



HPE

StoreOnce

Integration Guide

ESKM

The logo for utimaco, featuring the word "utimaco" in a bold, black, sans-serif font. A small blue diamond is positioned above the letter "i". A registered trademark symbol (®) is located to the upper right of the word.

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-08-17
Status	PUBLISHED
Document No.	IG-2026-0094
All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1	About This Guide	5
1.1	Intended Audience.....	5
1.2	Document Conventions and Symbols.....	5
1.3	Related Documentation.....	6
1.4	Utimaco Websites	6
1.4.1	OASIS Websites.....	6
1.5	Documentation Feedback	6
1.6	What is new in the ESKM v8.0 Appliance	7
2	Configuring the ESKM Server	8
2.1	First Run.....	8
2.2	Setting up Local CA	11
2.3	Setting up ESKM Certificate	13
2.4	Set up Cluster	18
2.4.1	Creating the Cluster.....	18
2.4.2	Adding ESKM Servers to the Cluster	19
2.5	Set up KMIP Server	21
2.6	Set up KMS Server.....	24
3	Configuring the HPE StoreOnce	27
3.1	Introduction.....	27
3.1.1	Pre-requisites for Integration	27
3.2	Configuration Overview	27
4	Integration	30
4.1	Data at Rest Encryption.....	30
4.1.1	Local Key Management	30
4.1.2	Centralized Key Management.....	32
4.2	Data in Flight Encryption.....	34
4.3	Steps for Integration	36
4.3.1	Creating an Admin User.....	36
4.3.2	Importing Certificate	42
4.3.3	Enrolling into External Key Manager Mode.....	43
4.3.4	Integrating HPE StoreOnce with ESKM	49

4.3.4.1 Importing Root Certificate..... 61

4.3.4.2 Importing Signed Certificate 62

4.3.5 Enrolling the StoreOnce..... 63

5 Accessing Serial Console via PuTTY66

6 Contact and Support Information68

6.1 Utimaco Technical Support 68

6.2 24-hour support..... 68

1 About This Guide

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

For more information on installing an Utimaco Enterprise Secure Key Manager refer to the *Utimaco Enterprise Secure Key Manager Installation and Replacement Guide (Chapter 1 Installing Hardware)*.

1.1 Intended Audience

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

- Data security administration.
- Network configuration.

1.2 Document Conventions and Symbols

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select Details and click on Properties button
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>certreq.exe -new</code> <code>request.inf</code> <code>IISCertRequest.csr</code>
<i>Italic</i>	References and important terms	Operating system listed in Tested Versions

Table 1: Document conventions

We use special icons to highlight the most important notes and information.



Indicates an action that can have consequences such as deletion of keys or changes to security settings.



Provides clarifying information or specific instructions.



Provides helpful hints and shortcuts.

1.3 Related Documentation

The following documents provide related information:

- *Enterprise Secure Key Manager v8.53.0 Installation and Replacement Guide.*
- *Enterprise Secure Key Manager v8.53.0 Software Version 8.53.0 Release Notes.*
- *Enterprise Secure Key Manager v8.53.0 User's Guide.*

1.4 Utimaco Websites

For additional information, see the following Utimaco websites: [Enterprise Secure Key Manager - Utimaco](#).

1.4.1 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 to:

support-atalla@utimaco.com

All submissions become the property of Utimaco.

1.6 What is new in the ESKM v8.0 Appliance

The ESKM v8.0 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.

2 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.

This section includes procedures on the following topics:

- First run.
- Setting up local CA.
- Setting up ESKM certificate.
- Setup cluster.
- Setup KMIP server.
- Setup KMS server.

2.1 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.

- Power on the ESKM server by pressing the Power On/Standby button located behind the front bezel door.
- When the startup sequence completes, the following prompt displays on the monitor 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.

- Follow the prompts to enter the necessary information and press Enter to accept the default.
 - 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.
 - Time zone.
 - Date.

- 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.
- The static IPv4 address of the ESKM server. The ESKM server cannot obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- Subnet mask.
- Default gateway.
- Hostname, including the domain. For example, eskm.example.com^[2]. 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.
- 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.
- Web interface port number.
- 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:aTp6A447vp8d0j43FTT5B/aux6V7zddPzNXxZB0C1SE SSH ECDSA key  
fingerprint:
```

```
521 SHA256:BK0/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 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** .



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 8.53.0 User Guide.

- 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.

2.2 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:

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

Create Local Certificate Authority

[Help ?](#)

Certificate Authority Name:	ESKMCA
Country Name:	US
State or Province Name:	CA
Locality Name:	Campbell
Organization Name:	Organization
Organizational Unit Name:	Information Security
Common Name:	ESKMLocalCA
Email Address:	support@organization.com
Algorithm:	RSA-2048
☒ Self-signed Root CA	
Certificate Authority Type:	CA Certificate Duration (days): 3650
	Maximum User Certificate Duration (days): 3650
☐ Intermediate CA Request	

Create

Figure 1 : Create Local Certificate Authority

- Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example ESKM Local CA.
- Enter your organizational information.
- Select the **Algorithm** (e.g., RSA-2048).
- 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.
- Click **Create**.
- If the local CA will be used to sign ESKM client certificate requests, add the CA to the **Trusted CA** list.
 - In **Certificates & CAs**, click **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.
 - Click on the **Default Profile Name** (not the radio button).
 - In the **Trusted Certificate Authority List**, click **Edit**.

- From the list of **Available CAs** in the right panel, select the CA you created in step 4. For example, ESKM Local CA.
- Click **Add**.
- 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 & CAs**, click **Known CAs** to display the **Install CA Certificate** section.
2. Enter a value for the **Certificate Name** and paste the CA certificate text in the **Certificate** field.
3. Click **Install**. The CA certificate will be added to the **Known CAs** list.

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

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

2.3 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.



By default, REST Server uses the system-generated server certificate. Utimaco highly recommends replacing the default certificate.

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** section of the window to create the ESKM server certificate.

Create Certificate

Help ?

Certificate Name:	ESKMServerCert
Country Name:	US
State or Province Name:	CA
Locality Name:	Campbell
Organization Name:	Organization
Organizational Unit Name:	Information Security
Common Name:	ESKM
Email Address:	infosec@organization.com
Subject Alternative Name:	IP:10.222.55.196
Algorithm:	RSA-2048 ▼
Creation Type:	☐ Certificate Request - to be signed by external CA ☒ Certificate Signed by Local CA
Local CA:	ESKMCA (maximum 2814 days) ▼
Certificate Purpose:	Server ▼

Create

Figure 2 : Create Certificate

- Enter a **Certificate Name** and **Common Name**. (For example, ESKM Cert).
- Enter your **Organizational** information.
- Enter/select the **Subject Alternative Name**, **Algorithm**, **Creation Type** as **Certificate Signed by Local CA**, **Local CA** (CA name you created in *Setting up local CA*, for example ESKM Local CA) and **Certificate Purpose**.

4. Click **Create**.

Certificate Information

[Help ?](#)

Certificate Name:	ESKMServerCert
Key Size:	2048
Start Date:	Nov 13 08:37:33 2022 GMT
Expiration:	Nov 10 08:37:33 2032 GMT
Issuer:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization.com
Subject:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKM emailAddress: infosec@organization.com
Subject Alternative Name:	IP Address: 10.222.55.196
Purpose:	SSL Server

-----BEGIN CERTIFICATE-----

```

MIID6sCCAtOgAwIBATANBgkqhkiG9w0BAQsFADCB0jELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRREwDwYDVQQHEwYwYmVsbDEwMDUwMDUwMDUwMDUw
emF0aW9uMR0wGwYDVQQLEwRjb250cm1hdG1vbiBTZWNTcm10eTEUMBIGA1UEA
MLRVNLTUxvY2FzQ0EwJzAlBgkqhkiG9w0BCEQEWGG1uZm9zZWNNAb3JnYW5p
emF0aW9uLmNvbTAeFw0yMjE0MTMwODMzNzNaFw0zMDUwMTAwODMzNzNaMIGb
MQswCQYDVQQGEwJVUzELMAkGA1UECmQ0EwETAPBgNVBAcTCENhbXBellZWxs
MRUwEwYDVQQKEwxEwYDVQIDF6YXNpb24xHTAbBgNVBAcTFE1uZm9zZWNTcm10e
TEUMBIGA1UEAQLVQ0EwRUFU0tNMSBwJQYJKoZIhvcNAQkBFhhpbmZvc2VjQ
G9yZ2FuaXphdG1vbi5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAo
IBAQD2eJpAadCp0oUuwVC3+6ICftWmFfEXk3FuKpwD1RRiVhKcbhGokbYwWp/
zmdb+3KoltsHo9H/uBxEs+MA8XI5rg9sg4VDxMMwtj78Eq4eOYhPop4oxEyKxU
fOnB8DFFM/hoy+PBWfVw74OxYJA/sBY8jv9Bx2M4ealWbgnocy9F2KsMMID/
y/TcCNjik8ehe0Tn78dWRVoy/UORwWIQ5nS1HXQGOonL6IGjeAd51PG19
CdNeFCX2fW8bBL1mWuT2UEsAHVJA8oN1A1YoOQ U2FFsBQMMPQinAQBXaX
FhPDazQOTGe4isEUtpfkaPnoaPzLdt1Oox9aKBgMeQMkvMKP5AgMBAAEg
MTAvMAkGA1UdEwQCMAAwEQQYJYI2IAyb4QgEBBAQDAgZAMA8GA1UdEQQIMA
aHBA8eN8QwDQYJKoZIhvcNAQELBQADggEBAJF02UfWn+1mlomHswi8DnG3
NkNj16OLco1POPiZrpP/s7U03tBi96GhVmb7Uwvdyb1AF0GEq50od8d6z
GRJwC9grV/1A3nvQeaUV3wyYJWHWeKxtxP0Ck3Fn4cqYOZfAPrJ+a+01+j
rhaSG0YPc4guV21M4xbkA35UNB+vPTWwQkPMkW1u5Fn8BL2Ett87LuOtjU
fanYb59CwZcQ5gx02PO9QU6ekRR6xRVt/9GcaTYTulDS3x95RS3uivdbmT077
xPAIF+7ENxringMPolpg5lHubYnQ9aBL1qjb0r1H4bwrLja6h5647+NBEeAy/3
Es4/r6BkccBuD960e3pJzM=
-----END CERTIFICATE-----

```

[Download](#)[Install Certificate](#)[Back](#)

Figure 3 : Certificate Information



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



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



The "Certificate Name" must remain same on all ESKM servers across the cluster.

Import a third-party server certificate

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

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

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

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

- In **Certificates & CAs**, click **Certificates** to display the **Import Certificate** section.
- Provide the source location of the certificate file.
- Specify the method for importing the certificate to the Enterprise Secure Key Manager.
 - If you are uploading the certificate through the browser, select **Upload from browser**, then click **Browse** and locate the file on the local drive or network.
 - If you are using SCP to copy the file to the Enterprise Secure Key Manager, select the appropriate option and enter the following information:
 - Host: the source host. IPv4 addresses are supported. IPv6 addresses are also supported if IPv6 is enabled.
 - Filename: the name of the file on the source host.

- Username: the username of the account on the source host.
- Password: the password for the user account on the source host.
- Enter the **Certificate Name** and **Private Key Password**.
- Click **Import Certificate**.



The Enterprise Secure Key Manager can import certificates in PEM-encoded PKCS #7, PEM-encoded PKCS #12, and PEM-encoded X509, as long as the private key is included with the certificate.

2.4 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.

2.4.1 Creating the Cluster

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

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

Create Cluster

[Help ?](#)

Local IP:	10.222.55.196 ▼
Local Cluster Port 1:	9001
Local Cluster Port 2:	9002
Cluster Password:	
Confirm Cluster Password:	

 **Note:** Cluster creation can take a while, please click the "Create" button once, and wait for the operation to complete.

Create

Figure 4 : Create Cluster

- 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.

All ESKM servers in a cluster must be time synchronized before creating the cluster.

- If required, change the **Local Cluster Port 1** value. Utimaco recommends using the default value of 9001.
- If required, change the **Local Cluster Port 2** value. Utimaco recommends using the default value of 9002.
- Choose a cluster password and enter it into the **Cluster Password** field. Enter the password a second time into the **Confirm Cluster Password** field.
- Click the **Create** button.
- 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.

2.4.2 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.

Join Cluster

Help ?

Local IP:	10.222.55.195 ▼
Cluster Member IP:	10.222.55.196
Cluster Member Port 1:	9001
Cluster Member Port 2:	9002
Cluster Key File:	Choose File eskm_cluster (1)
Cluster Password:	*****

 **Note:** Cluster join can take a while, please click the "Join", "Confirm" buttons once, and wait for the operation to complete.

[Join](#)

Figure 5 : Join Cluster



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



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

- Join the ESKM server to the cluster.
 - Select the **Device** tab.
 - In the **Device Configuration** menu, click on **Cluster**.
 - In the **Join Cluster** section of the window, select the appropriate **Local IP** value.
 - All ESKM servers in a cluster must use an IPV4 address for the cluster.
 - All ESKM servers in a cluster must be time-synchronized before creating the cluster.
 - Type the original cluster member's IP into **Cluster Member IP**.

- Type the original cluster member's port into **Cluster Member Port1**. The default value of this port is 9001. If this value was changed in while creating the cluster, use that value.
 - Type the original cluster member's port into **Cluster Member Port2**. The default value of this port is 9002. If this value was changed in while creating the cluster, use that value.
 - Click **Browse** and select the **Cluster Key File** you saved in while creating the cluster.
 - Type the cluster password into **Cluster Password**.
 - Click **Join**.
 - Click **Confirm** to synchronize with the cluster.
- After adding all members to the cluster, you can then delete the cluster key file from the desktop.
 - 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.



Make sure to use the same server certificate name as specified under KMS Server Settings and KMIP Server Settings.

- After creating the KMIP server certificate, restart the KMIP server manually. Navigate to the **Services List** section of the **Services Configuration** page (**Device -> Maintenance -> Services -> KMIP Server**).



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.

2.5 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:

- Select the **Device** tab.
- In the **Device Configuration** menu, click **KMIP Server** to display the **KMIP Server Configuration** window.
- In the **KMIP Server Settings** section, click **Edit**.
- 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*.

KMIP Server Settings

[Help ?](#)

IP:	[All] ▼
Port:	5696
Server Certificate:	kmip_server ▼
Local CA Certificate for Certify/Re-certify:	[Disabled] ▼
Connection Timeout (sec):	360
Default number of items returned in Locate:	100
Maximum number of items returned in Locate:	1000
Save Cancel	

Figure 6 : KMIP Server Settings

- Click **Save**.



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

- Confirm that the KMIP server is started.
 - Go to the **Services List** section of the **Services Configuration** page (Device -> **Maintenance** -> **Services** -> **KMIP Server**).
 - 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.

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



KMIP Server Authentication Settings Help ?

