NetApp

ONTAP

9.11.1P4

Integration Guide

ESKM

8.4.0 or later

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	0.0.1
Date	2026-03-24
Status	PUBLISHED
Document No.	IG-2025-0039

Table of Contents

1 Introduction 5
1.1 About This Guide 5
1.1.1 Target Audience for This Guide 5
1.1.2 Document Conventions 5
1.1.3 Abbreviations 6
2 Overview 9
2.1 NetApp ONTAP 9
2.2 Utimaco ESKM 9
3 Integration Requirements and Prerequisites 10
3.1 Tested Versions 10
3.2 Software Requirements 10
3.3 Hardware Requirements 10
3.4 Prerequisites 11
4 Installing and Configuring Utimaco ESKM Server 12
4.1 First Run 12
4.2 Setting Up Local CA 15
4.2.1 Add a Third-Party CA Certificate 17
4.3 Setting up ESKM Certificate 18
4.3.1 Import a Third-Party Server Certificate 22
4.4 Setup Cluster 23
4.4.1 Creating the Cluster 23
4.4.2 Adding ESKM Servers to the Cluster 24
4.5 Setup KMIP Server 26
5 Creating a Client Certificate for ONTAP 29
5.1 Configuring the ESKM Server 29
5.2 Configuring the KMIP Server Settings 29
5.3 Creating and Exporting a Client Certificate using ESKM 29
5.3.1 Creating Client Certificate 29
5.4 Create a Client Certificate and Key (Using openssl) 30
5.4.1 Create a CSR on the Client 30
5.4.2 Use the Local CA to Sign CSR 33

5.4.3 Exporting Certificate with Private Key from ESKM ... 36
6 Creating KMIP User and Password ... 37
7 Installing NetApp ONTAP using Simulate ONTAP ... 40
7.1 Deploying and Configuring a Two Node Cluster ... 40
8 Configuring ONTAP to use Utimaco ESKM ... 49
8.1 Importing the Client Certificate to ONTAP ... 49
8.2 Installing the Utimaco ESKM Server Certification Authority (CA) Certificate ... 51
8.3 Adding the Utimaco ESKM as Key Control Nodes on ONTAP ... 52
8.4 Verifying the communication between the external Key Manager and the cluster (ONTAP) ... 53
9 Performing NetApp Volume Encryption ... 54
9.1 Enabling Aggregate-level Encryption ... 54
9.2 Enabling Encryption on a New Volume ... 55
9.3 Enabling Encryption on an Existing Volume with the Volume Encryption Conversion Start Command ... 59
9.4 Enabling Encryption on an Existing Volume with the Volume Move Start command ... 60
10 Managing the Client and CA Certificates on ONTAP ... 64
10.1 Deleting Certificates ... 64
10.2 Replacing the ESKM Client Certificates ... 64
11 Troubleshooting ... 66
12 Further Information ... 67
13 References ... 68
14 Contact and Support Information ... 69

1 Introduction

This guide is part of the information and support provided by Utimaco. All Utimaco ESKM product documentation is available from Utimaco's web site at https://utimaco.com/.

1.1 About This Guide

This guide provides an integration explaining how to integrate Utimaco ESKM with NetApp ONTAP. Utimaco ESKM securely generates and stores the keys used by ONTAP for volume encryption.

1.1.1 Target Audience for This Guide

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

1.1.2 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 **OK**
`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 1: 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 indicates the expected result after the successful execution of an instruction.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CA	Certificate Authority
CN	Common Name
DHCP	Dynamic Host Configuration Protocol
ESKM	Enterprise Secure Key Manager
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IP	Internet Protocol

Abbreviation	Meaning
KMIP	Key Management Interoperability Protocol
KMS	Key Management System
NVE	NetApp Volume Encryption
ONTAP	On Net Transport Activation Process
PC	Personal Computer
PEM	Privacy Enhanced Mail
RAM	Random Access Memory
Abbreviation	*Meaning*
SCP	Secure Copy
SM	System Manager
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VT	Virtualization Technology

Abbreviation	Meaning
XML	Extensible Markup Language

Table 2: Abbreviations

2 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 that is built in to 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

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 the first industry-certified Key Management Interoperability Protocol (KMIP) v2.1 offering with market leading support for partner applications and pre-qualified solutions, integrating out-of-the-box with varied deployments, as well as custom integrations.

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 required software.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco ESKM with NetApp ONTAP.

NetApp Version	Utimaco ESKM Version
9.11.1P4	ESKM 8.4.0 or later

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
Netapp	9.11.1P4

Table 4: List of software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
ESKM	8.4.0 or later
RAM	6 GB of RAM for one instance of the simulator
RAM	12 GB of RAM for two instances of the simulator

Hardware	Hardware Requirements
Disk Space	40 GB of free disk space for each instance of the simulator
VT	VT support for Intel system

Table 5: List of hardware requirements

Setup an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/.

3.4 Prerequisites

Before you begin, please ensure that you have:

- Installed /set up the operating system as listed in Tested Versions.
- Installed /set up ESKM as listed in Tested Versions.
- Downloaded the NetApp ONTAP file from https://mysupport.netapp.com/ and installed it.
- Familiarized yourself with the NetApp ONTAP documents and setup process. Visit https://docs.netapp.com/us-en/ontap/ 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 Installing and Configuring Utimaco ESKM Server

ESKM server must be configured with specific values such as time zone, IP address, netmask, gateway, host name, and port number used for the ESKM Management Console interface.

If you have already setup the ESKM, then skip Setting up Local CA.

4.1 First Run

To configure the time zone, IP address, netmask, gateway, host name, and port number used for the ESKM Management Console interface, the following procedure must be performed once for each ESKM server. Ensure that the ESKM server is powered off before starting this procedure.

1. Power on the ESKM server by pressing the Power On/Standby button located behind the front bezel door.
2. When the startup sequence completes, the following prompt displays on the PC or laptop that is running the terminal emulator program (such as PuTTY):

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

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

Enter y.

3. Follow the prompts to enter the necessary information:

Press Enter to accept the default.

a. Admin account password. Be sure to record this value and store it in a safe place. The Security Officer will use the admin account to configure the ESKM servers.

