

NetApp

ONTAP

9.11.1P19, 9.12.1P17

Integration Guide

ESKM

8.53.1, 8.53.3, 8.54.0

Imprint

Copyright 2025	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2025-07-08
Status	PUBLISHED
Document No.	IG-2025-0039
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	Document Conventions	6
1.5	Abbreviations	6
2	Product Overview.....	9
2.1	NetApp ONTAP	9
2.2	Utimaco ESKM (Enterprise Secure Key Manager)	9
2.3	Joint Value Proposition	9
3	Integration Requirements and Prerequisites	11
3.1	Tested Versions.....	11
3.2	Supported Platforms	11
3.3	Software Requirements.....	11
3.4	Hardware Requirements.....	12
3.5	Prerequisites	12
4	Installation and Configuration.....	13
4.1	Installing and Configuring Utimaco ESKM Server	13
4.2	Installing NetApp ONTAP using Simulate ONTAP	14
4.2.1	Deploying and configuring a single node ONTAP Cluster	14
5	Integration Steps.....	18
5.1	Configuration on Utimaco ESKM	18
5.1.1	Local CA Creation	18
5.1.2	Server Certificate Creation	19
5.1.3	KMIP Server Configuration	20
5.1.4	Creating a Client Certificate for ONTAP (Using OpenSSL)	21
5.1.4.1	Create a CSR.....	21
5.1.4.2	Use the Local CA to Sign CSR.....	23
5.1.5	Creating KMIP User	26
5.2	Configuration on ONTAP	28
5.2.1	Importing the Client Certificate to ONTAP	28

5.2.2	Installing the Utimaco ESKM Server Certification Authority (CA) Certificate	30
5.2.3	Adding the Utimaco ESKM as Key Control Nodes on ONTAP	31
5.2.4	Verifying the communication between the external Key Manager and ONTAP	32
6	Verification and Testing	33
6.1	Performing NetApp Volume Encryption.....	33
6.1.1	Enabling Aggregate-level Encryption.....	33
6.1.2	Enabling Encryption on a New Volume	34
6.1.3	Enabling Encryption on an Existing Volume with the Volume Encryption Conversion Start Command	38
6.1.4	Enabling Encryption on an Existing Volume with the Volume Move Start command	41
7	Logs and Validation Steps	46
8	Troubleshooting	48
8.1	Common Issues	48
8.2	Managing the Client and CA Certificates on ONTAP	48
8.2.1	Deleting Certificates	48
8.2.2	Replacing the ESKM Client Certificates.....	49
8.3	Contact for support	49
8.3.1	Utimaco Technical Support	49
8.3.2	24-hour Support	50
9	Appendices	51
9.1	References	51

1 Introduction

This guide is part of the information and support provided by Utimaco. It outlines the detailed process of integrating Utimaco ESKM with NetApp ONTAP, with an emphasis on secure, centralized encryption key management for protecting data at rest. The guide outlines the step-by-step configuration process required to establish and validate the integration.

1.1 About This guide

This guide provides a detailed walkthrough of the integration process between Utimaco ESKM and NetApp ONTAP, focusing on establishing a secure and reliable encryption key management infrastructure. Utimaco ESKM plays a central role in the lifecycle of cryptographic keys. It generates, stores, and manages the keys that NetApp ONTAP utilizes to enable volume-level encryption through NetApp Volume Encryption (NVE). By leveraging the KMIP protocol, this integration ensures that sensitive data at rest is protected with strong encryption standards while also enabling centralized compliance and auditability across the storage environment.

1.2 Target Audience

This guide is intended for administrators of NetApp ONTAP and Utimaco ESKM.

1.3 Purpose of the Integration

Integrating NetApp ONTAP with Utimaco ESKM provides a powerful, secure, and standards-based approach to managing encryption keys for data-at-rest protection:

- **Secure Key Storage:** ONTAP protects data using volume-level encryption. Instead of storing encryption keys locally, it relies on Utimaco ESKM to securely generate, store, and serve keys, ensuring that sensitive data remains protected even if physical storage is compromised.
- **KMIP-Based Interoperability:** Utimaco ESKM supports the Key Management Interoperability Protocol (KMIP), allowing seamless communication with ONTAP. This standardization ensures compatibility and simplifies integration across diverse environments.
- **Centralized Key Management:** ESKM provides a single pane of glass for managing all cryptographic keys, which is especially useful in large or multi-cloud deployments. This centralization enhances control, simplifies audits, and supports compliance efforts.

- High Availability & Disaster Recovery: ONTAP supports configuring multiple KMIP servers for redundancy. This ensures that key access remains uninterrupted even during outages, which is critical for maintaining access to encrypted data.

In essence, this integration strengthens your data security posture by combining ONTAP's robust encryption with Utimaco's enterprise-grade key lifecycle management.

1.4 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI). e.g. Menu options	Click Create
<code>Monospaced</code>	File names, folder and directory names, commands, file outputs, programming code samples	It also creates a private key file called <code>KMIP_client.key</code>
<i>Italic</i>	Reference and important terms	Download a production data at rest encryption image from <i>NetApp Support</i>

Table 1: Document Conventions

1.5 Abbreviations

The following abbreviations are used in this guide.

Abbreviation	Meaning
CA	Certificate Authority

CN	Common Name
ESKM	Security Key Manager
GUI	Graphical User Interface
IP	Internet Protocol
KMIP	Key Management Interoperability Protocol
KMS	Key Management System
NVE	NetApp Volume Encryption
ONTAP	On Net Transport Activation Process
SM	System Manager
NAE	NetApp Aggregate Encryption
SVM	Storage Virtual Machine (also referred to as a Vserver)
RAM	Random Access Memory
VT	Virtualization Technology
BYOK	Bring Your Own Key
HYOK	Hold Your Own Key

TLS	Transport Layer Security
SSL	Secured Socket Layer
VE	Volume Encryption

Table 2: List of Abbreviations

2 Product Overview

2.1 NetApp ONTAP

ONTAP software provides a rock-solid foundation for data management on the broadest range of deployments. With the NetApp Volume Encryption feature built into ONTAP, you can easily and efficiently protect your at-rest data by encrypting any volume. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

2.2 Utimaco ESKM (Enterprise Secure Key Manager)

The ESKM is a complete solution for generating, storing, serving, controlling and auditing access to encryption keys. It enables you to protect and preserve access to business-critical, sensitive data-at-rest encryption keys, either locally or remotely. ESKM is offering industry-certified Key Management Interoperability Protocol (KMIP) with market-leading support for partner applications and pre-qualified solutions, integrating out-of-the-box with varied deployments and custom integrations.

2.3 Joint Value Proposition

Integrating Utimaco ESKM with NetApp ONTAP lies in delivering a secure, scalable, and standards-based encryption solution for protecting data at rest across on-premises and multi-cloud environments.

Here's what makes this integration compelling:

- **End-to-End Data Protection:** ONTAP provides native volume-level encryption, while ESKM securely generates, stores, and manages the encryption keys. This ensures that even if storage media is lost or stolen, the data remains inaccessible without the keys.
- **KMIP-Based Interoperability:** The integration is built on the Key Management Interoperability Protocol (KMIP), enabling seamless and standardized communication between ONTAP and ESKM. This reduces complexity and ensures compatibility across diverse IT ecosystems.
- **Centralized Key Governance:** ESKM offers centralized control over key lifecycle operations—generation, rotation, revocation, and auditing—helping organizations meet compliance requirements like GDPR, HIPAA, and PCI-DSS.

- Multi-Cloud and BYOK/HYOK Support: The joint solution supports Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) models, giving enterprises full control over encryption keys in hybrid and multi-cloud deployments.
- High Availability and Resilience: ONTAP supports multiple external key servers, ensuring continuous access to encrypted data even during outages. ESKM's robust architecture complements this with high availability and disaster recovery capabilities.
- Regulatory Compliance and Certification: ESKM is industry-certified and integrates with NetApp's secure storage to meet stringent data protection standards, including those required for classified or regulated environments.

This integration empowers organizations to secure sensitive data with confidence, maintain operational agility, and simplify compliance—all while reducing the risk of data breaches.

3 Integration Requirements and Prerequisites

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

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

3.1 Tested Versions

These integrations have been successfully tested with the Utimaco ESKM and NetApp ONTAP.