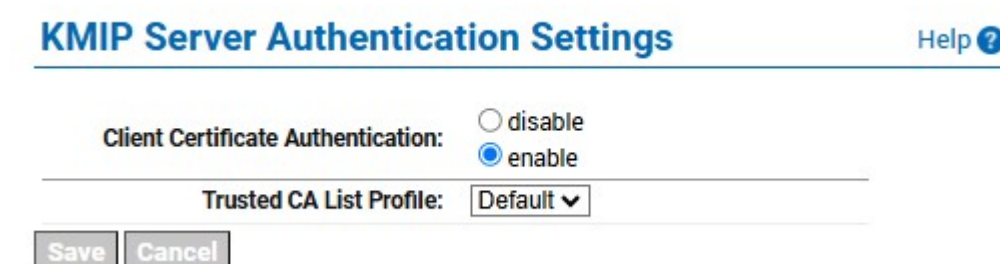
Client Certificate Authentication: disable

Trusted CA List Profile: [None]

Edit

Figure 7 : KMIP Server Authentication Settings

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



KMIP Server Authentication Settings Help ?

Client Certificate Authentication: ☐ disable ☒ enable

Trusted CA List Profile: Default ▼

Save **Cancel**

Figure 8 : Enable - MIP Server Authentication Settings

2.6 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:

- Select the **Device** tab.
- In the **Device Configuration** menu, click **KMS Server** to display the **KMS Server Configuration** window.
- In the **KMS Server Settings** section, click **Edit**.
- Configure the **KMS 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.

KMS Server Settings

[Help ?](#)

IP:	[All] ▼
Port:	9000
Use SSL:	☒
Server Certificate:	kms_server ▼
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☐
Allow Key Export:	☐

[Save](#) [Cancel](#)

Figure 9 : KMS Server Settings

- Click **Save**.
- Confirm that the KMS server is started.
 - Go to the **Services List** section of the **Services Configuration** page (Device -> **Maintenance** -> **Services** -> **KMS Server**).
 - 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.

- In the **KMS Server Authentication Settings** section, click **Edit**.

KMS Server Authentication Settings

[Help ?](#)

User Directory:	Local
Password Authentication:	Required
Client Certificate Authentication:	Not used
Trusted CA List Profile:	[None]
Username Field in Client Certificate:	[None]
Require Client Certificate to Contain Source IP:	☐

[Edit](#)

Figure 10 : KMS Server Authentication Settings

- 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**.

KMS Server Authentication Settings

[Help ?](#)

User Directory:	☒ Local ☐ LDAP
Password Authentication:	☐ Optional ☒ Required (most secure)
Client Certificate Authentication:	☒ Not used ☐ Used for SSL session only ☐ Used for SSL session and username (most secure)
Trusted CA List Profile:	[None] ▼
Username Field in Client Certificate:	[None] ▼
Require Client Certificate to Contain Source IP:	☐

[Save](#) [Cancel](#)

Figure 11 : Edit KMS Server Authentication Settings

3 Configuring the HPE StoreOnce

3.1 Introduction

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 StoreOnce 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 StoreOnce documentation. Should this section offer different instructions than StoreOnce's documentation, follow the instructions issued by HPE StoreOnce.

3.1.1 Pre-requisites for Integration

- You have “admin” access to and are familiar with the ESKM appliance and the HPE StoreOnce procedures, configuration, and protocols.
- The HPE StoreOnce is configured and functioning.



The examples in this document use ESKM v8.53.0 software and HPE StoreOnce v4500 Backup.

3.2 Configuration Overview

The solution presented here integrates HPE StoreOnce with ESKM into a purpose-built system to protect the backup data with the easy and efficient data protection (encryption) capability of HPE StoreOnce and the key management capability of ESKM.

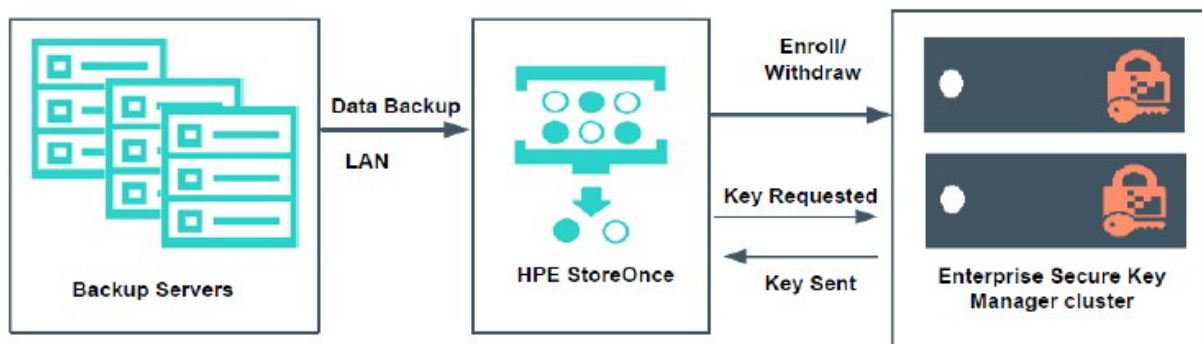


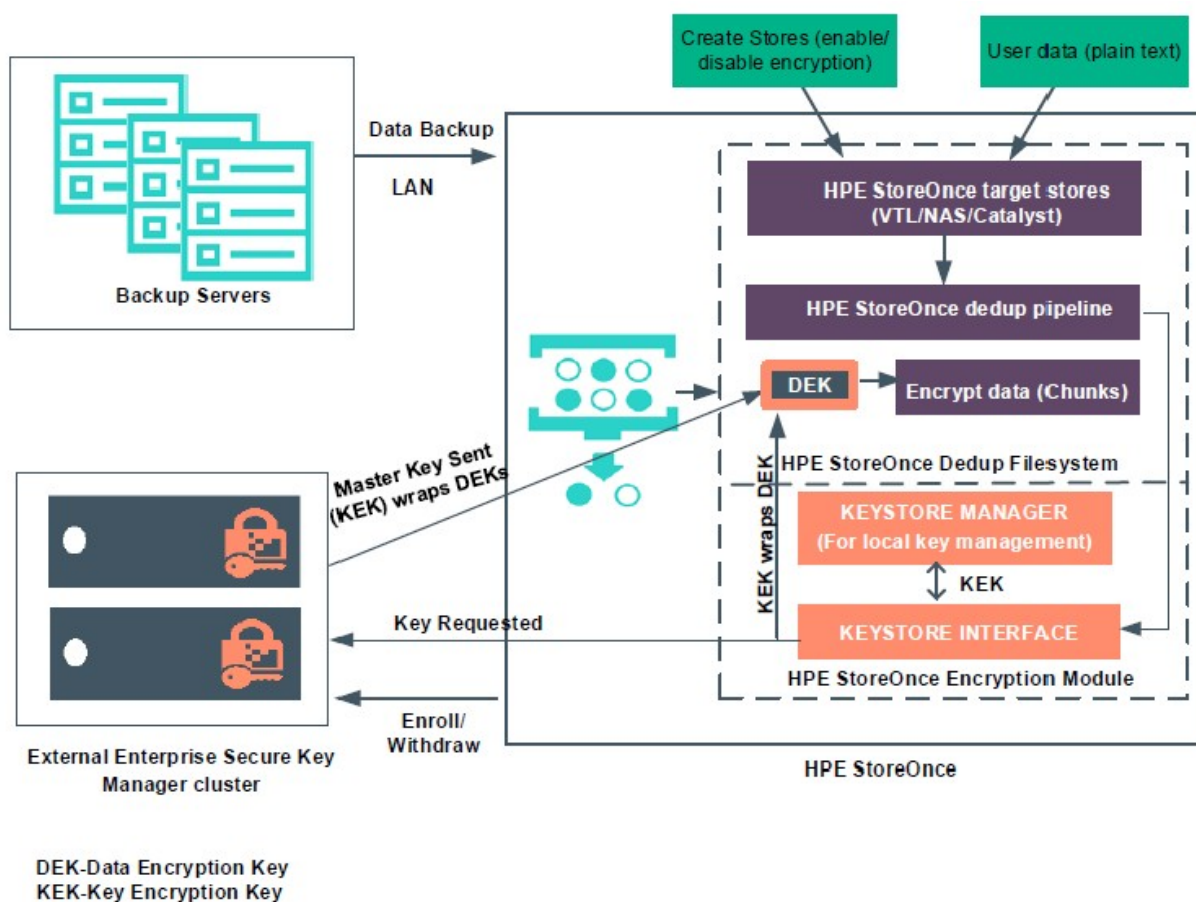
Figure 12 : HPE StoreOnce Configuration Overview



To perform the data backup, we have deployed a backup server on HPE Hyper Converged 380 with VMware® vSphere 6.0. However, please note that any backup platform is supported for data protection, provided the backup software installed on it supports integration with HPE StoreOnce.

HPE StoreOnce supports both local and external key management. Keys generated and managed are the Data Encryption Key (DEK), which is used for actual encryption of data on HPE StoreOnce, and the Key Encryption Key (KEK), which is used to encrypt the data encryption key itself. With local key management, the HPE StoreOnce key management system creates, manages, and stores both the data encryption key and the key encryption key. The HPE StoreOnce local keystore manager keeps track of all of the keys used for data encryption. With external key management, HPE StoreOnce is enrolled as a client to an external Enterprise Secure Key Manager.

ESKM creates and manages the key encryption key (KEK) that is used to encrypt the data encryption keys (DEKs) on HPE StoreOnce. There is one key encryption key created per node of HPE StoreOnce on ESKM and this KEK is also known as the “Master Key” which encrypts and decrypts all the data encryption keys belonging to the HPE StoreOnce.



So, both the StoreOnce OS in local key management mode and ESKM in external key management mode manage and store the Key Encryption Key, which is used to wrap (encrypt) the data encryption keys doing the actual encryption of data on HPE StoreOnce.

4 Integration

This section provides the detailed procedure of integrating ESKM with HPE StoreOnce.

4.1 Data at Rest Encryption

Data at Rest encryption ensures protection of stored data on StoreOnce so that data cannot be accessed from stolen, discarded or replaced disks. It is software based encryption that can be enabled on a per-store basis, which encrypts the data before writing it onto the disk. Data at Rest encryption can be used with Local Key Management or Centralized Encryption Key Management.

Data at Rest encryption must be enabled when creating a new VTL library, NAS share, or StoreOnce Catalyst store and it requires the StoreOnce Security Pack license to be in place.

4.1.1 Local Key Management

When using the local key management mode, the keystore manager on StoreOnce manages the encryption keys used for Data at Rest encryption and Data in Flight encryption. Each time a new encrypted VTL library, NAS share, or StoreOnce Catalyst store is created or deleted, the keystore on StoreOnce is updated. The keystore is also updated when a Data in Flight encryption link is created or deleted.

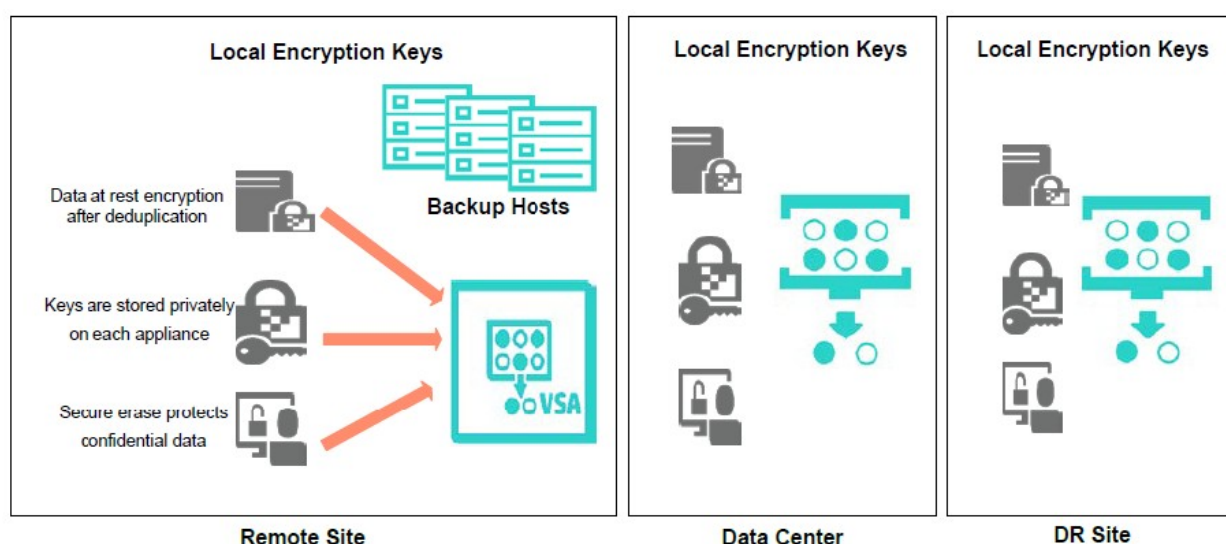


Figure 13 : Local key management

The above figure shows data protection of HPE StoreOnce VSA at the remote site, and also HPE StoreOnce at the primary data center and disaster recovery site using local encryption keys.



If using local key management, ensure to back up the local keystore using the StoreOnce CLI commands, and save it securely off-site in case the original keystore is corrupted. However, only the latest version of the keystore must be kept after each creation or deletion of an encrypted VTL library, NAS share, StoreOnce Catalyst store, or Data in Flight encryption link.

Encryption has to be enabled manually for each target store (either Catalyst, NAS or VTL libraries) created on HPE StoreOnce. To enable Data at Rest encryption on StoreOnce, select the Store Encryption Enabled checkbox of the StoreOnce at store creation time.

LKM_Store

Catalyst Store Details	Permissions	Catalyst Item Summary	Data Jobs	Outbound Copy Jobs	Inbound Copy Jobs
Name		LKM_Store			
Description		Catalyst Store 1			
Data Job Log Retention Period (Days)		90			
Inbound Copy Job Log Retention Period (Days)		90			
Outbound Copy Job Log Retention Period (Days)		90			
Primary (Default) Transfer Policy		Low Bandwidth			
Secondary Transfer Policy		High Bandwidth			
Physical Data Size Quota		(No Limit)			
Logical Data Size Quota		(No Limit)			
Store Encryption Enabled		☒			
Secure Erase Mode		None			
Store is Federated		☐			

Delete**Edit**

Figure 14 : LKM-Store



After the encryption is enabled on a store, it cannot be disabled.

4.1.2 Centralized Key Management

When using external key manager mode, StoreOnce is enrolled to an external key manager as a client. After successful enrollment, the key encryption key (KEK) used for encrypting data encryption keys (DEKs) on StoreOnce is generated, served, stored, and managed by the external key manager. One KEK is generated as a KMIP key on ESKM for one node of HPE StoreOnce, and it is used to encrypt and decrypt all the DEKs on that particular node of HPE StoreOnce.

Enrolling HPE StoreOnce to ESKM is based on secure identity-based access, administration, and logging, and HPE StoreOnce leverages the standard Key Management Interoperability Protocol (KMIP) for accessing and communicating with the external key manager.