Utimaco has no ability to assist or recover access if administrator credentials (username, password) are lost.

b. Time zone

c. Date

d. Time. The time is based on a 24–hour clock; there is no a.m. or p.m. designation. For example, 1:20 p.m. is 13:20:00

e. The static IPv4 address of the ESKM server. The ESKM server cannot obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server

f. Subnet mask

g. Default gateway

h. Hostname, including the domain. For example, eskm.example.com. The screen displays the information you entered and the message “Is this correct? (y/n):”If the information displayed is correct, enter y; if not, enter n and make the necessary corrections

i. Enable IPv6. If the ESKM server will be installed in an IPv6 network, enter y to the prompt and the confirmation prompt. If the ESKM server will not be installed in an IPv6 network, or you wish to enable IPv6 later, enter n. If you entered y, you will be prompted to specify the IPv6 address. If you know the IPv6 address enter y, and then at the next prompt enter the IPv6 address with prefix in this format

j. IPv6 address/prefix. The default prefix is /64.

If you do not know the IPv6 address, enter n. You can enter IPv6 addresses later using either the ESKM Management Console or Command Line Interface.

Only enable IPv6 if you are certain that the ESKM server is required to operate on an IPv6 network. Once enabled it cannot be disabled via the ESKM Management Console or the Command Line Interface.

Client systems can use IPv4 addresses to connect to the KMS and KMIP services running on the ESKM system. ESKM supports IPv6 addresses for clients that use either the KMIP or ESKM XML protocols and are on the same subnet as the ESKM server. The following ESKM features, which utilize SCP to move files, support IPv6 addresses: -

- backup, restore, scheduled backup, transfer logs, and software upgrade/install
- In addition, you can also use a server which has an IPv6 address to perform the following functions: -

- remotely administer the ESKM server via the ESKM Management Console or the command line interface-
- perform network diagnostics (ping and netstat)

If you decide later, after completing the setup process, that you need to enable IPv6 support, you can use the Command Line Interface command ipv6 enable, to enable IPv6. You can then use the ipv6 address command or the ESKM Management Console interface to specify the IPv6 address.

k. Web interface port number.

l. Press Enter to complete and save the configuration settings

At this point, you have given the setup program everything it needs. The ESKM creates SSH keys and also a self-signed Web Admin server certificate. They are used to authenticate the ESKM to users making SSH and Web Admin connections to the ESKM. Because the actual key is large, the ESKM displays the key fingerprint on the console, as shown below.

›_ Console

```
Creating certificate for Web administration server...
Creating certificate for signing logs...
```

```
Creating SSH host keys... SSH RSA key fingerprint:
2048 SHA256:aTp6A447vp8dOj43FTT5B/aux6V7zddPzNXxZB0C1SE
SSH ECDSA key fingerprint:
521 SHA256:BKO/EfVUKSFpIzVn/WiJ4fS+8CqLyGJSawoQAsvmUoM
SSH ed25519 key fingerprint:
256 SHA256:/hWJGM+7hzDRWPsyCP6/gKqWR99cgMh9/TV5WLTFIrs
Webadmin certificate fingerprint (SHA-1):
2048 64:50:e2:01:fb:2a:28:54:1a:3b:30:94:3b:25:b7:ff:97:73:13:70
Initializing key store. This could take several minutes. Performing KMIP setup
Starting services...
The Web-based Management Console will now be available at this URL:
<https://xxx.xxx.xxx.xxx:9443> This device has now been configured.
Press Enter to continue.
```

A log-in prompt display.

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

If necessary, you can install and specify a different server certificate for remote Web Administration. See the sub-section Configuring the web admin server certificate, which is in section 4 of the Enterprise Secure Key Manager 8.2.0 User Guide.

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

4.2 Setting Up Local CA

The local CA is used to sign and verify the server certificate and may also be used to sign client certificate requests. To create and install a local CA, perform the following steps:

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

Figure 1 : Create Local CA window

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

b. Enter your organizational information

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

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

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

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

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

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

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

e. Click Add.

f. Click Save.

Repeat the steps above any time when another local CA is needed. For example, you may want to create a KMIP Local CA to support the KMIP Certify/Re-certify operations.

4.2.1 Add a Third-Party CA Certificate

If your client certificates were signed by a third-party CA, you must install the third-party CA certificate, and then add it to the Trusted CA list.

To install a third-party CA certificate, perform the following steps:

1. In Certificates & CAs, click Known CAs to display the Install CA Certificate section.
2. Enter a value for the Certificate Name and paste the CA certificate text in the Certificate field.
3. Click Install. The CA certificate will be added to the Known CAs list.

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

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

6. Click Save.

4.3 Setting up ESKM Certificate

ESKM server certificates are used by the client to authenticate the ESKM server during the TLS/SSL handshake. ESKM supports two types of clients. Clients that use the ESKM protocol are referred to as ESKM clients. Clients that use the KMIP protocol are referred to as KMIPenabled clients. The ESKM clients communicate with the KMS server and KMIP-enabled clients communicate with the KMIP server.

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your ESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to

these server certificates should clearly indicate their purpose. For example: ESKM KMS Server and ESKM KMIP Server.

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

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

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

1. Click the Security tab.
2. In Certificates and CAs, select Certificates.
3. Enter information required by the Create Certificate Request section of the window to create the ESKM server certificate.

