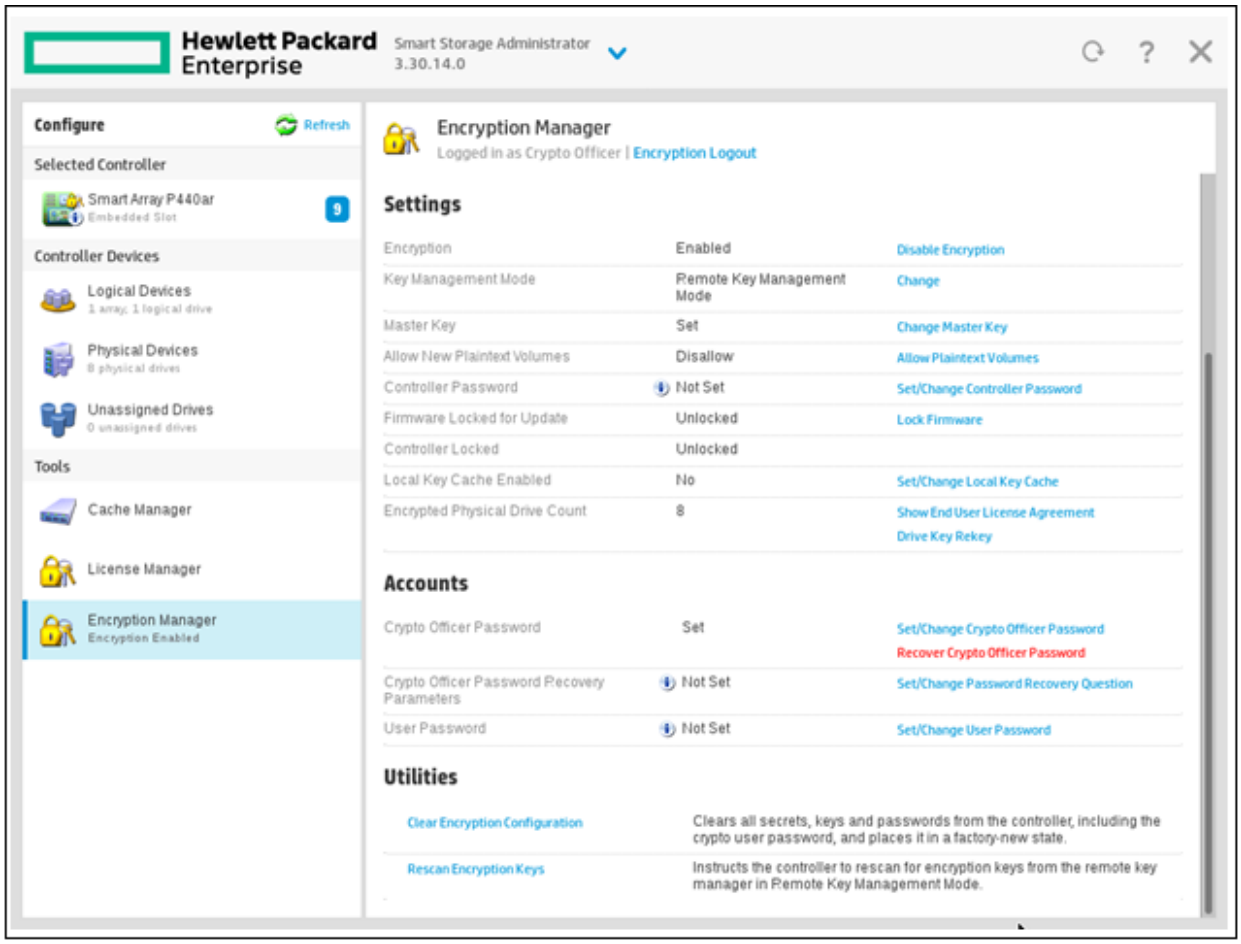

Figure 34 : Encryption Manager - Settings

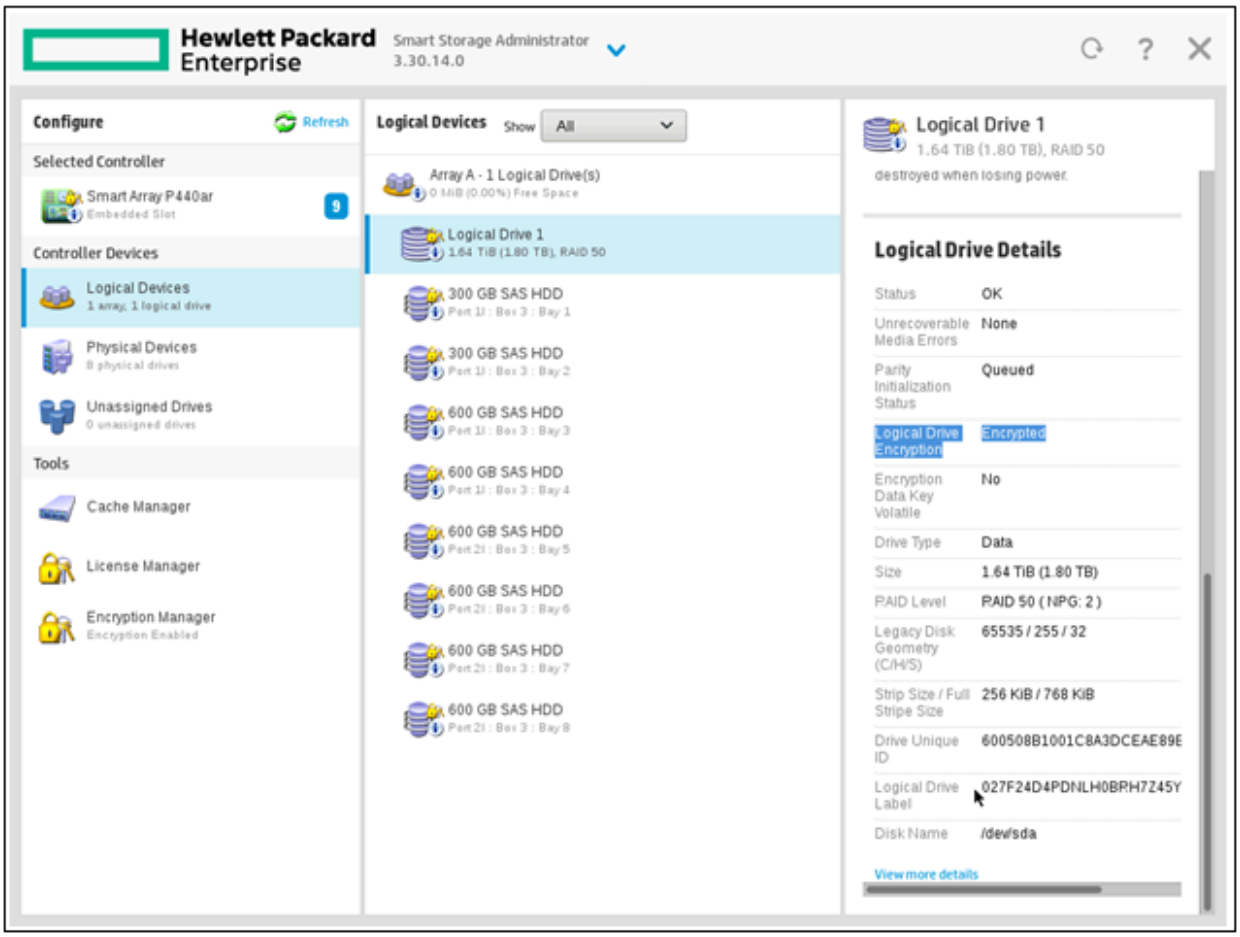

Figure 35 : Encryption Manager - Logical Devices

With this, ESKM will be successfully integrated with ProLiant by following the procedure described above.