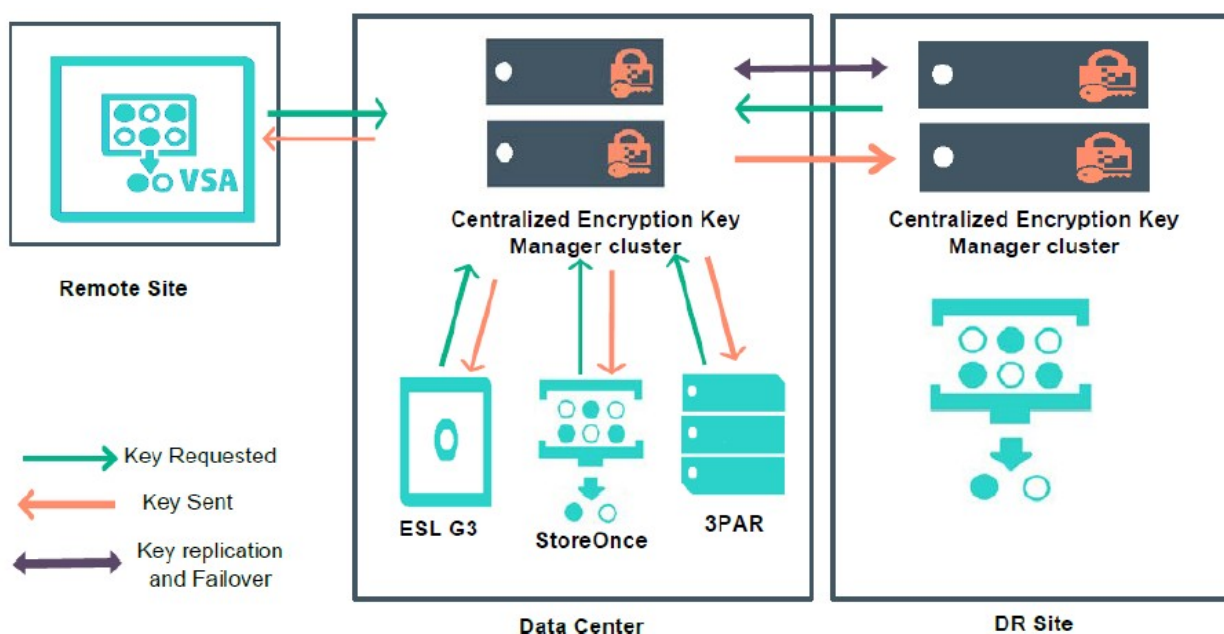


Figure 15 : Centralized key management

When enrolling StoreOnce to ESKM, if there are any target stores on StoreOnce using local key management mode, StoreOnce does a backup of the keystore for these existing LKM stores before enrolling StoreOnce to ESKM.

```

10.05.00.254 - PuTTY
# keymanager import HPE_KMIP_CA.crt signed.crt Password1234

CA and Certificate successfully imported and password has been verified

# keymanager mode external BusCon Password1234 address 10.85.80.216 type Utimaco_eskm HPE_KMIP_CA
Found encrypted device(s) on the appliance.
-----
In order to protect all configured encryption keys prior to 'external' mode enrolment:
  1) A backup of the existing local keystore will be initiated.
  2) The transition to 'external' key manager will then proceed.
  3) Check all of the encryption keys have migrated successfully.
Press 'y' to perform backup and then enrolment or 'n' to skip (abort) this command!
-----

Enter 'y' to continue or 'n' to skip [default='n']: y
Begin SAVE of keystore ...
Enter password to encrypt keystore: *****
Reenter password to confirm: *****
Backup: keystore_LKM_HP2M2516122F_2016-11-20T120721Z.kms
Attempting transition to external key manager ...

Enrollment into EKM Mode successful
Checking that all encryption keys are accessible ...

Check key 1 of 1

External enrolment complete. All keys have migrated successfully.

# keymanager mode show

Node:    EKM
Vendor:  Utimaco_eskm

```



The HPE StoreOnce can be configured to use only the local key manager or the external key manager. Both key manager types cannot be used at the same time.

After successful enrollment of HPE StoreOnce to ESKM, one KMIP key is created per node of HPE StoreOnce. This KMIP key is the key encryption key (KEK) that is used to encrypt the data encryption keys (DEKs) on HPE StoreOnce. Typically, one key is generated per service set running on HPE StoreOnce and since each StoreOnce node has one service set running on a regular basis, one key is generated per node of StoreOnce on ESKM.

Enterprise Secure Key Manager utimaco®

Home • Security • Device Help • Log Out

veskm-196
Logged in as admin

Keys & KMIP Objects

- Keys
 - Query Keys
 - Create Keys
 - Import Keys
 - Key Options
- KMIP Objects
- Cloud Integration
- Authorization Policies

Users & Groups

- Local Users & Groups
- LDAP

Certificates & CAs

- Certificates
- Trusted CA Lists
- Local CAs
- Known CAs

Advanced Security

- High Security
- SSL Options
- SSH Options
- FIPS Status Server

Security / Keys / Keys

Key and Policy Configuration

General Help

Saved Query Name: [All]

Global Summary Statistics	
Total keys returned in results:	2
Total keys:	2

ESKM Summary Statistics	
Total ESKM keys meeting search criteria:	2
Total ESKM keys returned in results:	2
Total ESKM Keys:	2

KMIP Summary Statistics	
Total KMIP keys meeting search criteria:	0
Total KMIP keys returned in results:	0
Total KMIP symmetric key objects:	0
Total KMIP Objects:	0

Keys Help

Query: [All] [Name Query]

Items per page: 10 [Submit]

Type	Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
☒ KMIP	K34303136-3538-4032-3236313531323265-076236356-633312616	5c04025a-485b-49b-8914-0f4e-436771	HP2M2515122F	AES-256	2020-07-04 10:45:42	1
☐ KMIP	K34303136-3538-4032-3236313531323265-24980000-170-53132620	8c5420f9-16b-45ca-afaa-23932ae09a1	HP2M2515140X	AES-256	2020-07-04 10:56:58	1

1 - 2 of 2

[Create](#) [Delete](#) [Convert](#) [Properties](#)

Figure 16 : Key and Policy Configuration

4.2 Data in Flight Encryption

Data in Flight encryption provides protection against unauthorized access to data replicated between HPE StoreOnce appliances or data transferred between clients (Microsoft® Windows® and Linux®) and an HPE StoreOnce appliance. When enabled, the Data in Flight encryption security feature protects data that is in transit, from forensic attack using the IPsec protocol. The data can be moving between two HPE StoreOnce appliances over a WAN, or a StoreOnce appliance and a backup server over a LAN or WAN.



Data in Flight encryption is not supported for IPv6 subnets. Using Data in Flight encryption for direct backup operations to the StoreOnce appliance over a local network is not supported due to the performance impact of the encryption.

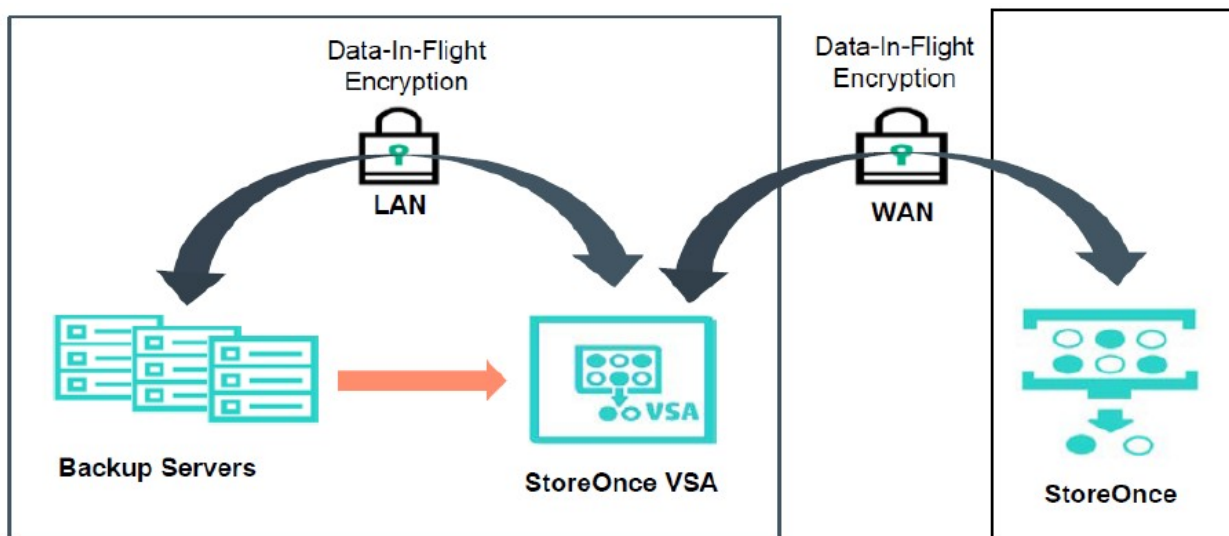
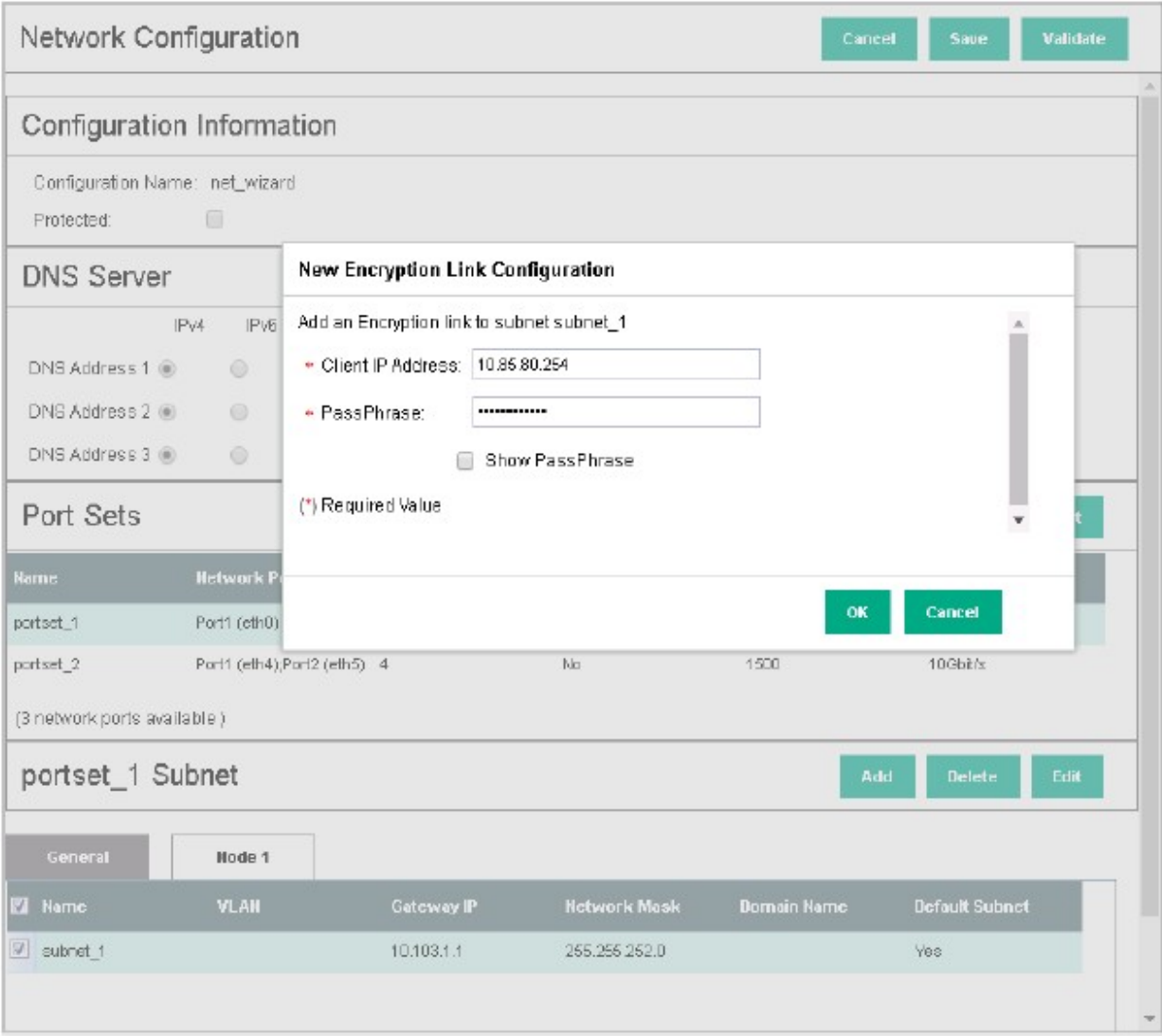


Figure 17 : Data in Flight encryption

After successfully enrolling HPE StoreOnce as a client to ESKM, the key management mode on HPE StoreOnce changes from local to external. When a new encryption link is created on HPE StoreOnce for Data in Flight encryption, one KMIP key is generated on ESKM which protects the data in transit by encrypting the data packets moving through the network. Each time a new encryption link is created or deleted, the keystore on StoreOnce is updated to include all the latest clients added for Data in Flight encryption.

Data in Flight requires customers to use a Static IP, not DHCP, for the client IP address.



Network Configuration [Cancel] [Save] [Validate]

Configuration Information

Configuration Name: net_wizard

Protected: ☐

DNS Server

	IPv4	IPv6
DNS Address 1	☒	☐
DNS Address 2	☒	☐
DNS Address 3	☒	☐

Port Sets

Name	Network P
portset_1	Port1 (eth0)
portset_2	Port1 (eth4), Port2 (eth5) 4

(3 network ports available)

portset_1 Subnet [Add] [Delete] [Edit]

General **Node 1**

Name	VLAN	Gateway IP	Network Mask	Domain Name	Default Subnet
subnet_1		10.103.1.1	255.255.252.0		Yes

New Encryption Link Configuration

Add an Encryption link to subnet subnet_1

* Client IP Address:

* PassPhrase:

☐ Show PassPhrase

(*) Required Value

[OK] [Cancel]

Figure 18 : Network Configuration

4.3 Steps for Integration

This procedure uses both KMS and KMIP protocols along with creating "Registration User". This "Registration User" is used to register the KMS StoreOnce nodes with the ESKM. Post registration, it uses KMIP protocol for key life cycle management activities.

4.3.1 Creating an Admin User

To create admin user, perform the following steps:



Admin user should not be confused with the administrator which is created on the ESKM to login to the **Management Console**.



Before proceeding, please make sure that you have created the **Local CA, Certificates**, and the KMS and KMIP servers are configured. Also make sure that the **Date & Time** is syncing with the NTP server and HPE StoreOnce and KMS and KMIP services are running.

Please refer to the *Configuring the ESKM server* page for details.