NetApp ONTAP Version	Utimaco ESKM Version
9.11.1P19, 9.12.1P17	8.53.1, 8.53.3, 8.54.0

Table 4: List of Tested Versions

3.2 Supported Platforms

- Utimaco ESKM hardware appliance
- Utimaco ESKM virtual/cloud appliance

3.3 Software Requirements

Software	Software Requirements
NetApp ONTAP	9.11.1P19, 9.12.1P17
Utimaco ESKM	8.53.1, 8.53.3, 8.54.0

Table 5: List of Software Requirements

3.4 Hardware Requirements

Hardware	Hardware Requirements
ESKM	ESKM hardware appliance or virtual appliance with 2 vCPU and 4GB RAM
NetApp ONTAP	6 GB RAM and 40 GB free disk space for each instance of the simulator
VT	VT support for Intel system

Table 6: List of Hardware Requirements

3.5 Prerequisites

Before you begin, please ensure that you have installed/setup:

- NetApp ONTAP listed in Tested Versions
- ESKM listed in Tested Versions
- Download NetApp ONTAP file from [NetApp Support](#)
- Familiarize yourself with the NetApp ONTAP documents and setup process. Visit [ONTAP Documentation](#) for more information related to ONTAP deployment and configuration.
- You can also deploy Simulate ONTAP software. The Simulate ONTAP software is a set of VMware files that have been packaged in an .ova file. You need to download the appropriate software and license files from the NetApp Support Site.

4 Installation and Configuration

The following section outlines the procedures required to configure both ESKM and NetApp ONTAP components for seamless integration.

4.1 Installing and Configuring Utimaco ESKM Server

The ESKM server must be configured with specific values, such as the time zone, IP address, netmask, gateway, hostname, and port number used for the ESKM Management Console interface. For detailed configuration steps, see the installation guide *“ESKM_Installation and Replacement_Guide_8.54.0.”*

After successful installation and configuration log in to ESKM.

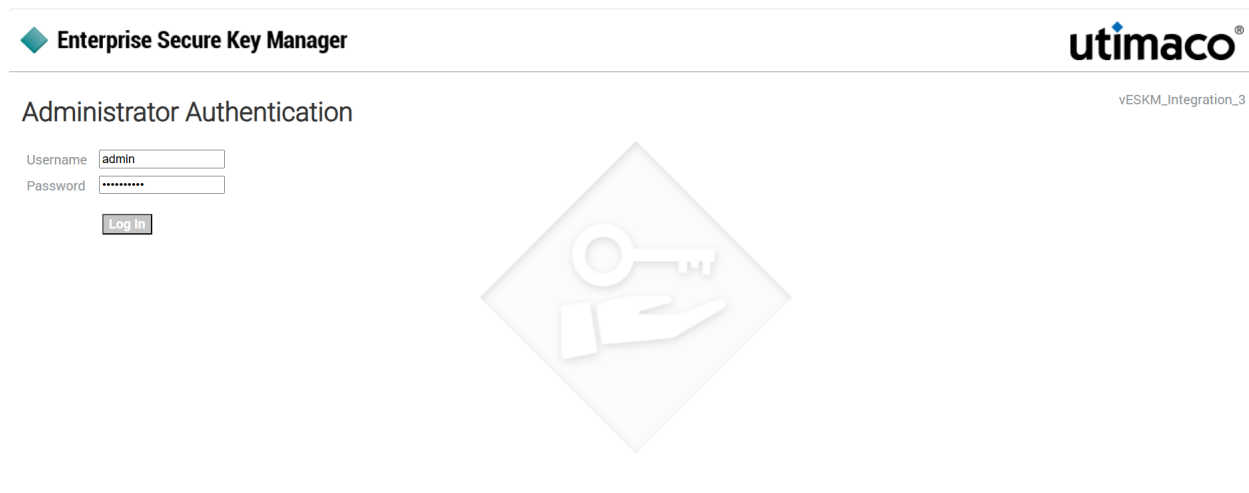
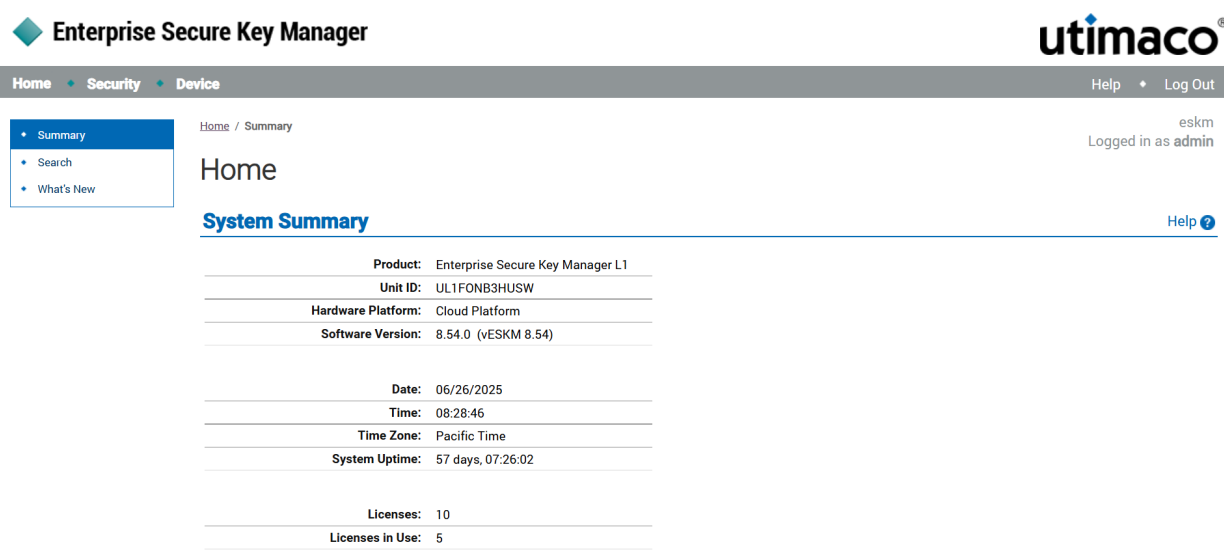


Figure 1 : ESKM Login Page



Enterprise Secure Key Manager

Home • Security • Device

Help • Log Out

Home / Summary

Summary

Search

What's New

Home

System Summary

Product: Enterprise Secure Key Manager L1

Unit ID: UL1FONB3HUSW

Hardware Platform: Cloud Platform

Software Version: 8.54.0 (vESKM 8.54)

Date: 06/26/2025

Time: 08:28:46

Time Zone: Pacific Time

System Uptime: 57 days, 07:26:02

Licenses: 10

Licenses in Use: 5

Help

eskm
Logged in as admin

Figure 2 : ESKM Home Page

4.2 Installing NetApp ONTAP using Simulate ONTAP



Skip this section if you already have NetApp ONTAP deployed. For demonstration purposes, Simulate ONTAP has been used. You can download Simulate ONTAP ova file from [NetApp Support](#) and deploy it by importing the ova file on VMware Workstation Pro, VMware Workstation Player, or VMware Fusion

4.2.1 Deploying and configuring a single node ONTAP Cluster

Start and configure a single-node ONTAP cluster using Simulate ONTAP, VMware, System Manager, and the command line.

1. Create Simulate ONTAP virtual machine using .ova file.
2. After a few minutes of starting the virtual machine, you will receive a message asking you to log in to the system. Manager to complete the cluster setup. This message includes an IP address. Copy and paste this IP address into your browser address bar to open System Manager.
3. System Manager will open. You can ignore the 'partner details were not found' error message.
4. If you have any issues with how System Manager displays pages, then try a different web browser or Java version on your laptop.

