

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	1.0.0
Date	2026-01-13
Status	PUBLISHED
Document No.	IG-2025-0067
All rights reserved	<p>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.</p> <p>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.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>

Table of Contents

1	Introduction	5
1.1	About This Guide	5
1.2	Target Audience	5
1.3	Purpose of the Integration	5
1.4	Abbreviations	5
1.5	Document Conventions	6
2	Product Overview.....	8
2.1	Overview of the Alletra Storage B10000.....	8
2.2	Overview of ESKM	8
2.3	Joint Value Proposition	8
3	Integration Requirements and Prerequisites	9
3.1	Tested Versions.....	9
3.2	Hardware and Software Requirements.....	9
3.3	Prerequisites	9
4	Installation and Configuration.....	10
4.1	Setting Up ESKM	10
4.2	Setting Up Alletra Storage B10000	11
5	Integration Steps	13
5.1	Configuration on Utimaco ESKM.....	13
5.1.1	Create a Local CA	13
5.1.2	Create a Server Certificate	14
5.1.3	Configure the KMIP Server	15
5.1.4	Create a KMIP User Group.....	16
5.1.4.1	Sign the Host Certificate using ESKM	18
5.1.5	Create a KMIP User	21
5.2	Configuration on Alletra Storage B10000.....	22
5.2.1	Create a CSR for KMIP User and Sign Using ESKM	22
5.2.2	Import Signed Client Certificate	24
5.2.3	Configure EKM settings.....	24
6	Verification and Testing	28
6.1	Enable Array Encryption	28

6.2	Verify ESKM Logs	28
6.3	Verify Key Added in ESKM.....	29
6.4	Verify KMIP Object	29
7	Troubleshooting	30
7.1	Log Locations and Interpretation	30
8	Contact and Support Information	31
9	Appendices	32
9.1	References	32

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
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

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.

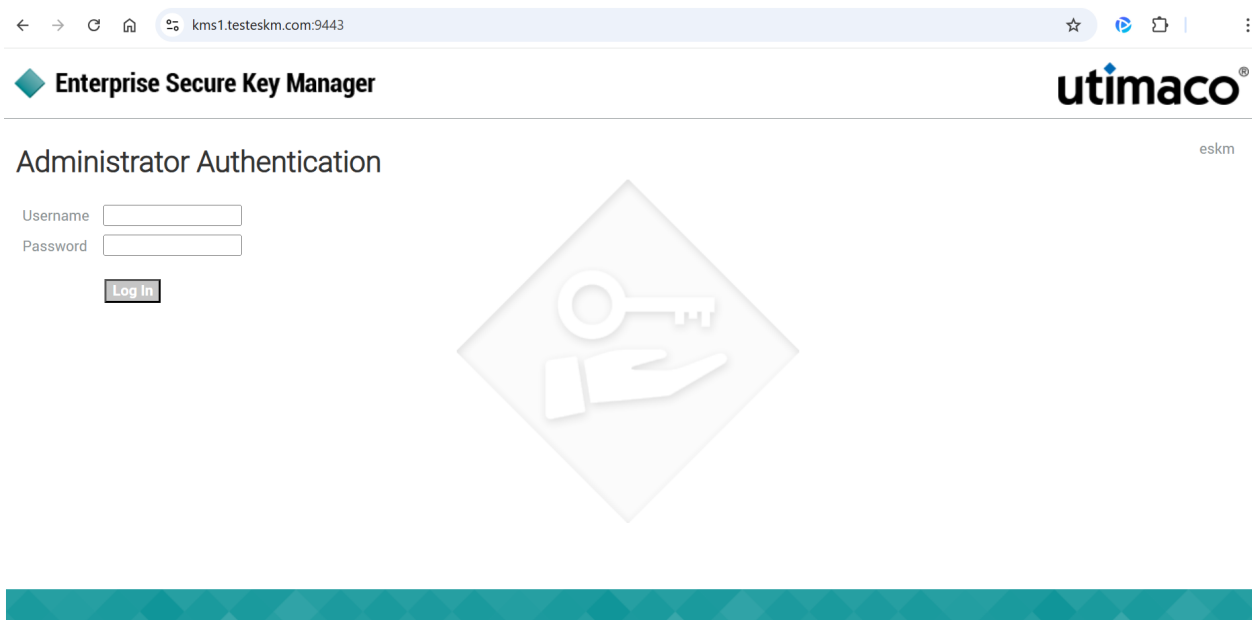


Figure 1 : ESKM login page

Enterprise Secure Key Manager

Home • Security • Device

Help • Log Out

eskm
Logged in as admin

Home / Summary

Home

System Summary [Help](#)

Product:	Enterprise Secure Key Manager L1
Unit ID:	UL14NFAB6HJK
Hardware Platform:	Cloud Platform
Software Version:	8.54.0 (vESKM 8.54)
Date:	09/08/2025
Time:	23:27:31
Time Zone:	Pacific Time
System Uptime:	26 days, 18:59:13
Licenses:	100
Licenses in Use:	25

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.