- Log in to the **Management Console** as an administrator and navigate to **Security>Local Users & Groups>Local Users**.
- Click on **Add**.



Please select **User Administration Permission** and **Change Password Permission** and do not select **Enable KMIP**.

Create Local User

Help ?

Username:	registration
Password:	
Confirm Password:	
License Type:	KMS
User Administration Permission:	☒
Change Password Permission:	☒
Enable KMIP:	☐
Map non-existent Object Group to x-Object Group:	☐
KMIP User Group:	default user group
KMIP Object Group:	default object group

KMIP Client Certificate:

Figure 19 : Create Local User

- Click Create.

Local Users

Help ?

Filtered by	---	where value	contains		Set Filter
Items per page:	10	Submit			
Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
☒ registration	☐	☒	☒	KMS	
1 - 1 of 1					
Add	Delete	Properties			

Figure 20 : Local Users

- Go to HPE StoreOnce CLI.
- Enter the command: `keymanager# create <username> <password> <DNvalue>`.
- Click enter to obtain the CSR.

```
create - command takes as input a username, password and optionally the DN information and generates a CSR
import - command imports the CA certificate and signed client certificate of the StoreOnce appliance.
expand - command enrolls new nodes of a cluster with the Key Manager.
update - command updates EKM information.
```

```
keymanager# create registration storeonce123 "/OU=Atalla/O=Utimaco/L=Sunnyvale/ST=CA/C=US"
```

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

```
MIICrTCCAUAQAwDEVMBMGA1UEAwMcmVnaXN0cmF0aW9uMQ8wDQYDVQQLDAZB
dGFsbGEExEDAOBgNVBAoMB1V0aW1hY28xEjAQBgNVBAcMCVN1bm55dmFsZTELMAG
A1UECAwCQ0ExCzAJBgNVBAYTA1VTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAs5kK5VloF2cB749dD7Y+L1/I5nwC2MKyeXBEEJnnghH4BZxuLdoHgpe
30oDVg+ttQvHk1nEYJA/an3zd2eEMaFSMp5m0pMN/x3dmVMYVGIL98pPJAPjeItot
WwJP1dQLQRpQCH9VhXtWvzCWyHmaExFtQUczfQ18AOx9HZBhN6T8sQYRcXePwqjQ
ZVeG9+dn64Vw+k8vPFd1apK8o5vaTyrQdozyFxOARbwVvjdaShaJMMr83oq6+T0X
KeSEmPGCwvY94yF2LTz95oz84/EnLHeDxSvXsHVlgI32MytdlWGKcip7y8+jajxS
U5E8MIpQqTT7QnoOJyJpv+bCURS0jwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
ADZU4zahdqW/TR07N1xoxIyZioVTAP+wFhL8TBvFdwY0WqbQ8CRj15uEcU83CD5h
pbnysmLQn67pY3w3FwzNdvj2HjncvnHPuzsZgWb2rppnYX2jRLc5REM3Th5QUAs0
aFsWokOYc8kvJd9nEaoVTR8yR000IvJ8ZqJFglKYJuiIRDmSQziYZTKMkBNQ+AtS
qmYFaD7yidLchSoMTCd3VH2MH5/ULawyqs9NQKQDK790IU57ae6e3nFQuxMC8Twk
OTXLW+FjiwWSepkMkkEer3//g44ctEVg8pCh469cDiDlmoCkjrQ+v0ZyQsybaXgC
9B3hZJ4s8HofdFlgFTxa4UU=
```

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

```
keymanager#
```

- Copy the CSR from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----` lines.
- Go to the ESKM Management Console and navigate to **Security>Certificates & CAs>Local CAs** and click on **Sign Request**.

Local Certificate Authority List

[Help ?](#)

CA Name	CA Information	CA Status
☒ ESKMCA	Common: ESKMLocalCA Issuer: Organization Expires: Nov 11 08:37:28 2032 GMT	CA Certificate Active
Edit	Delete	Download
Properties	Sign Request	Show Signed Certs

Figure 21 : Local Certificate Authority List

- Paste the CSR from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----` lines into the **Certificate Request** field.
- Select **Client** and click on **Sign Request**.

Sign Certificate Request

Help ?

Sign with Certificate Authority: ESKMCA (maximum 2813 days) ▾

Certificate Purpose:

- ☐ Server
- ☒ Client
- ☐ Server and Client

Certificate Duration (days):

Certificate Request:

```
-----BEGIN CERTIFICATE-----
MIIEExTCCA62gAwIBAgIBADANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRERDwYDVQQGEWhDYW1wYmVsbnBvbmEVBMBGA1UEChMTM3JnYW5p
emF0aw9uMR0wGwYDVQLExRjbmc1hdGlvb1BTZW1cm10eTEUMBIGA1UEAxML
RVNLTUxvY2FsOQE0ExJzAlBkgqhkig9w0BCQEWGGluZm9zZWNAab3JnYW5pemF0aw9u
LmNvbTAeFw0yMjExMTMwODMzMjhaFw0zMjExMTEwODMzMjhaIIGIMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCCQ0EXETAPBgNVBACTCENhbXBibWxsMRUwEwYDVQQKEwXP
cmdhbm16YXRpb24uXHTAbBgNVBAsTFEluZm9ybWwF0aw9uIFNlY3VyYXR5MRQwEgYD
VQDEwtFU0tNTG9jYXZDTEnMCUGCSqGSiB3DQEFARYYaW5mb3NlY0Bvcmdhbm16
YXRpb24uY29tMiBIb1anBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKAQAEEAzaTedJfm
tdguV3kBGLXCzTWZ2OnOTMPaBtzPwFZU30fMS33ZVDU/6QaeVGcj1KcTi2nhGtQs
myxcCape1URHrHbi27P0sMmx+HXS95Vp8O2PRzfWC2YB+SDFCrVbLVNG7Ah6Y3j90
9TXowznctbwftkJUhVXLG1RS8IyegA+UKFEmX0ogb7ak6FAXubRxoESwfH5iR7WF
nCMpX0jv1zpaXjen/FUFwxFB3QM/vGondxrQ3Y7v2btZg7S5vXeAAgHPA0pQZpkW
EKsbkqDdTYdbwLfAx17HQa9vHXDXyzssLZ+sSMoL7weJIbtXiOXQQ++M8LSEcn6D
```

Figure 22 : Sign Certificate Request

CA Certificate Information

Help ?

Key Size:	2048
Start Date:	Jul 8 06:35:11 2020 GMT
Expiration:	Mar 16 06:35:11 2030 GMT
Issuer:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization.com
Subject:	C: US ST: CA L: Sunnyvale O: Utimaco OU: Atalla CN: registration

-----BEGIN CERTIFICATE-----

MIID3TCCaSwGwIBAgIBeJANBgqhkiG9w0BAQsFADCBQjELMAkGA1UEBhMCVVMwCzAJBgNVBAGTAkNBMRewDwYDVQQHEwhDYWlwYmVsbDEVMBMGA1UEChMNT3JnYW5pemF0aW9uMR0wGwYDVQQLEwRjb2Vcm1hdGlvb1BTZWN1cm10eTEUMBIGA1UEAxMLRVNLTUxvY2FsQ0ExJzAlBgqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9uLmNvb1AeFw0yMDA3MDgwNjM1MTFaFw0zMDAzMTYwNjM1MTFaMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwDh21wYW55LCBjb2MxEDA0BgNVBAcTB0ZpbmFuY2UxETAPBgNVBAMTCE1vbmdvREIxMSIwIAYJKoZIhvcNAQkBFhNmaW5hbmNlQGNvbXBhbnkuY29tMIIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE4Zff7hxc6LMc9LE11bfPagsnsXuFyWQJSXiI3rG0htHwDV7Ese3+WAQ6DQaRrculYMrCuUfQynbAZSQWsjVWeafgiHoBrO3bhRv1CCjpIsQe0VLeOpEzq1pbhFl1puZzQv5BH8XK5vfdQY0FMPUM9fbkiZKxj+FQkGj0LBFImOmMk+Nt8QONHixig0uUaKFsLJqasm7ZMnB6cp6A4Y6eZ/HXctECzopRc1kVbcxXHawH2z7qrGRdb/f0DMWT5bybMod7EV23gM+DeA7PBcgf8XHaC+qsP6tj/tY9zdFZ7xJ27QatuA+8XF80ByLT4pmj4fmpp7rRIgWAWJVZLfEiwIDAQABozEwLzAJBgNVHRMEAIAAMBEGCWCsGSAAG+EIBAQQEAwIHgDAPBgNVHREECDAGhwQK3rLxMA0GCSqGSIb3DQEBCwUAA4IBAQCIEBkeI636KVALPAANut74GQsExwNVaWpQYKGQ098dLkPC1mGT8aJDva5bbnCRP8Y91TPWbVANKkoiC1VRSVtBrtk9vi1SJkujHtmc6J8cpCLdPF/n+77dbPmkKqFpWOZVW2Gbxr9vfnsg4D27219B01y1dbWVUhmEuNGT1Pytq6gOC33KVacyvgKZfAoepUeR30cFL8yicNYgrAFDE61bWUFm3PHz1AfXwc7/eQ87Huvn9dLX5AQgyuzGpFCvnc1Rw2M916jv1C/KdK6uWtaazF/ebMh6gL/4hvfwwC1930pw1RAS5/79szTYajIA1wwJuciWoc1wTcwD+mdML4c4e5

-----END CERTIFICATE-----

Download

Back

Figure 23 : Certificate Information

- Click on **Download** to save the certificate onto the system. For example: `signed.crt`.
- To download the local CA, navigate to **Security>Certificates & CAs>Local CAs**.
- Select the CA **Name** and click **Download** to save onto the system. For example `ESKMCA.crt`.

Local Certificate Authority List

[Help ?](#)

CA Name	CA Information	CA Status
☒ ESKMCA	Common: ESKMLocalCA Issuer: Organization Expires: Nov 11 08:37:28 2032 GMT	CA Certificate Active
Edit Delete Download Properties Sign Request Show Signed Certs		

Figure 24 : Local Certificate Authority List - Download

4.3.2 Importing Certificate

To import the certificates, perform the following steps:

1. Go to HPE StoreOnce CLI.
2. Enter the command: `Keymanager # import <ESKMCA.crt> <signed.crt> <password>`.
3. Click on enter and a message will be displayed as "CA and Certificate successfully imported and password has been verified."

```

[keymanager# create registration storeonce123 */OU=Atalla/O=Utimaco/L=Sunnyvale/ST=CA/C

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAUAQAwaDEVMBMGA1UEAwMcmVnaXN0cmF0aW9uMQ8wDQYDVQQLDAZB
dGFsbGEuEDAOBgNVBAoMB1V0aW1hY28xEjAQBgNVBAcMCVN1bm55dmFsZTELMaK
A1UECAwCQ0ExCzAJBgNVBAYTA1VTMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAs5kK5VLoF2cB749dD7Y+L1/I5nwC2MKyeXBEEJnnngnH4BZxuLdoHgpe
30oDVg+tQvHk1nEYJA/an3zd2eEMaFSMp5m0pMN/x3dmVMYVGIL98pPJAPjeItoT
WwJP1dqLQRpQCH9VhXtWvzCWyHmaExFtQUczfQ18AOx9HZBhN6TBsQYRcXePWqjQ
ZVeG9+dn64Vw+k8vPFd1apk8o5vaTyrQdozyFxOARbwVvjdaShaJMMr83oq6+T0X
KeSEmPGCwvY94yF2LTz95oz84/EnLHeDxSvXsHVlgI32MytdlWGKcip7y8+jajxS
U5E8MIpQqTT7QnoOJyJpv+bCurs0jwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
ADZU4zahdqW/TR07N1xoxIyZioVTAP+wFhL8TBvFdwYOWqbQ8CRjl5uEcU83CD5h
pbnySmLQn67pY3w3FwzNdvj2HjncvnHPuzsZgWb2rppnYX2jRLc5REM3Th5QUAs0
aFsWokOYc8kvJd9nEAoVTR8yR00IvJ8ZqJFglKYJuiIRDmSQZiYZTKMkBN+AtS
qmYFaD7yidLchSoMTCd3VH2MH5/ULawys9NQKQDK790IU57ae6e3nFQuXMC8Twk
OTXLW+FJiwWSepkMkkEer3//g44ctEVg8pCh469cDiDlm0CkjrQ+V0ZYQsybaXgC
9B3hZJ4s8HofdFLgFTxa4UU=
-----END CERTIFICATE REQUEST-----

[keymanager# import ESKMCA.crt signed.crt storeonce123

CA and Certificate successfully imported and password has been verified

keymanager#

```

Figure 25 : CA and Certificate successfully imported

4.3.3 Enrolling into External Key Manager Mode

To enroll in external key manager mode, perform the following steps:

1. Go to HPE StoreOnce CLI.
2. Enter the command: `Keymanager # mode external <username> <password> address <ip address of the EKM> type <ESKM brand> <ESKMCA> .`
3. Click on enter and a message will be displayed as "Enrollment into EKM Mode successful."

```

A1UECAwCQ0ExCzAJBgNVBAYTA1VTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAs5kK5VLoF2cB749dD7Y+L1/I5nwC2MKYeX8EEJnnghH4BZxuldoHgpe
30oDVg+tQvHk1nEYJA/an3zd2eEMaFSMp5m0pMN/x3dmVMYVGIL98pPJAPjeItOT
WwJP1dqLQRpQCH9VhXtWvzCWyHmaExFtQUczfQ18AOx9HZBhN6TBsQYRcXePWqjQ
ZVeG9+dn64Vw+k8vPFd1apk8o5vaTyrQdozyFxoARbwVvjdaShaJMMr83oq6+T0X
KeSEmPGCwvY94yF2LTz95oz84/EnLHeDxSvXsHVlgI32MytdlWGKcip7y8+jaJxS
U5E8MIpQqTT7QnoOJyJpv+bCurS0jwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
ADZU4zahdqW/TR07N1xoxIyZioVTAP+wFhL8TBvFdWYOWqbQ8CRj15uEcU83CD5h
pbnySmLQn67pY3w3FwzNdvj2HjncvnHPuzsZgWb2rppnYX2jRLc5REM3Th5QUAs0
aFsWokOYc8kvJd9nEAoVTR8yR0001vJ8ZqJFglKYJuiIRDmSQZiYZTKMk8QN+AtS
qmYFaD7yidLchSoMTCd3VH2MH5/ULawyqs9NQKQDK790IU57ae6e3nFQuxMC8Twk
OTXLW+FJiwWSepkMkkEer3//g44ctEVg8pCh469cDiDlmcKjRq+V0ZYQsybaXgC
9B3hZJ4s8HofdFLgFTxa4UU=
-----END CERTIFICATE REQUEST-----

keymanager# import ESKMCA.crt signed.crt storeonce123

CA and Certificate successfully imported and password has been verified

keymanager# mode external registration storeonce123 address 10.14.14.100 type hp_eskm

Enrollment into EKM Mode successful

keymanager#

```

Figure 26 : Enrollment into EKM Mode successful

4. The KMIP account is now created in the ESKM.
5. Go to ESKM and navigate to **Device>Logs & Statistics>Log Viewer>Activity**.
6. Under the “Activity Log”, click on **Display Log**.