5. Enter these details as per your requirement, leaving the other checkboxes unchecked, then click **Submit**.

a) Storage System Name: cluster1

b) Administrative Password: Utimaco@123

c) Cluster IP Address: 192.168.182.61 Subnet Mask: 255.255.255.0 Gateway: 192.168.182.1

d) Node IP Addresses: 192.168.182.62

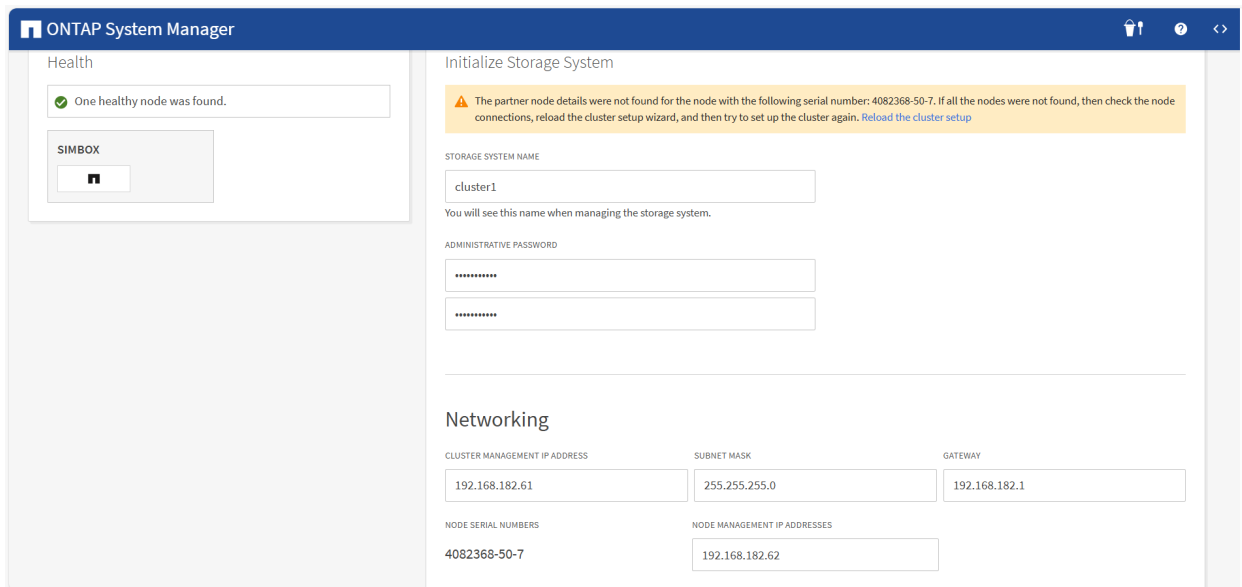


Figure 3 : System Manager Initialize Storage System Page.

6. Log in with the username admin and password in the VMware Workstation Player window.

7. Add all existing disks to Cluster 1 Node 1 with the below command.

>_Console

```
cluster1::> storage disk assign -all true -node cluster1-01
```



If you get an error message, it's because the system has already auto-assigned the disks; you can ignore it.

8. If necessary, add more disks to your root aggregate to increase its size and accommodate the additional space needed in your root volume.

>_Console

```
cluster1::> storage aggregate add-disks -diskcount 8 -aggregate
aggr0_cluster1_01
```

9. Set the root volume to a new size.

>_Console

```
cluster1::> volume modify -size 7.47GB -volume vol0 -vserver cluster1-01
```

10. Download a production data at rest encryption image from [NetApp Support](#).
 - a) Click download latest image, for example “Download Latest Release [9.12.1P17]”.
 - b) Click **I read the EULA**. Click **Accept and Continue**.
 - c) Click “**Download ONTAP 9.12.1P17 with NetApp Volume Encryption for FAS [2.54 GB]**”.
 - d) Save the file and make it accessible via a web server.
 - e) Download the package to ONTAP cluster and update the node using the below command.

>_Console

```
cluster1::> cluster image package get -url http://<web_server_ip>/
9121P17_q_image.tgz

cluster1::> cluster image package show

cluster1::> cluster image update -version 9.12.1P17 -nodes cluster1-01

cluster1::> cluster image show-update-progress
```

11. Unlock the diag account and set the password.

```
>_Console

cluster1::> security login unlock -username diag

cluster1::> security login password -username diag
```

12. Install the VE license.

```
>_Console

cluster1::> license add -license-code AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

13. Verify that the license is installed by displaying all the licenses on the cluster.

```
>_Console

cluster1::> system license show

cluster1::> system license show
Serial Number: 1-80-000011
Owner: cluster1
Installed License: Legacy Key
Capacity: -
Package      Type      Description      Expiration
-----
VE           demo     Volume Encryption License
                                           7/14/2025 08:00:00
```

Figure 4 : Show NVE license show.

5 Integration Steps

5.1 Configuration on Utimaco ESKM

Proper configuration of Utimaco ESKM is crucial for achieving secure and streamlined key management. This section guides you through the necessary steps to configure ESKM for ONTAP integration.

5.1.1 Local CA Creation

Inside ESKM create a local CA by following the below steps:

1. Go to **Security** tab.
2. Click on **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Create Certificate** section.
4. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example, ESKM Local CA.
5. Enter your **Organizational information**.
6. Select the **Algorithm** (e.g., RSA-2048).
7. Click on **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:	<input type="text" value="ESKMLocalCA"/>
Country Name:	<input type="text" value="US"/>
State or Province Name:	<input type="text" value="CA"/>
Locality Name:	<input type="text" value="Campbell"/>
Organization Name:	<input type="text" value="Organization"/>
Organizational Unit Name:	<input type="text" value="Information Security"/>
Common Name:	<input type="text" value="ESKMLocalCA"/>
Email Address:	<input type="text" value="infosec@organization.com"/>
Algorithm:	<input type="text" value="RSA-2048"/>
Certificate Authority Type:	<input checked="" type="radio"/> Self-signed Root CA
	CA Certificate Duration (days): <input type="text" value="3650"/>
	Maximum User Certificate Duration (days): <input type="text" value="3650"/>
	<input type="radio"/> Intermediate CA Request

Figure 5 : Create Local CA window.

- Click on **Local CA's** option listed under **Certificates & CA's** to view the created local CA certificate.

Local Certificate Authority List

[Help ?](#)

CA Name	CA Information	CA Status
<input checked="" type="radio"/> ESKMLocalCA	Common: ESKMLocalCA Issuer: Organization Expires: Jun 8 20:25:13 2035 GMT	CA Certificate Active
<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Download"/> <input type="button" value="Properties"/> <input type="button" value="Sign Request"/> <input type="button" value="Show Signed Certs"/>		

Figure 6 : Created Local CA certificate.

5.1.2 Server Certificate Creation

ESKM server certificates are used by the client to authenticate the ESKM server during the TLS/SSL handshake.

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

- Go to **Security** tab.
- Click on **Certificates** option listed under **Certificates & CAs**.

3. Scroll down to the **Create Certificate** section.
4. Enter **Certificate Name**, **Country Name**, **State and Province Name**, **Locality Name**, **Organization Name**, and **Organization Unit Name**
5. Select **RSA-2408** from the **Algorithm** dropdown list.
6. Select the previously created CA certificate name from the **Local CA** drop-down list.
7. Select **Server** from the **Certificate Purpose** dropdown list.
8. Click on **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:10.222.55.178
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 3633 days) ▼
Certificate Purpose:	Server ▼

Create

Figure 7 : Create Certificate Window.

5.1.3 KMIP Server Configuration

1. Go to the **Device** tab.
2. From the left side panel, click on the **KMIP Server** option listed under **Device Configuration**.
3. Click the **Edit** button on the main page.

4. Choose the above-created server certificate as the **server certificate** for the KMIP server.
5. Click the **Save** button.

KMIP Server Configuration

KMIP Server Settings

IP:	[All] ▼
Port:	5696
Server Certificate:	ESKMServerCert ▼
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

Figure 8 : KMIP Server Settings window.

5.1.4 Creating a Client Certificate for ONTAP (Using OpenSSL)

This section provides the step-by-step procedure for creating a client certificate for integrating ESKM with ONTAP.

5.1.4.1 Create a CSR

1. The certificate signing request (CSR) is created on a machine with OpenSSL installed.
2. Using OpenSSL, create a private key using the commands and syntax shown below. The example shows the creation of a 2048-bit RSA key.

>_Console

```
# openssl genrsa -out KMIP_client.key 2048
```

3. Generate a certificate signing request (CSR) using the private key.

>_Console

```
# openssl req -x509 -new -nodes -key KMIP_client.key -days 3650 -out
KMIP_client.cert -sha256
```

The following output appears.

>_Console

