HPE

ProLiant

iLO DL360 G11

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	0.1.0
Date	2025-12-16
Status	PUBLISHED
Document No.	IG-2025-0055

Table of Contents

1 About this guide

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

1.1 Intended audience

This guide is intended for system and security administrators with knowledge of:

- Data security administration
- Network configuration

1.2 Related documentation

The following documents provide related information:

- *Enterprise Secure Key Manager v5.2 Installation and Replacement Guide*
- *Enterprise Secure Key Manager v5.2 Software Version 7.2.0 Release Notes*
- *Enterprise Secure Key Manager v5.2 User's Guide*

1.3 Utimaco websites

For additional information, see the following Utimaco websites:

- https://hsm.utimaco.com/products-hardware-security-modules/key-management/eskm/

1.4 OASIS websites

In addition to the Utimaco websites, see the OASIS websites for more information on the Key Management Interoperability Protocol (KMIP) specification, usage guides and profiles:

- https://www.oasis-open.org/standards
- https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

1.5 Documentation feedback

Utimaco welcomes your feedback. To make comments and suggestions about product documentation, please send an email message to:

support-atalla@utimaco.com

All submissions become the property of Utimaco.

2 What's new in the ESKM v5.2 appliance

The ESKM v5.2 appliance is a complete solution for generating, storing, serving, controlling and auditing access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys, either locally or remotely.

3 Configuring the 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.

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

   Enter **y**.

To setup and configure PuTTY, please refer Accessing serial console via PuTTY.

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 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.

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 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.
```

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

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

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

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 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.

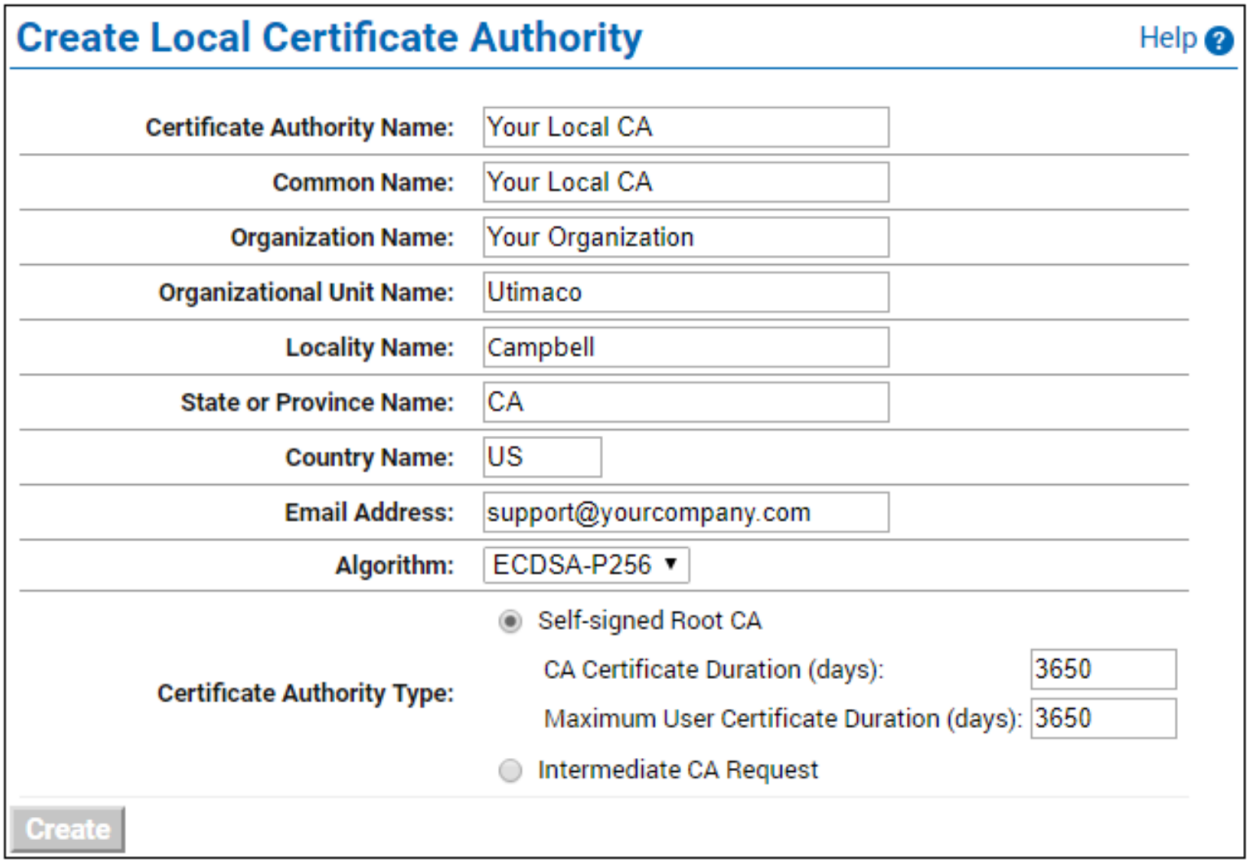
3.2 Setting up local CA

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.



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

b. Enter your organizational information.

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

d. Click **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.

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

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

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

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

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

e. Click **Add**.

f. Click **Save**.

Repeat the steps above any time another local CA is needed. For example,you may want to create a KMIP Local CA to support the KMIP Certify/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 & CA**s, click **Known CAs** to display the **Install CA Certificate section**.
2. Enter a value for the Certificate Name and paste the CA certificate text in the **Certificate** field.
3. Click **Install**. The CA certificate will be added to the Known CAs list.

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

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

5. Click **Add.**

6. Click **Save**.

3.3 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.

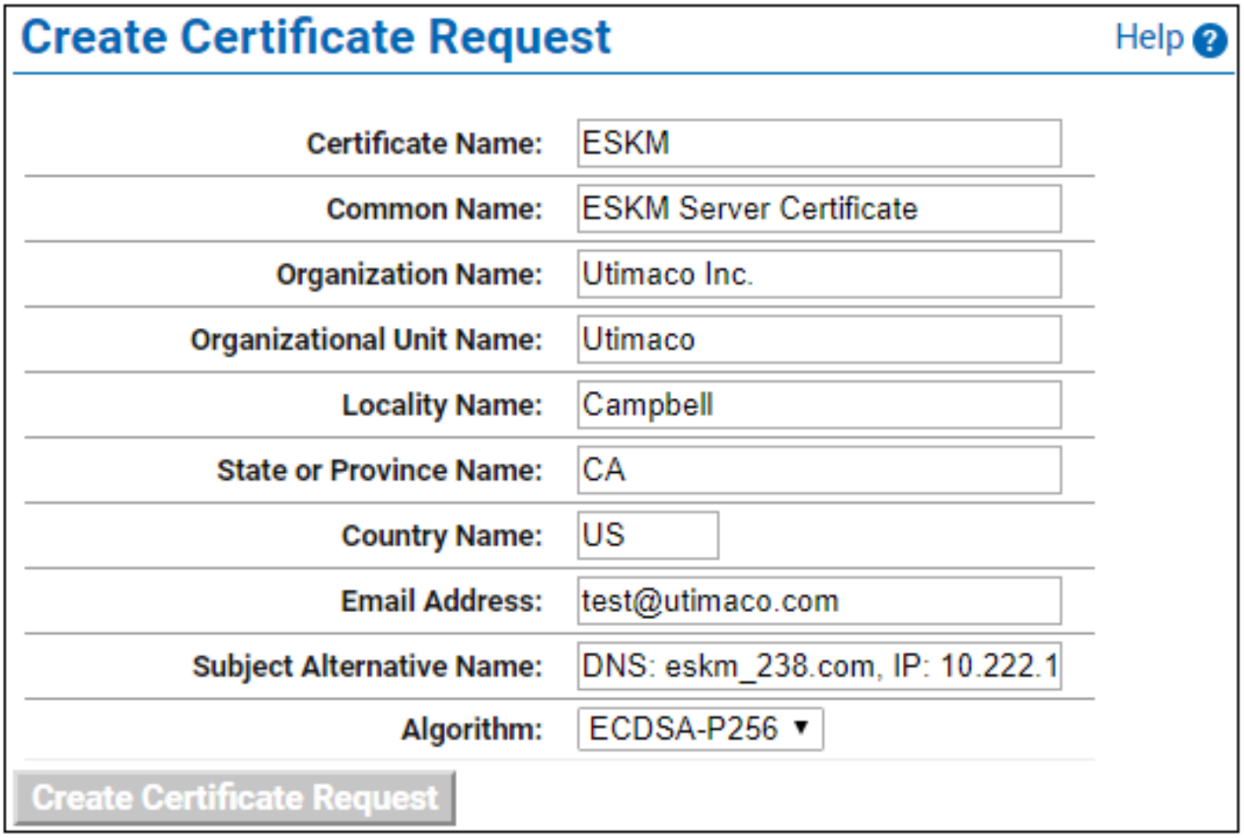
If you will be using a third-party CA, and wish to use an existing server certificate, see Import a third-party server certificate.

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.



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

Server.

b. Enter your Organizational information.

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

4. Click **Create Certificate Request.**

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.

6. Copy the certificate data, from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----` lines. This information will be used in step 10d of this section.

Certificate Request Information

Help

Certificate Name:	ESKM	
Key Size:	2048	
Subject:	CN:	ESKM Server Certificate
	O:	Utimaco Inc.
	OU:	Utimaco
	L:	Campbell
	ST:	CA
	C:	US
	emailAddress:	test@utimaco.com
Subject Alternative Name:	DNS:	eskm_238.com
	IP Address:	10.222.178.238

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDzCCAfcCAQAwgZkxIDAeBgNVBAMTF0VTS00gU2VydmVyIENlcnRpZmljYXRl
MRUwEwYDVQQKEwxVdGltYWNvIEluYy4xEDAOBgNVBAsTB1V0aW1hY28xETAPBgNV
BAcTCENhbXBiZWxsMQswCQYDVQQIEwJDQTELMAkGA1UEBhMCVVMxHzAdBgkqhkiG
9w0BCQEWEHRlc3RAdXRpbWFjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCm01rwBpnhz+rQOA3p7quPs240s0CMqm5hFPf1YNgh3CCa2oRDT5Ln
KfeBsI8GtuTH5v18v8rrz8jqsmb4uLF5aJJlsIMFK6rlmUyGumUr0d1K1xMYf50J
GFtOP6KukzucjU+IBE5uYI356C1PUABfVVpX88wn8P3DMkbCa4acVEbutOoONQeg
TD15Wy5OFeqku3s8D0Do9pz7uZFihJDmRy5pscmLKSUKAsW8CUYwITiBw2pNAYlc
l++png/7FIavzVq5GIl/VPDTwqcAKi78qNMNaRFpgckBbKXG/qoWc+J7VQcqFKjY
i+JNh9PyLgGC20uMDY5E0+SEDLcrgmx/AgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAf
MB0GA1UdEQQWMBSCDGVza21fMjM4LmNvbYcECt6y7jANBgkqhkiG9w0BAQsFAAOC
AQEAkA7CJz6AuQZ1gf+2BGO3ghbVt04EY7f+6vvo0QriilFO9q6FXKmrkaUJRSXQ
aF7UGT8Kv0j+/sChLjuGk+iZ2iiCtqHtOmsZgYTCMAvmu9HSqkA6Ofmg4UH/ri6w
rFZE8lnZ341Q0bhtkRS+OidgA/KyQAU0YNzjYr9fXuu5M8xx4q+Kfj5MRCNxLGbb
rYgzFLVUDvcBaWteMeucnmVB836wNITjKVL24NcicZCwu6LjyZtTcCA1aaevX6Hm
sxJjZLmwvJxxU6sdXZUu8+GTMH59XgFj3BK5xiDtW4aHGEYo4Hog4RTBoFXKAuGt
L4ITARZ9zJyVso8SYiG4k1z1Rg==
-----END CERTIFICATE REQUEST-----
```

Download | Install Certificate | Create Self Sign Certificate | Back

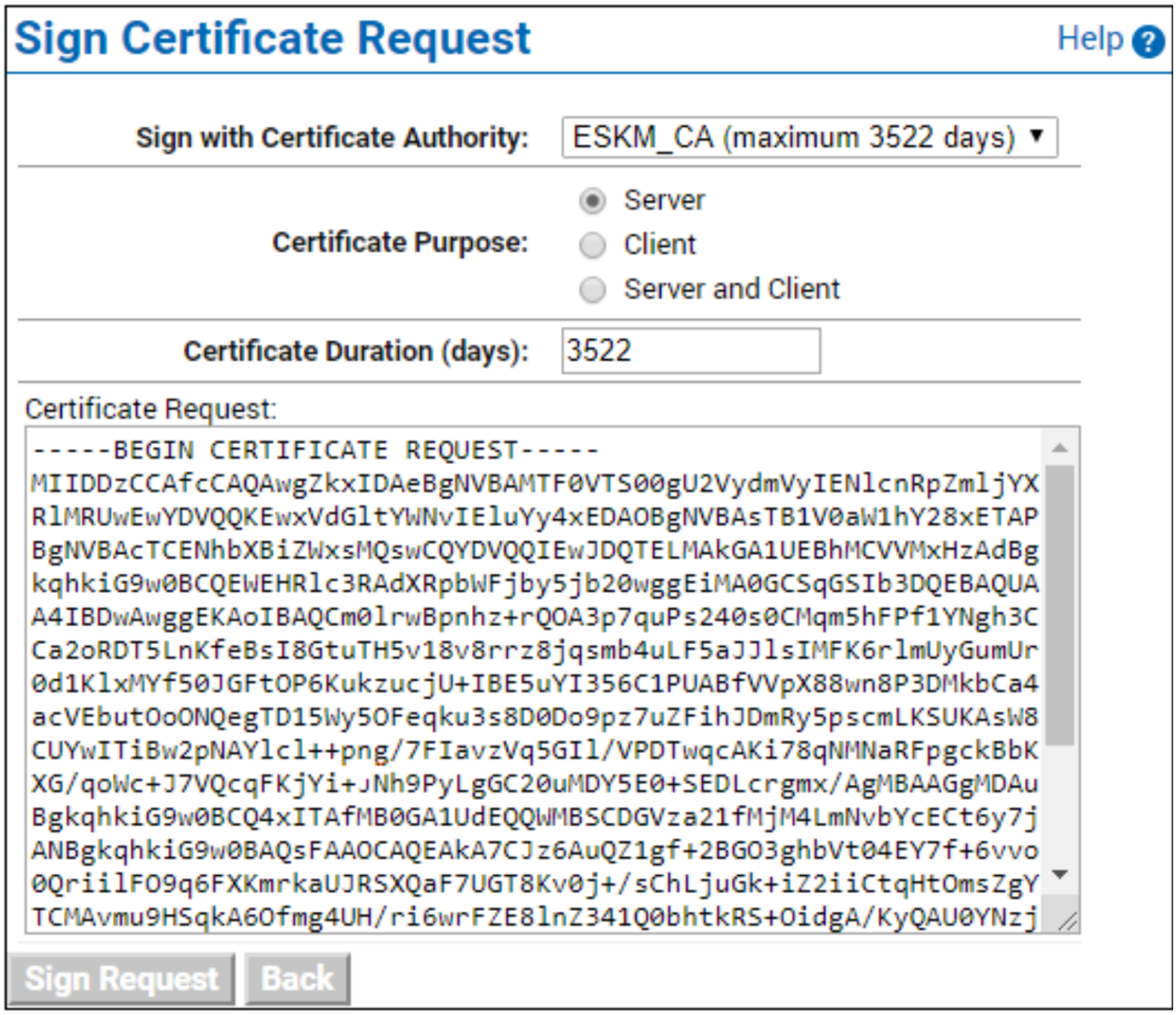
Key Size refers to the size of the key or elliptic curve associated with this certificate.