6 Accessing Serial Console via PuTTY

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

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

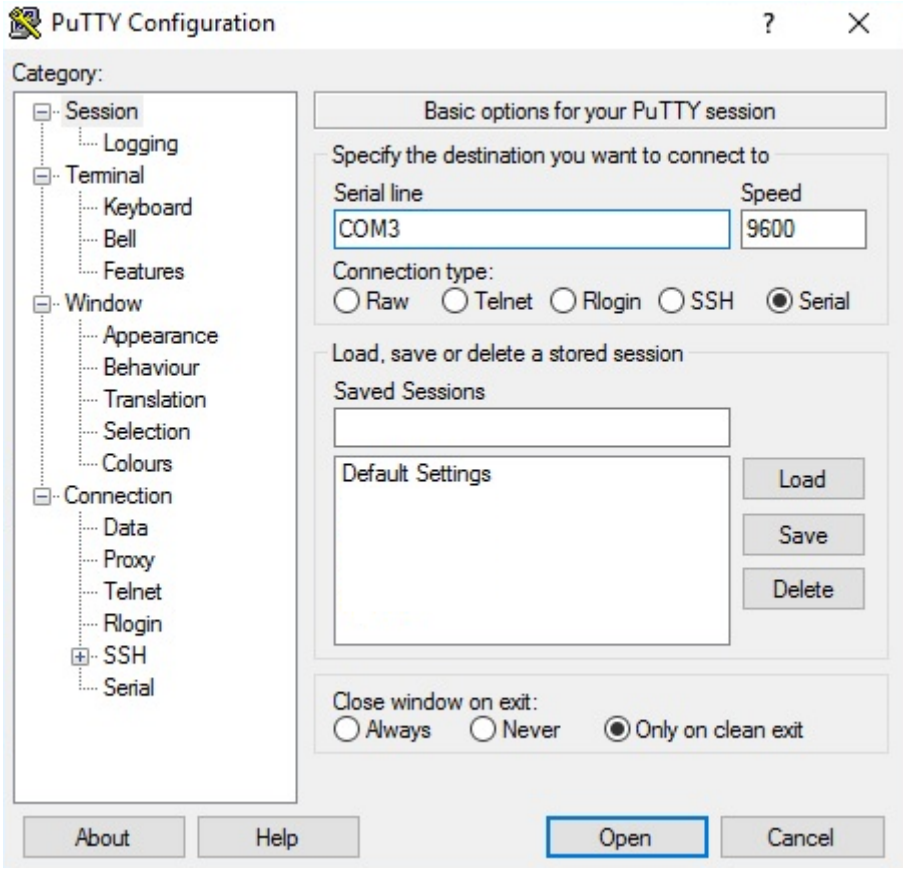

Figure 36 : PuTTY Configuration

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

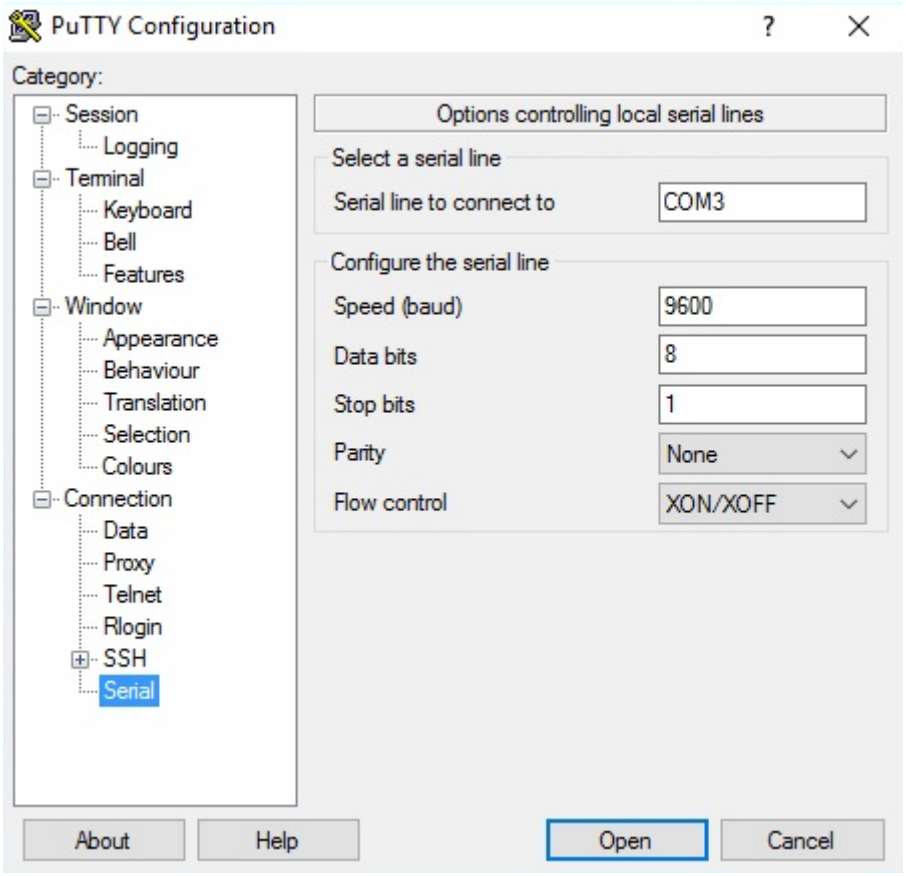

Figure 37 : PuTTY Configuration - edit serial line

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

7 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 Straße 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.

8 Appendices

8.1 References

Title	Document/Link
Utimaco ESKM website	https://hsm.utimaco.com/products-hardware-security-modules/key-management/eskm/
KMIP Specifications	https://www.oasis-open.org/standards
KMIP Implementations	https://wiki.oasis-open.org/kmip/KnownKMIPImplementations
HPE ProLiant's documentation	https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00020272en_us