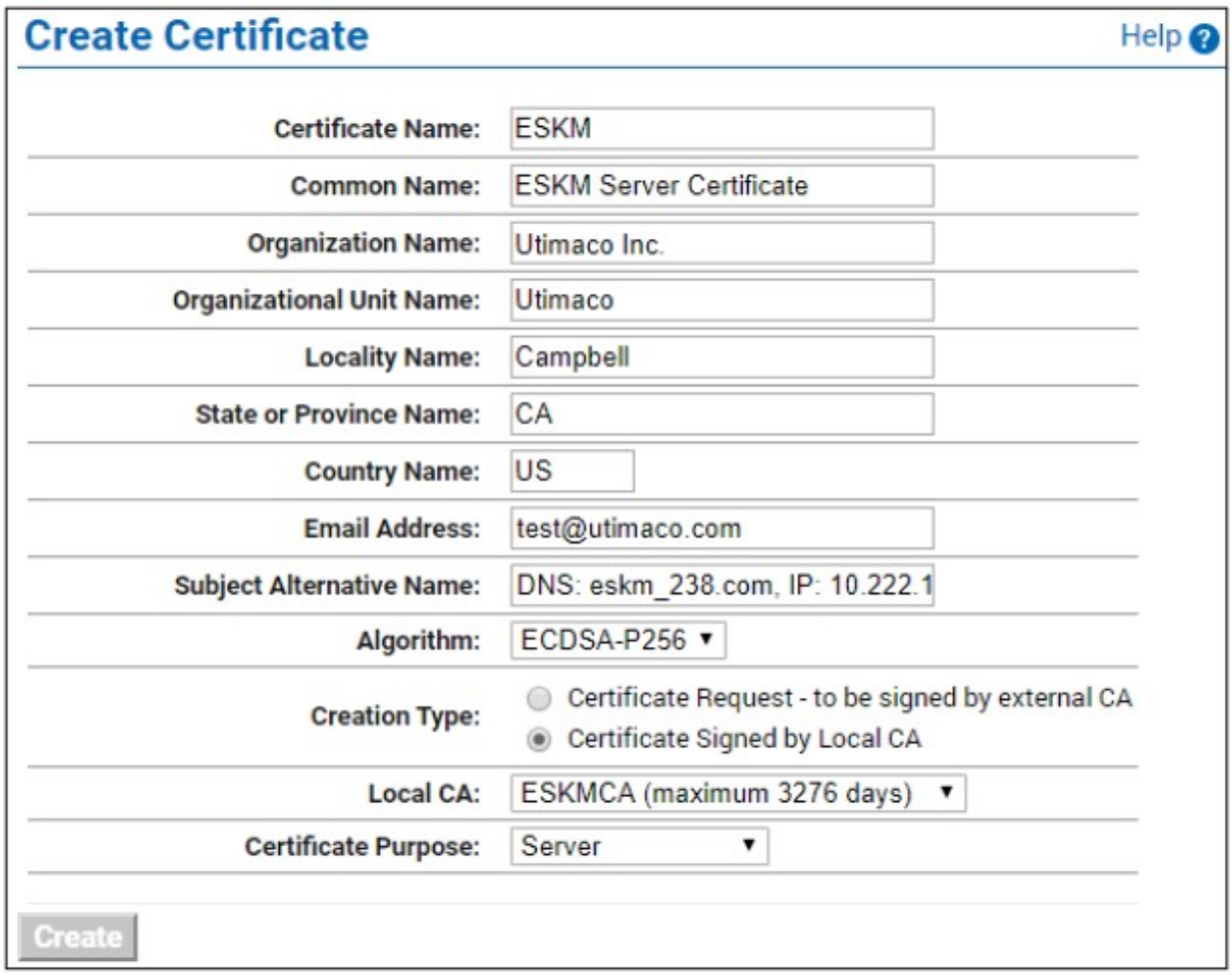


Figure 2 : Create Certificate window

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

b. Enter your Organizational information

c. Enter/Select the Subject Alternative Name, Algorithm, Creation Type, Local CA, and Certificate Purpose. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

4. Click Create.

5. The Certificate List will include the newly created certificate, its status will be Request Pending. Click on the certificate name. For example, ESKM Server Certificate.

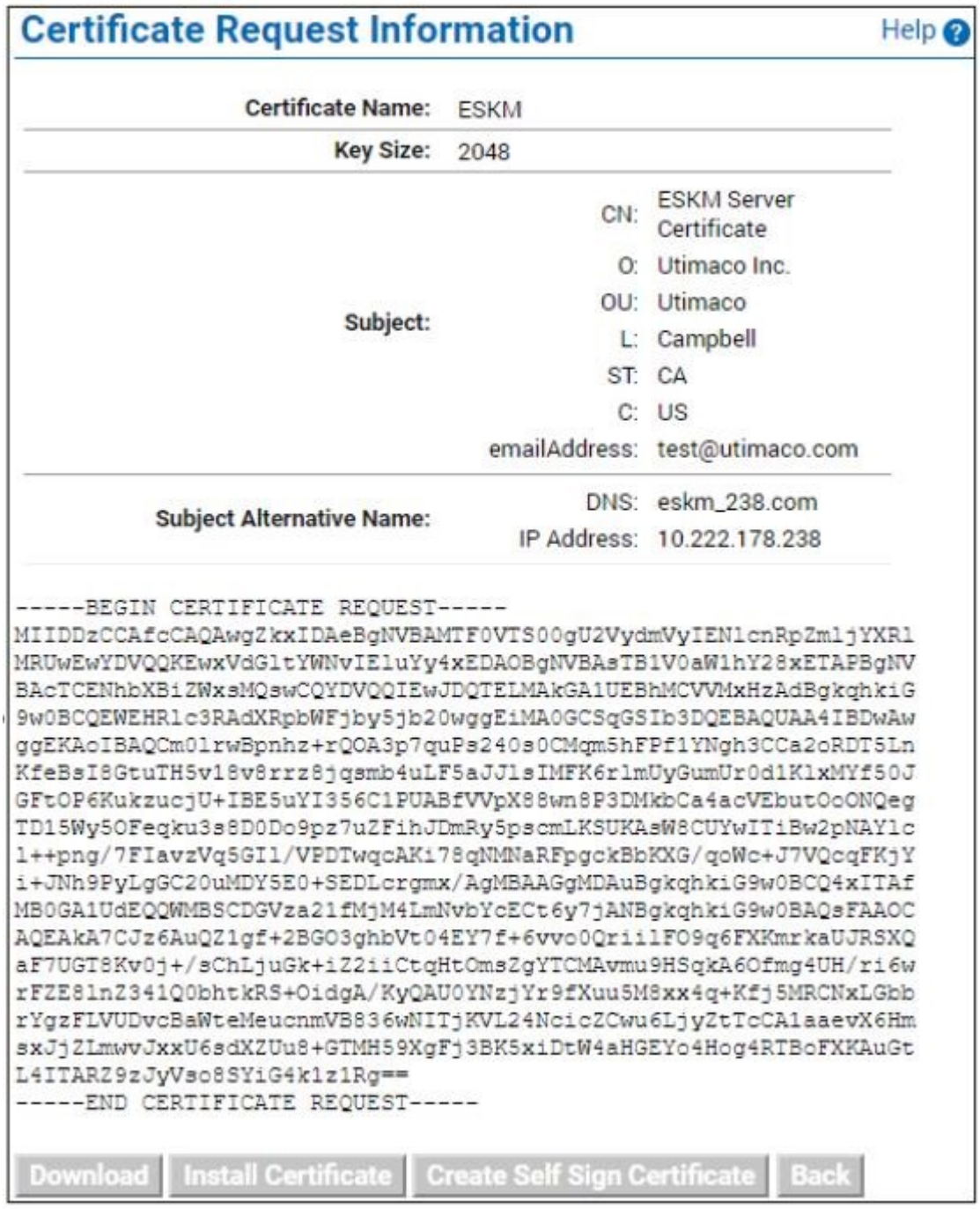


Figure 3 : Certificate Request Information window

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

6. In the Certificates & CAs menu, click Local Cas.

7. Click on the CA name you created in Setting up local CA for example ESKM Local CA.
8. Click Sign Request.
9. Enter data required by the Sign Certificate Request section of the window.