7. In the **Certificates & CAs** menu, click **Local CAs**.

8. Click on the CA name you created in Setting up local CA for example **ESKM Local CA**.

9. Click **Sign Request**.

10. Enter data required by the Sign Certificate Request section of the 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).

d. Paste the copied certificate data from step 6 into the **Certificate Request box**.

11. Click **Sign Request**.

12. Copy the signed certificate data, from `-----BEGIN CERTIFICATE to END CERTIFICATE----` lines. This information will be used in step 16.

13. In the **Certificates & CAs** menu, click on **Certificates**.

14. Click on the certificate name created in step 3 of this section. For example,

ESKM KMS Server.

15. Click **Install Certificate**.

16. 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.

3.3.1 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:

```
-----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**.

3.4 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 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.

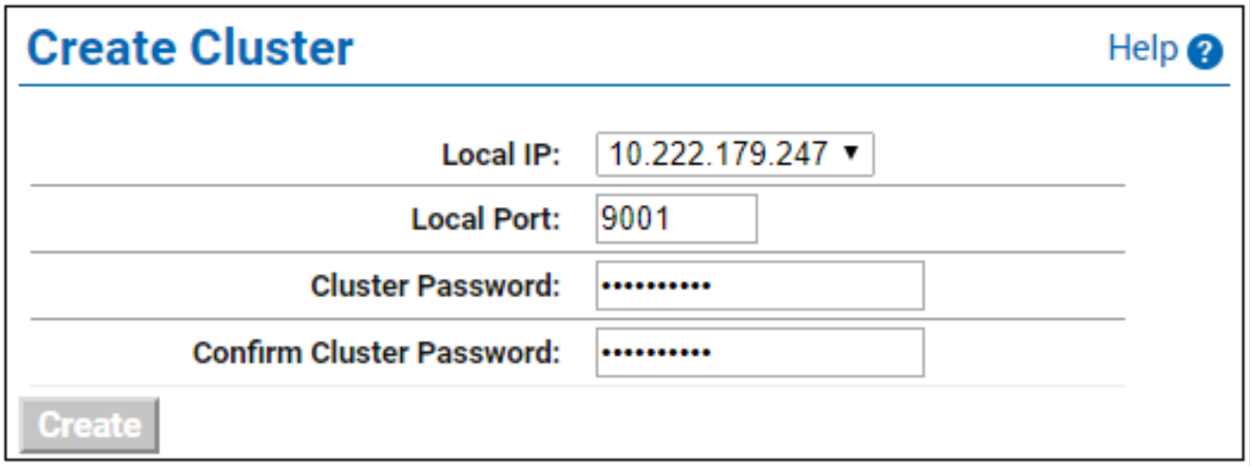
3.5 Creating the cluster

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**.



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

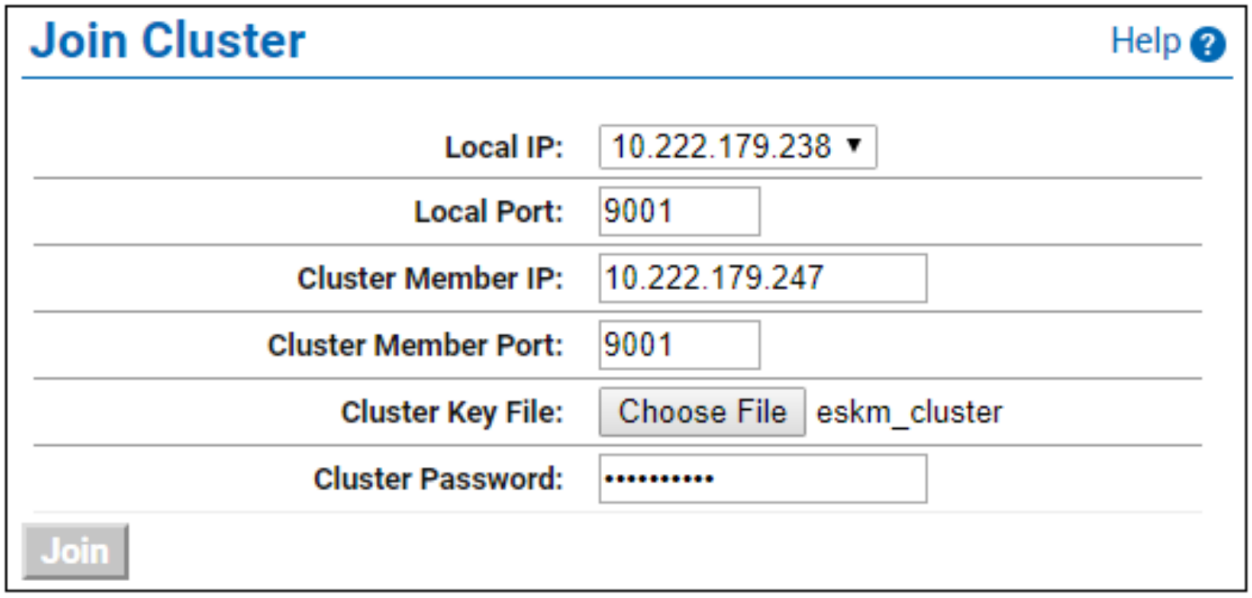
All ESKM servers in a cluster must use an IPv4 address for the cluster.

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.

3.6 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.



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

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.

3.7 Setup KMIP server

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

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

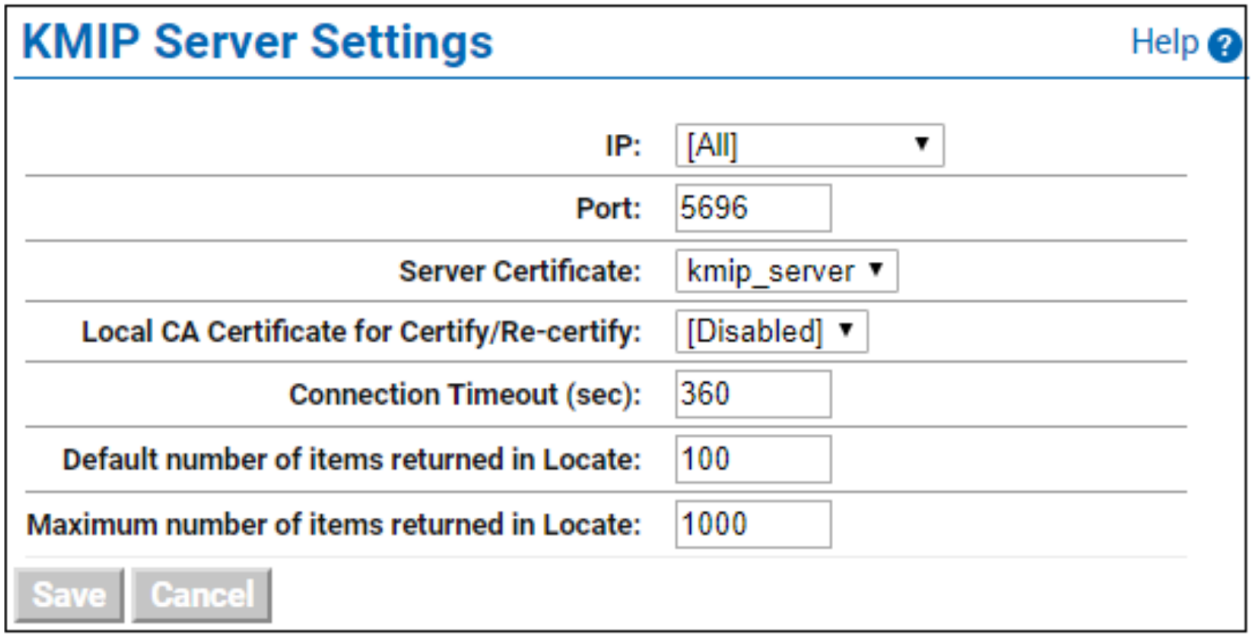
To configure the KMIP server, perform the following steps:

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

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

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

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



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**).

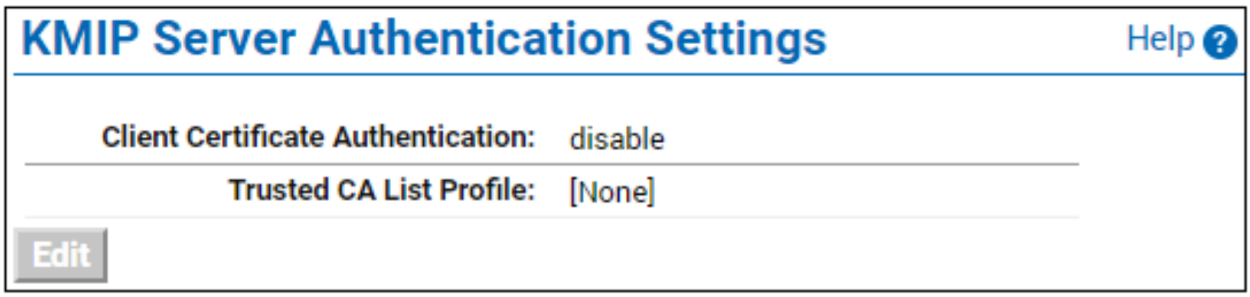
b. The status of the KMIP server should be Started. If the status is Stopped, select the KMIP Server, and then click **Start**.

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.

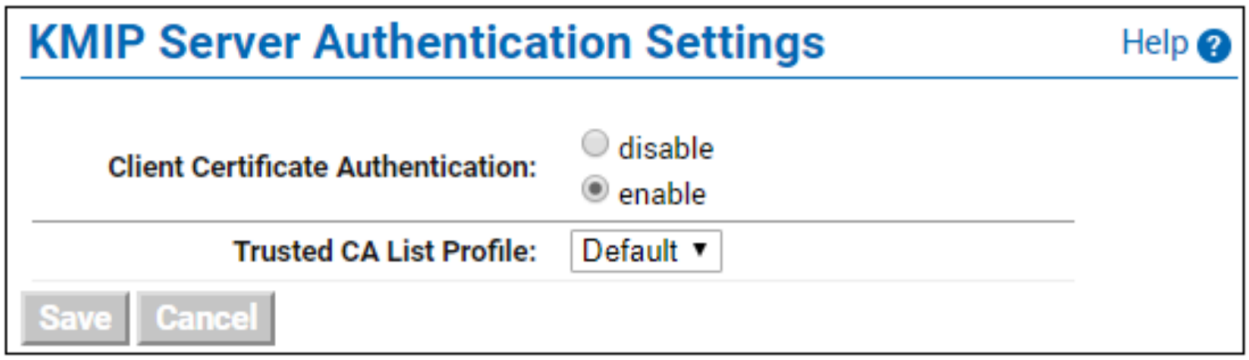
KMIP requires mutual authentication. After configuring the KMIP server, **enable** KMIP client certificate authentication. The KMIP client certificate authentication status is **disabled** by default.

To enable KMIP client certificate, perform the following steps.

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



