HPE

Alletra Storage

B10000

Integration Guide

ESKM

8.54.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.1
Date	2026-02-11
Status	PUBLISHED
Document No.	IG-2025-0067

Table of Contents

1 Introduction

1.1 About This Guide

This document serves as a technical reference for implementing external key management on HPE Alletra Storage B10000 using Utimaco ESKM. It explains the integration architecture, required components, configuration workflows, certificate, and KMIP settings, as well as post-integration validation steps.

1.2 Target Audience

This guide is intended for HPE Alletra B10000 and Utimaco ESKM administrators.

1.3 Purpose of the Integration

The purpose of integrating Utimaco ESKM with HPE Alletra Storage MP B10000 is to provide secure, centralized, and standards-based external key management for the array's self-encrypting drive (SED) data-at-rest encryption, ensuring that cryptographic keys are generated, stored, and governed within a hardened, FIPS-compliant KMIP platform rather than on the array itself. This integration enhances security, strengthens compliance, and enables consistent lifecycle control of encryption keys across enterprise environments.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
EKM	External Key Management

Abbreviation	Meaning
KMIP	Key Management Interoperability Protocol
FQDN	Fully Qualified Domain Name
VM	Virtual Machine
GUI	Graphical User Interface
SED	Self-Encrypting Drive
CSR	Certificate Signing Request
CA	Certificate Authority
IP	Internet Protocol
CN	Common Name
FIPS	Federal Information Processing Standards

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **ADD**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 2: Document Conventions

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

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

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

2 Product Overview

2.1 Overview of the Alletra Storage B10000

The HPE Alletra Storage MP B10000 is a mission-critical, cloud-managed, disaggregated storage platform built for ultra-low latency, extreme resiliency, and 100% data availability for enterprise workloads. It features a massively parallel, all-active architecture that enables linear scalability across compute and storage resources, allowing performance and capacity to scale independently without disruption. Designed for hybrid cloud operations and managed through HPE GreenLake, it offers AI-driven insights, simplified provisioning, and automated lifecycle management. The B10000 is optimized for high-intensity workloads such as large databases, VMs, and next-gen applications, and includes robust data-at-rest encryption, SED support, and strong security integrations.

2.2 Overview of ESKM

ESKM is a centralized key management solution that securely stores, distributes, and manages encryption keys throughout their lifecycle. It supports industry standards, including the KMIP, enabling integration with various enterprise applications and storage systems.

2.3 Joint Value Proposition

The combination of HPE Alletra Storage MP B10000 and Utimaco Enterprise Secure Key Manager (ESKM) delivers a powerful, end-to-end solution for organizations that require mission-critical performance and uncompromising data security. HPE Alletra B10000 provides a highly resilient, cloud-managed, all-active storage platform with ultra-low latency, linear scalability, and a 100% data-availability guarantee, while Utimaco ESKM adds centralized, standards-based KMIP key management with strong policy controls, high availability, and FIPS-compliant security. Together, they ensure that self-encrypting drives and data-at-rest encryption are managed with maximum reliability, auditability, and compliance. Gives enterprises unified key lifecycle management, protection against data breaches, simplified operations, and a future-ready security architecture across hybrid cloud environments.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	HPE Alletra Storage	Utimaco ESKM Version
Windows 10	B10000	8.54.0

Table 3: Tested versions

3.2 Hardware and Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.0
HPE Alletra Storage	B10000

Table 4: Hardware and software requirements

3.3 Prerequisites

1. Utimaco ESKM version 8.54.0 or later.
2. Admin access to Utimaco ESKM.
3. Data-at-Rest Encryption license for Alletra Storage B10000.

4 Installation and Configuration

The following section outlines the procedures required to set up and configure ESKM and Alletra Storage B10000.

4.1 Setting Up ESKM

The initial phase involves configuring the ESKM before proceeding to Alletra Storage B10000. For detailed configuration steps, refer to the *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to the ESKM.