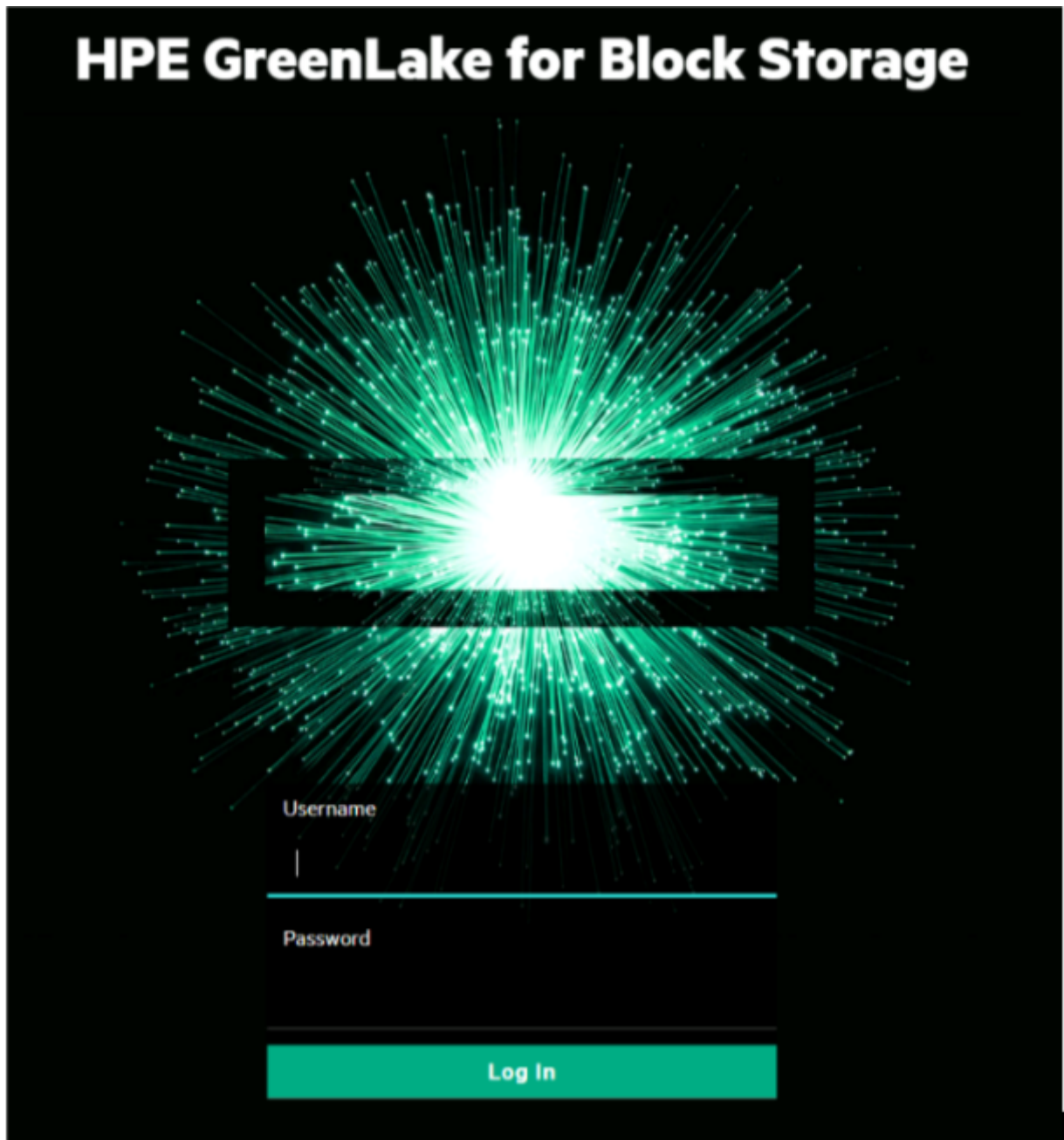


Figure 3 : Alletra Storage B10000 login

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**.