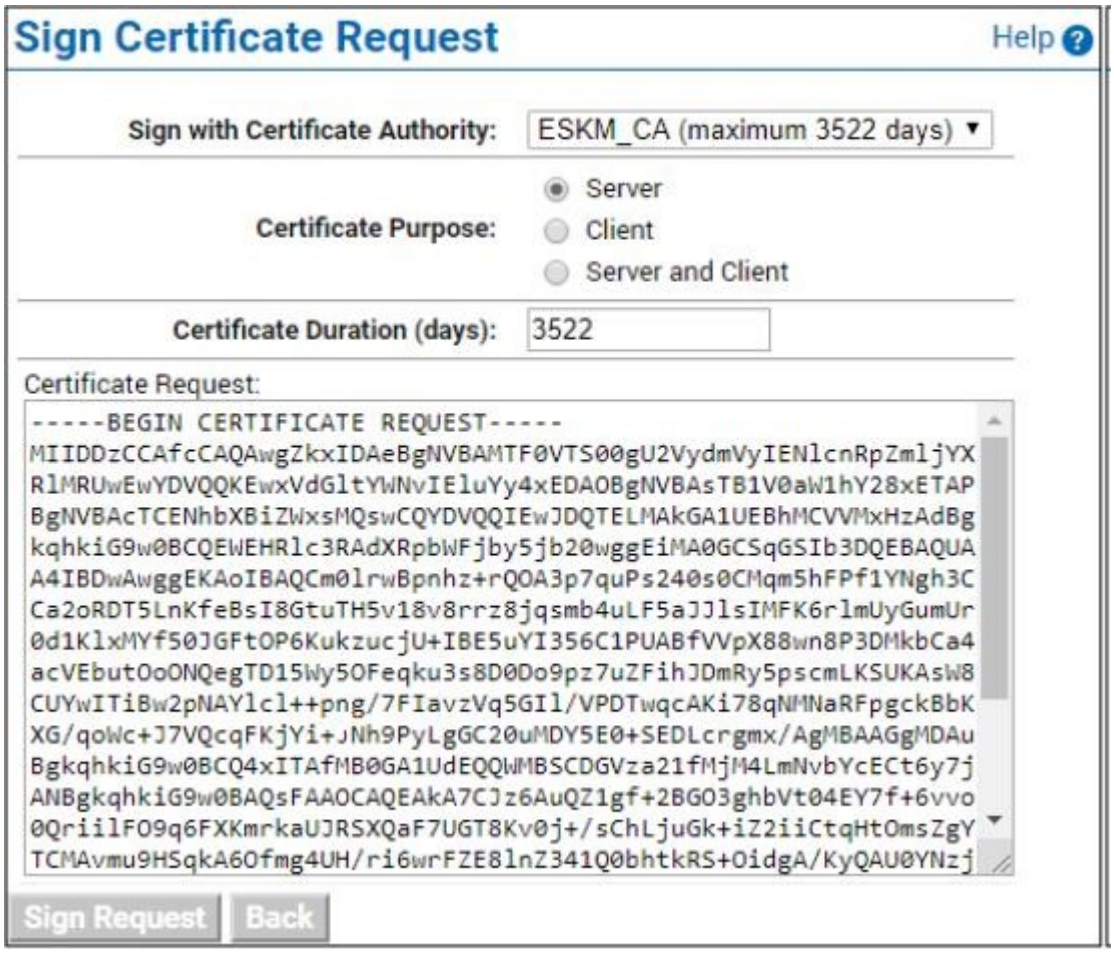


Figure 4 : Sign Certificate Request window

a. Select the CA name from the Sign with Certificate Authority drop down box. For example, ESKM Local CA.

b. Select Server as the Certificate Purpose.

c. Enter the number of days before the certificate must be renewed based on your site's security policies. The default value is 3649 days (10 years).

10. Click Sign Request.
11. In the Certificates & CAs menu, click on Certificates.

12. Click on the certificate name created in step 3 of this section. For example, ESKM Server Certificate.
13. Click Install Certificate.
14. Paste the signed certificate data from step 12, and then click Save. Note that the Certificate status is now Active.

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

The “certificate name” must remain same on all ESKM servers across the cluster.

4.3.1 Import a Third-Party Server Certificate

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

›_ Console

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

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

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

1. In Certificates & CAs, click Certificates to display the Import Certificate section.
2. Provide the source location of the certificate file.
3. Enter the Certificate Name and private key password.

4. Click Import Certificate.

4.4 Setup Cluster

The procedures in this section will establish a cluster configuration on one ESKM server and then transfer that configuration to the remaining ESKM servers.

If cluster is already setup, then skip Section 4.5 Setup KMIP Server.

- In Creating the Cluster, the cluster is created on one ESKM server.

If you only have one ESKM server, skip this section.

- In Adding ESKM servers to the cluster each of the additional ESKM servers will be added to the cluster.

4.4.1 Creating the Cluster

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

1. From the ESKM Management Console, click the Device tab.
2. In the Device Configuration menu, click Cluster.

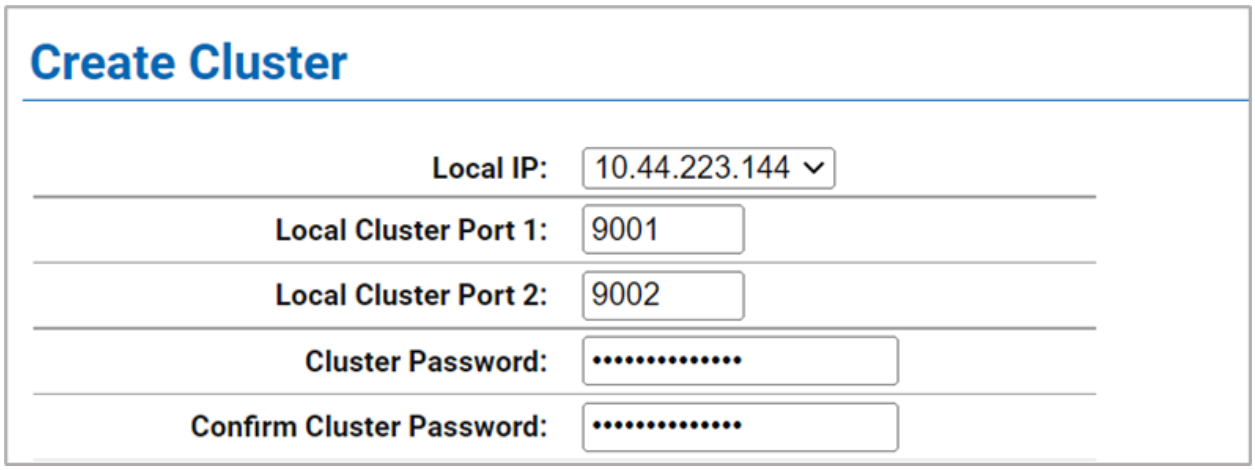


Figure 5 : Create Cluster window

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

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

4. If required, change the Local Port value. Utimaco recommends using the default value of 9001.
5. Choose a cluster password and enter it into the Cluster Password field. Enter the password a second time into the Confirm Cluster Password field.
6. Click the Create button.
7. In the Cluster Settings section of the window, click Download Cluster Key and save the key to a convenient location, such as your computer's desktop.