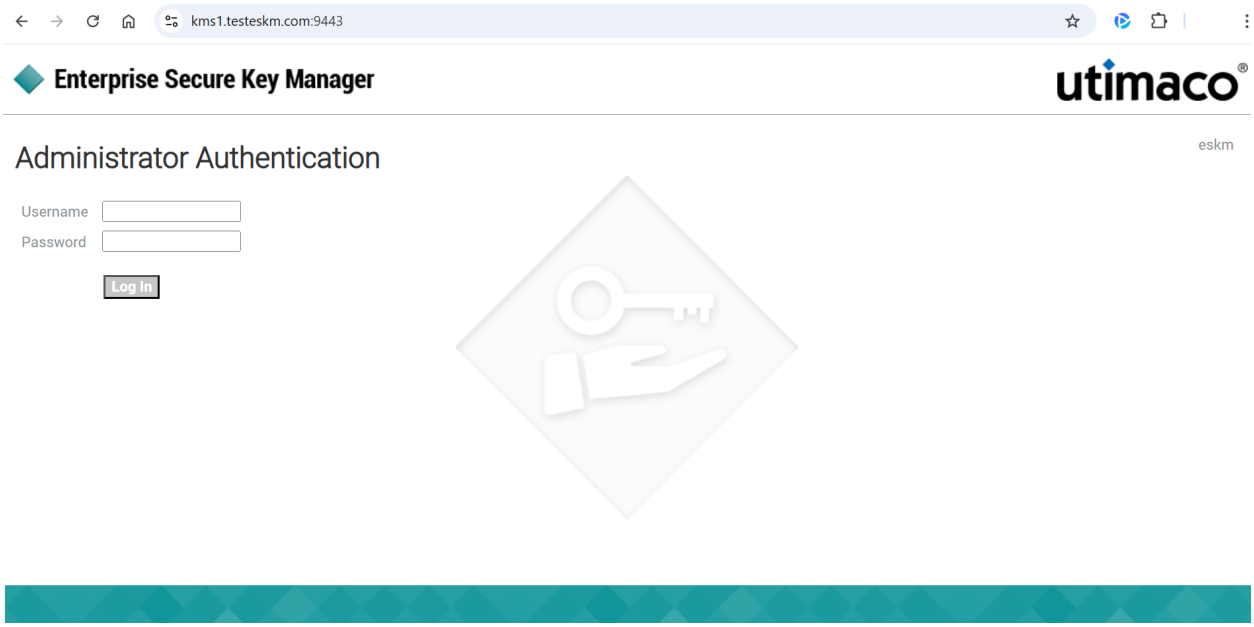


Figure 1 : ESKM login page

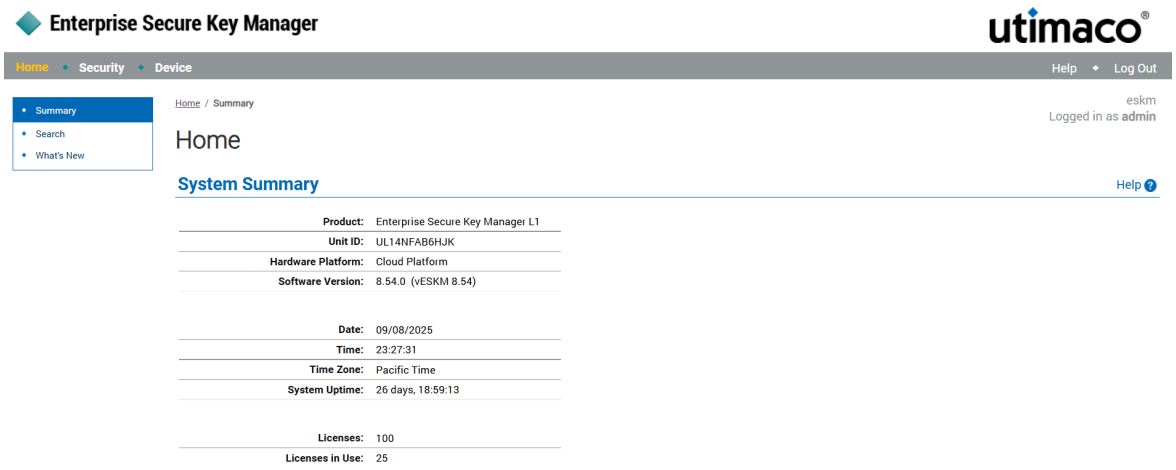


Figure 2 : ESKM home page

4.2 Setting Up Alletra Storage B10000

1. Install and set up Alletra Storage B10000. Please refer to *HPE Alletra Storage MP B10000: Planning and preparing the hardware and software* and *Installation Overview | HPE Alletra Storage MP B10000 – Parts Support Guide* for more details.

2. Log in to Alletra Storage B10000.

Figure 3 : Alletra Storage B10000 login

5 Integration Steps

5.1 Configuration on Utimaco ESKM

It is essential to configure the Utimaco ESKM to ensure secure and efficient key management. This section guides you through the necessary steps to configure ESKM for HPE Alletra Storage B10000.

5.1.1 Create a Local CA

The local CA signs and verifies the server certificate and may also sign client certificate requests. Follow these steps to create and install a local CA.

1. Go to the **Security** tab.
2. Click on the **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Create Certificate** section.
4. Enter a **Certificate Authority Name** and a **Common Name**. These may have the same value, such as ESKMLocalCA.
5. Enter your **Organizational information**.
6. Select the **Algorithm** (for example, RSA-2048).
7. Select **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.
8. Click on **Create**.

Figure 4 : Create Local CA

5.1.2 Create a Server Certificate

You must create an ESKM certificate to enable secure communication between Partner Product and the ESKM.

To create an ESKM server certificate, perform the following steps:

1. In the **ESKM Management** console, go to **Security** > **Certificates and CAs** and click **Certificates**.
2. Enter **Certificate Name**, **Country Name**, **State or Province Name**, **Locality Name**, **Organization Name,** and **Organizational Unit Name**.
3. Select **RSA-2048** from the **Algorithm** dropdown list.
4. Select the previously created CA certificate name from the **Local CA** dropdown list.
5. Select **Server** from the **Certificate Purpose** dropdown list.
6. Click **Create**.

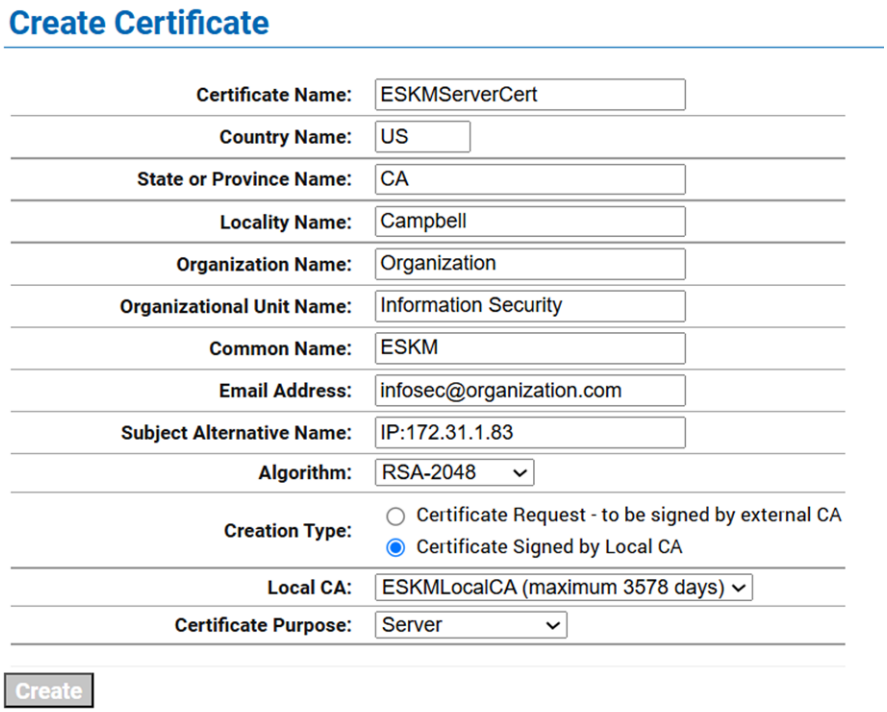


Figure 5 : Create Certificate

5.1.3 Configure the KMIP Server

1. In the **ESKM Management** console, go to **Device** > **KMIP Server** > **KMIP Server**.
2. Click the **Edit** button under the **KMIP Server Settings** section.
3. Select the relevant KMIP Port.
4. Select the created server certificate as the **Server Certificate** for the KMIP server.
5. Select the created Local CA from the dropdown list.

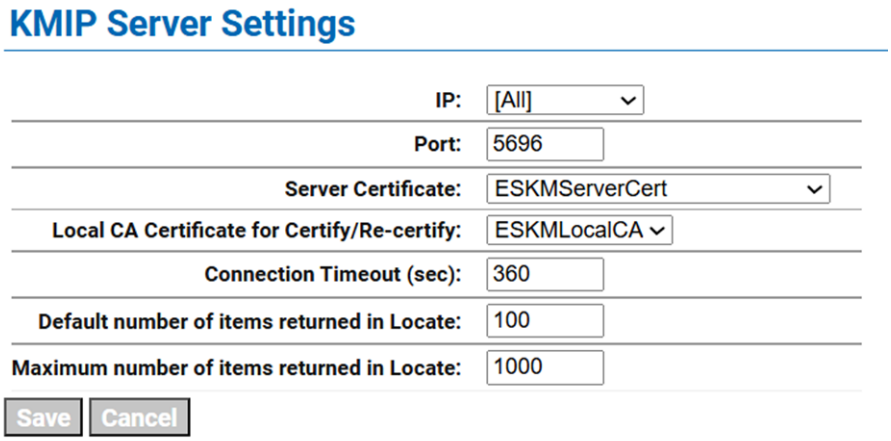


Figure 6 : KMIP server configuration

5. Click **Save**.
6. Click **Edit** under the **KMIP Server Configuration Settings** section.
7. Select the **enable** radio button in the **Certification Authentication** section and select a CA profile from the **Trusted CA List Profile** dropdown.