```
You are about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what is
called a Distinguished Name or a DN. There are quite a few fields but you
can leave some blank For some fields, there will be a default value, If you
enter '.', the field will be left blank. ----- Country
```

4. Enter the information in the fields as prompted.

Field	Example
Country Name	USA
State Name	CA
Locality Name	Campbell
Organization Name	Oraganization
Organization Unit Name	Information Security
Common Name	kmip_client_ontap
Email Address	infosec@organization.com

Table 7: List of Field with Example



The Common Name must match the name of the KMIP user

This process creates a certificate request file called `KMIP_client.csr`. It also creates a private key file called `KMIP_client.key`.

5.1.4.2 Use the Local CA to Sign CSR

The CSR needs to be signed by the local CA.

1. View the `KMIP_client.csr` file created above using the `cat` command (`cat kmip_client.csr`) or open it using any text editor.
2. Select the entire text and copy it to the clipboard.



Be sure to include the first and last lines (-----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST-----).

3. Log in to the Management Console and navigate to **Security > Certificates & CAs > Local CAs**.
4. Select the CA used by your ESKM (in this case, ESKMLocalCA), and click **Sign Request**. The Sign Request window is displayed.

Sign Certificate Request

Sign with Certificate Authority:

Certificate Purpose: Server
 Client
 Server and Client

Certificate Duration (days):

Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC2DCCAcACAQAwgZIx CzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybm1h
MREwDwYDVQQHDAhDYW1wYmVsbDEQMA4GA1UECgwHVXRpbWVjZEPMA0GA1UECwwG
QXRhbGxhMRcwFQYDVQQDDA5rbWlwX2NsawVudF8wMTEfMFB0GCSqGSIb3DQEJARYQ
ZXNrbUB1dGltYWVvLmNvbTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AL3mcGSX5/CAxWZ03YLYu44RCUk5yqgAviRkLFEzw/KWGDQoy6fIMOJlnojt1uVd
zASjbmqCcTo3qZiiz1PISUy87yGZJ+PeVxiGfQwcAVDS1qS+GfRi+9urrvczCikf
ng5fF64XG1A6gYiMkw+UW3GpJgsQ9obtONqv8HYDY+c+jOKZpXHoEo61AbFrJ2pS
nkum6GDobegx17xr7KYenJU/yiR030hUqKsFmdgERYcJ+LXLbvG/uSD4qFWamR/1
KTkj42J20fR6tEGFg1oSj36SMWeQJbnJrYfVo6+hf2TTPGJcQaD5002G6B29RFyT
vpQ6fgoqhpK9EL6cJ/WAMtcCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQC7hqCv
87j4HcZJpBo0g6btY1Hf1Tu1T+YzYzX9oIqHAX0hY21WVx6z9ksh0E0tFsdWqYsA
cyGN7SPMJKPt9TuNPjVVDki9JFayF3Q0KDtSWcUeLF0t2r/7FXi+PGj6G85HmzEn
rB46pvSHh1CxaVzovzVL064GebBgxVt5zM8tK5WwMkeQhh49xdgW0fowQX0Q1sd9
3x55b+8Vf/tCSqoUWP9oiLzak4vs2AsqLiZVC9r6HIhuMhGwqtGu+eIyljmuwKmb
ZG7H/2zhePw6yANWFe7zZtmlzQ/FM7+961C+uBDoygyPMfjj2aL7WBE7BZCDsbx5
yTHKnY2Fi5rMFT1g
-----END CERTIFICATE REQUEST-----
```

Figure 9 : Sign Certificate Request Window.

- For Certificate Purpose, select Client.
- Paste the CSR text that you have copied to your clipboard (Step 2 above) into the Certificate Request window.
- Click **Sign Request**. The signed client certificate is displayed.

Certificate and CA Configuration

CA Certificate Information

Key Size:	2048
Start Date:	Jun 24 17:28:38 2025 GMT
Expiration:	Jun 8 17:28:38 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: kmip_client_01 emailAddress: eskm@utimaco.com

```
-----BEGIN CERTIFICATE-----
MIID1DCCAvagAwIBAgIBCTAKBggqhkjOPQQDAjCB0jELMAkGA1UEBhMCVVMxChAkJ
BgNVBAgTAkNEMREwDwYDVQQHEwhDYW1wYmVzbDEVMBMGA1UEChMNT3JnYW5pemF0
aW9uMR0wGwYDVQQLEwRlbnZvcmlhdG1vbiBTZWN1cm10eTEUMBIGA1UEAmdLRVNL
TUxvY2FzQ0ExJzAlBgkqhkiG9w0BCQEWGgluzm9zZWNAb3JnYW5pemF0aW9uLmNv
bTAAeFw0yNTA2MjY0ODUzI4MzhaFw0zNTA2MDg0ODUzI4MzhaMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECAwKQ2FzZWZvcmlhdG1vbiBTZWN1cm10eTEUMBIGA1UEBwwIQ2FtcGJlbGwxE
DAOBgNV
BAoMB1V0aW1hY28xMzA2MjY0ODUzI4MzhaMBkF0YXksYXNjaW50eTEUMBIGA1UEAwwOa21p
cF9jbG1l
bnRfMDEuXzAdBgkqhkiG9w0BCQEWGzA21AdXRpbWVfby5jb20wgGElMA0GC8qG
S1b3DQEBAQUAA4IBDwAwggEKAoIBAQC95nBk1+fwgMvmdN2C2LuOEQ1J0cqpAL4k
ZC3xM8Pylhg0KManyDDiZ26I7db1XcwEo25qgnE6N6m3Im2TyElMvO8hm3fj31cY
hn0MHAFQ0pakvhn0Yvvbq673MwopH54OXxeuFxtQ0oGIjJFv1FtxqSYLEPaG7Tja
r/B2A2PnPoizimaVx6BK0tQGxaydqUp5Lpuhg6G3oMZe8a+ymHpyVP8okdNzoVKir
BZnYBEWHCfi1y27xv7kg+KhVmpkf58k5I+NidH0erRBhYNaEo9+kjFnkCW5ya2H
1aOvoX9k06RiXEGg+TjthugdvURck76UOn4KKoaZPRC+nCf1gDLXAgMBAAGjYDBe
MAkGA1UdEwQCMAAwHQYDVIR0OBByEFJ9um61S+XhBVanaIaTTCsvTbR2JMB8GA1Ud
IwQYMBaAFNYGNr4gb0znQkxDZXdJ3owq7INWMBEGCWC8AGG+EIBAQQEAwIHgDAK
BggqhkjOPQQDAQOBiAwgYcCQgCkze34TavR8B32qwIKesJGCFe8VyOCVD3ztCVO
VoIhJwrUEMeFRMlyOdGVhXp5mmPY9U1Wix7rwTCyznyEFH/GlwJEGt23KL69hmo+
udidN8UFXxMtyqDjapB2imuA5qNL+dnP8Xh2iOXCEBz3NqHNd7dezhr+tteS2Oh
K8wL218tHZg=
-----END CERTIFICATE-----
```

[Download](#) [Back](#)

Figure 10 : Certificate Information window.

8. Copy the signed client certificate data to the clipboard.

5.1.5 Creating KMIP User

Perform the following steps to create a local KMIP user in the ESKM.



A client license is required for each user created on the ESKM server. See the ESKM Installation and Replacement Guide for information about how to request and install the license pack.

1. Log in to the Management Console, and navigate to **Security > Local Users & Groups > Local Users**.
2. At the bottom of the list, click **Add**.
3. Create a “username” and “password” for the KMIP user.

The “Username” must match the “Common Name (CN)” provided during the client certificate creation.

4. Click the **Enable KMIP** option.
5. If required, from the drop-down lists, select the **KMIP User Group** and **KMIP Object group** to which the user belongs.
6. Paste the signed client certificate into the **KMIP Client Certificate** field.

Create Local User

Username:	<input type="text" value="kmp_client_ontap"/>
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="default user group"/>
KMIP Object Group:	<input type="text" value="default object group"/>

KMIP Client Certificate:

```

-----BEGIN CERTIFICATE-----
MIID1DCCAvagAwIBAgIBCTAKBgqhkjOPQDAjCBojELMAkGA1UEBhMCVVMx CzAJ
BgNVBAGTAKNBREwYDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYw
aW9uMR0wGwYDVQQLEXRjbmZvcmlhdGlvbiBTZW50eTEUMBIGA1UEAxMLRVNL
TUxvY2FsQ0ExZjA1BgkqhkiG9w0BCQEWG1uZm9zZWNA3JnYW5pemF0aW9uLmNv
bTAEFw0yNTA2MjQxNzI0MzhaFw0zNTA2MDgxNzI0MzhaMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcmlpYTERMA8GA1UEBwwIQ2FtcGJlbGwxEADA0BgNV
BAoMB1V0aW1hY28xMzI0MzhaANBgNVBASMBkF0YXN0YXN0YXN0YXN0YXN0YXN0
bnRfMDExHjAdBgkqhkiG9w0BCQEWEGVza21AdXRpbWVjby5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC95nBkl+fWgMVmdN2C2Lu0EQ1J0cqaL4k
ZC3xM8Py1hg0KMunYDDiZZ6I7dblXcWEO25qgnE6N6mSImZTyElMvO8hmSfj31cY
hn0MHAfQ0pakvhn0YvVbq673MwopH540XxeuFxtQ0oGIjJFv1FtxqSYLEPaG7Tja
r/B2A2PnPozimaVx6BK0tQGxaydqUp5Lpuhg6G3oMZe8a+ymHpyVP8okdNzoVKir
BZnYBEWHCFi1y27xv7kg+KhVmpkf5S5k5I+NidT0erRBhYNaEo9+kjFnkCW5ya2H
1aOvoX9k06RiXEGg+TjtHugdvURck76UOn4KKoaZPRC+nCf1gDLXAgMBAAGjYDBE
MAkGA1UdEwQCAAAwHQYDVR00BBYEFJ9um61S+XhBVanaIaTTCsvTbRZJMB8GA1Ud
IwQYMBaAFNYGNr4gb0znQkxDZXdJ3owq7INwMBEGCwCGSAGG+EIBAQQEAWIHgDAK
BggqhkiG9w0BCQEWG1uZm9zZWNA3JnYW5pemF0aW9uLmNvLmNvLmNvLmNvLmNv
VoIhJwrUEmFRM1y0dGVhXp5mmPY9U1Wir7rwTCyznyEFH/G1wJBGtZ3KL69hmo+
udidN8UFXxMtyqDjapB2imuA5qN1+dnP8Xh2i0XCEBz3NqHNd7dezhkrt+tes20h
K8wL218tHZg=
-----END CERTIFICATE-----
    
```

Figure 11 : Create Local User window.