Activity Log

Log File: Current

Show Last Number of Lines: 25

Wrap Lines: ☐

Display Log Rotate Logs

Log File: Current (Showing Last 25 Lines)

Download Entire Log Clear

Activity Log:

```

[2020-04-28 16:07:36] INFO 10.14.14.15 [-] - 100000 Version - [1.11.01- [Success] [-]
[2020-04-28 16:07:36] INFO 10.14.14.15 [-] registration 100001 Auth -[registration] - [Success] [-]
[2020-04-28 16:07:37] INFO 10.14.14.15 [-] - 200000 Version - [1.11.01- [Success] [-]
[2020-04-28 16:07:37] INFO 10.14.14.15 [-] registration 200001 Auth -[registration] - [Success] [-]
[2020-04-28 16:07:37] INFO 10.14.14.15 [-] registration 200002 UserGroupCreate - [HP2M233601JM and HP2M233601JM_user] - [Success]
[2020-04-28 16:07:37] INFO 10.14.14.15 [-] registration 200003 SignCertificate - [-] - [Success] [-]
[2020-04-28 16:07:38] INFO 10.14.14.15 [-] registration 200004 UserCreate - [HP2M233601JM] - [Success] [-]

```

Figure 27 : Activity Log

7. The user is now created.
8. Now again, navigate to **Device>Logs & Statistics>Log Viewer>KMIP**.
9. Under the “KMIP Log”, click on **Display Log**.

KMIP Log

Log File: Current

Show Last Number of Lines: 25

Wrap Lines: ☐

Log File: Current (Showing Last 25 Lines)

KMIP Log:

```
2020-04-28 16:07:38 [KMIP Server] [Authentication Success] User: [HP2M233601JM] From IP: 10.14.14.15
2020-04-28 16:07:38 [KMIP Server] [ClientOperation] User: [HP2M233601JM] UUID: [] Operation: [DISCOVER_VERSIONS] Result: [Success]
2020-04-28 16:07:38 [KMIP Server] [Authentication Success] User: [HP2M233601JM] From IP: 10.14.14.15
2020-04-28 16:07:38 [KMIP Server] [ClientOperation] User: [HP2M233601JM] UUID: [] Operation: [QUERY] Result: [Success]
2020-04-28 16:07:38 [KMIP Server] [Authentication Success] User: [HP2M233601JM] From IP: 10.14.14.15
2020-04-28 16:07:38 [KMIP Server] [ClientOperation] User: [HP2M233601JM] UUID: [bfc7c910-fe4b-428f-a0f7-f9c0b8b9bc03]
Operation: [REGISTER] Operation Type: [SYMMETRIC KEY] Result: [Success]
2020-04-28 16:07:38 [KMIP Server] [Authentication Success] User: [HP2M233601JM] From IP: 10.14.14.15
2020-04-28 16:07:38 [KMIP Server] [ClientOperation] User: [HP2M233601JM] UUID: [bfc7c910-fe4b-428f-a0f7-f9c0b8b9bc03]
Operation: [REGISTER] Operation Type: [SYMMETRIC KEY] Result: [Success]
2020-04-28 16:07:41 [KMIP Server] [Authentication Success] User: [HP2M233601JM] From IP: 10.14.14.15
2020-04-28 16:07:41 [KMIP Server] [ClientOperation] User: [HP2M233601JM] UUID: [] Operation: [QUERY] Result: [Success]
```

Figure 28 : KMIP Log

10. To view the created group, navigate to **Security>Users & Groups>Local Groups**.

Local Groups

[Help ?](#)

Filtered by --- where value contains

Items per page: 10

Group	Group Type	Group Sub-Type
☒ All Groups	KMIP	Groups
☐ All Users	KMIP	Users
☐ default object group	KMIP	Object Group
☐ default user group	KMIP	User Group
☐ HP2M233601JM	KMIP	Object Group
☐ HP2M233601JM_user	KMIP	User Group

1 - 6 of 6

Figure 29 : Local Groups

11. To view the created user, navigate to **Security>Users & Groups>Local Users**. It has “KMIP-Enabled” selected and “User Administration Permission” and “Change Password Permission” unselected.

Local Users

[Help ?](#)Filtered by: --- where value contains Items per page: 10

▲ Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
☒ HP2MM233601JM	☒	☐	☐	Uncategorised	
☐ registration	☐	☒	☒	KMS	

1 - 2 of 2

Figure 30 : Local Users

Selected Local User

Help ?

Username:	HP2M233601JM
Password:	*****
License Type:	Uncategorised
User Administration Permission:	☐
Change Password Permission:	☐
Enable KMIP:	☒
Default KMIP Object Group:	HP2M233601JM
	C: US
	ST: MA
Subject:	L: Andover
	O: HP
Client Certificate:	emailAddress:
	Common Name: HP2M233601JM
	Not Valid Before: Apr 20 13:13:35 2020 GMT
	Not Valid After: Oct 19 13:13:35 2029 GMT
Date Created:	2020-07-09 00:56:14
Date Last Modified:	2020-07-09 00:56:14
Last Access Time:	

KMIP Client Certificate Contents:

```
-----BEGIN CERTIFICATE-----
MIID0jCCARqgAwIBAgIBDzANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAKNBMRERwDwYDVQQHEwhDYW1wYmVsDbEUMBIGA1UEChMLVXRpbWJf
byBjb2MxEADAQBgNVBAStB1V0aW1hY2xETAPBgNVBAMTCEVTS0Q0ExMR8wHQY
KOTIhOtcNAQKBFBh80ZXN0QHV0aW1hY28uY29tMB4XDTEwMDQyMDEzMTMzMzNVoXDTIS
MTAxOTc2MTMzMzNVoZSxczAJBgNVBAYTA1VTMQSwCQYDVQIEwJDQTERMA8GA1UE
BxMIQ2FtcG31bGxwFTATBgNVBAoTDE9yZ2FuaXphdGlvbqJEdMBsJG1UECXMUSW5m
b3JtYXRpb24gU2VjdXJpdHhkzDTALBgNVBAMTBETVS00xJzAlBgkqhkiG9w0BCQEW
GGluZm9zZWNAb3JnYW5pemF0aW9uLmNmVbTCCASiWdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAM8HvyfLGAHizQzx80ei3R+Bz/WyVvSGDTCVZd9QUg9Iary/Iwg
ftZGMO4ppI60+16qUKI78X+NlDR70ltlAD2Bf6b930YgcVSiOBhMfmQmeGsYLcX
q7NH9/F4WPDBsPnPndPPSH0s18X8B1+mNckMIKPEmCMjmdndiH+gQhRQvIcokD
v/cpk5LLG49/1V7qCewYwny9/TXYQMMMKkHs/jxH9hJFIssUWW6X3JM1ktHytCm3
g/ra38iL7f8f8M6cdqQ3EsQcM5WwgjGr4eu1NHX16+N7EQSG0kFxiow2hltn4DED
BbISN0k5nAOXgaHFCEHr6EhNMoKzyMmmZL8CAwEAAMxMC8wCQYDVROTBAlwADAR
BgllghkgBhvChCAQEBAEMCBkAwDwYDVROBBAgBMCect6y8TANBgkqhkiG9w0BAQsF
AAOCAQEA2C/o/9ldoff+512svxhoLnoHqTlqLz0tExr1++nzH8Mly4CyGpQC3FB
w2yikNwFG3rvLFpCNWxEd4Leb+T9fDR+FJlX0u0XUqlNp+r0DVCsyom7tdATVL/
wAniQwrVI+63WlyapZPIpKXgqH4+rEK6F8oarTCCGJYwjdLOjaLHDI5IZeaCdgvo
WkhoE+nPag2gEOEeiftPr6zS83m6ZPpS1lz22SbqB03juH4UuggSg4LRYEwRHgEP
PHp9S3BHJzKeOA+1xj/JW53Ft/V6Lmk6enmqazCCI5tWHHxtoe41P9gzmnXaG72q
Iw/+GfADvqx3fydiN1VctWw5r1Tow==
-----END CERTIFICATE-----
```

Edit Back

Figure 31 : Selected local user

12. Now it is safe to delete the “registration” user. Navigate to **Security>Users & Groups>Local Users** and select “registration” and click on **delete**.

Local Users Help ?

Filtered by: --- where value: contains **Set Filter**

Items per page: 10 **Submit**

Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
☐ HP2MM233601JM	☒	☐	☐	Uncategorised	
☒ registration	☐	☒	☒	KMS	

1 - 2 of 2

Add **Delete** **Properties**

Figure 32 : Delete Local User

13. To confirm, navigate to **Security>Certificates & CAs>LocalCAs** and click on the “CA Name”.

Local Certificate Authority List Help ?

CA Name	CA Information	CA Status
☒ ESKMCA	Common: ESKMLocalCA Issuer: Organization Expires: Nov 11 08:37:28 2032 GMT	CA Certificate Active

Edit **Delete** **Download** **Properties** **Sign Request** **Show Signed Certs**

Figure 33 : Local Certificate Authority List

Local Certificate Authority

[Help ?](#)

CA Name: ESKMCA

[Back](#)

Signed Certificates (1 to 3; total 3)

[Help ?](#)

Serial Number	Status	Subject Name
☒ 0x0	Active	/C=US/ST=CA/L=Campbell/O=Organization/OU=Information Security/CN=ESKMLocalCA/emailAddress=infosec@organization.com
☐ 0x1	Active	/C=US/ST=CA/L=Campbell/O=Organization/OU=Information Security/CN=ESKM/emailAddress=infosec@organization.com
☐ 0x12	Active	/C=US/ST=CA/L=Campbell/O=Company, Inc/OU=Finance/CN=MongoDB1/emailAddress=finance@company.com
☐ 0x12	Active	/C=US/ST=MA/L=Andover/O=HP/OU=HPSP/CN=HP2M2336D1JM

[Properties](#)

Figure 34 : Local Signed Certs

4.3.4 Integrating HPE StoreOnce with ESKM

To integrate HPE StoreOnce with ESKM, perform the following steps:

- Login to the HPE StoreOnce Management Console.

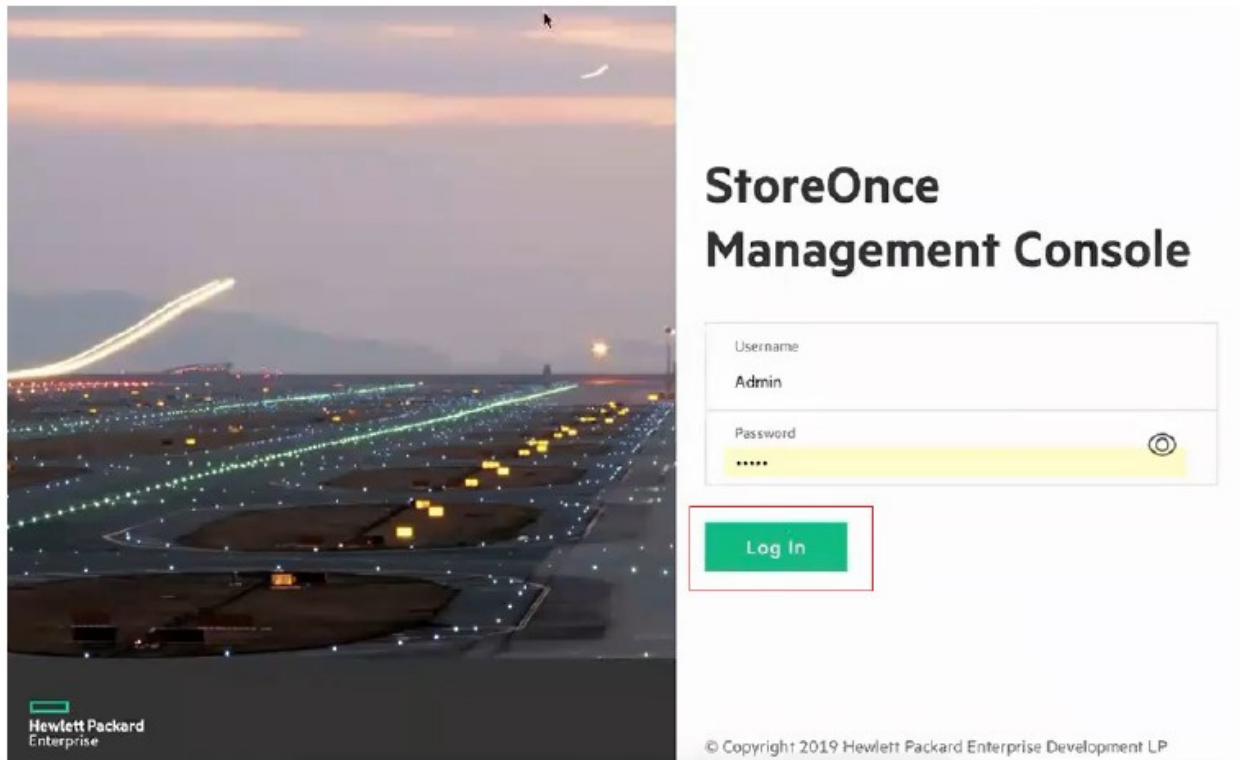


Figure 35 : StoreOnce Console - Log In

- Navigate to **StoreOnce>System Dashboard** and check the availability of the encryption license.