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



3.8 Setup KMS server

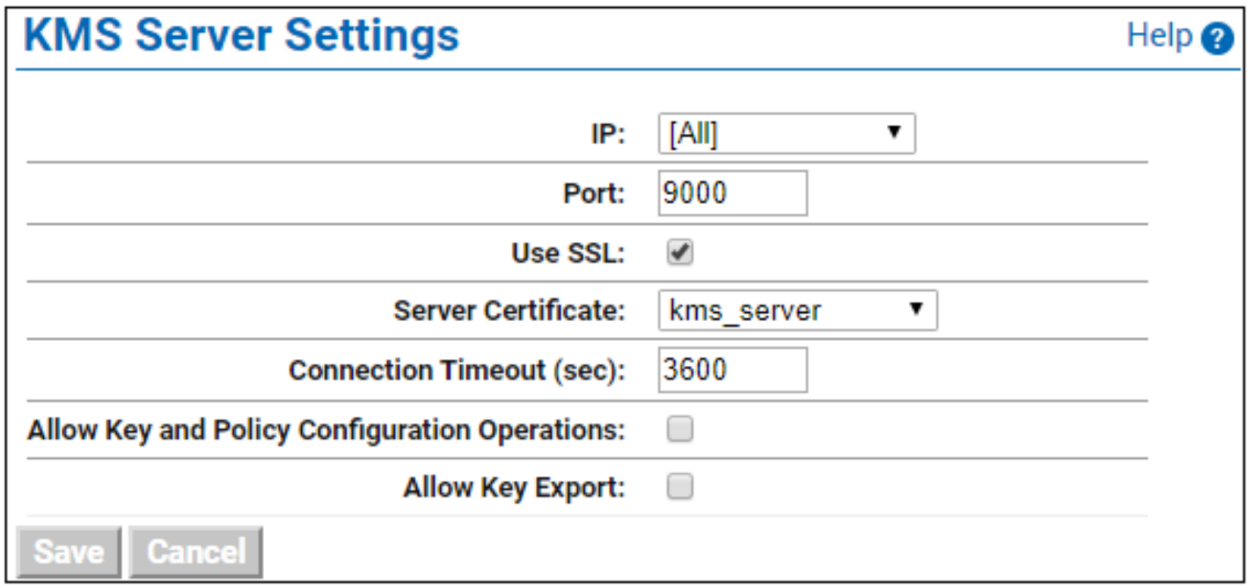
Setup KMS server

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

To configure the KMS server, perform the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMS Server** to display the **KMS Server Configuration** window.
3. In the **KMS Server Settings** section of the window, click **Edit**.

4. Configure the KMIP Server Settings. The IP address can be an IPv4 address, or IPv6 address. If support for IPv6 has been enabled, see First run. If necessary, change the Port and Connection Timeout values. Utimaco recommends the default values of 9000 for the Port and 3600 for the Connection Timeout. For **Server Certificate**, select the name of the certificate you created in Setting up ESKM certificate. For example, ESKM KMS Server.



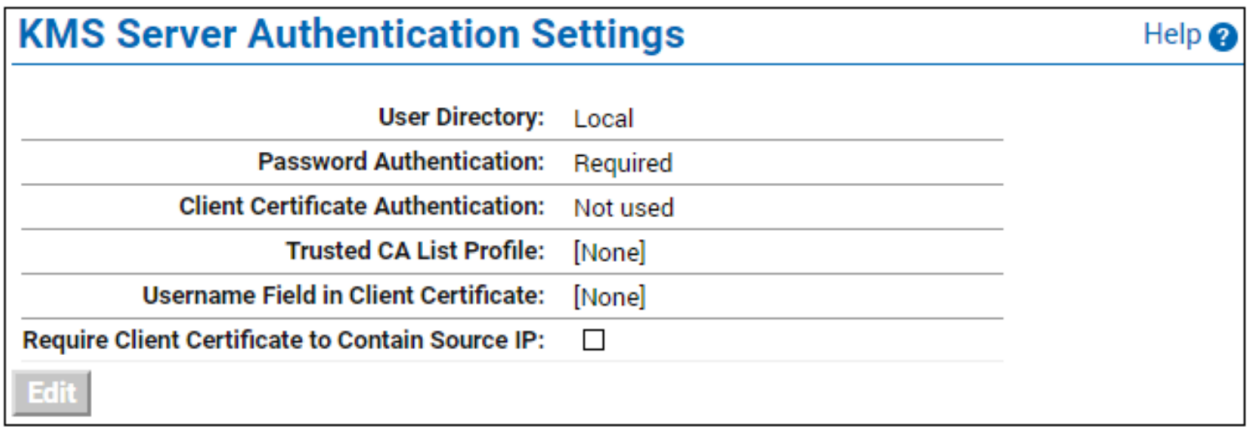
5. Click **Save**.

6. Confirm that the KMS server is started.

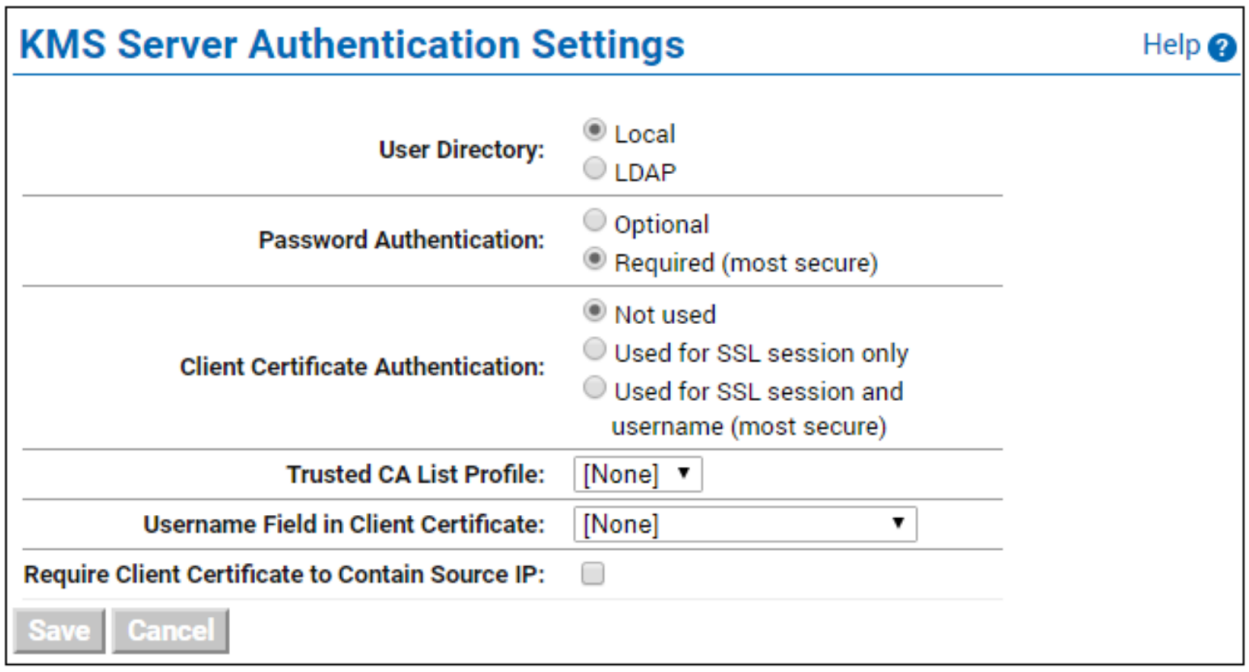
a. Go to the Services List section of the Services Configuration page (**Device -> Maintenance -> Services -> KMS Server**).

b. The status of the KMS server should be Started. If the status is Stopped, select the KMS Server, and then click **Start**. To enable KMIP client certificate, perform the following steps.

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



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



4 Configuring the HPE ProLiant Server

Utimaco's Enterprise Secure Key Manager (ESKM) is a most versatile scalable key manager to securely manage encryption keys across the enterprise. The ESKM can use its native protocol (KMS – Key Management Service) or industry-standard OASIS KMIP (Key Management Interoperability Protocol) for its client integrations. This integration guide concentrates on enabling client-side encryption for HPE ProLiant servers and centralized key management to simplify security operations like compliance auditing, centralized key management and policy execution along with enforcement.

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

4.1 Pre-requisites for Integration

- Requires Secure Encryption license for the Proliant server from HPE.
- Requires iLO Advance license for the Proliant server from HPE.
- Requires minimum HPE ProLiant Gen8/9/10 (iLO v4).
- Requires retrieving and installing HPE SSA (Smart Storage Administrator) software.
- Requires installing and configuring a Smart Array Controller compatible for Secure Encryption (typically Px3x and Px4x).
- Enterprise Secure Key Manager.

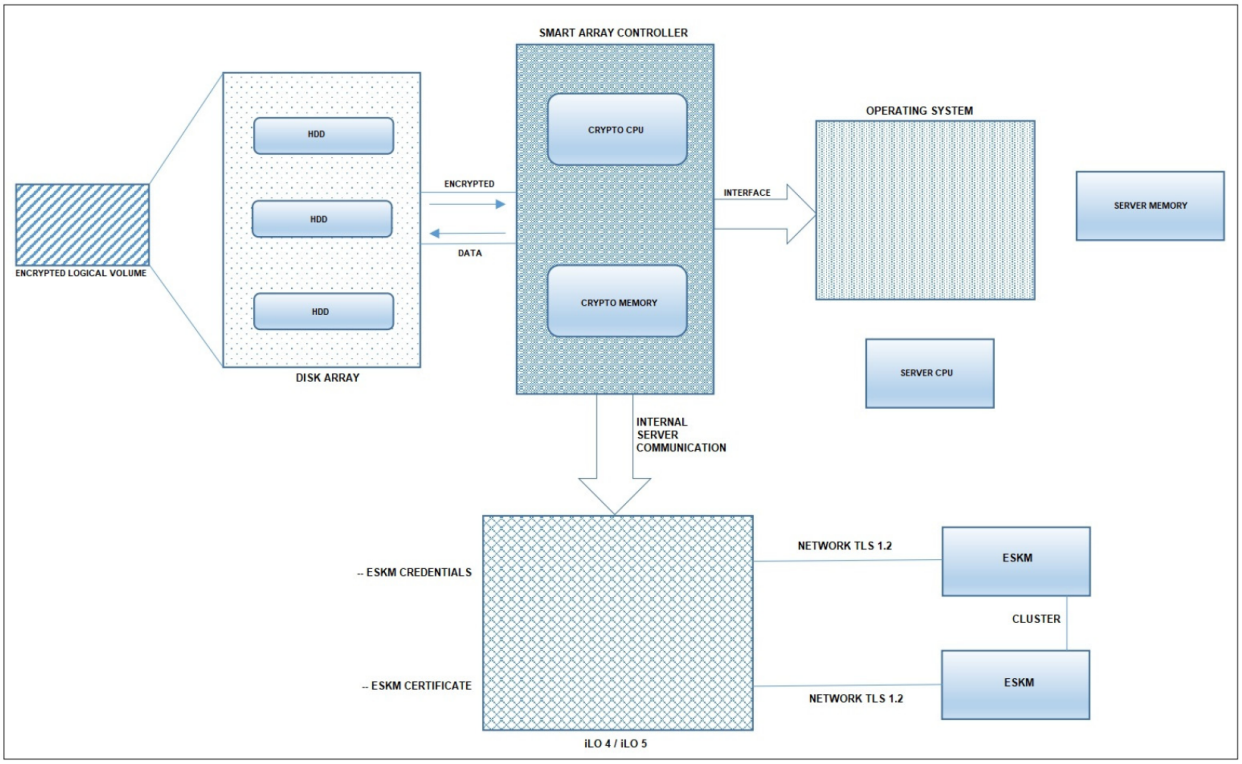
For more information about HPE ProLiant's documentation, refer to https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00020272en_us