7. Click Create.

The user kmp_client_ontap now appears on the list of Local Users.

The configuration of the ESKM server is now complete.

5.2 Configuration on ONTAP

5.2.1 Importing the Client Certificate to ONTAP

The client certificates must be installed before running the key manager setup.

1. Install the KMIP client certificate.

>_Console

```
cluster1::> security certificate install -type client
```

You will be prompted to paste the certificate and private key content.

Paste the signed client certificate, and the private key content from the private key file `KMIP_client.key` generated in Chapter [Create a CSR](#).

```
cluster1::> security certificate install -type client

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDmDCCAvmgAwIBAgIBDDAKBggqhkiOPQQDAjCBojELMAkGA1UEBhMCVVMxCzAJ
BgNVBAGTAKNBMRewDwYDVQQHEwhDYWlwYmVsbDEVMBMGAlUEChMMT3JnYW5pemF0
aW9uMR0wGwYDVQQLExRjbmZvcmlhdGlvbiBTZW50eTEUMBIGAlUEAxMLRVNL
TUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNA3JnYW5pemF0aW9uLmNv
bTAeFw0yNTA2MjQyMTE5MzZaFw0zNTA2MDgyMTE5MzZaMIGVMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcmlhdGlvbiBTZW50eTEUMBIGAlUEBwwIQ2FtcGJlbGwxE
DAOBgNVBAoMB1V0aWlhY28xDzANBgNVBASMBkF0YWxsYTEaMBGAlUEAwRa21pcF9jbG1l
bnRfb250YXAxHzAdBgkqhkiG9w0BCQEWEGVza21AdXRpbWFjby5jb20wgGEmMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvaOZ0Vy3wJcITin1S19GCZtF1NFZT
KgbZedyQ75dFbwKvWzbhSa/Q8BTjSX2CAyUHJMbbWSiwCmC0dEkvGdLIakStggJ
31Yfq8SH8EhGb3d4iMIhYy9VTOV0d80Jq3WX5ltaJ+zTmkNcSw9ftvew4JrcDGMa
DawEKxAxL5BUiD8SaZVIOErakw0WnHQe5gi+y1RTvhUXmsYxShVZQp5emWmqn8pG
MAv+RekQwSNkiDmsQ3LVLzGVP6DyAVqJQnd0IcKup1aCynn0NQaelftOz5d7QkpT
2KWBsRRw9MkmthOMN2AfXFhVk+g1HPpJEp0lM//WahK/iq/i8i4YsxCTAgMBAAGj
YDBEMAkGA1UdEwQCMAAwHQYDVR0OBBYEFK/4qdT+lzRTTWPW6zjcGCGCm00hMB8G
AlUdIwQYMBaAFNYGNr4gb0znQkxDZXdJ3owq7INWMBEGCWCsAGG+EIBAQQEAWIH
gDAKBggqhkiOPQQDAgOBjAAwgYgCQgFMcLKh5yfwmuCsA9F6Wu90W9U6pnJmDwFc
losQ500nkVDQbessLYMuyfLPPW4n1CwPR4C8DJa5jmG6sxoAWa2nUAJCA07ASmHp
gI9D/3dD0RouFwp5Ua08OfhSoWTWtEtVp7KeUYXL42+rcPQu7QZ3VHr3BYM/Wtkw
9a+jmyPgPbpKQi6y
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAcwggSjAgEAAoIBAQCvaOZ0Vy3wJcIT
in1S19GCZtF1NFZTKgbZedyQ75dFbwKvWzbhSa/Q8BTjSX2CAyUHJMbbWSiwCmC
0dEkvGdLIakStggJ31Yfq8SH8EhGb3d4iMIhYy9VTOV0d80Jq3WX5ltaJ+zTmkNc
Sw9ftvew4JrcDGMAv+RekQwSNkiDmsQ3LVLzGVP6DyAVqJQnd0IcKup1aCynn0
NQaelftOz5d7QkpT2KWBsRRw9MkmthOMN2AfXFhVk+g1HPpJEp0lM//WahK/iq/i
8i4YsxCTAgMBAECCggEAN4+7x8hBldpu0+XXMolCYNLesAhm+6rJ9ZdaI5iPuP6E
```

```

8i4YsxCTAgMBAAEcGgEAN4+7x8hBldpuO+XXMo1CYNLesAhm+6rJ9ZdaI5iPuP6E
dMZxr8sqbdUxG4YPKzJ7gYLXmg15ng/OViCoPcGr2mGMI5AjVbTmhNuswf57dkwi
hLyU+WxodtWHRo+usXHtKrNd5l3VJ2WqxpZEBWZ4aL+Mbf1CeumvxJY7Z8kQJ6YF
IWPkKMBkRclYenMefw77iujXP9t18bMNG6qmukZjUT30mXEy2jf3Jl+xDxVwNhrj
S3YFrTMFnrdNjYcZLQZOizCVOrkKg+LreedYuBziGMikgzLJOSZ/z+2YEgixI3kl
6g0b18EBYpDwDqnR816eSlP87rUPoyzh4lm49nrh+QKBgQDx0Ln52cOi9de7QDqk
RNQyMuhX4oiXlgh/Uf8ONr5LSv3zWnF51K9+ySW3l2Ees2RR7Xp0iqoYQFENfcx
lfHCFgkPg4ndW4AflK0z2AX5KFStmF8nQte4HC9nFexfk11EE6/3pjuTWI4RGQ7K
xV6+XIY8iCQEH9WxVfS+LAMrzwKBgQC5svrTWWLGLbFKUUNaQG6EmgOwSJRJP/xa
l2zWXNiITlqC7699AY3zsdEKIE2Q5oF50dWLRlXckgaQuV9lCwtPLbEbHG/Me1Fp
ZMRXJEQQi3nsZEIy/OGXmPaF3FyKcAddeKoP9Kv+/bWc2E/VZvY+wpoQxE21li3c
B9V3H7sr/QKBgBcUU9u75Ac2rZtqmu44v4P3BePldBIB1JfKTKyfnvPyuWAznqcB
HKreKeJm6VcTyhxjrQ9YeLmN0e6MyQ0F4KgkELRzCO7avQYrZtIH/HS3poe8938
bdHfQEr3dbL9jqZDtsTNMdxzVEPff2DtC4jhrdIzMDTafhPJ320TKE5TAoGBAJoz
kkqJlrx4txFmFA3Zzr7ZGBN3LQOEtB/rGiQseiOle8XVM3w9zxGjBY/EltqWLNwi
FoVfkbZYLwW7gfrF/Xg6zinJaYdzgVsvNRbaCYvJAOKHK6MRYlI2z8PISnmgNhJy
hWHXTRqJmGAJgzMQ+qsZzJGFJl6pJZxdUau0ufYVAoGAAfe4kzT2DUSEltrJfYoD
n+wVtxcBb/SIdWyKCaSCUgcHDkeONSXLnnQwLi9k0nhlf43Kf9WXOmonCXV0YC/8
0EVZefAsOACiGbkTsmnKscDYIcLvVUworlXnSAm0iRRFbnc2B6ImOvD7byicSx60
bevm0zgZ0ZmtrOS6ySbv7aE=
-----END PRIVATE KEY-----

```

Enter certificates of certification authorities (CA) which form the certificate chain of the client certificate. This starts with the issuing CA certificate of the client certificate and can range up to the root CA certificate.

Do you want to continue entering root and/or intermediate certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

```

CA: ESKMLocalCA
serial: 0C

```

The certificate's generated name for reference: kmip_client_ontap

```

cluster1::> █

```

Figure 12 : Client Certificate & Private Key Installation.