Create Local Certificate Authority

Certificate Authority Name:	ESKMLocalCA
Country Name:	US
State or Province Name:	CA
Locality Name:	Campbell
Organization Name:	Organization
Organizational Unit Name:	Information Security
Common Name:	ESKMLocalCA
Email Address:	infosec@organization.com
Algorithm:	RSA-2048
Certificate Authority Type:	<input checked="" type="radio"/> Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 <input type="radio"/> Intermediate CA Request

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**.

Create Certificate

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:172.31.1.83
Algorithm:	RSA-2048
Creation Type:	<input type="radio"/> Certificate Request - to be signed by external CA <input checked="" type="radio"/> Certificate Signed by Local CA
Local CA:	ESKMLocalCA (maximum 3578 days)
Certificate Purpose:	Server

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.

KMIP Server Settings

IP:	[All] ▾
Port:	5696
Server Certificate:	ESKMServerCert ▾
Local CA Certificate for Certify/Re-certify:	ESKMLocalCA ▾
Connection Timeout (sec):	360
Default number of items returned in Locate:	100
Maximum number of items returned in Locate:	1000
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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.

KMIP Server Authentication Settings

Client Certificate Authentication:	<input type="radio"/> disable <input checked="" type="radio"/> enable
Trusted CA List Profile:	Default ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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.

Local Group Configuration

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
AlletraGroup	KMIP	

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**.

Local Certificate Authority List

[Help ?](#)

CA Name	CA Information	CA Status
<input type="radio"/> ESKMCAVBR	Common: ESKMLocalCAVBR Issuer: Organization Expires: Jun 3 06:33:47 2035 GMT	CA Certificate Active
<input checked="" type="radio"/> ESKMLocalCA	Common: ESKMLocalCA Issuer: Organization Expires: Jun 3 04:47:57 2035 GMT	CA Certificate Active
<input type="radio"/> ESKMVeeam	Common: ESKMVeeam Issuer: Organization Expires: Aug 30 08:58:20 2035 GMT	CA Certificate Active

Figure 10 : Local CA

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

[Security](#) / [Local Users & Groups](#) / [Local Users](#)

Create Local User

Create Local User

Username:	<input type="text" value="AlletraUser"/>
Password:	<input type="password" value="....."/>
Confirm Password:	<input type="password" value="....."/>
License Type:	<input type="text" value="KMIP"/> ▼
User Administration Permission:	<input type="checkbox"/>
Change Password Permission:	<input type="checkbox"/>
Enable KMIP:	<input checked="" type="checkbox"/>
Map non-existent Object Group to x-Object Group:	<input type="checkbox"/>
KMIP User Group:	<input type="text" value="AlletraGroup_user"/> ▼
KMIP Object Group:	<input type="text" value="AlletraGroup"/> ▼

KMIP Client Certificate:

```
-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgIBFDANBgkqhkiG9w0BAQsFADCB0jELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRERwYDVQQHEwhDYW1wYmVsbnBDEVMBMGA1UEChMNT3JnYW5p
emF0aW9uMR0wGwYDVQQLEXRJbmZvcmlhdGlvbiBTZW51cm10eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWG1uZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTEyMjI0MDZaFw0zNTA2MTQxNjQyMDZaMHMxMzAJBgNVBAYT
A1VTMQswCQYDVQQIDAJUWDELMakGA1UEBwwCQVUxDjAMBgNVBAoMBU90VEFQMzsw
CQYDVQQLEDAJRzEOMAwGA1UEAwwFT05UQVxHTAbBgkqhkiG9w0BCQEWdk90VEFQ
```

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.

The screenshot shows a dialog box titled "Add array certificate" with a close button (X) in the top right corner. The dialog is divided into three main sections:

- Type:** Three radio button options are present:
 - Create a self signed certificate
 - Create a certificate signing request
 - Add a CA Certificate
- Array service:** A dropdown menu showing "ekm-client" with a downward arrow.
- Certificate signing request:** A form with several fields:
 - Key length:** A dropdown menu showing "2048".
 - Common name:** A text field containing "AlletraUser".
 - Subject Alternative Name:** A text field containing "Example - DNS:myhost, DNS:myhost.example.com, IP:1.2.3.4. All addresses must be prefixed with either DNS: or IP:".
 - Organization unit:** A text field containing "TestGroup".
 - Organization:** A text field containing "Utimaco".
 - Locality:** A text field containing "Campbell".
 - Province/State:** A text field containing "California".
 - Country:** A dropdown menu showing "United States (US)".

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.

Set EKM Servers ✕

For EKM environments, backups are for configuration information only. While the configuration file is important for disaster recovery, the keys are stored only on the EKM and must be backed up independently.