5 Integration

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

5.1 Steps for integration

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



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.

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**.

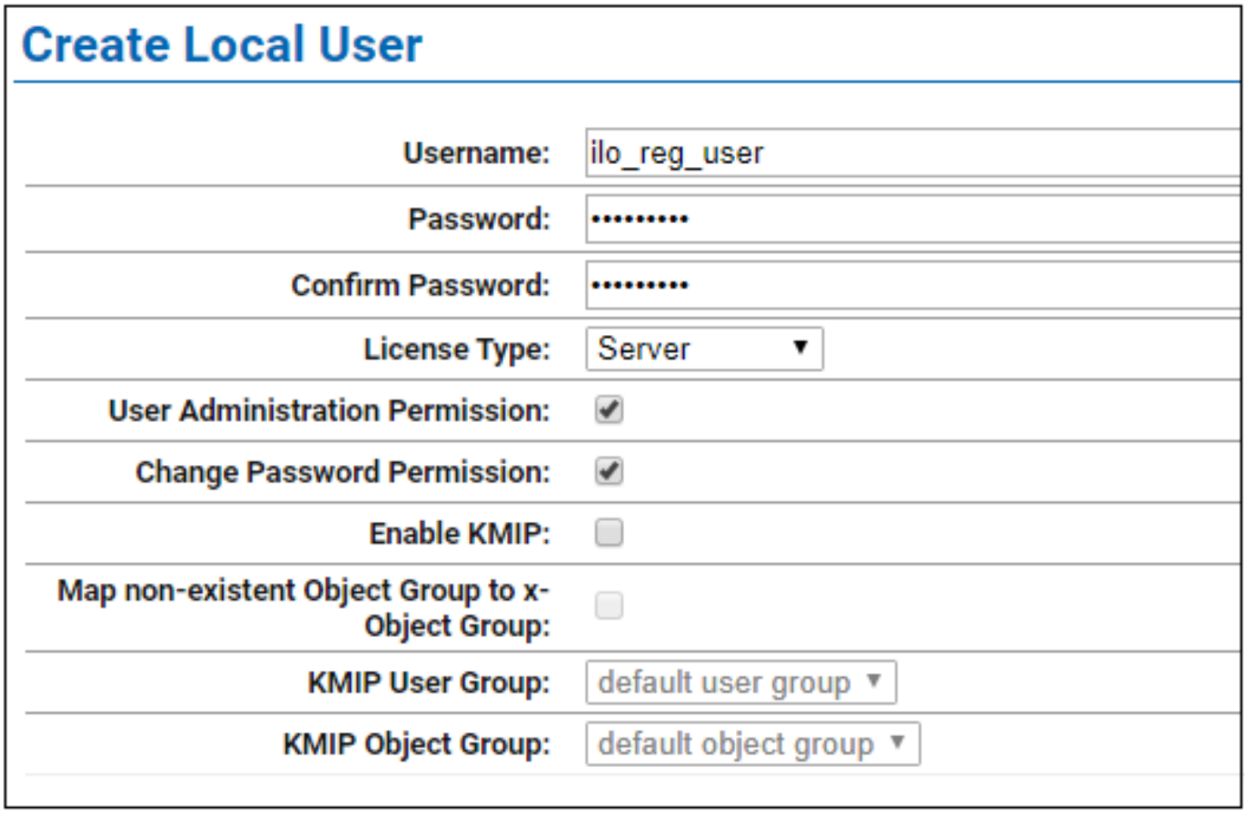
4. Create a local user with the username, “ilo_reg_user”.

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.



5. Go to **Security > Users & Groups > Local Groups**.

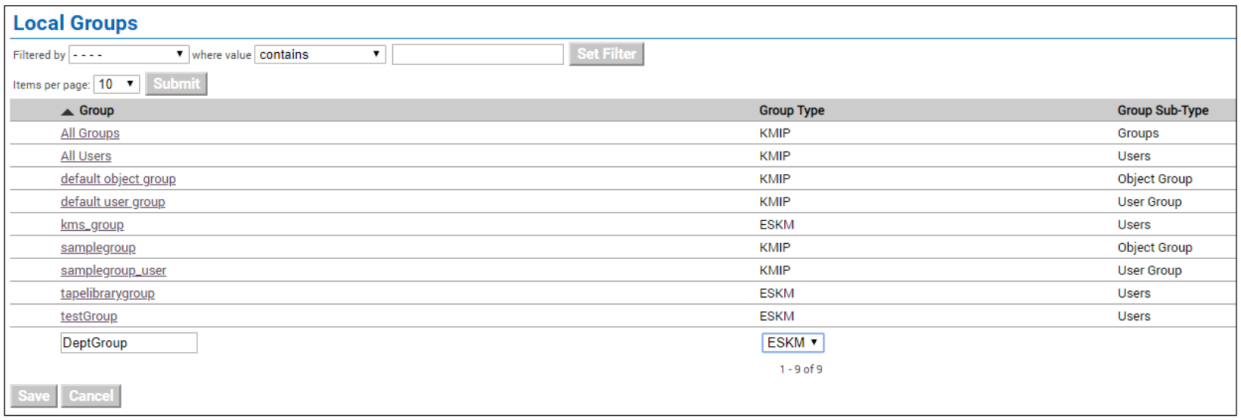
6. Click on **ADD**.

7. Create a user group which 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.



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.

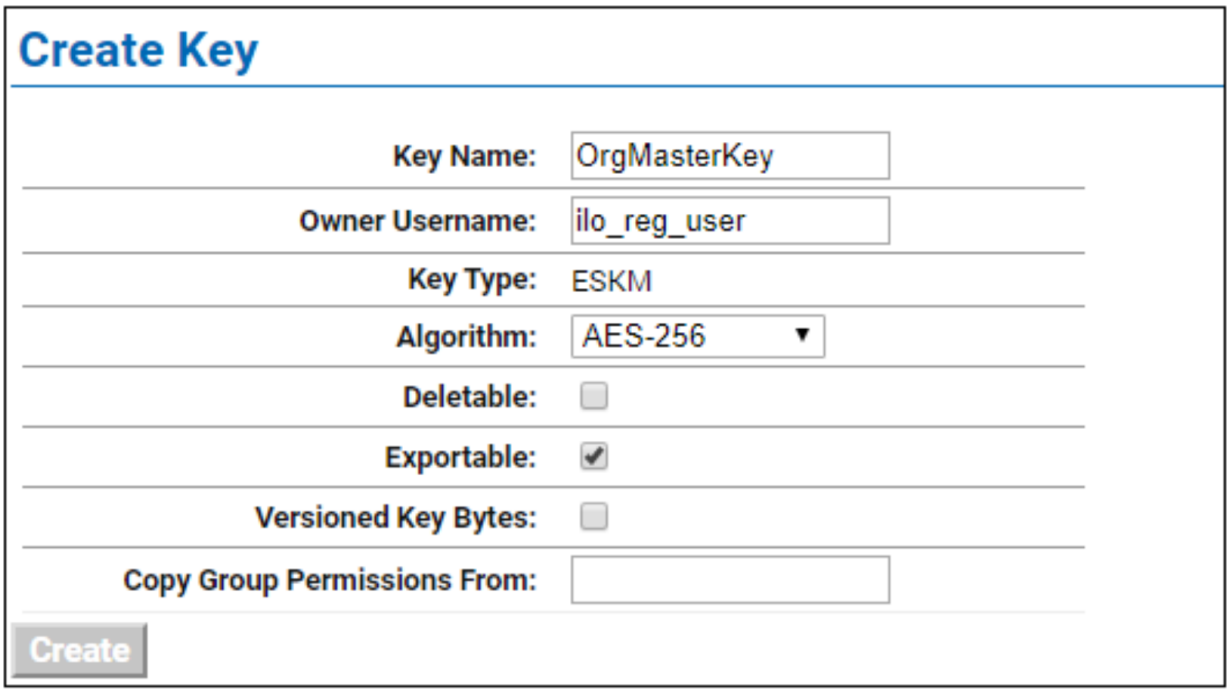
The master user created earlier.

c. Key Type: ESKM.

d. Algorithm: AES-256.

e. Exportable: Enable.

11. Click on **Create**.



12. Assign the master key to the group that was previously created.

13. Run a Key Query in the ESKM

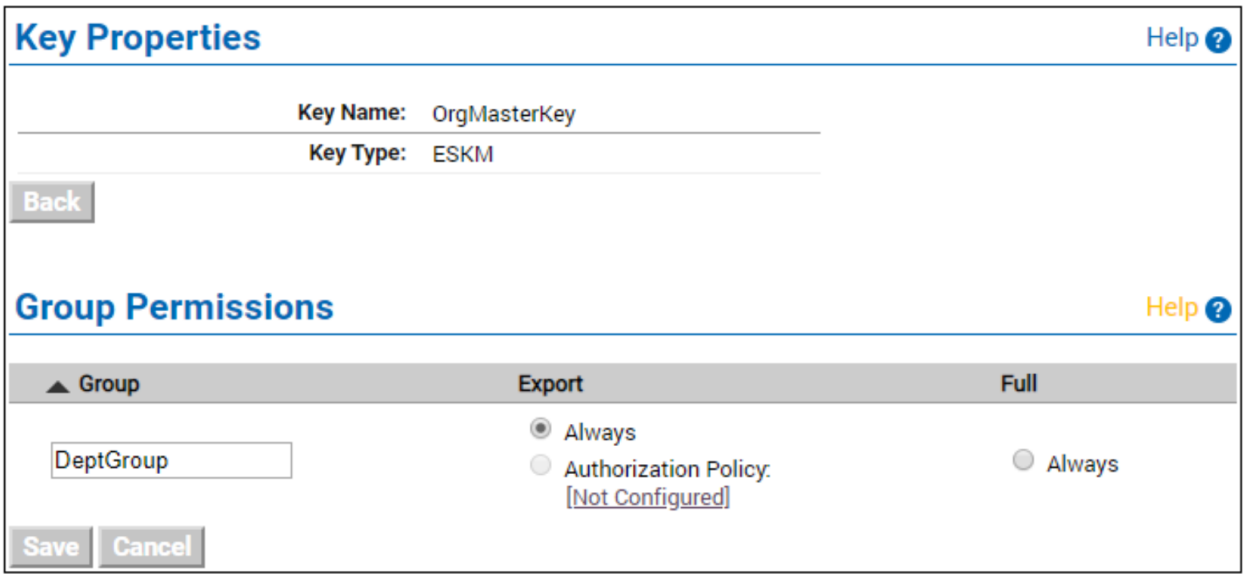
14. Find the key that you created in step 10.

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”.

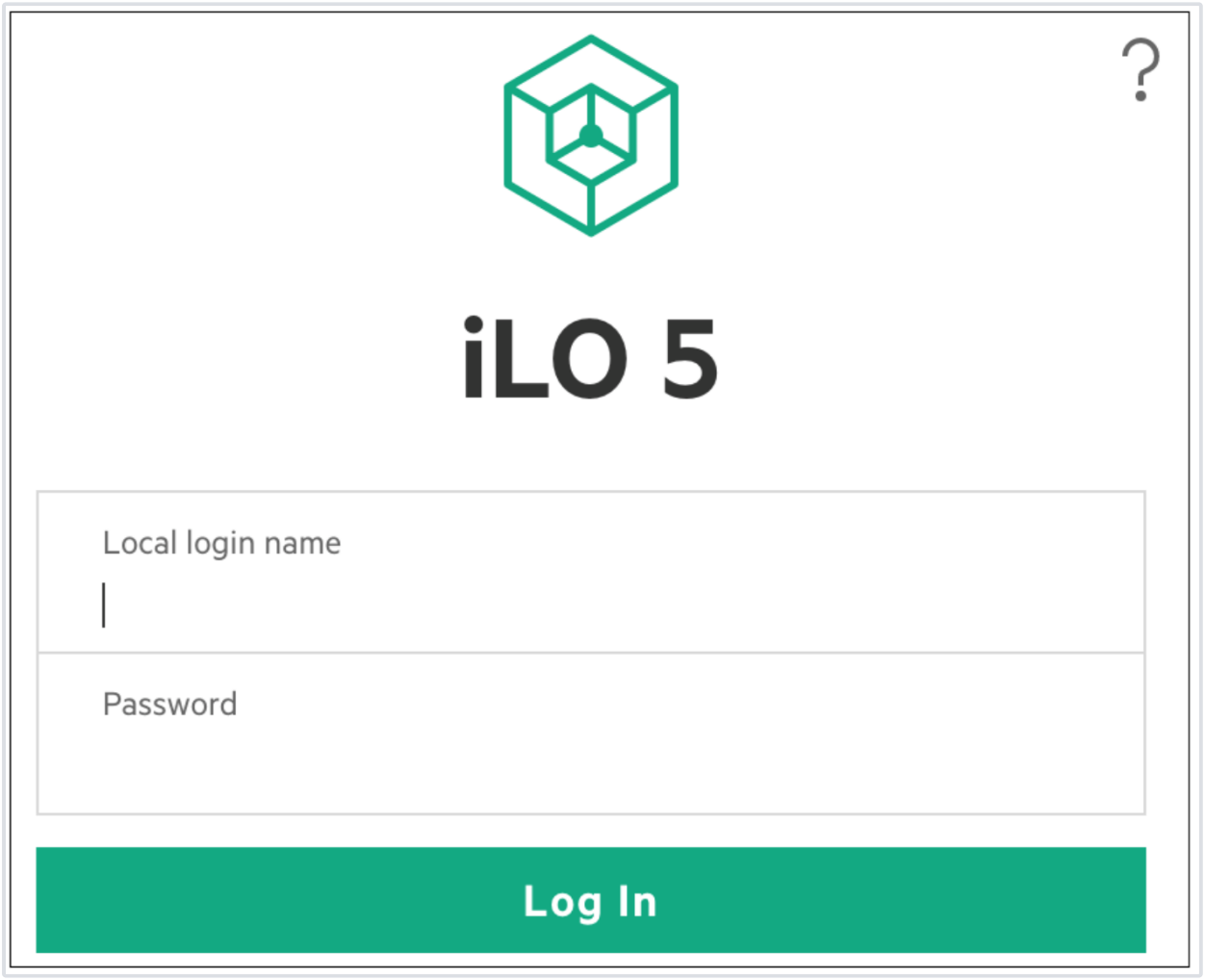


17. Click on Save.

5.2 Configuring iLO for enrollment with ESKM

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

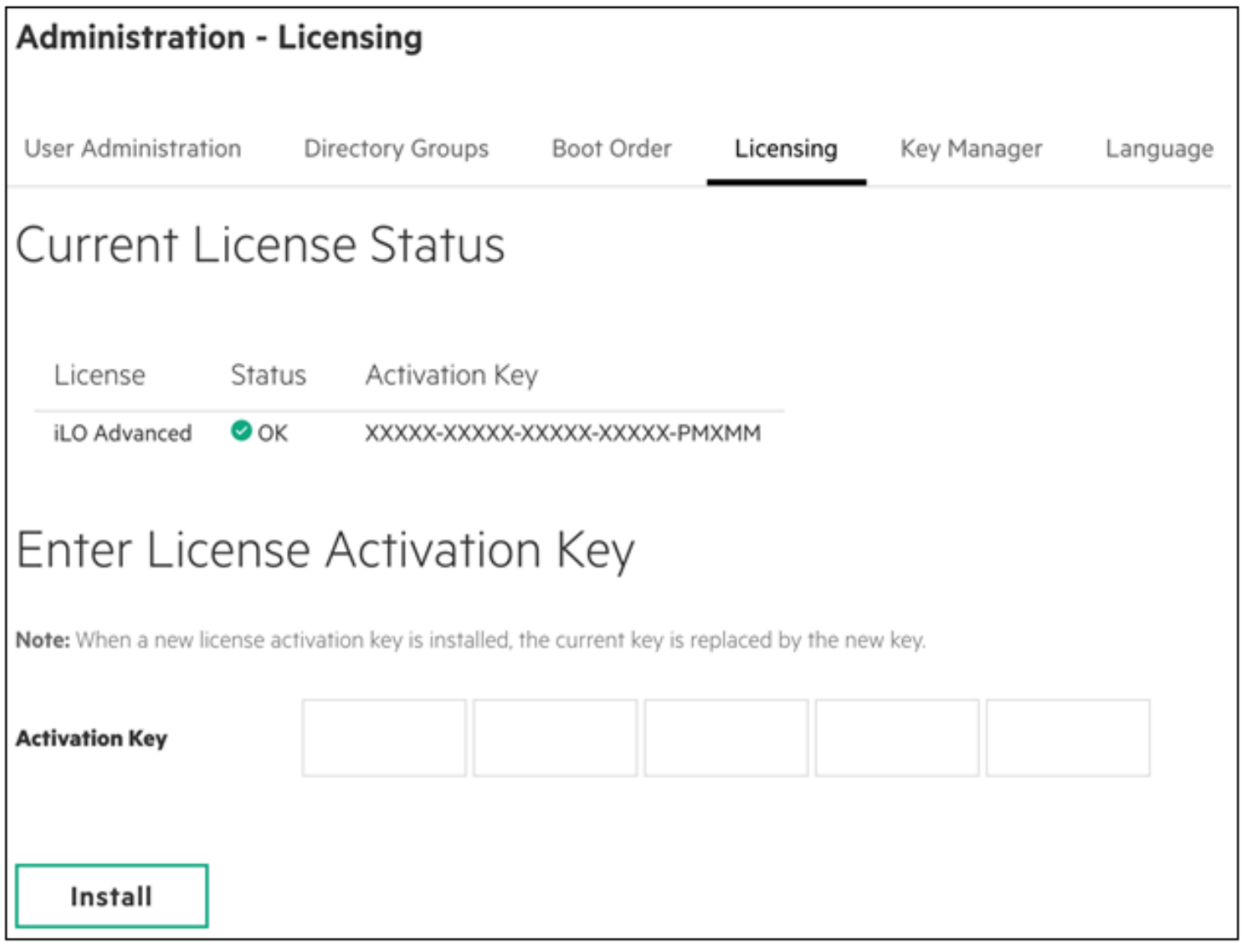
1. Login to the iLO interface with “Local login name” and Password”.



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

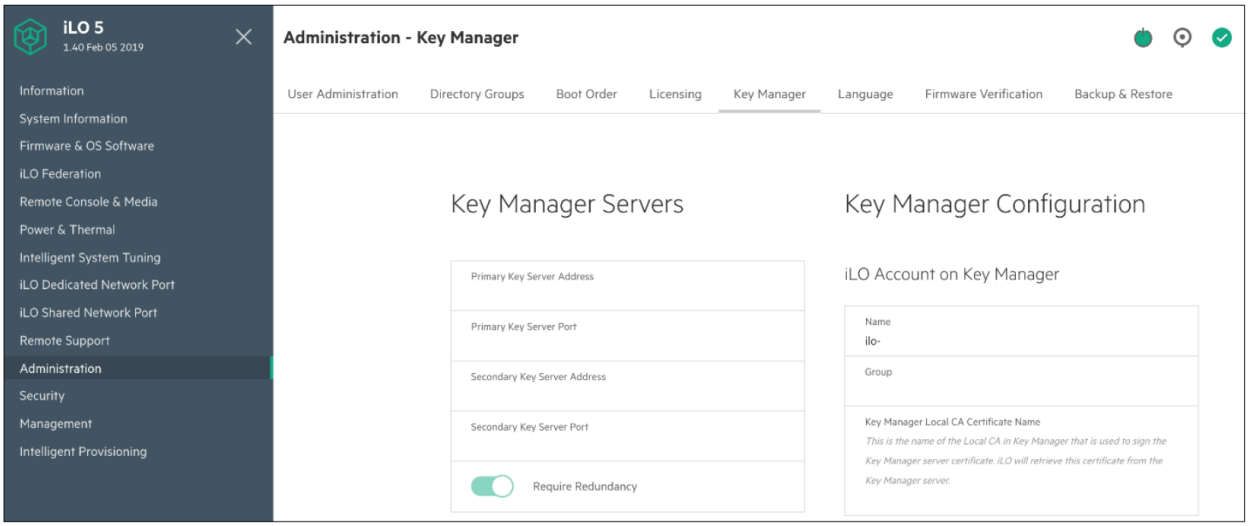


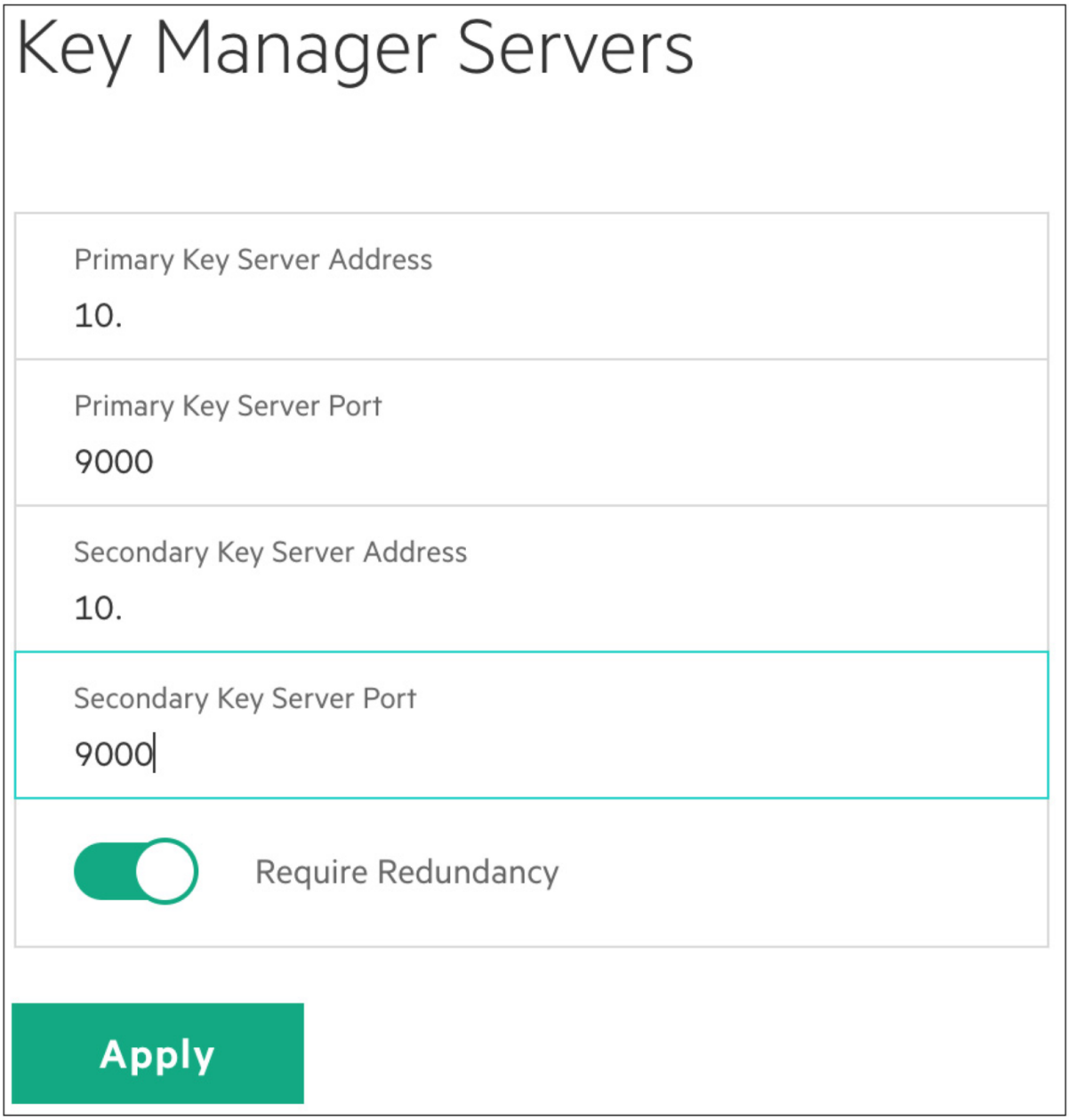
3. Click on the “Administration” menu and click on the “Key Manager” tab.
4. Fill out the “Key Manager Servers” form.

a. Primary Key Server Address: ESKM server IP Address.

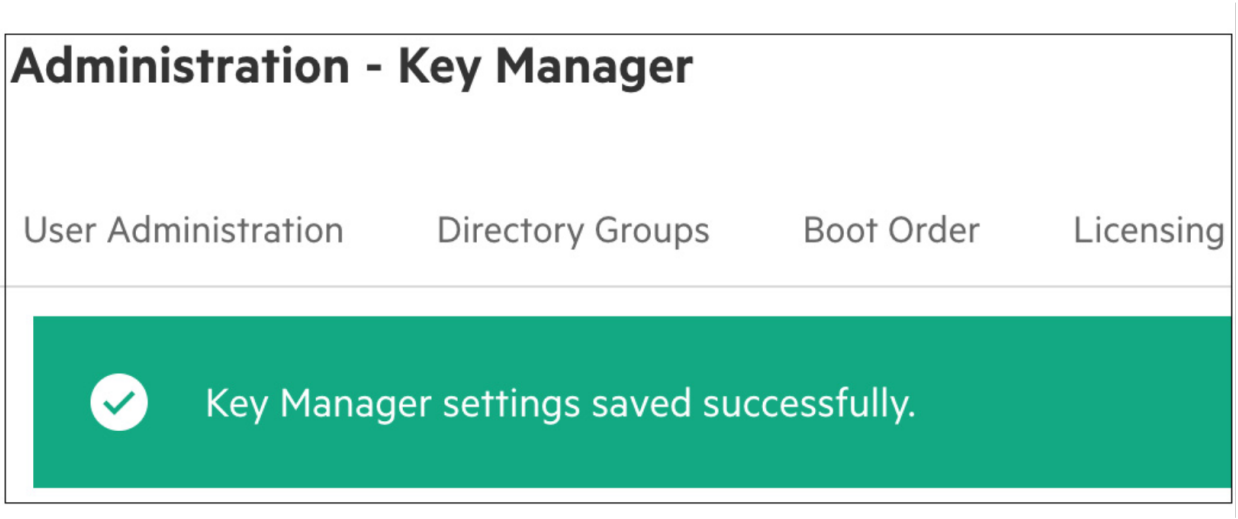
b. Primary Key Server Port: ESKM KMS Server Port (9000).

c. Require Redundancy: Enable.


iLO 5
1.40 Feb 05 2019
Information
System Information
Firmware & OS Software
iLO Federation
Remote Console & Media
Power & Thermal
Intelligent System Tuning
iLO Dedicated Network Port
iLO Shared Network Port
Remote Support
Administration
Security
Management
Intelligent Provisioning
Administration - Key Manager
User Administration
Directory Groups
Boot Order
Licensing
Key Manager
Language
Firmware Verification
Backup & Restore
Key Manager Servers
Primary Key Server Address
Primary Key Server Port
Secondary Key Server Address
Secondary Key Server Port
Require Redundancy
Key Manager Configuration
iLO Account on Key Manager
Name
ilo-
Group
Key Manager Local CA Certificate Name
This is the name of the Local CA in Key Manager that is used to sign the Key Manager server certificate. iLO will retrieve this certificate from the Key Manager server.



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