5.2.2 Installing the Utimaco ESKM Server Certification Authority (CA) Certificate

Run the below command to install the certificate.

>_Console

```
cluster1::> security certificate install -type server-ca
```

If prompted to enter the Server CA certificate, paste the ESKM Server CA certificate.

```
cluster1::> security certificate install -type server-ca

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDDzCCAnGgAwIBAgIBADAKBggqhkiG9w0BCQEWGgluZm9zZWNAb3JnYW5pemF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZW51cm10eTEUMBIGA1UEAxMLRVNL
TUxvY2FsQ0ExJzAlBglkqhkiG9w0BCQEWGgluZm9zZWNAb3JnYW5pemF0aW9uLmNv
bTAeFw0yNTA2MDkyMDI1MTNaFw0zNTA2MDgyMDI1MTNaMIGiMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExETAPBgNVBACtCENhbXBiZWxsMRUwEwYDVQQKEwxFcmVh
bml6YXRpb24xHTAbBgNVBAsTFEluZm9ybWF0aW9uIFNlY3VyaXR5MRQwEgYDVQQD
EwtFU0tNTG9jYWxkQ0TEncMCUGCSqGSIb3DQEJARYYaW5mb3NlY0Bvcmdhbml6YXRp
b24uY29tMIGbMBAGByqGSM49AgEGSuBBAAjA4GGAAQawz3C0rSGysFVn8XOY3sc
o2VdhtWaNvfNggRJSoteM1UVKDNKM4cw/Hbh/hiO+yh2NaTj178RcCyu/Yz/gIav
aRgAPVx3PIcJpkwgo5TCtRZ/Jh1AYJ93SdGsFnSO+OmW9USRGazYhYcjpIjN0MM
gCI2cu7Wocmhq/rVR7SNVcIK4mqjUzBRMB0GA1UdDgQWBBTWbja+IG9M50JM2V3
Sd6MKuyDVjAfBgNVHSMEGDAWgBTWbja+IG9M50JM2V3Sd6MKuyDVjAPBgNVHRMB
Af8EBTADAQH/MAoGCCqGSM49BAMCA4GLADCBhwJCADEyLQJMsoKWjXPS0nFSwQsy
w3r9FGuk2S/0rX8kUI+CwS90fL0hHC8V/7CX2zvaRtwXLxvEA+VjflDXPblHIoWN
AkFX2rLKvpTWqo8OQFtaYuSNM/cOqgsyQcjaXDHyQ0mlwbgkoed6ofgjBP6Q0Kl8
F9vpxmVbsi+ADXKMrIVU6ogBMQ==
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ESKMLocalCA
serial: 00

The certificate's generated name for reference: ESKMLocalCA
```

Figure 13 : Server CA Certificate Installation.

5.2.3 Adding the Utimaco ESKM as Key Control Nodes on ONTAP

Run the command below to enable the external key manager.

>_Console

```
Cluster1::> security key-manager external enable -key-servers
192.168.182.164:5696 -client-cert kmip_client_ontap -server-ca-certs
ESKMLocalCA
```

5.2.4 Verifying the communication between the external Key Manager and ONTAP

Run the command below to show the status of the key manager.

>_Console

```
Cluster1::> security key-manager show -status
```

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	10.222.55.178	available

Figure 14 : Key manager status.

6 Verification and Testing

In this chapter, we will validate the integration between Utimaco ESKM and NetApp ONTAP. This includes confirming KMIP-based connectivity, verifying that encryption keys are properly generated, stored, and retrieved by ONTAP, and ensuring that volume encryption workflows — such as enabling NVE (NetApp Volume Encryption) or transitioning volumes — function as expected. By the end of this section, you should be able to confirm that the integration is fully operational and that ONTAP volumes are securely encrypted using keys managed by Utimaco ESKM.

6.1 Performing NetApp Volume Encryption

6.1.1 Enabling Aggregate-level Encryption

If you plan to perform inline or background aggregate-level deduplication, you must use aggregate-level encryption. NVE does not support aggregate-level deduplication otherwise. When you encrypt a volume, ONTAP automatically “pushes” an encryption key to the Utimaco ESKM server.



Plain text volumes are not supported in NAE aggregates

Enable or disable aggregate-level encryption.

1. The following command enables aggregate-level encryption on aggr1.

>_Console

```
Cluster1::> storage aggregate create -aggregate aggr1 -diskcount 6
```

2. Verify that the aggregate aggr1 is enabled for encryption.

>_Console

```
Cluster1::> storage aggregate show -fields encrypt-with-aggr-key
```

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate          encrypt-with-aggr-key
-----
aggr0_cluster1_01 false
aggr1              true
2 entries were displayed.
```

Figure 15: Verifying encryption on aggregate.

6.1.2 Enabling Encryption on a New Volume

1. Create a new SVM (Storage Virtual Machine).

>_Cluster

```
Cluster1::> vservers create -vservers svm1
```

2. Create a new volume and verify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default, the volume will be an NAE volume.

>_Cluster

```
Cluster1::> volume create -vservers SVM_name -volume volume_name - aggregate
aggregate_name
```

Example

```
Cluster1::> volume create -vservers svm1 -volume vol0 -aggregate aggr1
```

3. View the newly created NAE volume.

>_Cluster

```
Cluster1::> volume show -vservers svm1 -volume vol0
```

```
cluster1::> volume show -vserver svml -volume vol0

Vserver Name: svml
Volume Name: vol0
Aggregate Name: aggr1
List of Aggregates for FlexGroup Constituents: aggr1
Encryption Type: aggregate
List of Nodes Hosting the Volume: cluster1-01
Volume Size: 20MB
Volume Data Set ID: 1026
Volume Master Data Set ID: 2154299374
Volume State: online
Volume Style: flex
Extended Volume Style: flexvol
FlexCache Endpoint Type: none
Is Cluster-Mode Volume: true
Is Constituent Volume: false
Number of Constituent Volumes: -
Export Policy: default
User ID: 0
Group ID: 0
Security Style: unix
UNIX Permissions: ---rwxr-xr-x
Junction Path: -
Junction Path Source: -
Junction Active: -
Junction Parent Volume: -
Comment:
Available Size: 18.77MB
Filesystem Size: 20MB
Total User-Visible Size: 19MB
Used Size: 240KB
Used Percentage: 1%
Volume Nearly Full Threshold Percent: 95%
Volume Full Threshold Percent: 98%
Maximum Autosize: 24MB
Minimum Autosize: 20MB
Autosize Grow Threshold Percentage: 85%
Autosize Shrink Threshold Percentage: 50%
Autosize Mode: off
```

Figure 16 : Volume show output.

4. Create an NVE volume.

>_Cluster

```
Cluster1::> volume create -vserver SVM_name -volume volume_name - aggregate  
aggregate_name -encrypt true
```

Example:

```
Cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -  
encrypt true
```

5. View the newly created NVE Volume.

>_Cluster

```
Cluster1::> volume show -vserver svm1 -volume vol1
```

```
cluster1::> volume show -vserver svml -volume voll

                                Vserver Name: svml
                                Volume Name: voll
                                Aggregate Name: aggr1
List of Aggregates for FlexGroup Constituents: aggr1
                                Encryption Type: volume
List of Nodes Hosting the Volume: cluster1-01
                                Volume Size: 20MB
                                Volume Data Set ID: 1027
Volume Master Data Set ID: 2154299375
                                Volume State: online
                                Volume Style: flex
                                Extended Volume Style: flexvol
FlexCache Endpoint Type: none
                                Is Cluster-Mode Volume: true
                                Is Constituent Volume: false
Number of Constituent Volumes: -
                                Export Policy: default
                                User ID: 0
                                Group ID: 0
                                Security Style: unix
                                UNIX Permissions: ---rwxr-xr-x
                                Junction Path: -
                                Junction Path Source: -
                                Junction Active: -
                                Junction Parent Volume: -
                                Comment:
                                Available Size: 18.76MB
                                Filesystem Size: 20MB
Total User-Visible Size: 19MB
                                Used Size: 248KB
                                Used Percentage: 1%
Volume Nearly Full Threshold Percent: 95%
Volume Full Threshold Percent: 98%
                                Maximum Autosize: 24MB
                                Minimum Autosize: 20MB
Autosize Grow Threshold Percentage: 95%
```

Figure 17 : Volume show output.

6. Verify that volumes are enabled for encryption.