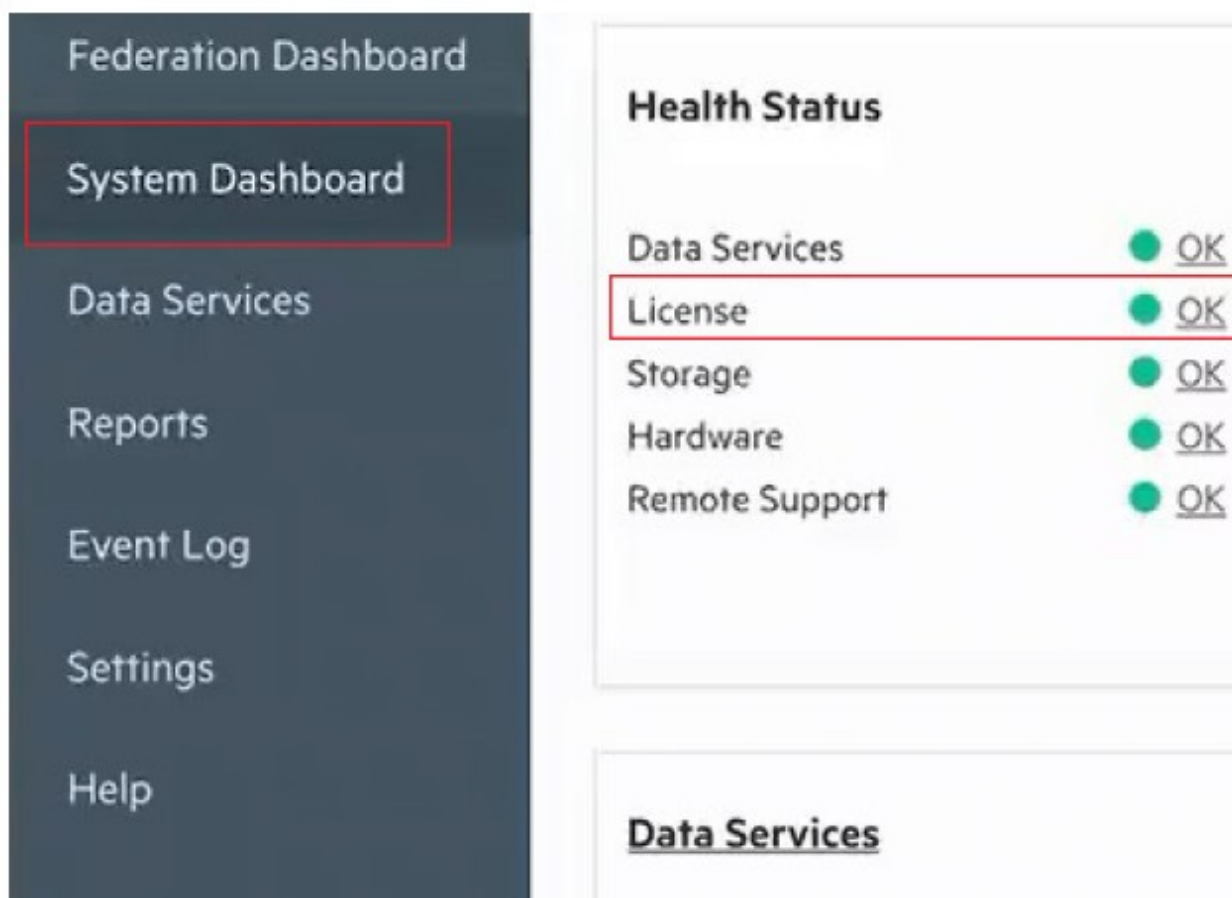


Figure 36 : System Dashboard

To start with the integration, navigate to **StoreOnce>Settings>Key Manager**.

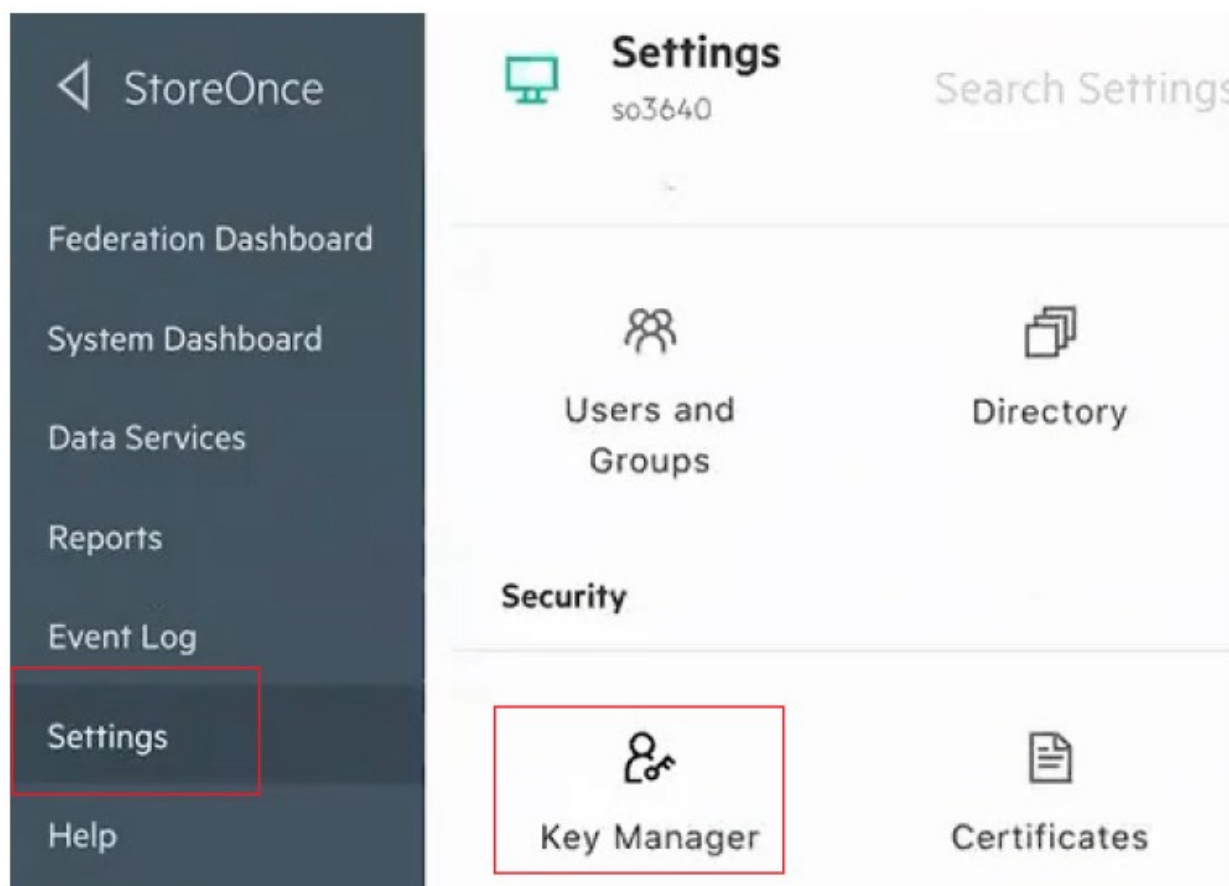


Figure 37 : Key Manager

- Click on **Generate CSR** and click on “Provide External Key Manager Credentials”.



The “External Key Manager Credentials” are to be created on the ESKM.

Login to the ESKM and create a local user with username as “registration”, choose a password and confirm it, select the license type as storage, select the user administration permission and change password permission, do not select KMIP, and click create.

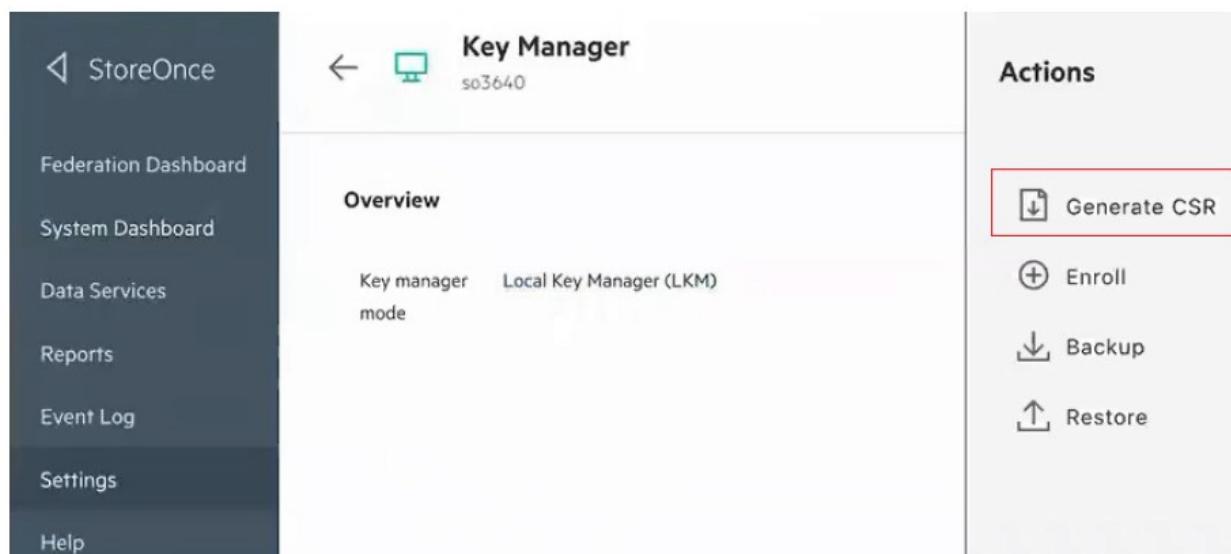


Figure 38 : Generate CSR

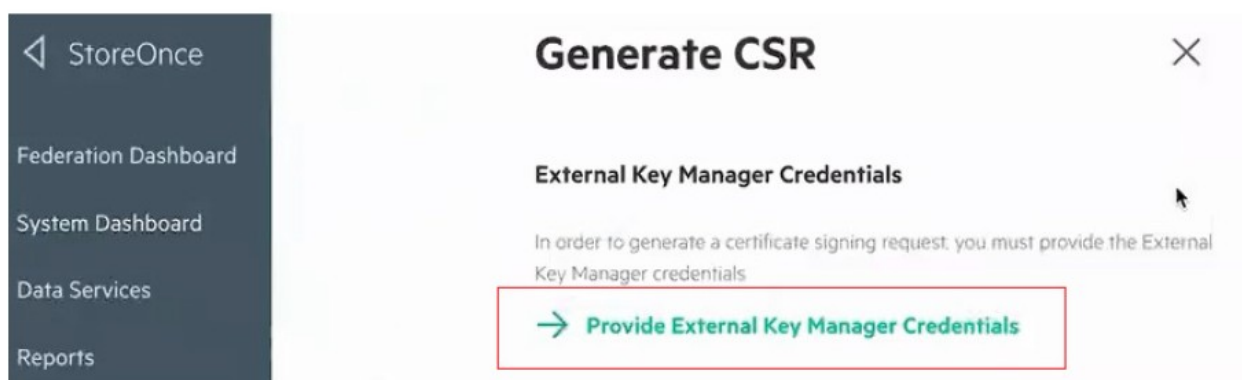


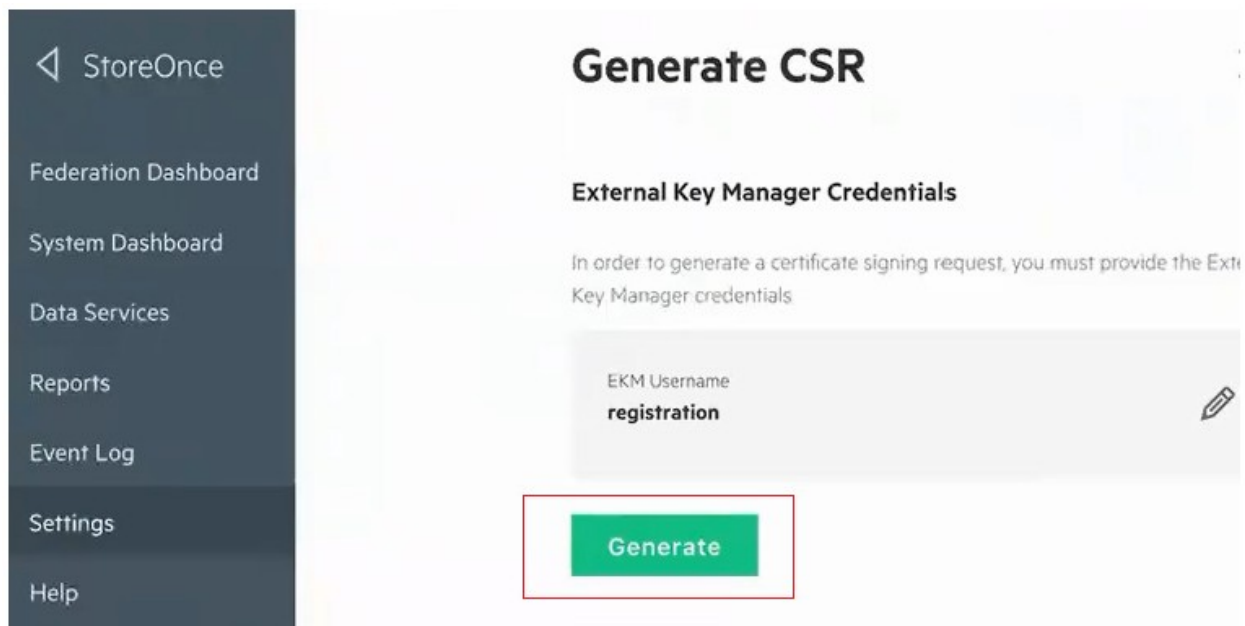
Figure 39 : Generate CSR

- Provide the same username and password that was created on the ESKM and click **OK**.

The screenshot shows the 'External Key Manager Credentials' form within the StoreOnce management console. The left sidebar contains navigation links: StoreOnce, Federation Dashboard, System Dashboard, Data Services, Reports, Event Log, Settings, Help, HPE InfoSight, and HPE Privacy Statement. The main content area has a title 'External Key Manager Credentials' and a subtitle 'Provide the External Key Manager credentials.' Below this are two input fields: 'EKM Username' with the value 'registration' and 'EKM Password' with masked characters. A 'Learn more' link is positioned below the password field. At the bottom is a green 'OK' button. Red rectangular boxes highlight the 'EKM Username' field, the 'EKM Password' field, the 'Learn more' link, and the 'OK' button.

Figure 40 : External key manager credentials

- Click on **Generate** and the CSR will be displayed. Click on **Select and Copy** to copy the certificate and go to ESKM.



The screenshot displays the 'Generate CSR' page in the StoreOnce interface. On the left is a dark sidebar with the following navigation links: StoreOnce, Federation Dashboard, System Dashboard, Data Services, Reports, Event Log, Settings, and Help. The main content area has a title 'Generate CSR' and a section 'External Key Manager Credentials'. Below this, a text box explains: 'In order to generate a certificate signing request, you must provide the External Key Manager credentials'. A form field labeled 'EKM Username' contains the text 'registration'. To the right of the text box is a pencil icon. At the bottom of the form is a green 'Generate' button, which is highlighted by a red rectangular box.