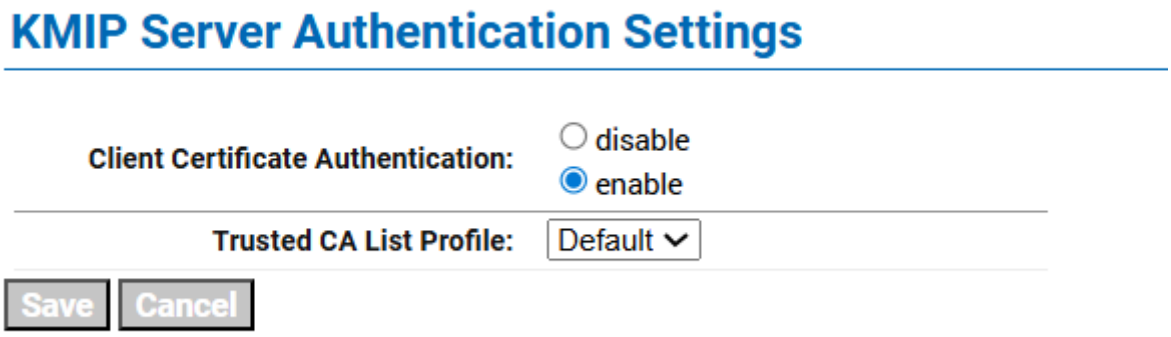


Figure 7 : Enable client certification authentication

8. Click **Save**.

5.1.4 Create a KMIP User Group

1. Click **Security** > **Local Users & Groups** > **Local Groups**.

2. Click the **Add** button in the **Local Groups** section.
3. Enter a group name (AlletraGroup in our example).
4. Select KMIP from the Group Type drop-down box.

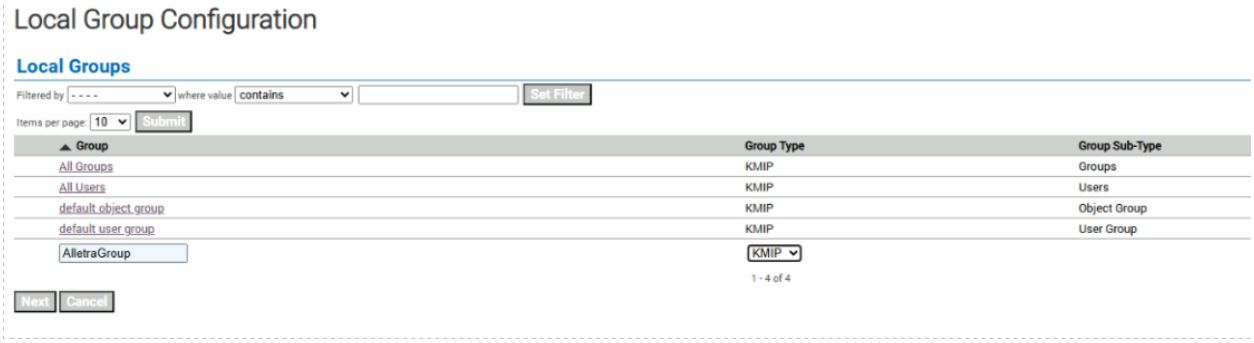


Figure 8 : Create a KMIP group

5. Click **Next**.

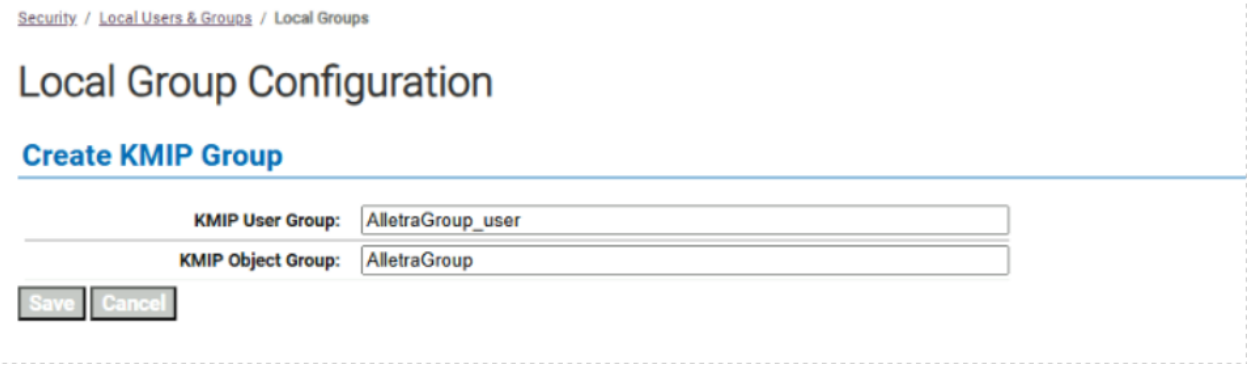


Figure 9 : KMIP user group and object group created

6. Click **Save**.

The new KMIP group pair, consisting of a KMIP user group named AlletraGroup_user and a KMIP object group named AlletraGroup, will be created. By default, all users who are members of the KMIP user group AlletraGroup_user will have permission to

perform all KMIP operations on the KMIP object group AlletraGroup. Refer to the ESKM User Guide for more information on KMIP user and object groups and permissions, and how to fine-tune permissions for KMIP users.

5.1.4.1 Sign the Host Certificate using ESKM

1. Copy the generated CSR from Partner Product and submit it to the ESKM for signing by the ESKMLocalCA as a client certificate.
2. Go to **ESKM Management Console** > **Security** > **Certificates & CAs > Local CAs**.