```
>_Cluster
```

```
Cluster1::> volume show -is-encrypted true
```

```
cluster1::> volume show -is-encrypted true
Vserver   Volume      Aggregate   State    Type    Size   Available  Used%
-----
svml      svml_root   aggr1       online   RW      20MB   18.72MB    1%
svml      vol0        aggr1       online   RW      20MB   18.75MB    1%
svml      vol1        aggr1       online   RW      20MB   18.74MB    1%
3 entries were displayed.
```

Figure 18 : Verifying encrypted volumes.

6.1.3 Enabling Encryption on an Existing Volume with the Volume Encryption Conversion Start Command

1. Create a new aggregate aggr2 without encryption.

```
>_Console

Cluster1:> storage aggregate create aggr2 -diskcount 5 -encrypt-with-aggr-
key false

cluster1::> storage aggregate create aggr2 -diskcount 5 -encrypt-with-aggr-key false
Info: The layout for aggregate "aggr2" on node "cluster1-01" would be:

First Plex

RAID Group rg0, 5 disks (block checksum, raid_dp)

Position  Disk          Type          Usable Physical
-----
dparity   NET-1.15      FCAL          -         -
parity    NET-1.24      FCAL          -         -
data      NET-1.16      FCAL          1000MB    1.00GB
data      NET-1.25      FCAL          1000MB    1.00GB
data      NET-1.17      FCAL          1000MB    1.00GB

Aggregate capacity available for volume use would be 2.64GB.

Do you want to continue? {y|n}: y
[Job 44] Job succeeded: DONE
```

Figure 19 : Create aggregate without encryption.

2. Create a plain text volume vol2 by running the command below.

>_Console

```
Cluster1::> volume create -volume vol2 -aggregate aggr2 -encrypt false
```

3. View the volume vol2 by running the command below.

>_Console

```
Cluster::> volume show -volume vol2 -vserver svml
```

```
cluster1::> volume show -volume vol2 -vserver svml
                                     Vserver Name: svml
                                     Volume Name: vol2
                                     Aggregate Name: aggr2
List of Aggregates for FlexGroup Constituents: aggr2
                                     Encryption Type: none
List of Nodes Hosting the Volume: cluster1-01
                                     Volume Size: 20MB
                                     Volume Data Set ID: 1030
Volume Master Data Set ID: 2154299378
                                     Volume State: online
                                     Volume Style: flex
Extended Volume Style: flexvol
FlexCache Endpoint Type: none
Is Cluster-Mode Volume: true
Is Constituent Volume: false
Number of Constituent Volumes: -
                                     Export Policy: default
                                     User ID: 0
                                     Group ID: 0
                                     Security Style: unix
UNIX Permissions: ---rwxr-xr-x
                                     Junction Path: -
Junction Path Source: -
Junction Active: -
Junction Parent Volume: -
Comment:
Available Size: 18.74MB
Filesystem Size: 20MB
Total User-Visible Size: 19MB
Used Size: 264KB
```

Figure 20 : Volume show output.

- Convert the existing volume vol2 (plain text volume) to an encrypted volume by running the command below.

```

>_Console

cluster1::> volume encryption conversion start -vserver SVM_name -volume
volume_name

Example:

Cluster1::> volume encryption conversion start -vserver svm1 -volume vol2

cluster1::> volume encryption conversion start -vserver svm1 -volume vol2
Warning: Conversion from non-encrypted to encrypted volume scans and encrypts all of the data in the specified volume. It might take a significant amount of
time, and might degrade performance during that time.
Do you want to continue? [y/n]: y
Conversion started on volume "vol2". Run "volume encryption conversion show -volume vol2 -vserver svm1" to see the status of this operation.
cluster1::> volume encryption conversion show -volume vol2 -vserver svm1
Vserver Name: svm1
Volume Name: vol2
Start Time: 6/25/2025 20:07:56
Status: running

```

Figure 21 : Volume encryption conversion start running.

- When the conversion operation is complete, verify that the volume is enabled for encryption.

```

>_Console

Cluster1::> volume show -is-encrypted true

cluster1::> volume show -is-encrypted true
Vserver   Volume      Aggregate   State   Type   Size   Available   Used%
-----
svm1      svm1_root   aggr1       online  RW     20MB   18.69MB    1%
svm1      vol0        aggr1       online  RW     20MB   18.72MB    1%
svm1      vol1        aggr1       online  RW     20MB   18.71MB    1%
svm1      vol2        aggr2       online  RW     20MB   18.75MB    1%
4 entries were displayed.

```

Figure 22 : Verifying encrypted volumes.

6.1.4 Enabling Encryption on an Existing Volume with the Volume Move Start command

You can use the volume move start command to enable encryption by moving an existing volume.

1. Move an NAE volume to an NVE volume (vol0 is an NAE volume will convert this to NVE volume) and verify its status.

>_Console

```
cluster1::>volume move start -vserver SVM_name -volume volume_name -
destination-aggregate aggregate_name -encrypt-with-aggr-key false
```

Example:

```
Cluster1::> volume move start -vserver svm1 -volume vol0
-destinationaggregate aggr1 -encrypt-with-aggr-key false
```

```
Cluster1::> volume move show -vserver svm1 -volume vol0
```

```
cluster1::> volume move start -vserver svm1 -volume vol0 -destination-aggregate aggr1 -encrypt-with-aggr-key false
[Job 51] Job is queued: Move "vol0" in Vserver "svm1" to aggregate "aggr1". Use the "volume move show -vserver svm1 -volume vol0" command to view the status of this operation.
```

```
cluster1::> volume move show -vserver svm1 -volume vol0
```

```

Vserver Name: svm1
Volume Name: vol0
Actual Completion Time: -
Bytes Remaining: -
Destination Aggregate: aggr1
Detailed Status: Volume move job preparing transfer
Estimated Time of Completion: -
Managing Node: cluster1-01
Percentage Complete: -
Move Phase: replicating
Estimated Remaining Duration: -
Replication Throughput: -
Duration of Move: 00:00:02
Source Aggregate: aggr1
Start Time of Move: Wed Jun 25 20:17:02 2025
Move State: healthy
Is Source Volume Encrypted: true
Encryption Key ID of Source Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a1000000000000000
Is Destination Volume Encrypted: true
Encryption Key ID of Destination Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a100000000000000000
```

```
cluster1::> volume move show -vserver svml -volume vol0

      Vserver Name: svml
      Volume Name: vol0
Actual Completion Time: Wed Jun 25 20:17:26 2025
      Bytes Remaining: -
Destination Aggregate: aggr1
      Detailed Status: Successful
Estimated Time of Completion: -
      Managing Node: cluster1-01
      Percentage Complete: 100%
      Move Phase: completed
Estimated Remaining Duration: -
Replication Throughput: -
      Duration of Move: 00:00:24
      Source Aggregate: aggr1
      Start Time of Move: Wed Jun 25 20:17:02 2025
      Move State: done
      Is Source Volume Encrypted: true
Encryption Key ID of Source Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a10000000000000000
      Is Destination Volume Encrypted: true
Encryption Key ID of Destination Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a10000000000000000
```

Figure 23 : Moving an NAE volume to an NVE volume.

2. View the volume vol0 once the operation is completed.

>_Console

```
cluster1::> volume show -volume vol0 -vserver svml
```

```
cluster1::> volume show -volume vol0 -vserver svml

Vserver Name: svml
Volume Name: vol0
Aggregate Name: aggr1
List of Aggregates for FlexGroup Constituents: aggr1
Encryption Type: volume
List of Nodes Hosting the Volume: cluster1-01
Volume Size: 20MB
Volume Data Set ID: 1032
Volume Master Data Set ID: 2154299374
Volume State: online
Volume Style: flex
Extended Volume Style: flexvol
FlexCache Endpoint Type: none
Is Cluster-Mode Volume: true
Is Constituent Volume: false
Number of Constituent Volumes: -
Export Policy: default
User ID: 0
Group ID: 0
Security Style: unix
UNIX Permissions: ---rwxr-xr-x
Junction Path: -
Junction Path Source: -
Junction Active: -
Junction Parent Volume: -
Comment:
Available Size: 18.66MB
Filesystem Size: 20MB
Total User-Visible Size: 19MB
```

Figure 24 : Volume show output.

3. Move an NVE volume to an NAE volume (vol0 is an NVE volume will convert this to NAE volume) and verify its status.

>_Console

```
Cluster1::> volume move start -vserver SVM_name -volume volume_name -
destination-aggregate aggregate_name -encrypt-with-aggr-key true
```

For example:

```
Cluster1::> volume move start -vserver svm1 -volume vol0 -destination-
aggregate aggr1 -encrypt-with-aggr-key true
```