Figure 41 : Generate CSR

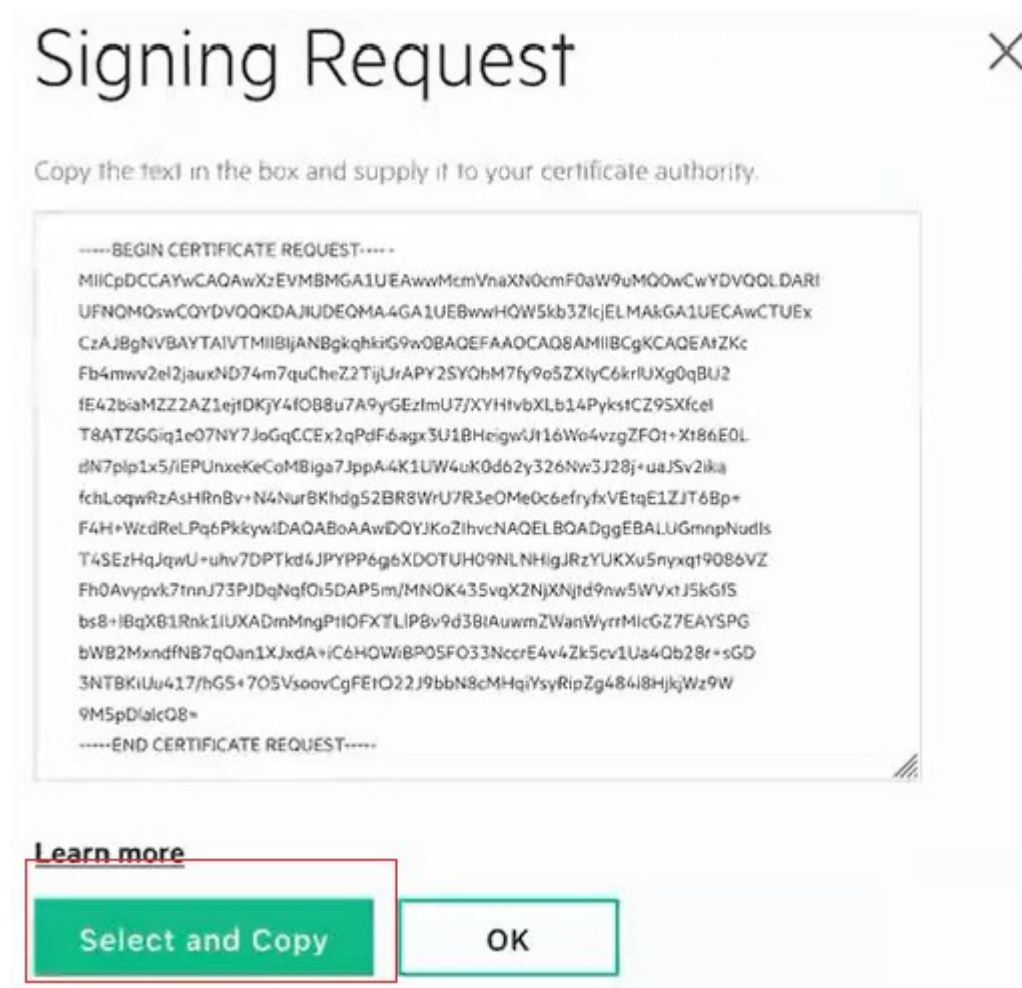


Figure 42 : Sign Request

- Navigate to **Security>Certificates & CAs>Local CAs** and click on **Sign Request**. Select the certificate purpose as "Client" and paste the certificate in "Certificate Request" pane and click on **Sign Request**.

Local Certificate Authority List

[Help ?](#)

CA Name	CA Information	CA Status
☒ ESKMCA	Common: ESKMLocalCA Issuer: Organization Expires: Nov 11 08:37:28 2032 GMT	CA Certificate Active
Edit	Delete	Download
Properties	Sign Request	Show Signed Certs

Figure 43 : Local Certificate Authority List

Sign Certificate Request

[Help ?](#)

Sign with Certificate Authority:	ESKMCA (maximum 2813 days) ▼
Certificate Purpose:	☐ Server ☒ Client ☐ Server and Client
Certificate Duration (days):	2813

Certificate Request:

```
-----BEGIN CERTIFICATE-----
MIIExTCCA62gAwIBAgIBADANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRERDwYDVQQHEWhDYW1wYmVsbnBDEVMBMGA1UEChMNT3JnYW5p
emF0aW9uMR0wGwYDVQQLEXRJbmZvcmlhdGlvbiBTZW50eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCEwGgluZm9zZW50eTEUMBIGA1UEAxML
LmNvbTAeFw0yMjExMTMwODM3MjhaFw0zMTExMTMwODM3MjhaMIGiMQswCQYDVQQG
EwJVVzELMAkGA1UECBMCQ0ExETAPBgNVBACTCENhbXBibWVzMRUwEwYDVQQKEwxP
cmdhbm16YXRpb24xHTAbBgNVBAsTFEluZm9ybW9uIFN1Y3VyaXR5MRQwEgYD
VQQDEwtFU0tNTG9jYXZ0TEtMCUGCSqGSIb3DQEJARYYaW5mb3N1Y0Bvcmdhbm16
YXRpb24uY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEazaTedJfm
tdguV3kBgLXczTWZ2OnOTMPaBtzPwFZU30fMS33ZVDU/6QaevGCj1KcTi2nhGtQs
myxcCape1URhrHbi27P0sMmx+WXs95Vp802PRzWfC2YB+SDfCRvVLNG7Ah6Y3j90
9TXowznctbwftKjUhVXLG1RS8IyegA+UkFEmX0ogb7ak6FAXubRxoESwfh5iR7WF
nCMpX0jv1zpaXjen/FUFwxFB3qM/vGondxrQ3Y7v2bTZg7S5vXeAAgHPA0pQZpkW
EKsbkqDdTYdbwLFAx17HQA9vHXDXyZssLZ+sSMoL7wEjIbTxioxQQ++M8LSEcn6D
-----
```

[Sign Request](#) [Back](#)

Figure 44 : Sign Request

CA Certificate Information

Help ?

Key Size:	2048
Start Date:	Jul 8 06:35:11 2020 GMT
Expiration:	Mar 16 06:35:11 2030 GMT
Issuer:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization.com
Subject:	C: US ST: CA L: Andover O: HP OU: HPSP CN: registration

-----BEGIN CERTIFICATE-----

MIID3TCCAsWgAwIBAgIBEjANBgkqhkiG9w0BAQsFADCBobjELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRewDwyDVQQHEwhDYWlwYmVsbDEVMBMGA1UEChMTMT3JnYW5p
emF0aW9uMR0wGwYDVQLExRJBmZvcmlhdGlvb1BTZWNIcm10eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWEWgluzm9zZWNAbz3JnYW5pemF0aW9u
LmNvbTAEFw0yMDA3MDgwNjM1MTFaFw0zMDAzMTYwNjM1MTFaMIGNMQswCQYDVQQG
EwJVUzELMAkGA1UECBMQ0EXETAPBgNVBAoTCENhbXBib2ZwxsMRUwEwYDVQQKEwxDb21wYW55LCBJbmMxEADAOGBNVBAsTB0ZpbmFuY2UxETAPBgNVBAMTCE1vbmdvREIx
MSIWIAYJKoZIhvcNAQkBFBhNmaw5hbmlNQGNvbXBhbnkuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2ff7hxc6LMc9LE11bfPagsnsXuFyWQJSXiI
3rG0htHwDV7Ese3+WaQ6DQaRrculYMrCuuFqynbAZSQWsjVWeafgihoBrO3bhRy
iCCjpIsQe0VLeOpEZglpbhfFl1puZzQv5BH8XK5vfdQYoFMPUM9fbki2Kxj+FQKGj
oLBfImOmMk+Nt8QONHiXigouUAkFsLJqasm7ZMnB6cp6A4Y6eZ/HXctECzopRclK
VbcxXHawH2z7qrGRdb/f0DMWT5bybMod7EV23gm+DeA7PBcgf8XHaC+qsP6tj/tY
9zdFZ7xJ27QatuA+8XF80ByLT4pmj4fmpp7rRIgWAWJVZLfEiwIDAQABozEWLzAJ
BgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIHgDAPBgNVHREECDAGhwQK3rLxMA0G
CSqGSIB3DQEBcwAA4IBAQCIEBkeI636KVALPAANut74GQsExwNVaWpQYKQG098d
LkPClmgT8aJDva5bbnCRP8Y91TFWbVANkkoiC1VRsvtBrtk9viLSJKujHtmC6J8c
pCLdPF/n+77dbPmkKqFpWOZVWZGbxx9vfnsG4DZ7219BOlyldBVWuHuEuNGT1Pyt
Qn6gOC33KVacvqKZYAoPeUCER3oFL8yyNYgrAFDE61WUFM3PHzlAfXwc7/eQ87Hu
v9dLX5AQGYuzjGPfcvnC1Rw2M916jviC/KdK6uwTaazF/ebMh6gL/4hvfwWC1930
pwIRAS5/z9szTYaiIA1wwJuciWoC1wTcd+mdML4c4e5

-----END CERTIFICATE-----

Download

Back

Figure 45 : Certificate Information

- Go to HPE StoreOnce Management Console, navigate **StoreOnce>Settings>Key Manager>Actions** and click on **Enroll**.

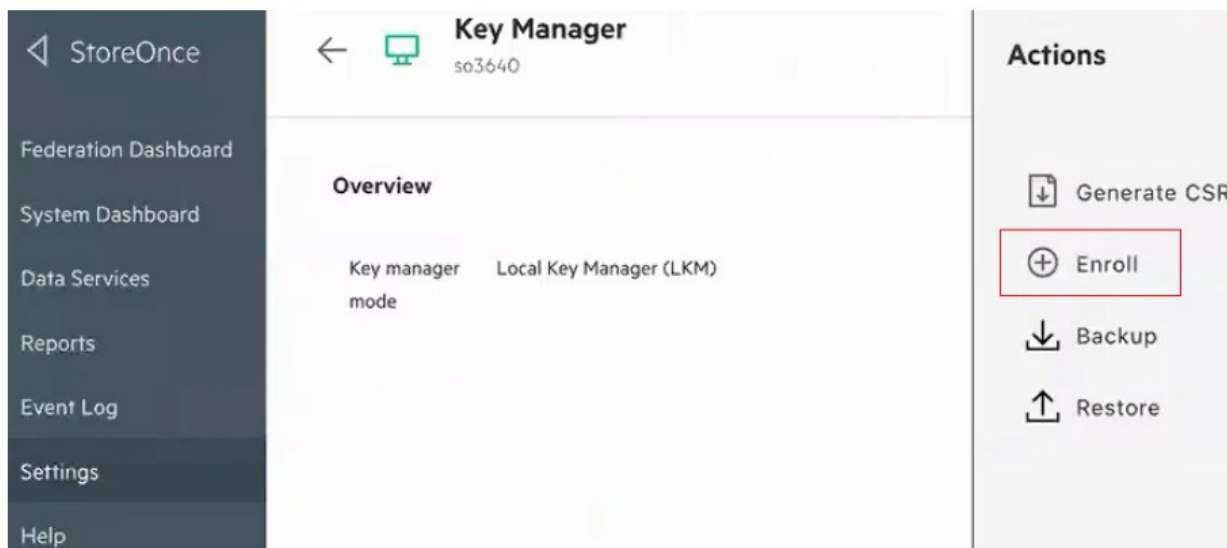


Figure 46 : Key Manager - Enroll



Figure 47 : Backup Configuration

- To backup the local configuration, create a password and confirm it and click **Backup**.



The backup of local configuration is important if the local key management configuration mode has to be switched back or unenroll from the key manager.

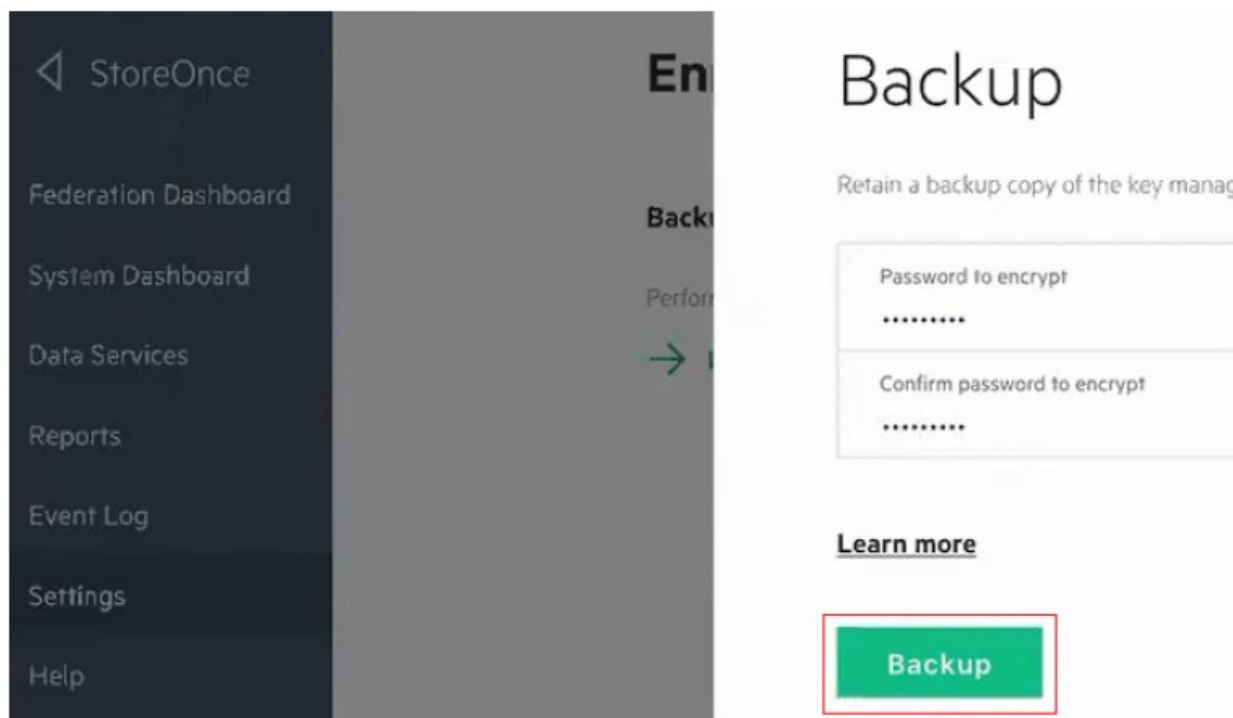


Figure 48 : Backup

- Download the backup file and save it onto the local machine.
- To configure the external key manager server, click on **Configure External Key Manger Server**. A pop-up window will be displayed. Select the “ESKM” as option and enter the IP address, CA name, Port, EKM username, EKM password, and click **OK**. The ESKM is now registered.



Figure 49 : Configure External Key Manager Server

Configure External Key Manager Server

Provide information needed by External Key Manager server.

☒ ESKM ☐ SafeNet

IP addresses
10.14.14.100 ESKM IP address

Certificate authority name
ESKMCA ESKM CA name

Port
5696

EKM Username
registration

EKM Password
.....

[Learn more](#)

OK

Figure 50 : Configure External Key Manager server

4.3.4.1 Importing Root Certificate

1. To import the root certificate, click on "Import Root Certificate" and a popup window will be displayed. Go to ESKM and navigate to **Security>Certificates and CAs>Local CAs**. Select the CA name and click on it. In the "CA Certificate Information" page copy the certificate from `----- BEGIN CERTIFICATE -----` to `-----END CERTIFICATE -----` lines.
2. Go to StoreOnce Management Console and paste the certificate from `--- --BEGIN CERTIFICATE -----` to `-----END CERTIFICATE -----` lines into "Import Root Certificate" pane. Click OK. The root certificate is now provided.