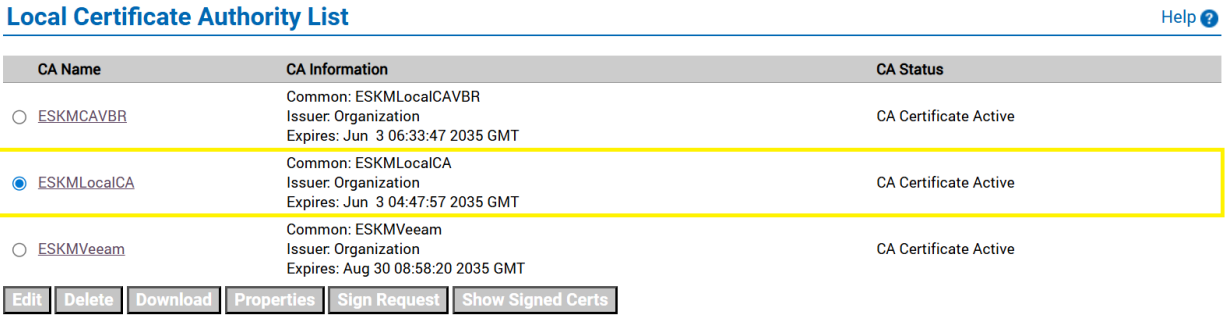


Figure 10 : Local CA

3. Select the created **CA** and click **Sign Request**.

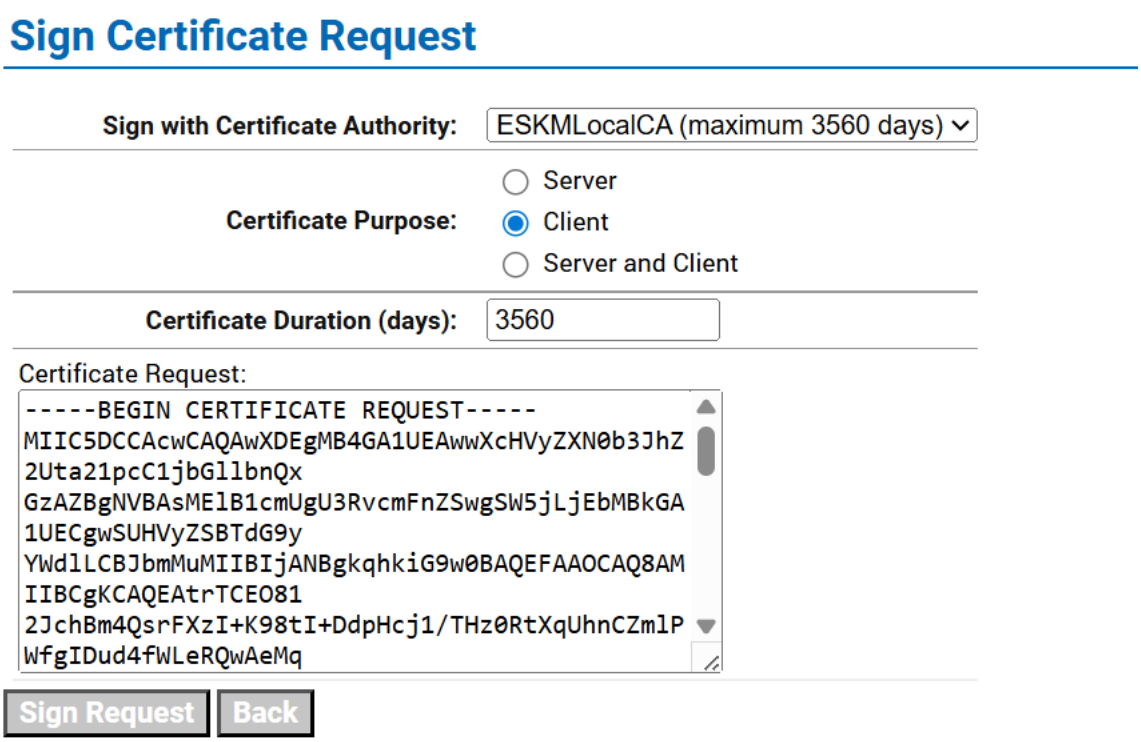
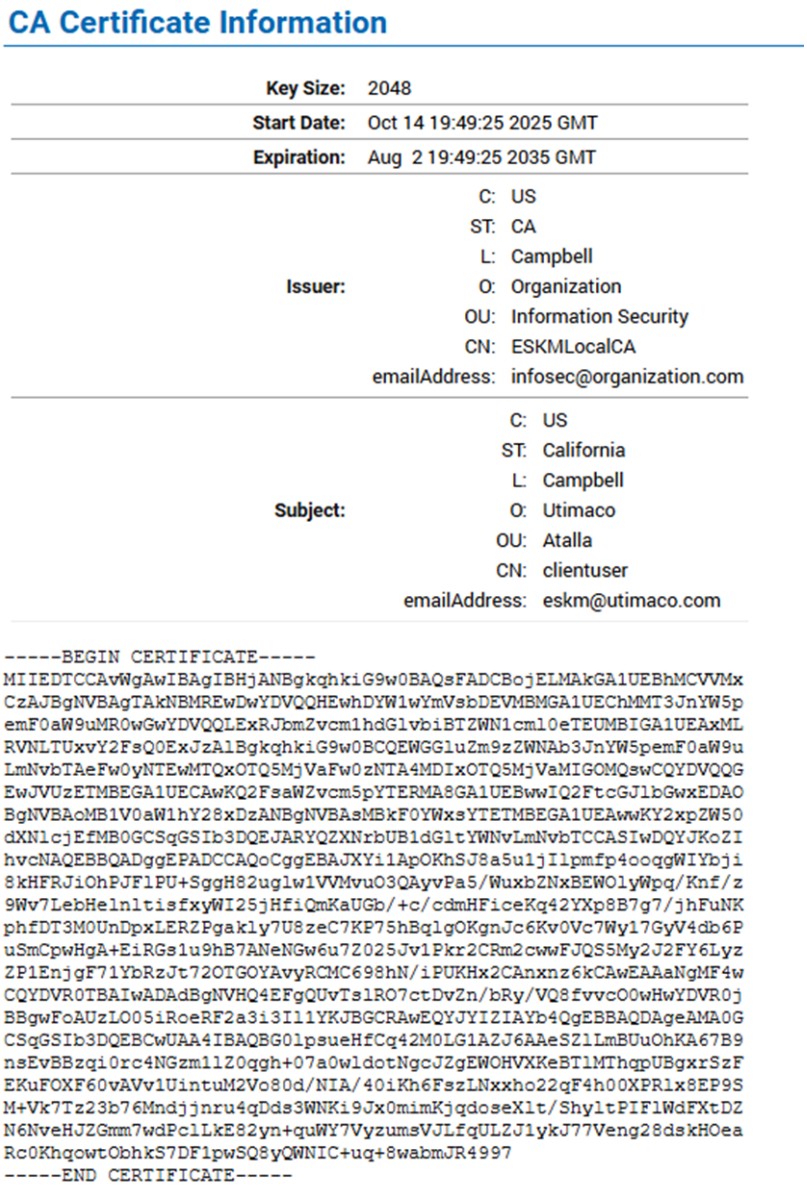


Figure 11 : Sign certificate request

4. Select the previously created CA certificate name from the **Sign with Certificate Authority** dropdown list.
5. Select **Client** in the **Certificate Purpose** section.
6. Copy the host certificate content to the **Certificate Request** box and click **Sign Request**.