```
Cluster1::> volume move show -vserver svm1 -volume vol0
```

```
cluster1::> volume move start -vserver svm1 -volume vol0 -destination-aggregate aggr1 -encrypt-with-aggr-key true
[Job 52] Job is queued: Move "vol0" in Vserver "svm1" to aggregate "aggr1". Use the "volume move show -vserver svm1 -volume vol0" command to view the status
of this operation.

cluster1::> volume move show -vserver svm1 -volume vol0

      Vserver Name: svm1
      Volume Name: vol0
      Actual Completion Time: -
      Bytes Remaining: -
      Destination Aggregate: aggr1
      Detailed Status: Volume move job preparing transfer
      Estimated Time of Completion: -
      Managing Node: cluster1-01
      Percentage Complete: -
      Move Phase: replicating
      Estimated Remaining Duration: -
      Replication Throughput: -
      Duration of Move: 00:00:02
      Source Aggregate: aggr1
      Start Time of Move: Wed Jun 25 20:33:17 2025
      Move State: healthy
      Is Source Volume Encrypted: true
      Encryption Key ID of Source Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a10000000000000000
      Is Destination Volume Encrypted: true
      Encryption Key ID of Destination Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a100000000000000000

cluster1::> volume move show -vserver svm1 -volume vol0

      Vserver Name: svm1
      Volume Name: vol0
      Actual Completion Time: Wed Jun 25 20:33:39 2025
      Bytes Remaining: -
      Destination Aggregate: aggr1
      Detailed Status: Successful
      Estimated Time of Completion: -
      Managing Node: cluster1-01
      Percentage Complete: 100%
      Move Phase: completed
      Estimated Remaining Duration: -
      Replication Throughput: -
      Duration of Move: 00:00:22
      Source Aggregate: aggr1
      Start Time of Move: Wed Jun 25 20:33:17 2025
      Move State: done
      Is Source Volume Encrypted: true
      Encryption Key ID of Source Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a10000000000000000
      Is Destination Volume Encrypted: true
      Encryption Key ID of Destination Volume: 0000000000000000200000000000500fb8dd9b93aa9e158d630443bbf4b96a100000000000000000
```

Figure 25 : Moving an NVE volume to an NAE volume.

4. View the volume vol0 once the operation is completed.

>_Console

```
cluster1::> volume show -volume vol0 -vserver svm1
```

```
cluster1::> volume show -volume vol0 -vserver svm1
                                     Vserver Name: svm1
                                     Volume Name: vol0
                                     Aggregate Name: aggr1
List of Aggregates for FlexGroup Constituents: aggr1
                                     Encryption Type: aggregate
List of Nodes Hosting the Volume: cluster1-01
                                     Volume Size: 20MB
                                     Volume Data Set ID: 1033
Volume Master Data Set ID: 2154299374
                                     Volume State: online
                                     Volume Style: flex
Extended Volume Style: flexvol
FlexCache Endpoint Type: none
Is Cluster-Mode Volume: true
Is Constituent Volume: false
Number of Constituent Volumes: -
Export Policy: default
User ID: 0
Group ID: 0
Security Style: unix
UNIX Permissions: ---rwxr-xr-x
Junction Path: -
Junction Path Source: -
Junction Active: -
Junction Parent Volume: -
Comment:
Available Size: 18.58MB
```

Figure 26 : Volume show output.

7 Logs and Validation Steps

ONTAP volume encryption creates cryptographic keys on Utimaco ESKM, which are then used to encrypt and decrypt the volumes. You can verify the logs from Utimaco ESKM.

1. Open the Utimaco ESKM page and click on the **Device** tab.
2. Click on **Log Viewer** under **Logs & Statistics**.
3. Click on **KMIP** under **Log Viewer**.
4. Review the logs.

The screenshot shows the 'Log File: Current (Showing Last 25 Lines)' interface. On the left is a navigation menu with sections: Administrators, Logs & Statistics (expanded), and Maintenance. Under 'Logs & Statistics', 'Log Viewer' is expanded to show 'System', 'Audit', 'Activity', 'Client Event', 'KMIP' (selected), 'KMIP Traffic', 'REST', and 'Statistics'. Below the menu are buttons for 'Download Entire Log' and 'Clear'. The main area displays a 'KMIP Log' with 25 lines of log entries. Each entry includes a timestamp (2025-06-25), time (e.g., 20:06:23), source ([KMIP Server]), operation type ([ClientOperation]), user ([kmp_client_ontap_11]), UUID, and operation result ([SUCCESS]).

Figure 27 : KMIP logs.

5. To view the keys, go to the **Security** tab
6. Select **KMIP Objects** under the **Keys & KMIP Objects** section
7. The generated keys will be displayed here.

Keys & KMIP Objects

- ▶ Keys
- ▼ KMIP Objects
 - KMIP Objects
 - Create KMIP Objects
 - Cloud Integration
 - Authorization Policies

Security / KMIP Objects / KMIP Objects

KMIP Object Configuration

vESKM_Integration_3
Logged in as admin

[Help ?](#)

Query:

Items per page: Page of 22 [Next >](#)

UUID	Object Name	Owner	Object Type	State	Creation Date	FIPS Security Level
<input checked="" type="radio"/> 38e17cc5-c6eb-4b90-b353-fc1b0812ffd4	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 03:07:54	1
<input type="radio"/> 36fd307c-4900-4d1c-84cd-4b16f0899087	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 03:07:54	1
<input type="radio"/> 5dafaa065-6080-4b4c-a4c8-2bcb82949f08	-	kmip_client_ontap_11	SymmetricKey	Destroyed	2025-06-26 03:02:37	1
<input type="radio"/> 2e87645a-b5d0-4972-9a6d-593d78f3cf65	-	kmip_client_ontap_11	SymmetricKey	Destroyed	2025-06-26 03:02:37	1
<input type="radio"/> 0240f248-e1ff-4585-9b93-2ab40895244b	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 02:37:22	1
<input type="radio"/> 87efce4a-b85f-484f-8d92-6924b969a2a2	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 02:37:21	1
<input type="radio"/> b64be5d6-ccc5-4a3e-84f3-798f7c26be99	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 02:28:35	1
<input type="radio"/> cbc539aa-9bdb-410d-950a-bc1e72d8968f	-	kmip_client_ontap_11	SymmetricKey	Active	2025-06-26 02:28:35	1
<input type="radio"/> a831ae3b-59ce-4fd1-8e1e-ff73f0348f5c	-	kmip_client_ontap_11	SymmetricKey	Destroyed	2025-06-26 02:26:40	1
<input type="radio"/> ab18cad5-9757-498b-8e9c-7aff96684069	-	kmip_client_ontap_11	SymmetricKey	Destroyed	2025-06-26 02:26:40	1

1 - 10 of 214

[Next >](#)

Figure 28 : KMIP Objects.

8 Troubleshooting

8.1 Common Issues

Error	Diagnosis
<pre>volume move start -vserver svm1 -volume svm1_root -destination-aggregate aggr1 -encrypt-with-aggr-key false</pre> <p>Error:</p> <p>command failed: Encryption of the Vserver root volume using NVE (NetApp Volume Encryption) is not supported. Vserver root volumes only support encryption using NAE (NetApp Aggregate Encryption). You can encrypt the volume by moving it to an aggregate that supports NAE, using the "volume move start svm_root -vserver svm1 -encrypt-destination true -encrypt-with-aggr-key true" command.</p>	<pre>cluster1::> storage aggregate create -aggregate aggr2 -diskcount 6 -encrypt-with- aggr-key false</pre>

Table 8: List of Error and its Diagnosis.

8.2 Managing the Client and CA Certificates on ONTAP

8.2.1 Deleting Certificates

Before you begin installing the new certificates, you must remove the old certificates and make sure to use updated certificates.

1. Disable the connection to the key management (KMIP) server.

```
>_Console
Cluster1::> security key-manager delete -address
```

2. Remove certificates for the cluster.

>_Console

```
Cluster1::> security certificate delete -vserver cluster1 -type client  
-common-name kmip_client_on_tap_11 -ca ESKMLocalCA -serial 0D
```

8.2.2 Replacing the ESKM Client Certificates

ESKM Client certificates have an expiration period after initial creation. After a predetermined time, the certificates are no longer valid. They should be replaced before the expiration date. Follow the steps in [Creatng a Client Certificate for ONTAP \(Using OpenSSL\)](#).

8.3 Contact for support

8.3.1 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

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

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

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

8.3.2 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)

9 Appendices

9.1 References

This document serves as a comprehensive guide for integrating Utimaco's ESKM module with NetApp ONTAP.

For more information on other Utimaco products and offerings, please visit the official [Utimaco Website](#).