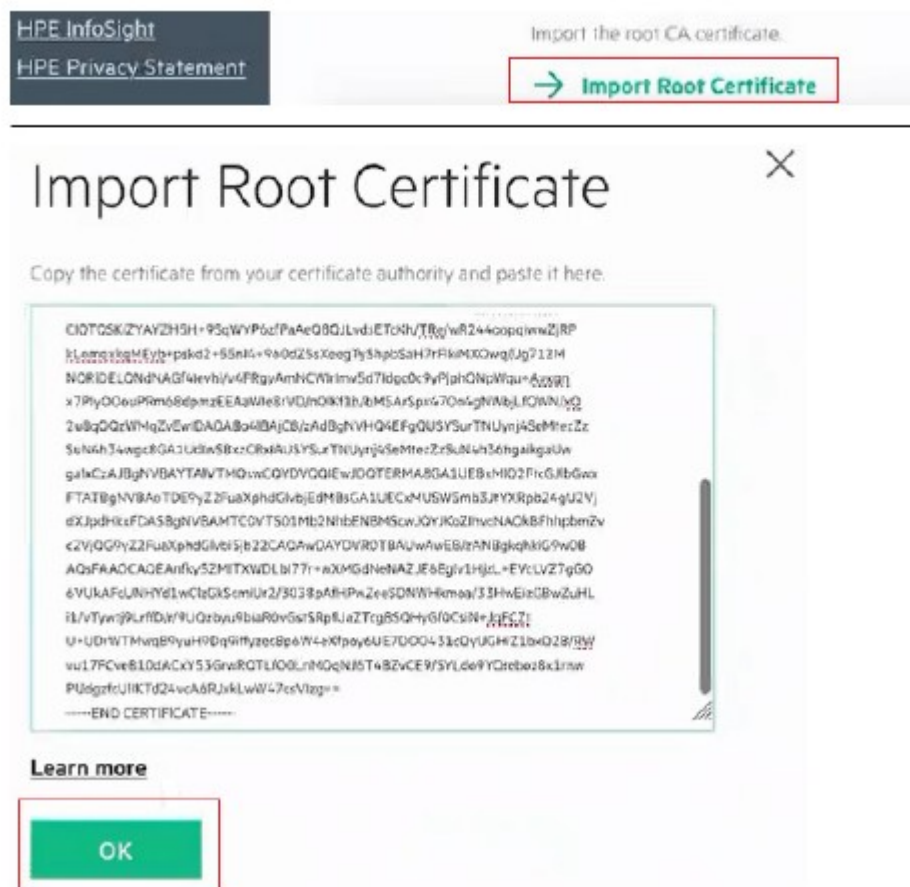


Figure 51 : Import root certificate

4.3.4.2 Importing Signed Certificate

1. To import the root certificate, click on "Import Signed Certificate" and a pop-up window will be displayed. Go to ESKM and navigate to **Security>Certificates and CAs>Local CAs** and click on **Show Signed Certs**. Click on the appropriate signed certificate. In this case it is the one with the name "registration". In the "Signed Certificate Information" page copy the certificate from `-----BEGIN CERTIFICATE ----- to -----END CERTIFICATE -----` lines.
2. Go to StoreOnce Management Console and paste the certificate from `--- --BEGIN CERTIFICATE ----- to -----END CERTIFICATE -----` lines into "Import Signed Certificate" pane. Click **OK**. The signed certificate is now provided.

[HPE InfoSight](#)
[HPE Privacy Statement](#)

Import the signed certificate from the certificate authority
→ **Import Signed Certificate**

Import Signed Certificate

Copy the signed certificate from your certificate authority and paste it here

```

LnHvbtAefW0yMDA0NjcyMzI5MjhaFw0zMDA0MjUyMzI5MjhaMF8xZAAJBgnVBAYT
AIVTMQswCQYDVQIQIDAJNzEQAQMGAJUEBwwHQW5kb3ZlcjELMAkGAJUECgwCSFAk
DTALBgNVBAAsMBEhQUJ3AFTATBghNVBAMMDHJlZ2dHJndGxvbjCCAStwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALW5n6W+Jsl9npdo2esTQ++Ju6rgeXndk4o1
KwD2NkmEI TO38va0WVvYmgupK5vF4NkgVNeCQNm6mGWdgGdXo7Qyo2OHagfLuwPc
h88yJlQ/12B7b21y29eD8pLLOmfUj33HIE/AE2Rhoq1X10zW0ysBqggHMDqj3Rem
cHd3NOR3ooMFLdelfqOL84GRTrll7fOhNC3Te6Zadcef4hD1J8XingoDAyoGeyaaQ
QCvFulHiet9ujcNydvltemU9agGn3IS6KsEcnL80ZwlvjgDbbw5oXY08gUJ
IFq1O0d3jH1HOail58n8VRLahNW5U+ggfheB/inHUxiz6uj5JMsCAwEAkAMgMBAw
CQYDVROTBAlwADARBgJghkgBhvHCAQEEBAMCB4AwDQYJKoZIhvcNAQELBQADggEB
AKAjt7q1XOX/SX7K0H/xXpXE7RM8V8EtoBFR84y5Pmwn0NjFkDrcChmLuhk2OO
HR2/7m9nExSnCqUkEYXabfshQIFgZwJf7MA/bALw+T46W4ArCelt5mDxKDS3Gh
AK7+6LI+moobHPGcAV5bcGnsZDpaIDVMPqawL0cXChbHOPEXm4JFcF3OO1cSEG
lHf029UJne00+He2Gyc2i5Vxe7veVtsVdBCXyWwHyyNLwTYRM05vaB7p8xxNGj
JC67xFeVCoKUM3uyVDpck43XGf0SXyorl++Tu7XjbmIM97TMOlghWCMY2Hj3O
cKFjDKMYeL3IYDCtGMEaZe8=
-----END CERTIFICATE-----

```

[Learn more](#)

OK

Figure 52 : Import signed certificate

4.3.5 Enrolling the StoreOnce

Once all the information related to backup key manager configuration, external key manager, root certificate authority, and signed certificate click on **Enroll**.



In case there are any failed integrations, please make sure to delete all the entries related to failed integration from the ESKM.

Enroll

×

Backup the key manager configuration

Perform a backup of the key manager configuration.

Key Manager Configuration Backup

The backup action has completed

Configure External Key Manager Server

This information is required for importing certificates and enrolling with the External Key Manager server.

Server type

ESKM

Root Certificate Authority

Import the root CA certificate.

Certificate Authority root certificate

Root certificate was provided

Signed Certificate

Import the signed certificate from the certificate authority.

Signed certificate

Signed certificate was provided

Enroll

Figure 53 : Enrolling StoreOnce

The screenshot displays the StoreOnce management interface. On the left is a dark sidebar with navigation links: StoreOnce, Federation Dashboard, System Dashboard, Data Services, Reports, Event Log, Settings, Help, and a user profile icon. The main content area is divided into two sections: Overview and Certificates. The Overview section shows key manager details: mode (External Key Manager (EKM)), type (ESKM), and IP addresses (10.14.14.100). The Certificates section lists two certificates, each with a green status dot, a label, and a valid until date. On the right, an Actions panel contains icons and labels for Generate CSR, Edit EKM settings, Renew certificates, Backup, Restore, and Withdraw.

Overview	
Key manager mode	External Key Manager (EKM)
Key manager type	ESKM
Key manager IP addresses	10.14.14.100

Certificates	
Certification Authority	valid until Apr 25, 2030 2:27:05 pm
storeonce-CZ28120HZB	valid until Apr 24, 2030 4:37:18 pm

Actions	
	Generate CSR
	Edit EKM settings
	Renew certificates
	Backup
	Restore
	Withdraw

Figure 54 : Enrolling StoreOnce

With this, the HPE StoreOnce is now integrated with the ESKM.

5 Accessing Serial Console via PuTTY

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

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

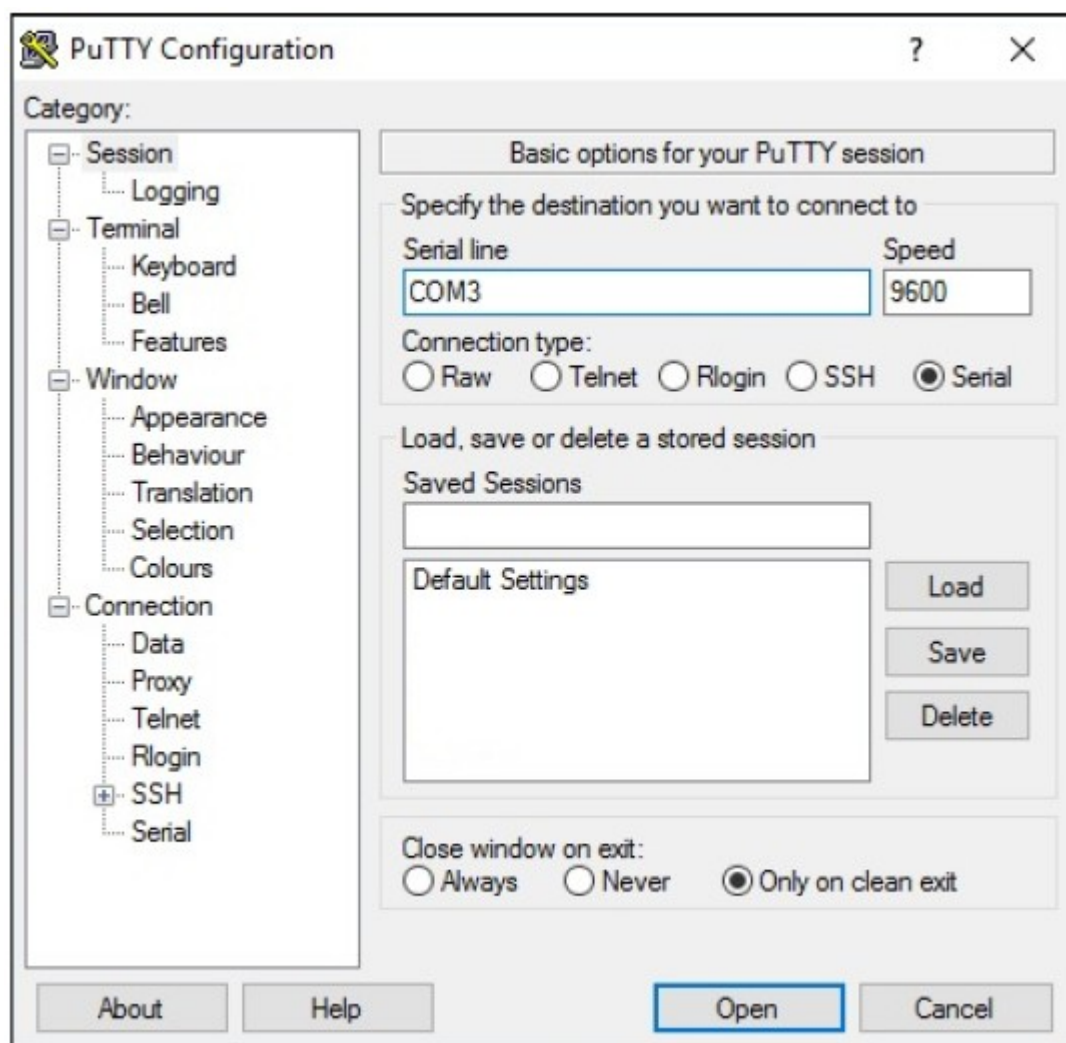


Figure 55 : PuTTY configuration

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

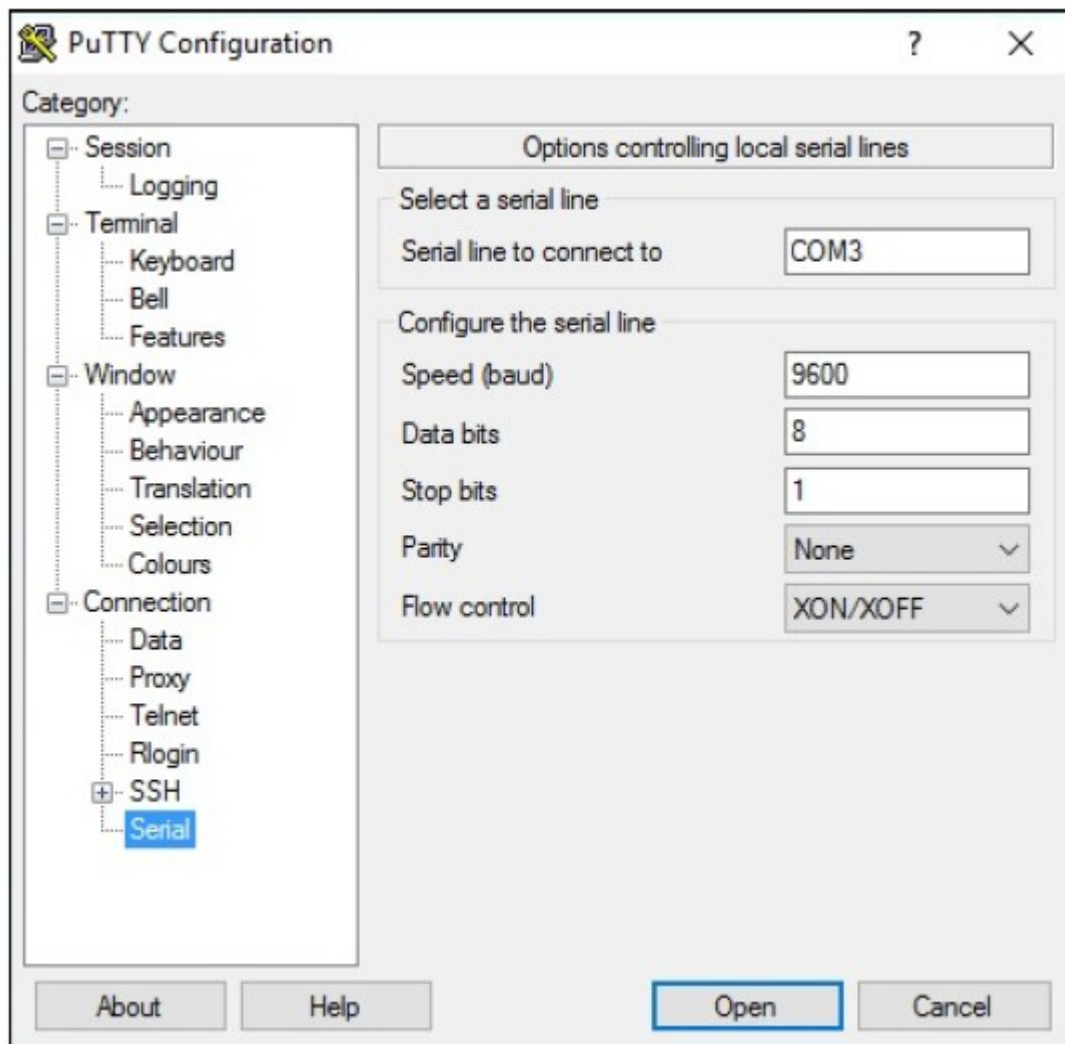


Figure 56 : Edit Serial Line

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

6 Contact and Support Information

6.1 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com^[3]
- 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

6.2 24-hour support

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

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