The cluster key is a text file and is only required temporarily. It may be deleted from your computer's desktop after all ESKM servers have been added to the cluster.

4.4.2 Adding ESKM Servers to the Cluster

To setup ESKM servers to the cluster, perform the following steps in the Join Cluster section on each additional ESKM server.

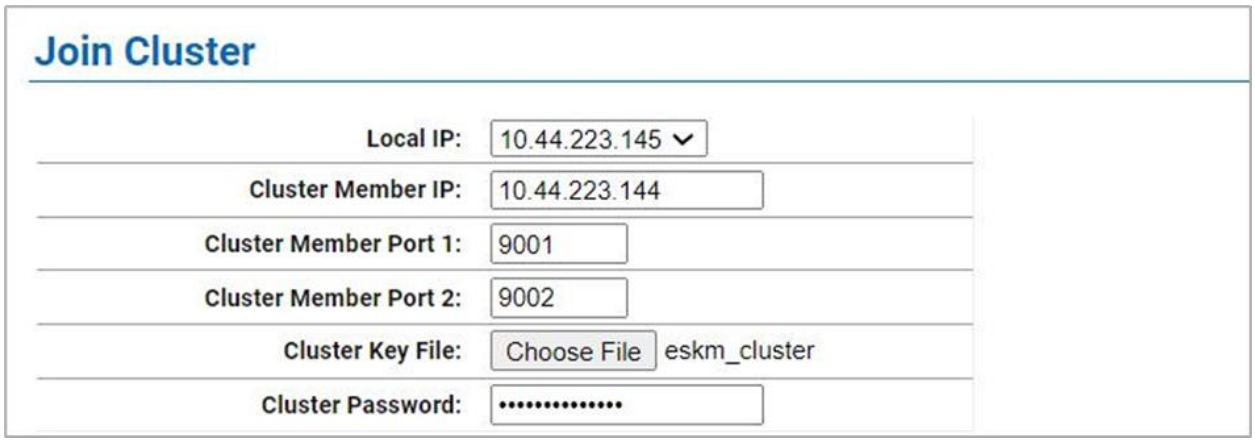


Figure 6 : Join Cluster window

Adding multiple ESKM servers to the cluster is a serial process. Add the first ESKM server and then monitor the system log for the status of the synchronization process. Wait until the

"Cluster synchronization succeeded." message appears in the system log before attempting to add the next ESKM server to the cluster. The amount of time required to complete the synchronization process is a function of the number of keys in the cluster.

If the new ESKM server is a replacement and is configured with the same IP address as the failed ESKM server, make sure the client does not send any key generation requests until the new ESKM server has successfully completed the cluster synchronization process.

Alternately, you can stop the KMS and KMIP servers and then start them once the cluster synchronization process is complete. Use the system log to monitor the progress of the cluster synchronization process.

1. Join the ESKM server to the cluster.

   a. Select the Device tab.

   b. In the Device Configuration menu, click on Cluster.

   c. In the Join Cluster section of the window, select the appropriate Local IP value and then input the appropriate value for the Local Port.

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

   d. Type the original cluster member's IP into Cluster Member IP.

   e. Type the original cluster member's port into Cluster Member Port. The default value of this port is 9001. If this value was changed in while creating the cluster, use that value.

   f. Click Browse and select the Cluster Key File you saved in while creating the cluster.

   g. Type the cluster password into Cluster Password.

   h. Click Join.

   i. Click Confirm to synchronize with the cluster.

If the ESKM server joining the cluster is SSL enabled, this step will cause the WebAdmin service and the KMS and KMIP servers to restart, resulting in a temporary connection loss.

To restore the connection, refresh the browser.

2. After adding all members to the cluster, you can then delete the cluster key file from the desktop.
3. After clustering the ESKM servers, follow the steps in Setting up ESKM certificate to create and install the server certificates on each ESKM server that has joined the cluster. Depending on the KMS and KMIP configuration, two server certificates may need to be created for each ESKM server in the cluster. Be sure to use the same server certificate name as specified under KMS Server Settings and KMIP Server Settings.
4. After creating the KMIP server certificate you must manually restart the KMIP server. Go to the Services List section of the Services Configuration page (Device -> Maintenance -> Services -> KMIP Server).
5. Go to the Services List section (Device > Services) and start the KMIP server.

4.5 Setup KMIP Server

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

To configure the KMIP server, perform the following steps:

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

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

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

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

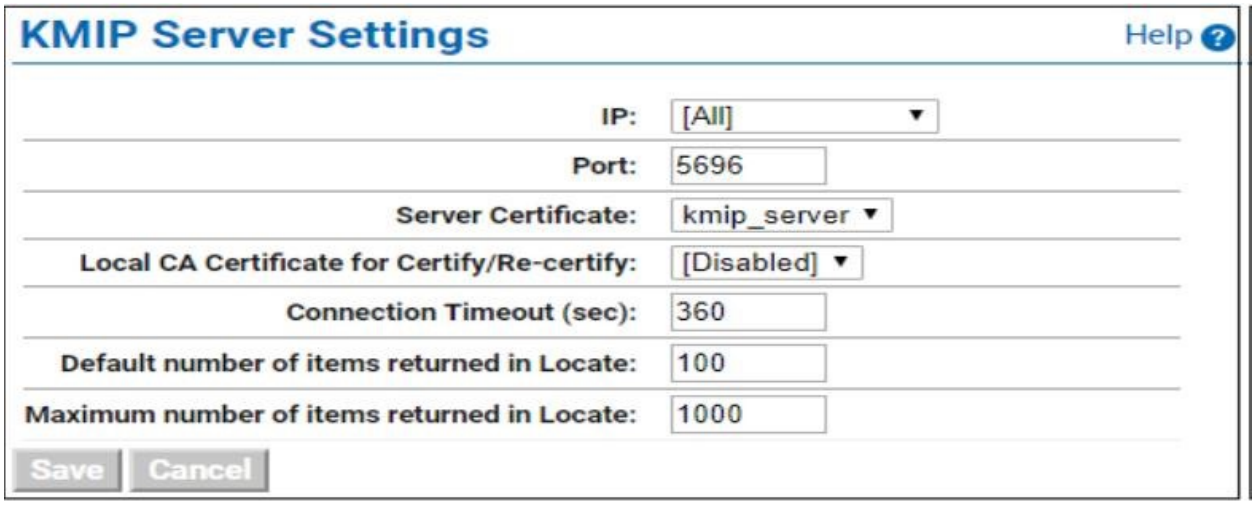


Figure 7 : KMIP Server Setting window

5. Click Save.

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

6. Confirm that the KMIP server is started.

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

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

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your ESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to