CA Certificate Information

Key Size:	2048
Start Date:	Oct 14 19:49:25 2025 GMT
Expiration:	Aug 2 19:49:25 2035 GMT
Issuer:	C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization.com
Subject:	C: US ST: California L: Campbell O: Utimaco OU: Atalla CN: clientuser emailAddress: eskm@utimaco.com

```
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIBHjANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTEwMTQxOTQ5MjVaFw0zNTA4MDIxOTQ5MjVaMIGOMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwIQ2FtcGJlbGwxEDAO
BgNVBAoMB1V0aW1hY28xDzANBgNVBAsMBkF0YWxsYTETMBEGA1UEAwwKY2xpZW50
dXNlcjEfMB0GCSqGSIb3DQEJARYQZXNrbUB1dGltYWNvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJXYi1ApOKhSJ8a5u1jIlpmfp4ooqgWIYbji
8kHFRJiOhPJFlPU+SggH82ug1w1VVMvuO3QAyvPa5/WuxbZNxBEWOlyWpq/Knf/z
9Wv7LebHelnltisfxyWI25jHfiQmKaUGb/+c/cdmHFiceKq42YXp8B7g7/jhFuNK
phfDT3M0UnDpxLERZPgakly7U8zeC7KP75hBqlgOKgnJc6Kv0Vc7Wy17GyV4db6P
uSmCpwHgA+EiRGs1u9hB7ANeNGw6u7Z025Jv1Pkr2CRm2cwwFJQS5My2J2FY6Lyz
ZP1EnjgF71YbRzJt72OTGOYAvyRCMC698hN/iPUKHx2CAnxnz6kCAwEAAaNgMF4w
CQYDVR0TBAIwADAdBgNVHQ4EFgQUvTslRO7ctDvZn/bRy/VQ8fvvcO0wHwYDVR0j
BBgwFoAUzLO05iRoeRF2a3i3Il1YKJBGCRAwEQYJYIZIAYb4QgEBBAQDAgeAMA0G
CSqGSIb3DQEBCwUAA4IBAQBG0lpsueHfCq42M0LG1AZJ6AAeSZlLmBUuOhKA67B9
nsEvBBzqi0rc4NGzm1lZ0qgh+07a0wldotNgcJZgEWOHVXKeBTlMThqpUBgxrSzF
EKuFOXF60vAVv1UintuM2Vo80d/NIA/40iKh6FszLNxxho22qF4h00XPRlx8EP9S
M+Vk7Tz23b76Mndjjnru4qDds3WNKi9Jx0mimKjqdoseXlt/ShyltPIFlWdFXtDZ
N6NveHJZGmm7wdPclLkE82yn+quWY7VyzumsVJLfqULZJ1ykJ77Veng28dskHOea
Rc0KhqowtObhkS7DF1pwSQ8yQWNIC+uq+8wabmJR4997
-----END CERTIFICATE-----
```

Figure 12 : Signed certificate information

7. Copy the signed certificate and paste it into a notepad.
8. Click **ESKMLocalCA** from **Local CAs**, copy the ESKMLocalCA certificate, and paste it into a notepad.

CA Certificate Information

CA Certificate Name:	ESKMLocalCA
Key Size:	2048
Start Date:	Aug 4 00:48:44 2025 GMT
Expiration:	Aug 3 00:48:44 2035 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: ESKMLocalCA emailAddress: infosec@organization.com


```
-----BEGIN CERTIFICATE-----
MIIEFDCCAvygAwIBAgIBADANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTA4MDQwMDQ4NDRaFw0zNTA4MDMwMDQ4NDRaMIGiMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxP
cmdhbml6YXRpb24xHTAbBgNVBAsTFEluZm9ybWF0aW9uIFN1Y3VyaXR5MRQwEgYD
VQQDEwtFU0tNTG9jYWxDQTEnMCUGCSqGSIb3DQEJARYYaW5mb3N1Y0Bvcmdhbml6
YXRpb24uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAySb/YPWh
aQEKFdmXjwlUk32swOqjk+dBMb9meLOoI2kKQjX3+DzE2uSCX/DDL46dBwe7y30D
IdwmKlBm/xSWgplrmludmmnyJhOj4MiQOSv5PIoymGlaAYNaqBlxb0FFdlxp4wdP
ME4827hiUqZ46zZ72XclDD4ToSU28EW0MaM6vbt128Q/n+PZu2897iOp/cuxwgll
qufbRAptJXCJxeNLPudhDQlLaXxgKPcZtPaxEV394bVM9MKvOzyztJFgzElAaiDy
9q4xwgswagA8MJmXkHohmUsCnFaQKyesbsObo+sDNWWYDOxsavzE6cxq+pDH5K1k
o3QqN/0Z8Y9PEwIDAQABo1MwUTAdBgNVHQ4EFgQUzLO05iRoeRF2a3i3I11YKJBG
CRAwHwYDVR0jBBgwFoAUzLO05iRoeRF2a3i3I11YKJBGCRAwDwYDVR0TAQH/BAUw
AwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAFTOVHxQstxbKQqE6qAy262vFC034tqKP
4UhbezC2r+vD+ZGmxt09z3UvgGnjEBhVkyuZKBk6KkoaaFl1YcMbfWZbUoJvG5ee
VikFCZJSfsO2AH5hVRdGWhlPPBZ/0+j0qyl0rJOnjbRMo1Pkz+JAmylf0G6cPWed
5EcuWZXUgF4uxz+m2PQWy+4n3KsX7mmDWEWmyWVpJN0pBdQ7PhCAkyS39tWuhrQl
cgnS53HUhpvoz49J1Vd4s2RKflDIUQ3ocV9XbMbM7df2zxbEJ1n+hhggThLL3i64
x83t/00THhjn12UvuSHBtg3PyltH04ZVoHuIRUGIpPOu9MsdtAH/sg==
-----END CERTIFICATE-----
```


Figure 13 : CA certificate information

5.1.5 Create a KMIP User

1. In the **ESKM Management console**, go to **Security** > **Users & Groups** > **Local Users & Groups** > **Local Users**.
2. Click **Add**.
3. Enter the **Username** exactly as the common name specified while creating the host certificate.
4. Select **Enable KMIP**.
5. Select **KMIP** as **License Type**.
6. Select the user group and object group created for the Alletra user from the **KMIP User Group** and **KMIP Object Group** dropdown.
7. Provide the client certificate in the KMIP Client Certificate that is produced by signing the CSR with ESKMLocalCA.