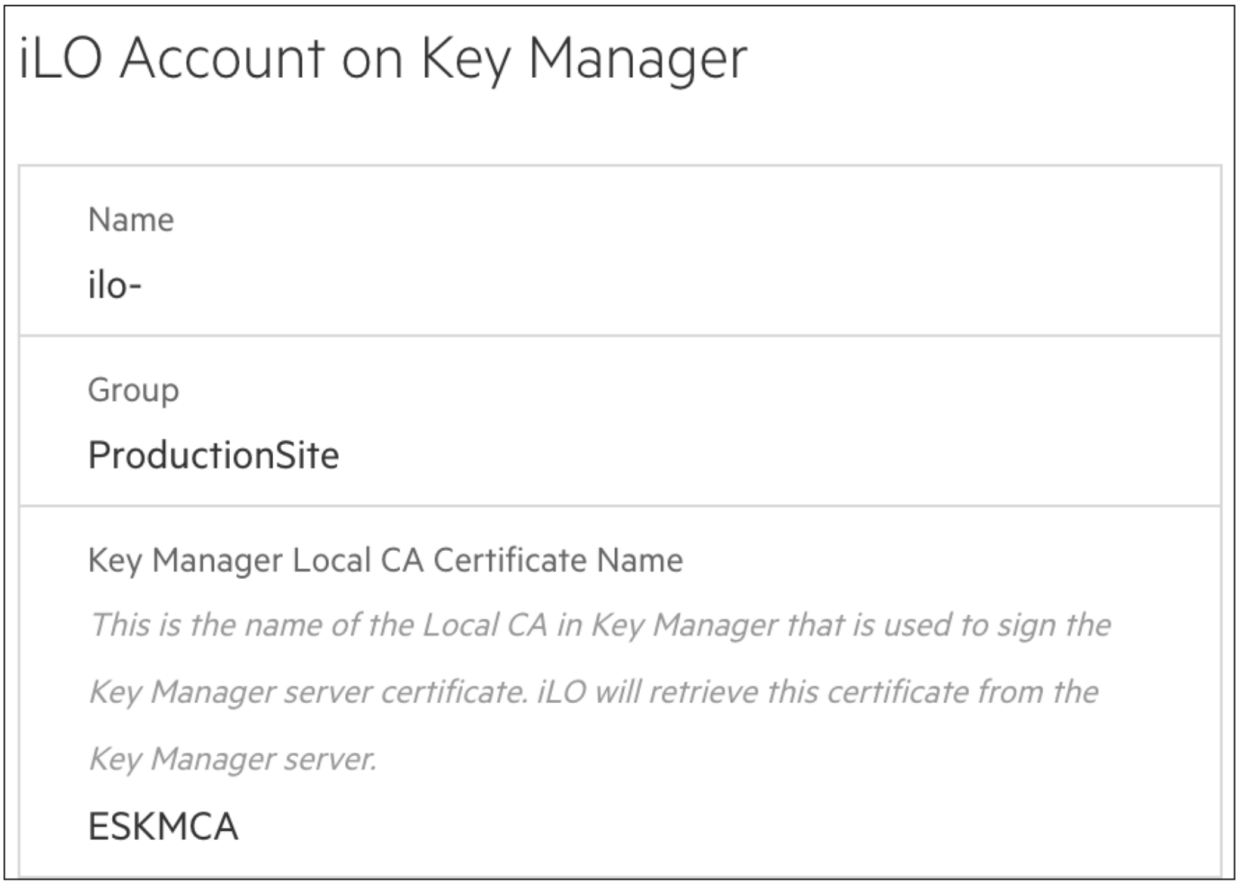
6. Again click on the “Administration” menu and click on the “Key Manager” tab.
7. Fill out the “iLO Account on Key Manager” form under “Key Manager Configuration”.

a. Name: Will already be populated.

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

b. Group: The user group we created in the ESKM.

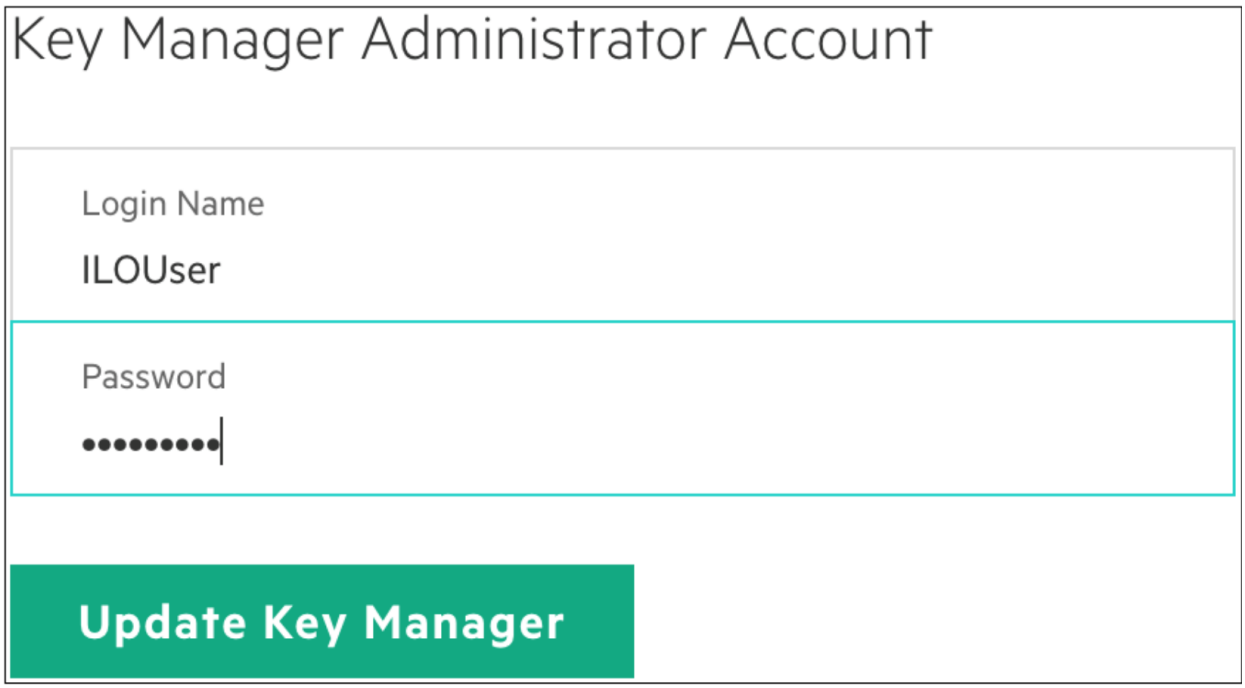
c. Key Manager Local CA Certificate Name: The name of the Local CA created on the ESKMs.



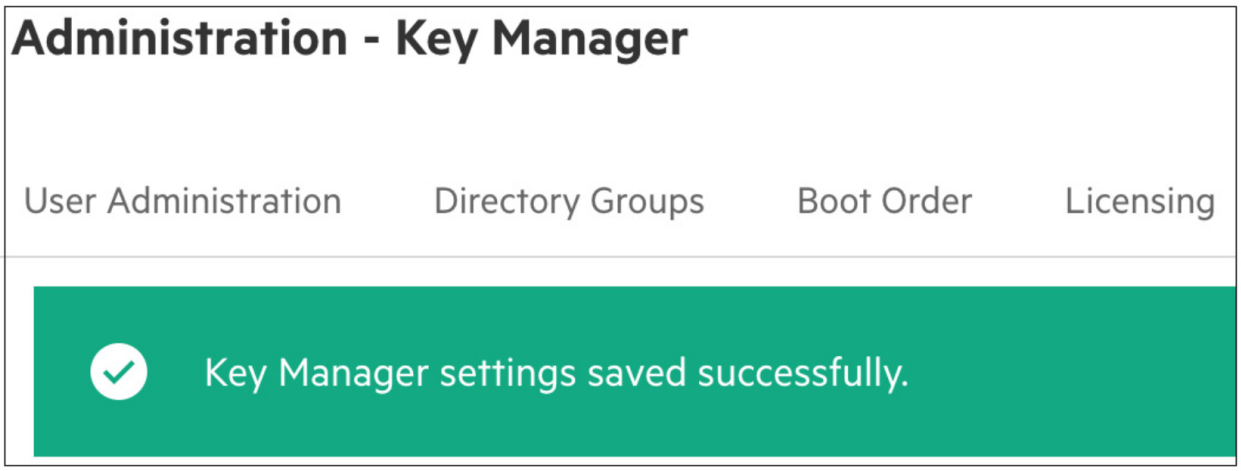
8. Fill out the “Key Manager Administrator Account” form under “Key Manager Configuration”.

a. Login Name: ilo_reg_user (User we created on ESKM).

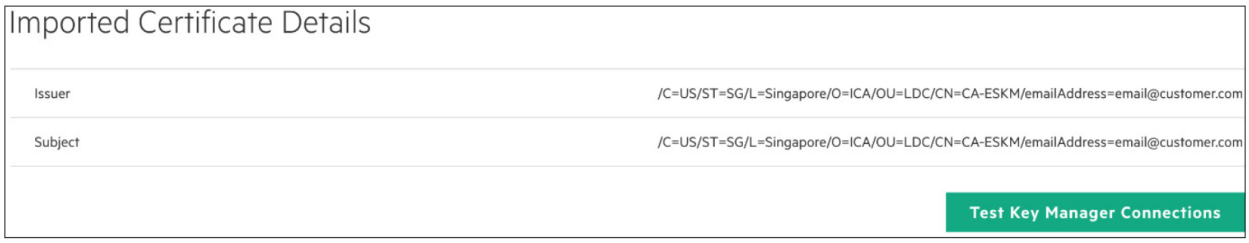
b. Password: The password created on ESKM.

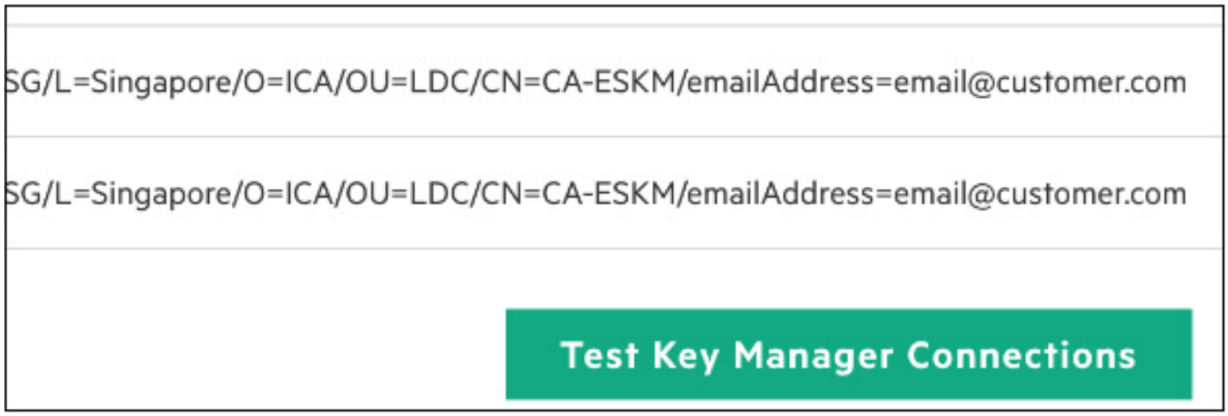


9. Click on Update Key Manager, and again the “Key Manager settings saved successfully” will be displayed.



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”.

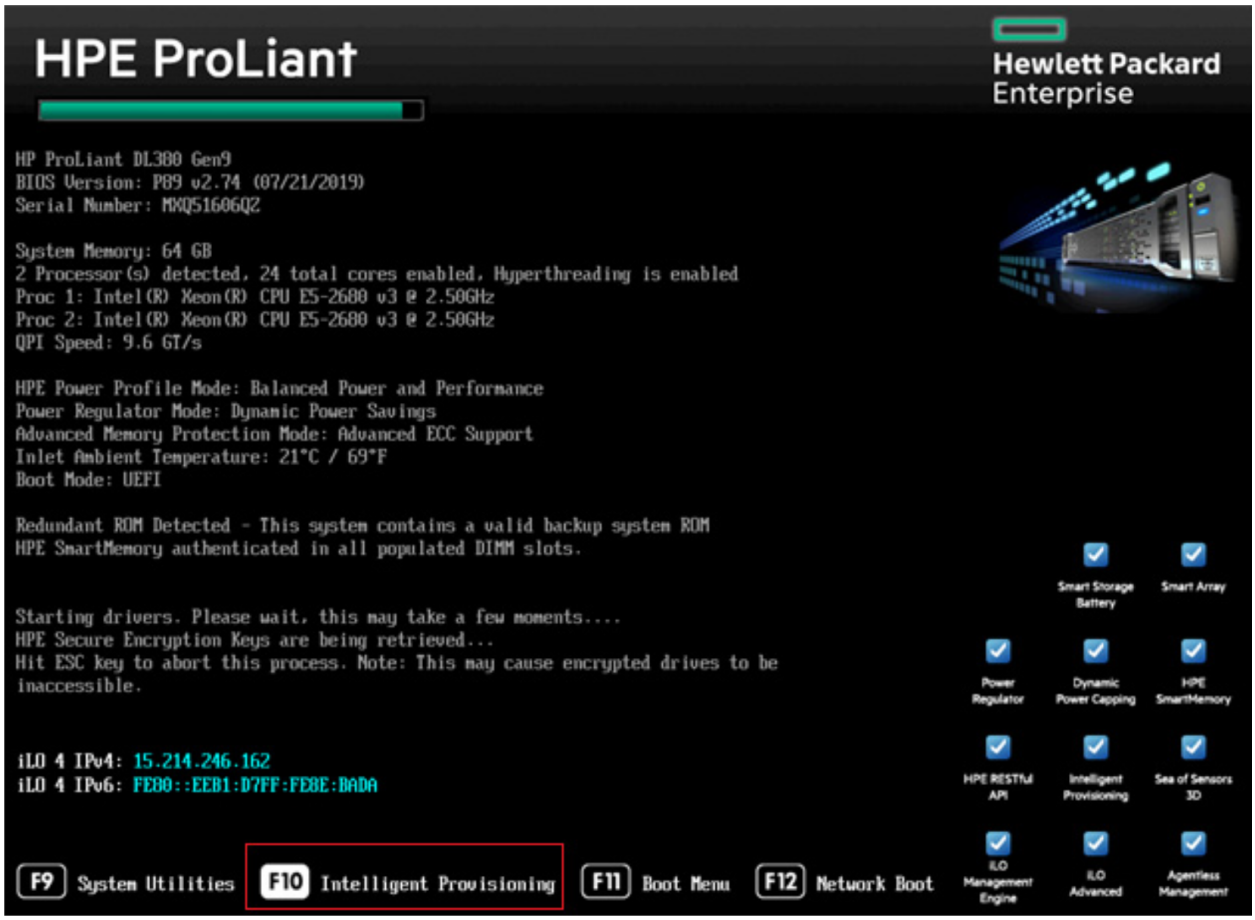




5.3 Configure the HPE Smart Array Controller

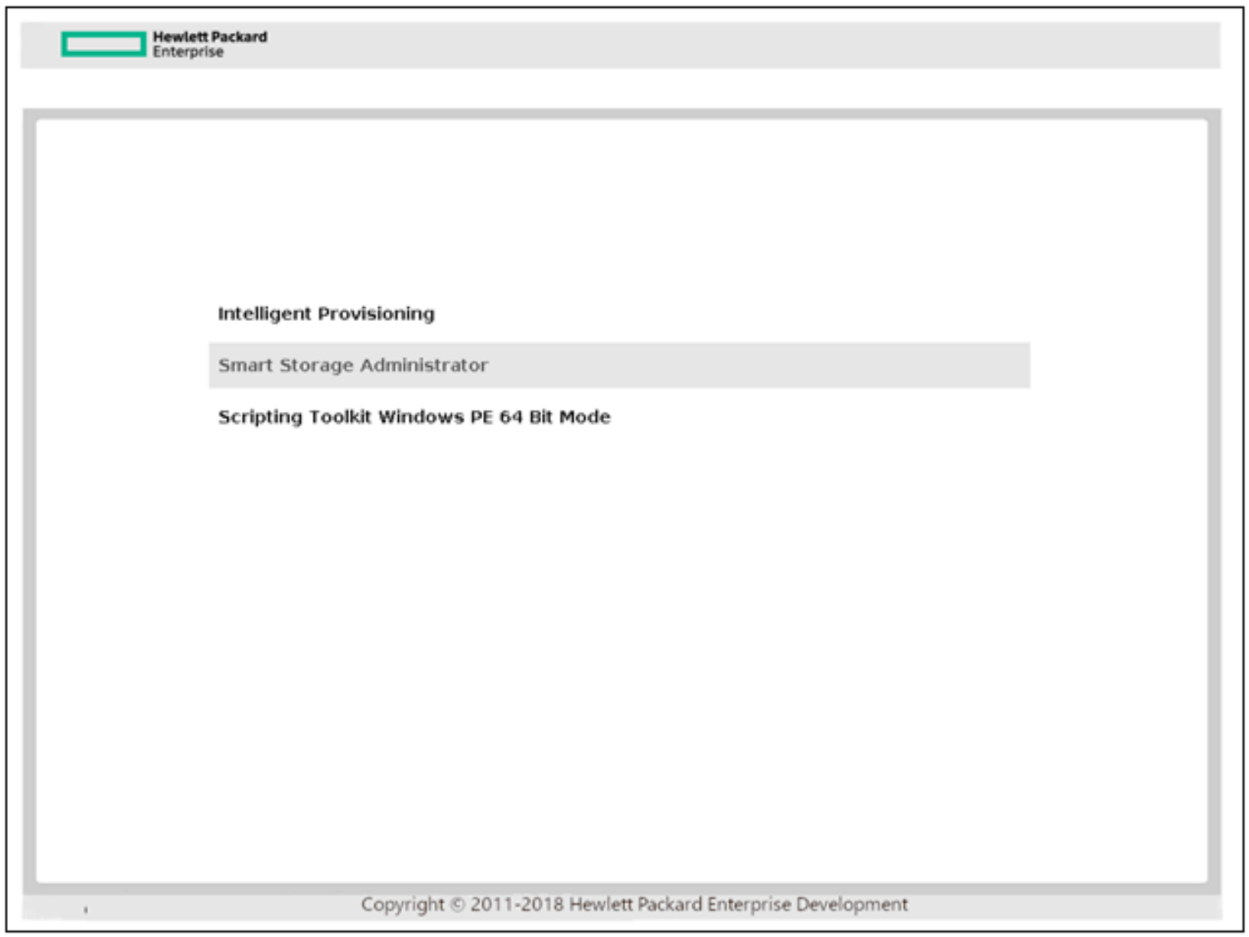
Please perform the following steps to configure HPE Smart Array Controller.

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

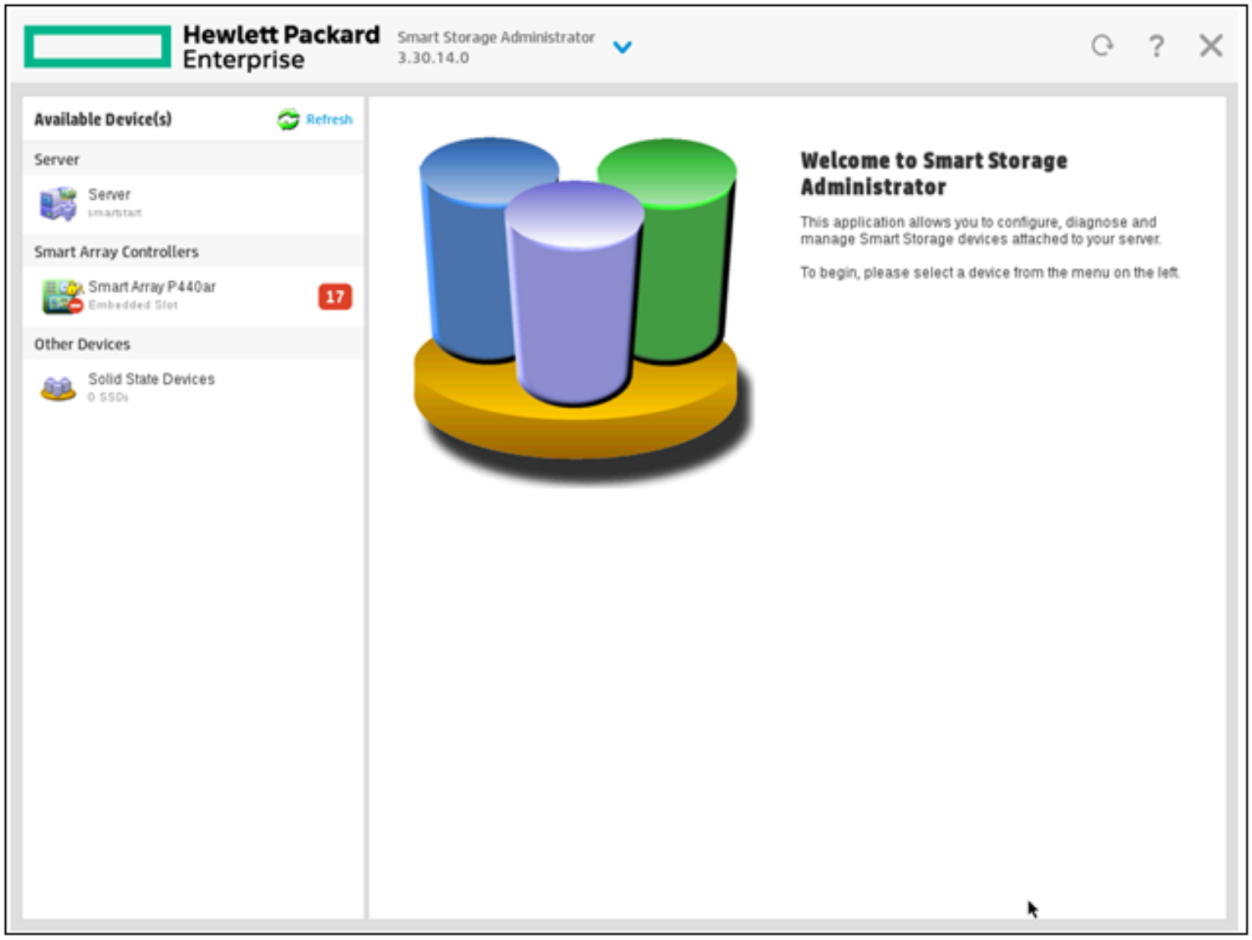


2. Open the HPE Smart Array Controller.

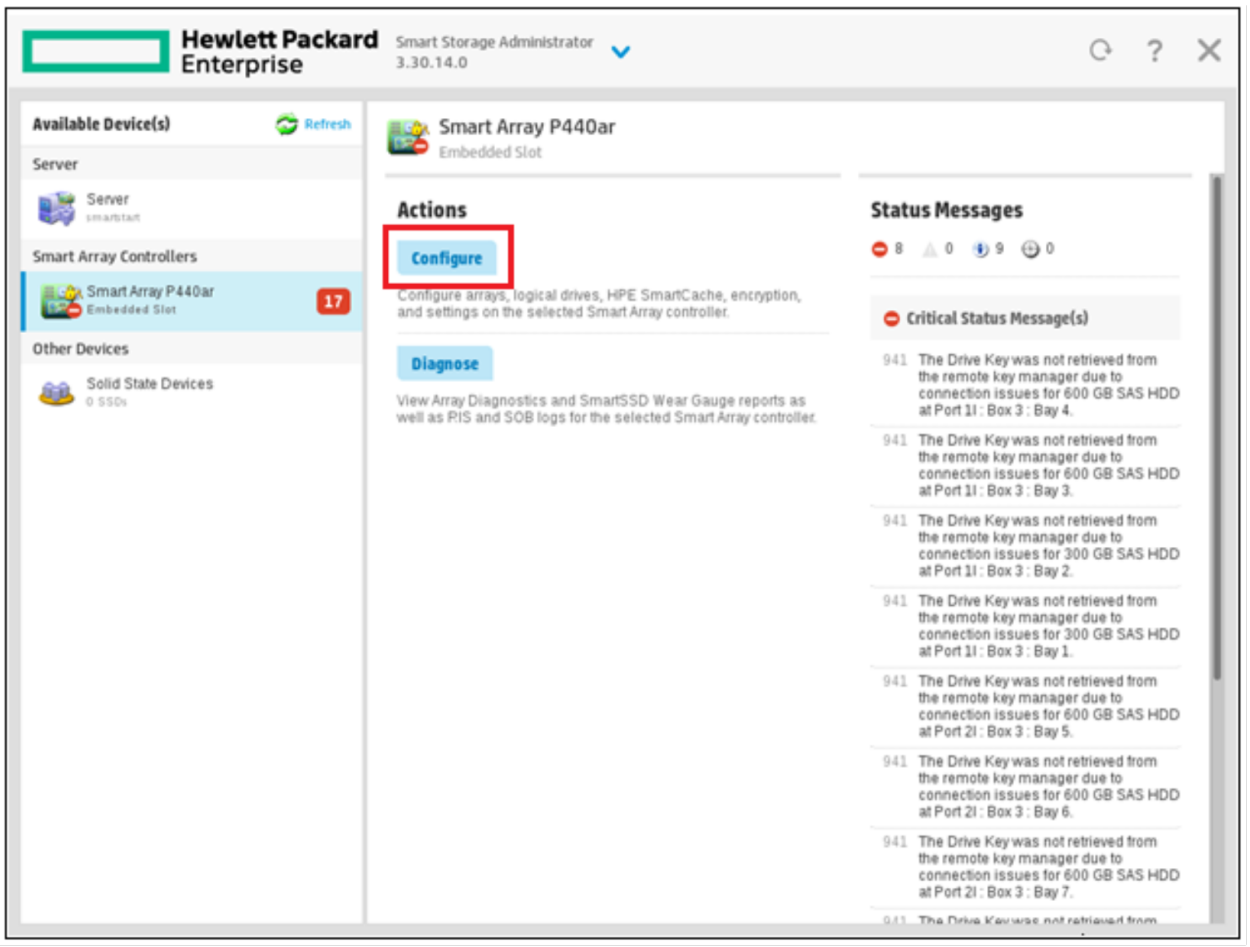
Please refer to the “HPE Smart Storage Administrator guide” for more details using the following link, https://support.hpe.com/hpsc/doc/public/display?docId=c03909334



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



4. Click on **Configure**.



5. Go to “Tools” and click on “Encryption Manager” to open it.

a. Create a new crypto officer password.

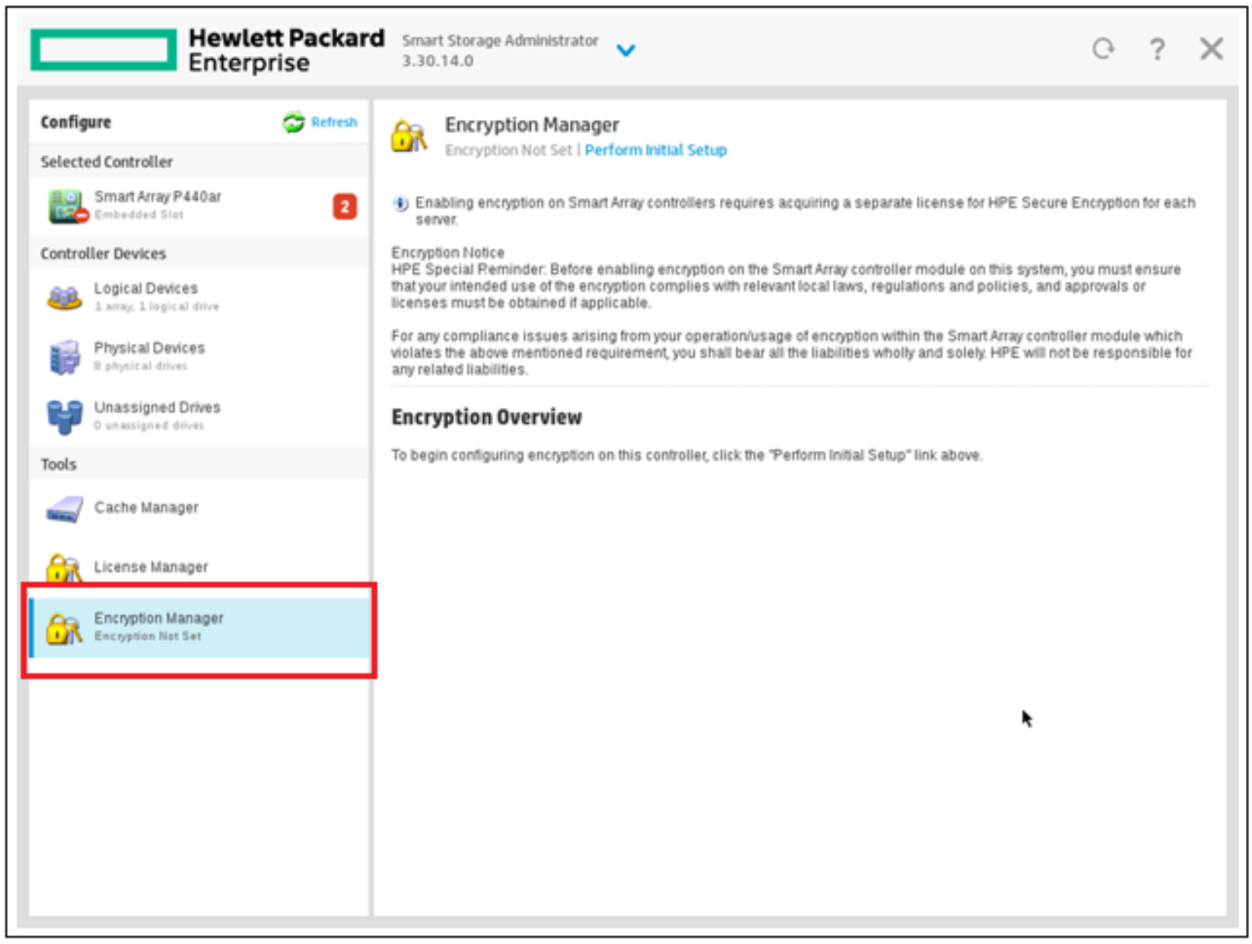
b. Perform the initial setup.

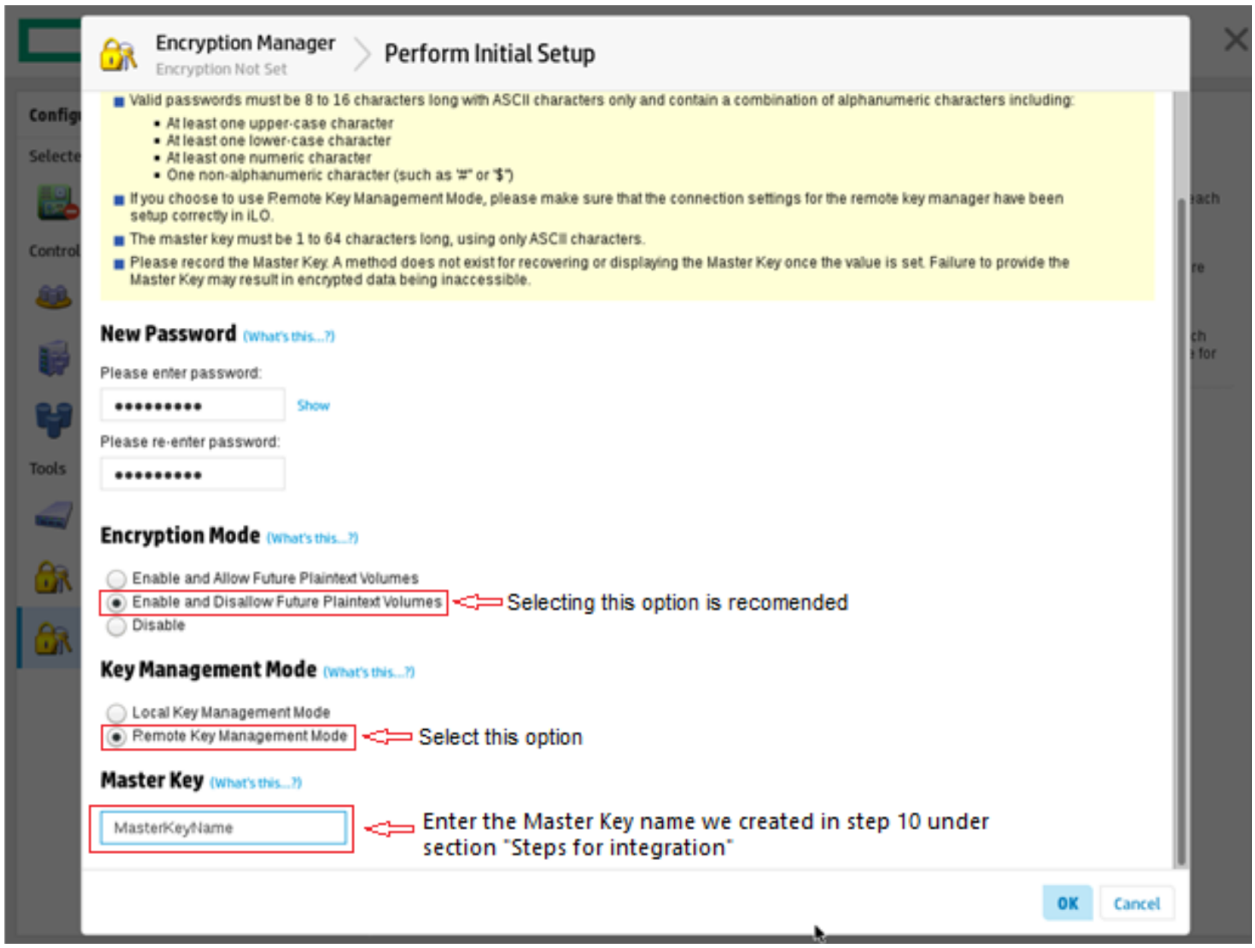
c. Perform the full setup.

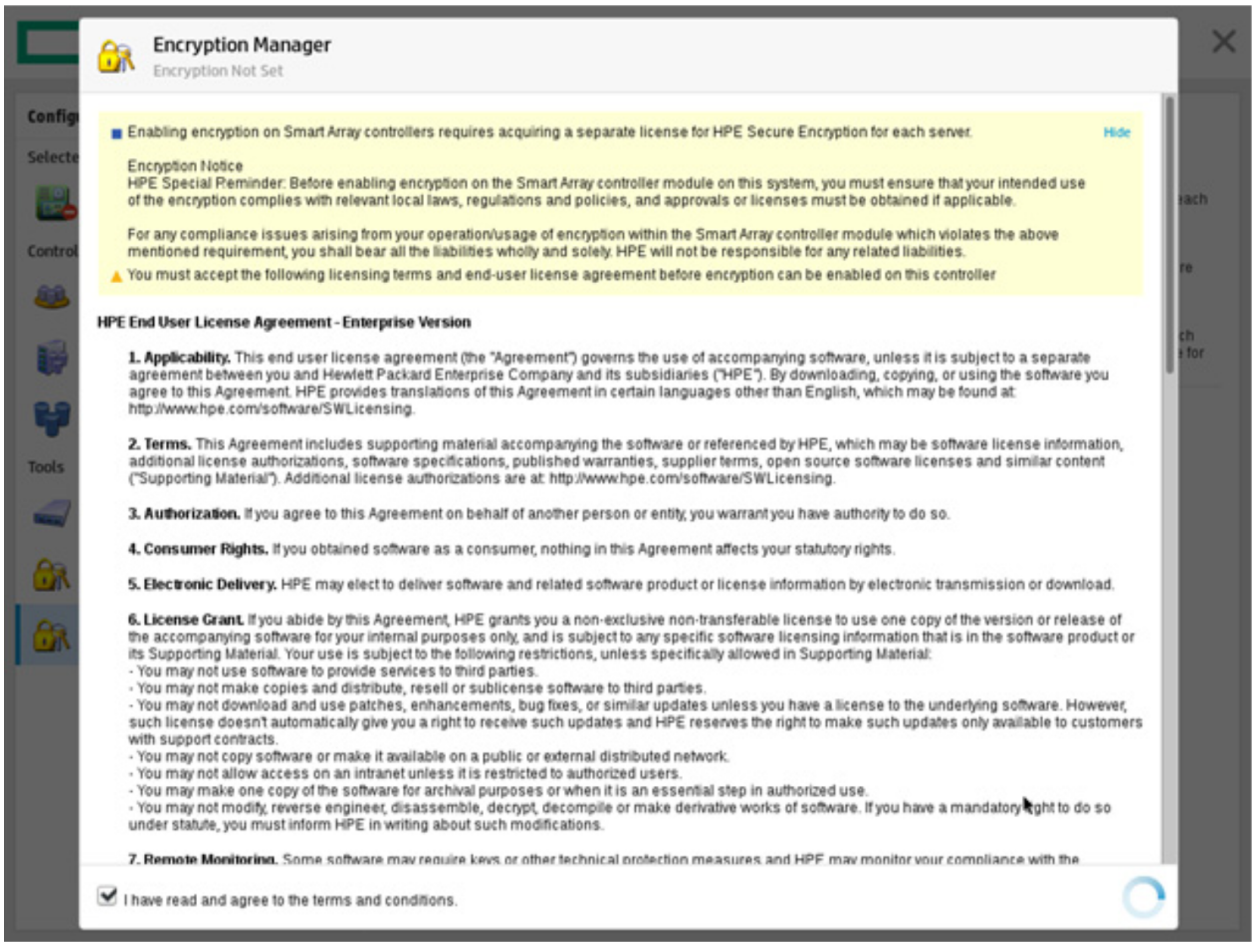
d. Enter a crypto/security officer password.

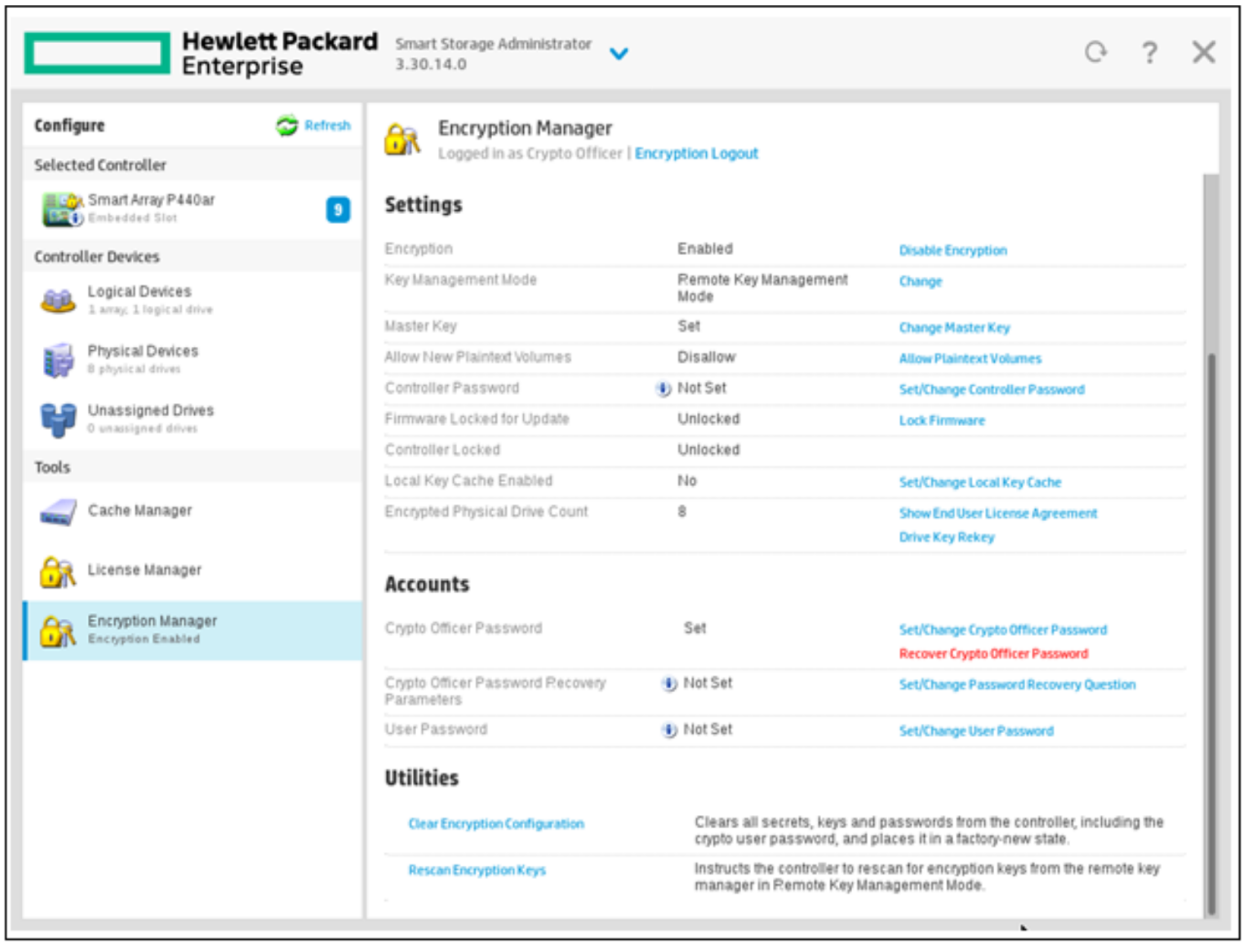
> Please make sure that these are admins for Secure Encryption and must be trusted employees.

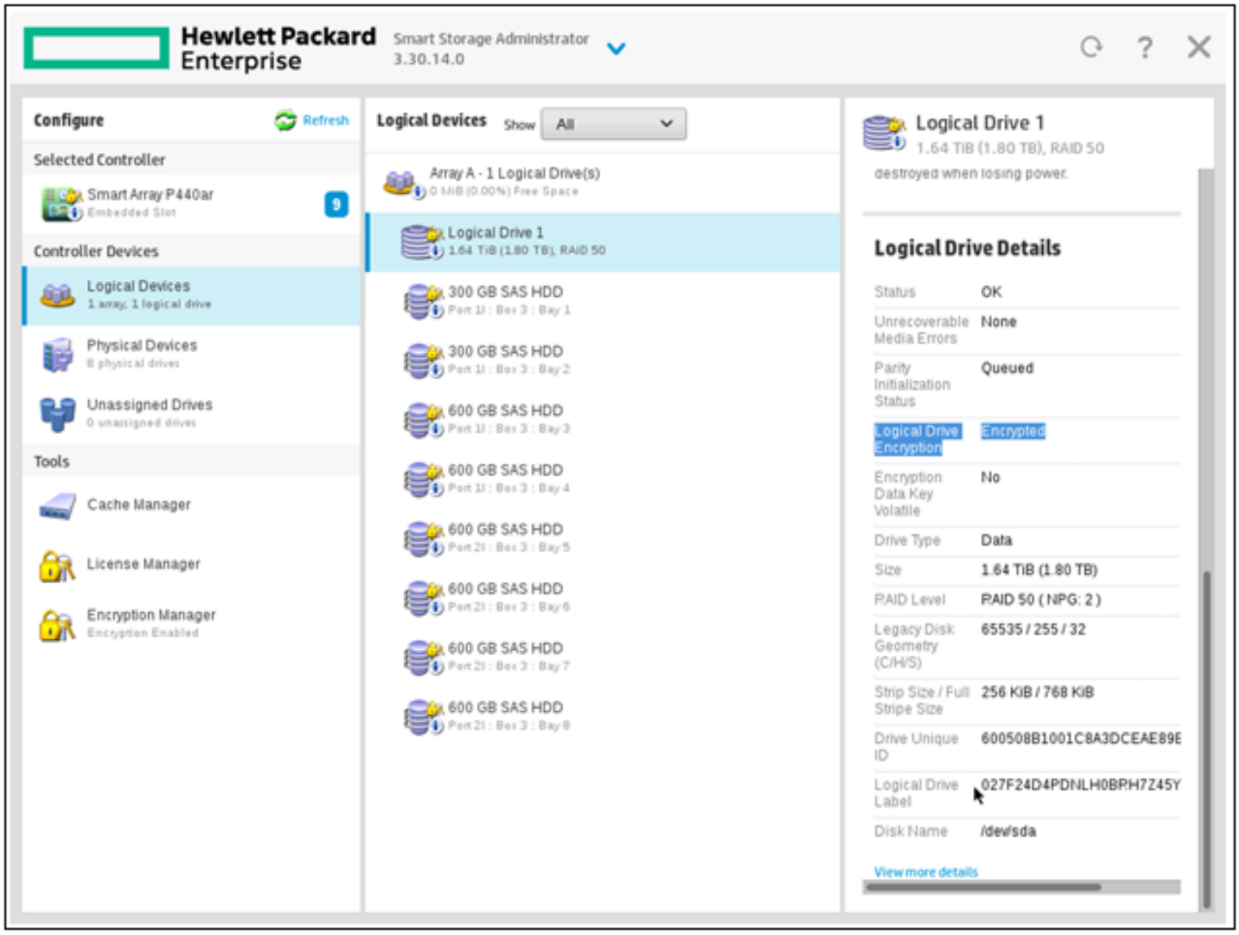
e. Enable and disallow future plaintext volumes **(Recommended)**.


Hewlett Packard Enterprise
Smart Storage Administrator
3.30.14.0
Configure
Refresh
Selected Controller
Smart Array P440ar
Embedded Slot
2
Controller Devices
Logical Devices
1 array, 1 logical drive
Physical Devices
8 physical drives
Unassigned Drives
0 unassigned drives
Tools
Cache Manager
License Manager
Encryption Manager
Encryption Not Set
Encryption Manager
Encryption Not Set | Perform Initial Setup
Enabling encryption on Smart Array controllers requires acquiring a separate license for HPE Secure Encryption for each server.