these server certificates should clearly indicate their purpose. For example: ESKM KMS Server and ESKM KMIP Server.

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

To enable KMIP client certificate, perform the following steps.

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

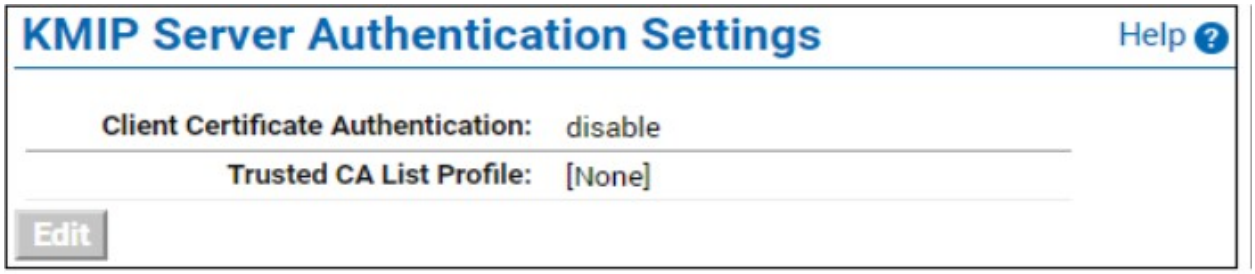


Figure 8 : KMIP Server Authentication Setting window

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

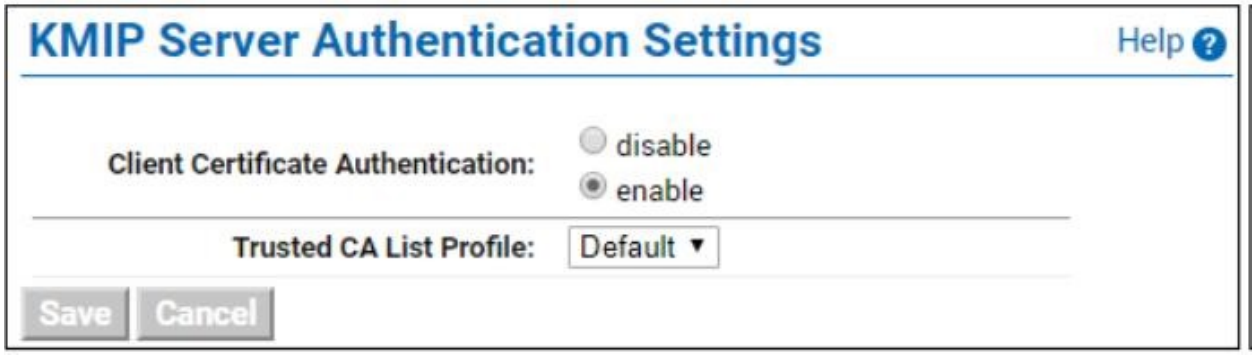


Figure 9 : KMIP Server Authentication Setting window

5 Creating a Client Certificate for ONTAP

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

The following steps provide a high-level overview of the process to configure communication between ONTAP and the ESKM system.

1. Configure the ESKM server, including:
    a. Configure the KMIP server settings.
2. Create KMIP user and password.
3. Connect ONTAP to the ESKM server.

5.1 Configuring the ESKM Server

This process begins with ensuring that Utimaco's Enterprise Secure Key Manager (ESKM) appliance is set up and configured correctly.

5.2 Configuring the KMIP Server Settings

For more information about configuring the KMIP server settings, refer to Setup KMIP server.

For "Server Certificate", under the Server Certificate drop-down, it shall be ESKM_server_cert in this case.

The KMIP server is now configured to use the server certificate.