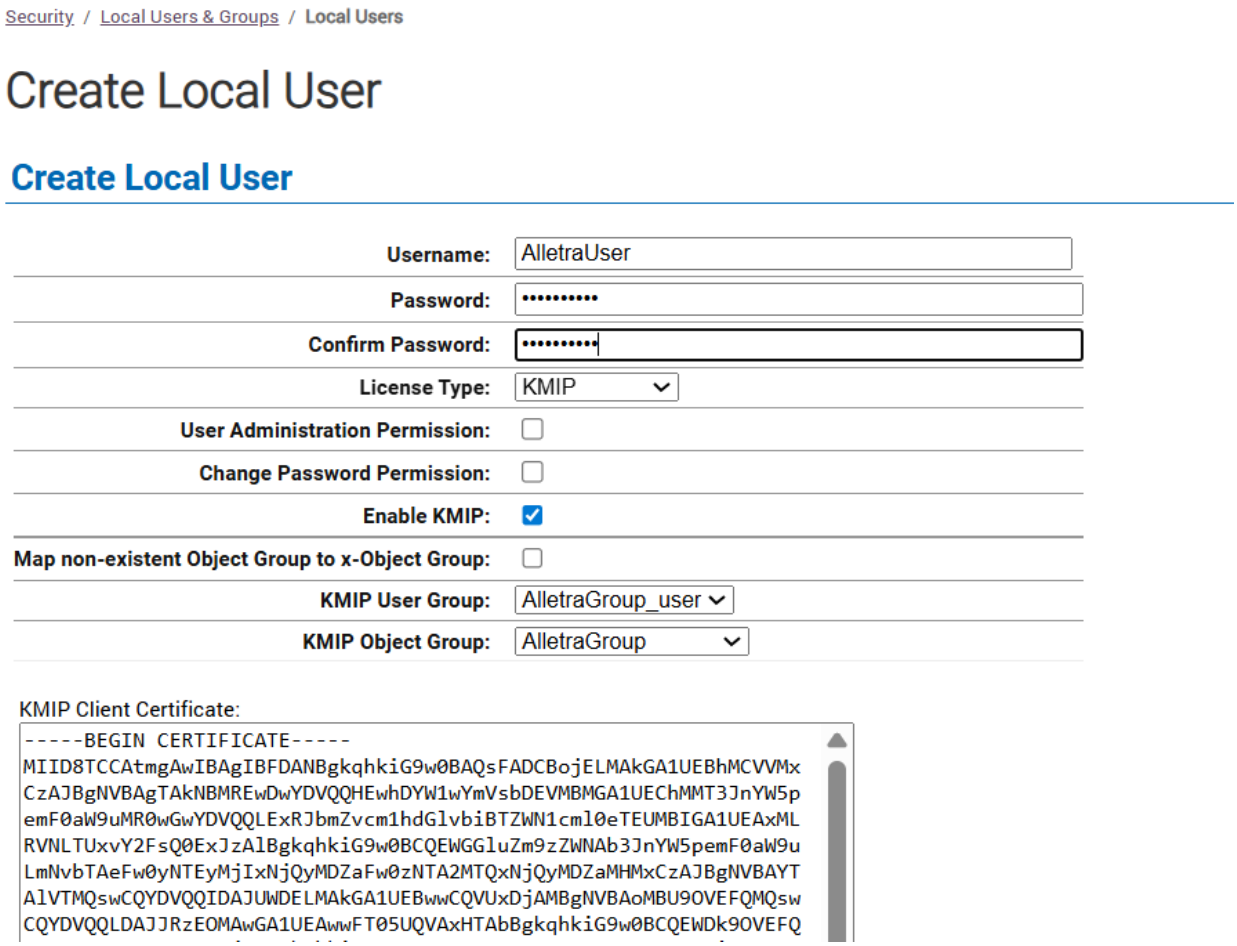


Figure 14 : Create a KMIP user

5.2 Configuration on Alletra Storage B10000

5.2.1 Create a CSR for KMIP User and Sign Using ESKM

1. Click **Settings** > **Array Certificates**.
2. Click on the + symbol at the top right of the screen and select **Create a certificate signing request**.
3. Choose ekm-client in the drop-down for the **Array service**.
4. Fill out CSR details.

You must use the certificate's Common Name (CN) as the KMIP username when creating the KMIP user.

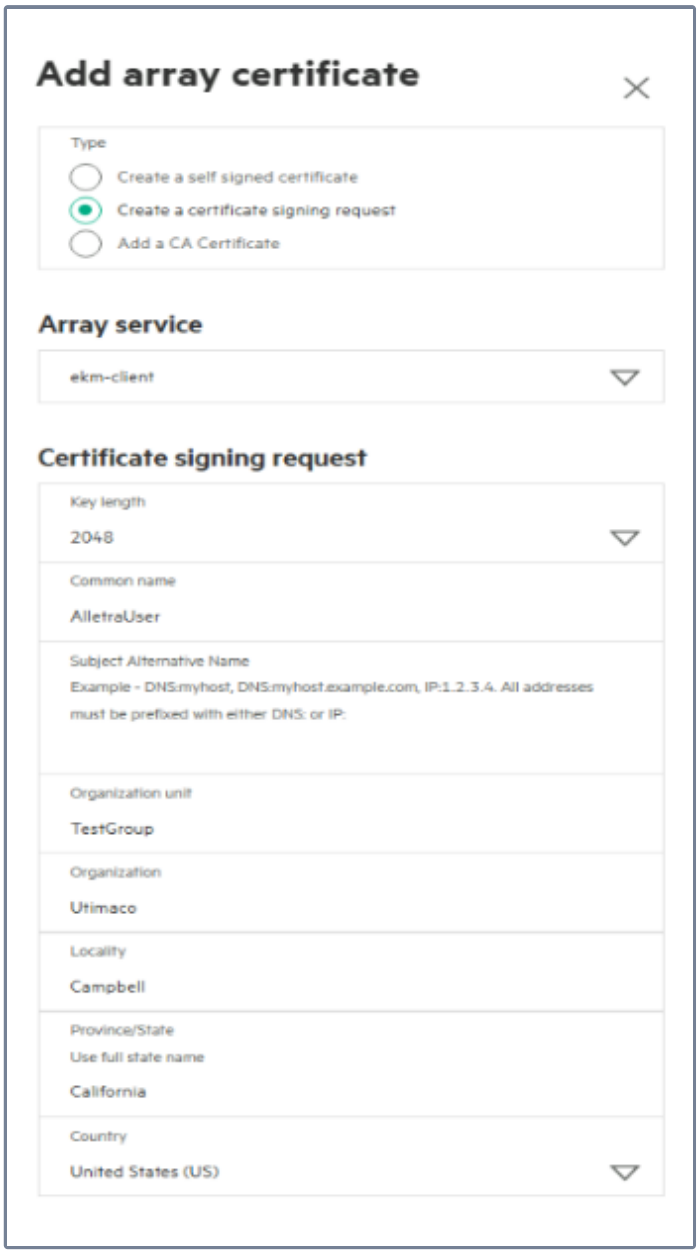


Figure 15 : Create a CSR

5. After the CSR is generated, the GUI will bring you back to the **Array Certificates** window, and click the newly created signing request.

6. Copy the CSR from ----- BEGIN CERTIFICATE REQUEST----- to the end of -----END CERTIFICATE REQUEST----.
7. Please refer to section *Sign the Host Certificate using ESKM* to sign the CSR using ESKM.

If you are using a third-party CA, send a CSR request to the CA to sign instead of signing using LocalCA in ESKM.

8. Refer *to Create a KMIP User Group* and *Create a KMIP User*, then create a KMIP User Group and User.

5.2.2 Import Signed Client Certificate

1. Click **Settings > Array Certificates**.
2. Take the ekm-client certificate that was signed and select **Import Signed CSR**.
3. Paste the certificate in the top window titled **'Certificate'**.
4. In the bottom window titled **'Authority Chain'**, paste the Root CA. If there were Issuing CAs, Intermediate CAs involved in the signing of the certificate, they would need to be added as well. The order would be issuing CA at the top, followed by any intermediate CAs, and finally the root CA at the bottom.
5. Click **ADD.**

5.2.3 Configure EKM settings

1. Log into the array UI and go to **Settings > System**.
2. On the **Encryption** panel, check the encryption status. The status must be *LKM Enabled* or *EKM Enabled*. (Local Key Manager/External Key Manager.
3. In the **Encryption** section, choose the 3 dots (…) on the far right side and click **Set EKM Servers**.