Encryption Notice
HPE Special Reminder: Before enabling encryption on the Smart Array controller module on this system, you must ensure that your intended use of the encryption complies with relevant local laws, regulations and policies, and approvals or licenses must be obtained if applicable.
For any compliance issues arising from your operation/usage of encryption within the Smart Array controller module which violates the above mentioned requirement, you shall bear all the liabilities wholly and solely. HPE will not be responsible for any related liabilities.
Encryption Overview
To begin configuring encryption on this controller, click the "Perform Initial Setup" link above.


Encryption Manager
Encryption Not Set
Perform Initial Setup
Valid passwords must be 8 to 16 characters long with ASCII characters only and contain a combination of alphanumeric characters including:
At least one upper-case character
At least one lower-case character
At least one numeric character
One non-alphanumeric character (such as '#' or '$')
If you choose to use Remote Key Management Mode, please make sure that the connection settings for the remote key manager have been setup correctly in iLO.
The master key must be 1 to 64 characters long, using only ASCII characters.
Please record the Master Key. A method does not exist for recovering or displaying the Master Key once the value is set. Failure to provide the Master Key may result in encrypted data being inaccessible.
New Password (What's this...?)
Please enter password:
Show
Please re-enter password:
Encryption Mode (What's this...?)
Enable and Allow Future Plaintext Volumes
Enable and Disallow Future Plaintext Volumes
Selecting this option is recomended
Disable
Key Management Mode (What's this...?)
Local Key Management Mode
Remote Key Management Mode
Select this option
Master Key (What's this...?)
MasterKeyName
Enter the Master Key name we created in step 10 under section "Steps for integration"
OK
Cancel


Encryption Manager
Encryption Not Set
Enabling encryption on Smart Array controllers requires acquiring a separate license for HPE Secure Encryption for each server.
Hide
Encryption Notice
HPE Special Reminder: Before enabling encryption on the Smart Array controller module on this system, you must ensure that your intended use of the encryption complies with relevant local laws, regulations and policies, and approvals or licenses must be obtained if applicable.
For any compliance issues arising from your operation/usage of encryption within the Smart Array controller module which violates the above mentioned requirement, you shall bear all the liabilities wholly and solely. HPE will not be responsible for any related liabilities.