5.3 Creating and Exporting a Client Certificate using ESKM

5.3.1 Creating Client Certificate

1. Login to the Management Console, and navigate to Security > Certificates and CAs > LocalCA.
2. Select certificate.

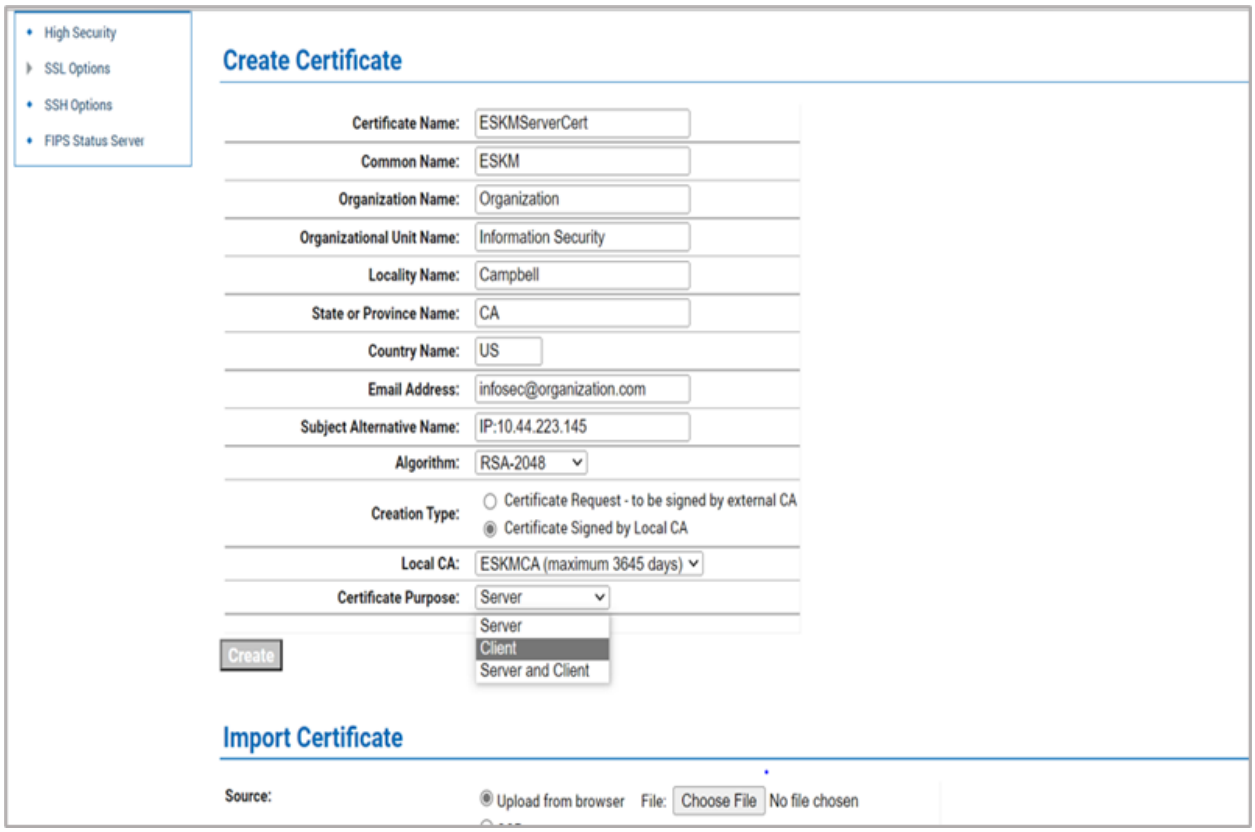


Figure 10 : Create Certificate window

The Common Name must match the name of the KMIP user (in these examples, this is KMIP_client).

3. After crating the certificate with a local CA, click on Download to download the file.
4. Save as the correct name; in this case, /home/user/cert.pem.

5.4 Create a Client Certificate and Key (Using openssl)

5.4.1 Create a CSR on the Client

1. The certificate signing request (CSR) is created on the machine running the client.

Before performing this step, ensure that OpenSSL is already installed on your system.

2. Using OpenSSL, create a private key, using the commands and syntax shown below. This example shows the creation of a 2048-bit RSA key.

›_ Console

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

The following output appears:

›_ Console

```
Generating RSA private key, 2048 bit long modulus

.........................+++
.........................+++ e is 65537 (0x10001)
```

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

›_ Console

```
# openssl req -config "<path>openssl.cnf" -new -key KMIP_client.key >
KMIP_client.csr
```