Figure 16 : System screen

3. Enter the EKM server IP address(es) or FQDN(s), port information, user name, KMIP versions, and password.

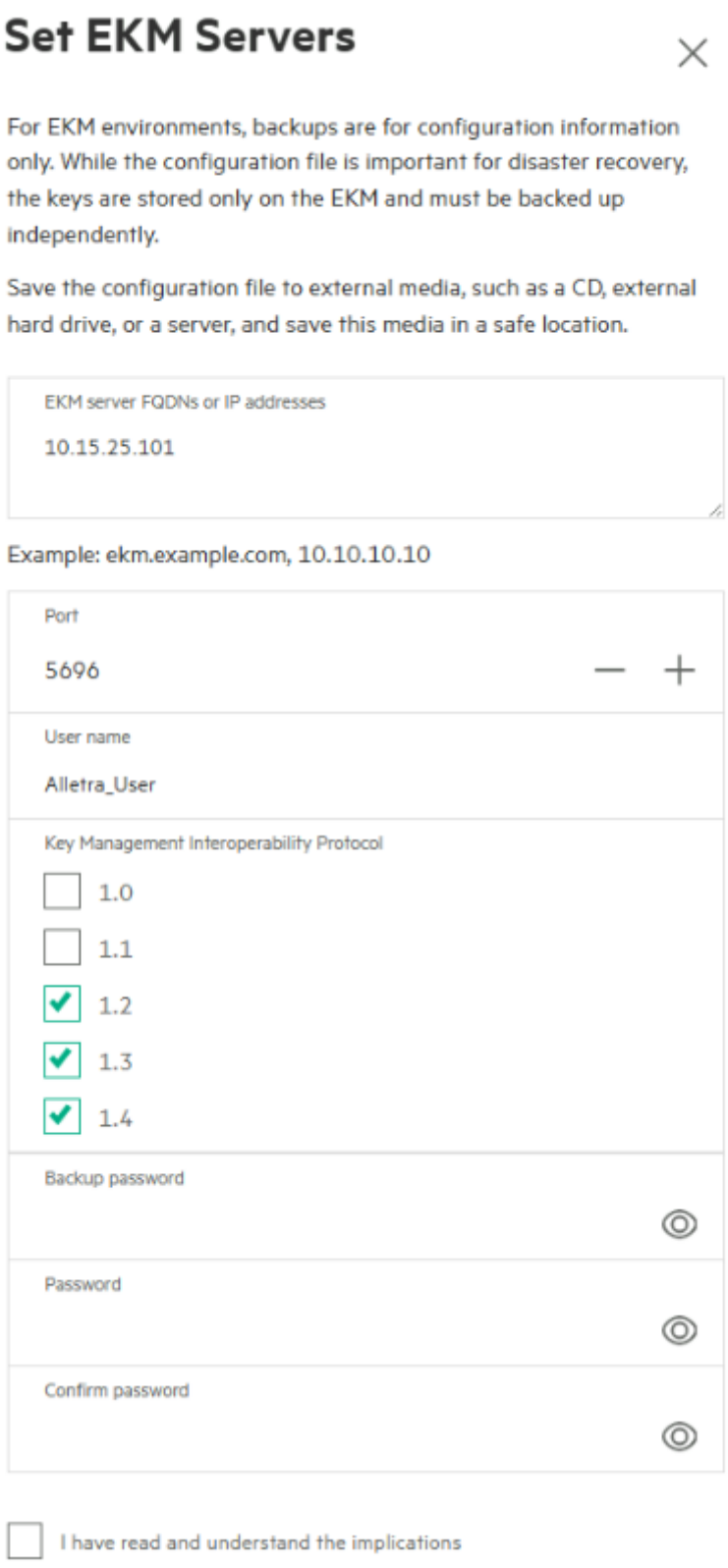


Figure 17 : Set EKM Server screen

4. Click the acknowledgement checkbox and click **Save**.
5. This will return you to the system window. Click the same 3 buttons to the right of the **Encryption** section and click **Check EKM Servers**.

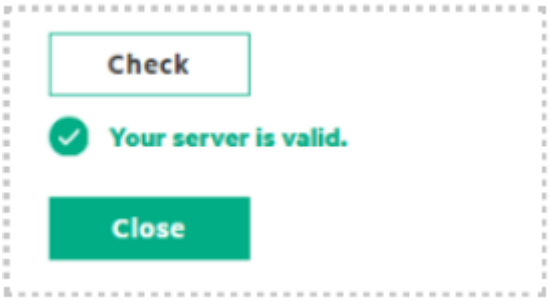


Figure 18 : EKM server validated

6 Verification and Testing

6.1 Enable Array Encryption

1. Choose **Enable** from the **Encryption** menu.
2. Click **External Key Management** (EKM), specify a password for the backup file, select the confirmation box, and click **Configure**. The backup file is downloaded from the array.

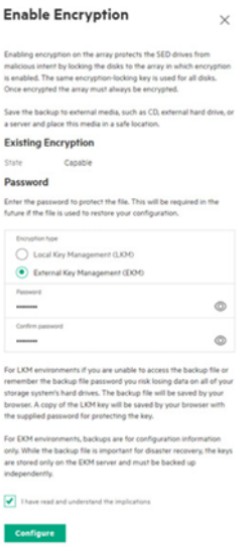


Figure 19 : Enable Encryption

3. Save this backup file to external media and place the media in a safe location.

6.2 Verify ESKM Logs

1. Log in to ESKM and click **Device** → **Logs Statistics** → **Log Viewer ->KMIP**.

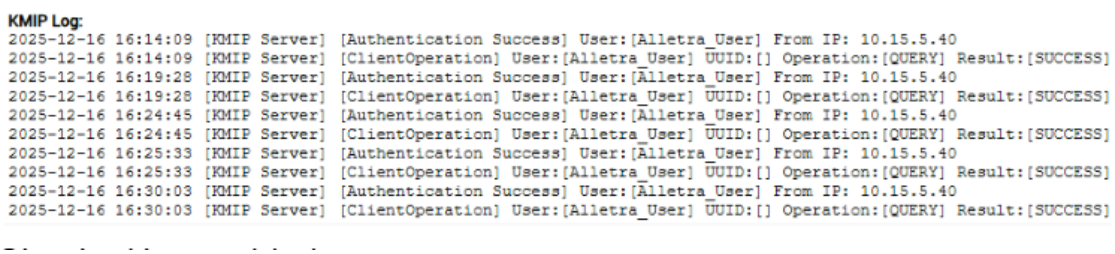


Figure 20 : KMIP logs

6.3 Verify Key Added in ESKM

1. Select Security → Keys & KMIP Objects → Keys → Keys.

Figure 21 : Key details displayed

6.4 Verify KMIP Object

1. Select Security → Keys & KMIP Objects → KMIP Objects → KIMP Objects.

Figure 22 : KMIP object created

7 Troubleshooting

7.1 Common Issues

Issue 1:

Description

Occasionally, when enabling data-at-rest encryption with an External Key Manager for the first time, the system may incorrectly register the encryption configuration using the Local Key Manager (LKM) instead of the selected External Key Manager (EKM). As a result, encryption keys are not sent to the Utimaco ESKM, and no KMIP objects are created.