You must accept the following licensing terms and end-user license agreement before encryption can be enabled on this controller
HPE End User License Agreement - Enterprise Version
1. Applicability. This end user license agreement (the "Agreement") governs the use of accompanying software, unless it is subject to a separate agreement between you and Hewlett Packard Enterprise Company and its subsidiaries ("HPE"). By downloading, copying, or using the software you agree to this Agreement. HPE provides translations of this Agreement in certain languages other than English, which may be found at: http://www.hpe.com/software/SWLicensing.
2. Terms. This Agreement includes supporting material accompanying the software or referenced by HPE, which may be software license information, additional license authorizations, software specifications, published warranties, supplier terms, open source software licenses and similar content ("Supporting Material"). Additional license authorizations are at: http://www.hpe.com/software/SWLicensing.
3. Authorization. If you agree to this Agreement on behalf of another person or entity, you warrant you have authority to do so.
4. Consumer Rights. If you obtained software as a consumer, nothing in this Agreement affects your statutory rights.
5. Electronic Delivery. HPE may elect to deliver software and related software product or license information by electronic transmission or download.
6. License Grant. If you abide by this Agreement, HPE grants you a non-exclusive non-transferable license to use one copy of the version or release of the accompanying software for your internal purposes only, and is subject to any specific software licensing information that is in the software product or its Supporting Material. Your use is subject to the following restrictions, unless specifically allowed in Supporting Material:
· You may not use software to provide services to third parties.
· You may not make copies and distribute, resell or sublicense software to third parties.
· You may not download and use patches, enhancements, bug fixes, or similar updates unless you have a license to the underlying software. However, such license doesn't automatically give you a right to receive such updates and HPE reserves the right to make such updates only available to customers with support contracts.
· You may not copy software or make it available on a public or external distributed network.
· You may not allow access on an intranet unless it is restricted to authorized users.
· You may make one copy of the software for archival purposes or when it is an essential step in authorized use.