Save the configuration file to external media, such as a CD, external hard drive, or a server, and save this media in a safe location.

EKM server FQDNs or IP addresses

10.15.25.101

Example: ekm.example.com, 10.10.10.10

Port	5696 - +
User name	Alletra_User
Key Management Interoperability Protocol	<input type="checkbox"/> 1.0 <input type="checkbox"/> 1.1 <input checked="" type="checkbox"/> 1.2 <input checked="" type="checkbox"/> 1.3 <input checked="" type="checkbox"/> 1.4
Backup password	<input type="password"/>
Password	<input type="password"/>
Confirm password	<input type="password"/>

I have read and understand the implications

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**.

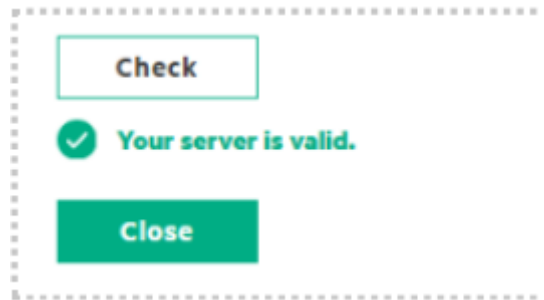


Figure 18 : EKM server validated

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.

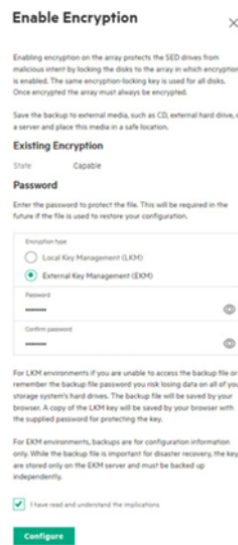


Figure 19 : Enable Encryption

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**.

```

KMIP Log:
2025-12-16 16:14:09 [KMIP Server] [Authentication Success] User:[Alletra User] From IP: 10.15.5.40
2025-12-16 16:14:09 [KMIP Server] [ClientOperation] User:[Alletra User] UUID:[ ] Operation:[QUERY] Result:[SUCCESS]
2025-12-16 16:19:28 [KMIP Server] [Authentication Success] User:[Alletra User] From IP: 10.15.5.40
2025-12-16 16:19:28 [KMIP Server] [ClientOperation] User:[Alletra User] UUID:[ ] Operation:[QUERY] Result:[SUCCESS]
2025-12-16 16:24:45 [KMIP Server] [Authentication Success] User:[Alletra User] From IP: 10.15.5.40
2025-12-16 16:24:45 [KMIP Server] [ClientOperation] User:[Alletra User] UUID:[ ] Operation:[QUERY] Result:[SUCCESS]
2025-12-16 16:25:33 [KMIP Server] [Authentication Success] User:[Alletra User] From IP: 10.15.5.40
2025-12-16 16:25:33 [KMIP Server] [ClientOperation] User:[Alletra User] UUID:[ ] Operation:[QUERY] Result:[SUCCESS]
2025-12-16 16:30:03 [KMIP Server] [Authentication Success] User:[Alletra User] From IP: 10.15.5.40
2025-12-16 16:30:03 [KMIP Server] [ClientOperation] User:[Alletra User] UUID:[ ] Operation:[QUERY] Result:[SUCCESS]
    
```

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 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.

Enterprise Secure Key Manager

The screenshot shows the ESKM Management Console interface. At the top, there is a breadcrumb trail: Home > Security > Device. Below this, there are two main navigation panels on the left. The first panel, 'Device Configuration', lists various server and system settings like KMS Server, KMP Server, REST Server, Cluster, Date & Time, Network, Kerberos, HSM Integration, SNMP, and Administrators. The second panel, 'Logs & Statistics', lists log categories such as Log Configuration, Log Viewer (expanded to show System, Audit, Activity, Client Event, KMIP, and REST), and REST. The main content area is titled 'Log Viewer' and 'KMIP Log'. It features a 'Log File' dropdown menu set to 'Current', a 'Show Last Number of Lines' dropdown set to '10', and a 'Wrap Lines' checkbox which is unchecked. Below these controls are 'Display Log' and 'Rotate Logs' buttons. A sub-header reads 'Log File: Current (Showing Last 10 Lines)'. Underneath are 'Download Entire Log' and 'Clear' buttons. The log content itself is titled 'KMIP Log:' and shows a single entry: '2025-12-26 03:45:26 [KMIP Server] [StateChange] Starting KMIP server'.

Figure 23 : 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	<i>2021-0047 Installation and Replacement Guide.</i>

Table 5: References