HPE has acknowledged this behavior and is currently working on a permanent fix.

Official Statement from HPE on the issue

“Occasionally, when enabling data at rest encryption with an external key manager for the first time on a HPE Alletra Storage MP B10000 running 10.5.50, the system may register data at rest encryption using the local key manager. To resolve, check the external key manager settings using the GUI or CLI and re-enable data at rest encryption with the external key manager specified. To verify success, check for a created KMIP object in the Utimaco ESKM GUI.”

Step to Reproduce the Issue

After completing the integration, no keys or KMIP objects appear in the Utimaco ESKM.

Using the Alletra CLI, run the following command to check the encryption configuration:

```
showencryption -d
```

If the output indicates that the keystore is set to LKM, the issue is present.

```
TAC4-Arcus cli% showencryption -d
Licensed Enabled BackupSaved State  SeqNum Keystore FIPS         non-SEDs FailedDisks nodeNonSED
yes      yes     yes         normal      2 LKM      NotCompliant        0           0          0
```

Figure 23 : Issue

Troubleshooting Steps

As part of the integration process, a backup file is created. This backup can be used to re-enable encryption with the correct key manager configuration.

1. Restore or reference the integration backup file created during setup.
2. Re-enable data-at-rest encryption, explicitly selecting the **External Key Manager (EKM)**.
3. Verify the configuration again using the CLI:

```
showencryption -d
```

4. Confirm successful operation by logging into the Utimaco ESKM GUI and verifying that KMIP objects are created and keys are received from the Alletra system.
5. The system correctly uses the External Key Manager and successfully exchanges keys with Utimaco ESKM.

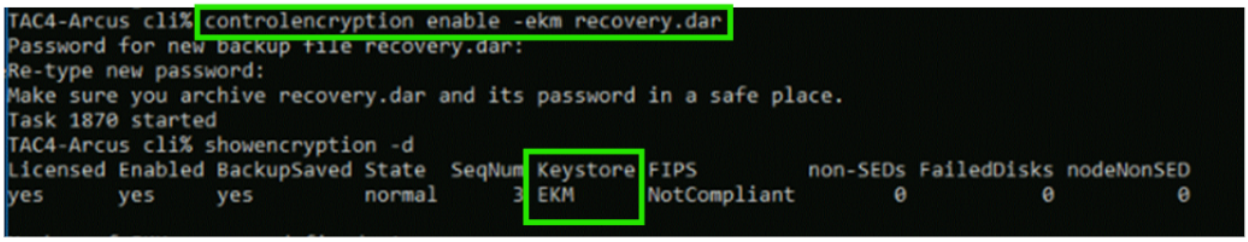


Figure 24 : Keystore updated as EKM

7.2 Log Locations and Interpretation

You can verify the logs from Utimaco ESKM by following the steps below:

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **KMIP**.

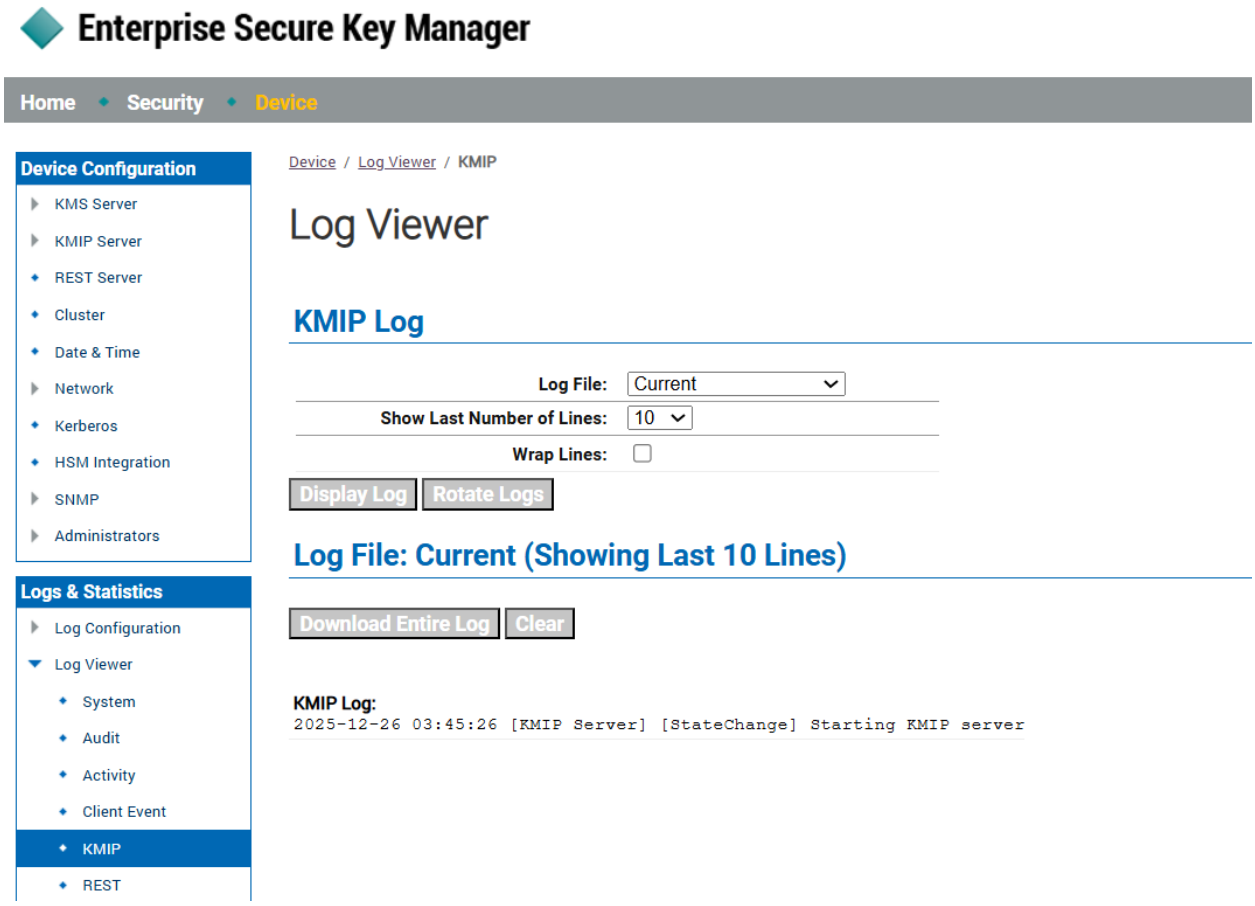


Figure 25 : Log viewer

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 References

Title	Description	Document/Link
HPE GreenLake UI	HPE GreenLake UI detailed user guide.	*HPE GreenLake for Block Storage UI 2.5 User Guide*
ESKM Installation Guide	Step-by-step guide for installing and configuring ESKM	*2021-0047 Installation and Replacement Guide.*

Table 5: References