· You may not modify, reverse engineer, disassemble, decrypt, decompile or make derivative works of software. If you have a mandatory right to do so under statute, you must inform HPE in writing about such modifications.
7. Remote Monitoring. Some software may require keys or other technical protection measures and HPE may monitor your compliance with the
I have read and agree to the terms and conditions.


Hewlett Packard Enterprise
Smart Storage Administrator
3.30.14.0
Configure
Refresh
Selected Controller
Smart Array P440ar
Embedded Slot
9
Controller Devices
Logical Devices
1 array, 1 logical drive
Physical Devices
8 physical drives
Unassigned Drives
0 unassigned drives
Tools
Cache Manager
License Manager
Encryption Manager
Encryption Enabled
Encryption Manager
Logged in as Crypto Officer | Encryption Logout
Settings
Encryption
Enabled
Disable Encryption
Key Management Mode
Remote Key Management Mode
Change
Master Key
Set
Change Master Key
Allow New Plaintext Volumes
Disallow
Allow Plaintext Volumes
Controller Password
Not Set
Set/Change Controller Password
Firmware Locked for Update
Unlocked
Lock Firmware
Controller Locked
Unlocked
Local Key Cache Enabled
No
Set/Change Local Key Cache
Encrypted Physical Drive Count
8
Show End User License Agreement
Drive Key Rekey
Accounts
Crypto Officer Password
Set
Set/Change Crypto Officer Password
Recover Crypto Officer Password
Crypto Officer Password Recovery Parameters
Not Set
Set/Change Password Recovery Question
User Password
Not Set
Set/Change User Password
Utilities
Clear Encryption Configuration
Clears all secrets, keys and passwords from the controller, including the crypto user password, and places it in a factory-new state.
Rescan Encryption Keys
Instructs the controller to rescan for encryption keys from the remote key manager in Remote Key Management Mode.

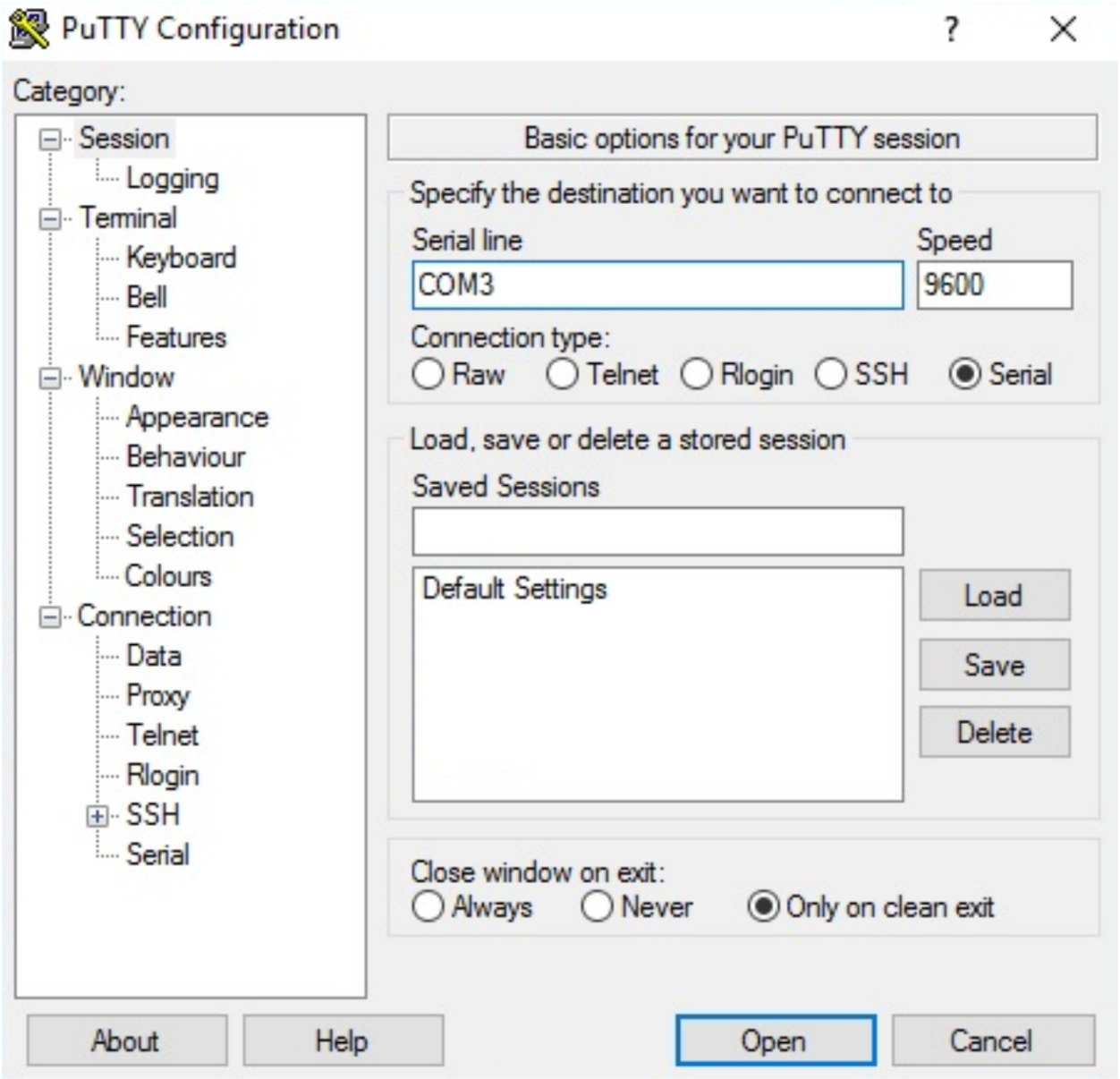


With this, ESKM will be successfully integrated with ProLiant by following the procedure described above.

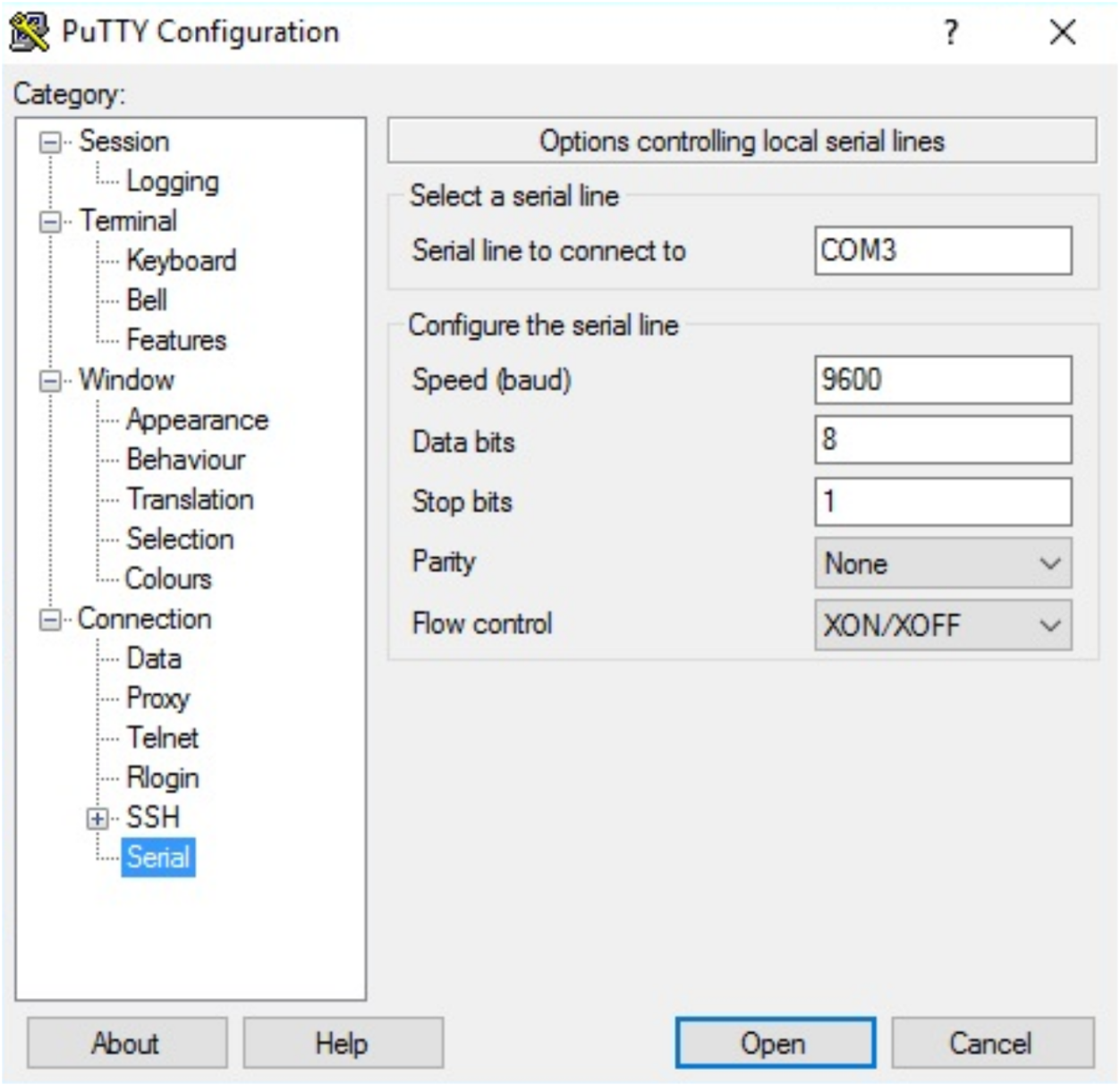
6 Accessing serial console via PuTTY

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

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



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



5. Make sure all of the settings are correct.

6. Click **Open** to start the session.

7 Obtaining Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

Before contacting Utimaco with your questions, collect the following information:

- Product model names and numbers
- Technical support registration number or NonStop system number (if applicable)
- Service Agreement ID number (SAID)
- Product serial numbers
- Error messages
- Software version number

24-hour support

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

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