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 Name (2 letter code) [AU]:
...
```

4. Enter the information in the fields as prompted.

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

Table 6: List of Field with Example

The Common Name must match the name of the KMIP user.

5. You are then prompted to add other parameters, such as a “challenge password” or “optional company name”. To skip those parameters, press Enter.

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

6. Download KMIP_client.key file to client system with correct name; in this case, /var/lib/mysql/mysql-keyring-okv/ssl/key.pem.

5.4.2 Use the Local CA to Sign CSR

The CSR now needs to be signed by the local CA.

1. Using a text editor (or using the more <filename> command), open the KMIP_client.csr file.
2. Select the entire text and copy to your clipboard.
3. Now, login to the Management Console and navigate to Security > Certificates & CAs > Local Cas.

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

4. Select the CA used by your ESKM (in this case, LocalCA), and click Sign Request. The Sign Request window appears.

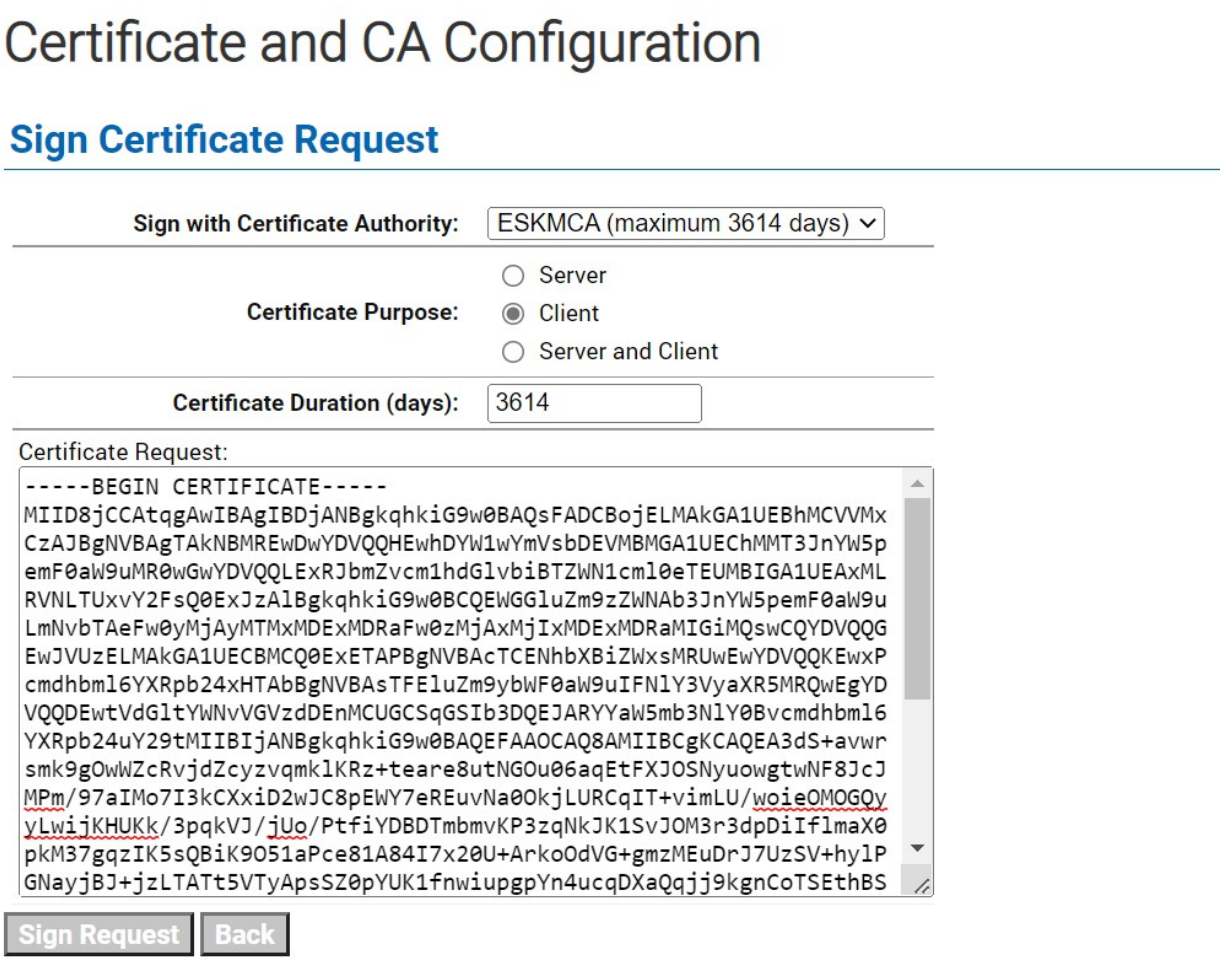


Figure 11 : Sign Certificate Request Window

5. For Certificate Purpose, select Client.
6. Paste the CSR text that you have copied to your clipboard (Step 2 above) into the Certificate Request window.
7. Click Sign Request. The signed client certificate now appears.

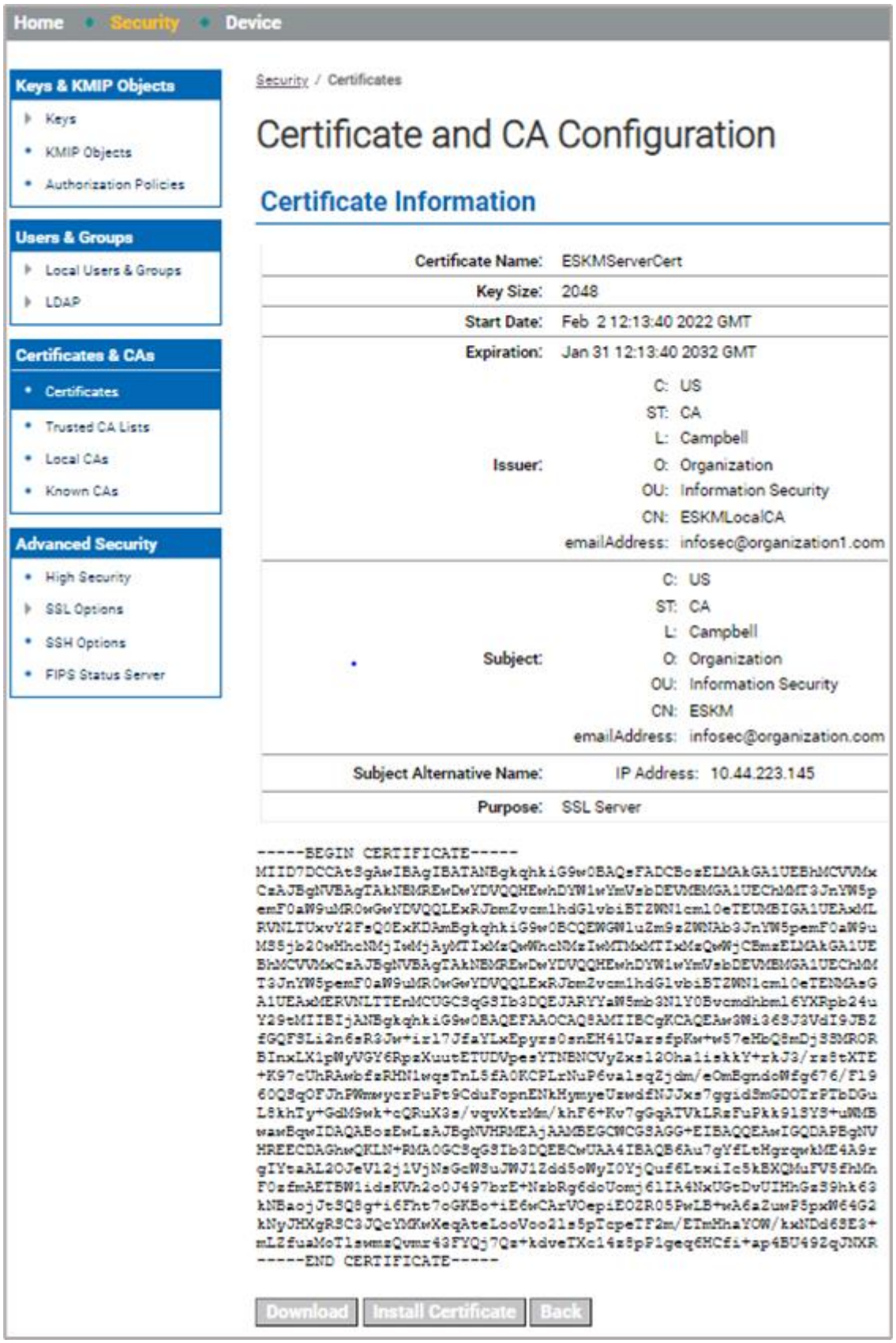

Home
Security
Device
Keys & KMIP Objects
Keys
KMIP Objects
Authorization Policies
Users & Groups
Local Users & Groups
LDAP
Certificates & CAs
Certificates
Trusted CA Lists
Local CAs
Known CAs
Advanced Security
High Security
SSL Options
SSH Options
FIPS Status Server
Security / Certificates
Certificate and CA Configuration
Certificate Information
Certificate Name: ESKMServerCert
Key Size: 2048
Start Date: Feb 2 12:13:40 2022 GMT
Expiration: Jan 31 12:13:40 2032 GMT
Issuer: C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKMLocalCA emailAddress: infosec@organization1.com
Subject: C: US ST: CA L: Campbell O: Organization OU: Information Security CN: ESKM emailAddress: infosec@organization.com
Subject Alternative Name: IP Address: 10.44.223.145
Purpose: SSL Server
-----BEGIN CERTIFICATE-----
MIID7DCCAtSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBozELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNEMREwDwYDVQQHEwhDYWlwYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExKDAmBgkqhkiG9w0BCQEWGW1uZm9zZWNAb3JnYW5pemF0aW9u
MS5jb20wHhcNMjIwMjAyMTIxMzQwWhcNMzIwMTMxMTIxMzQwWjCBmzELMAkGA1UE
BhMCVVMxCzAJBgNVBAgTAkNEMREwDwYDVQQHEwhDYWlwYmVsbDEVMBMGA1UEChMM
T3JnYW5pemF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZWN1cml0eTENMAsG
A1UEAxMERVNLTTEnMCUGCSqGSIb3DQEJARYYaW5mb3N1Y0Bvcmdhbml6YXRpb24u
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw3Wi36SJ3VdI9JB2
fGQF8Li2n6sR3Jw+ir17JfaYLxEpyrs0snEH41UarsfpKw+w57eMbQ8mDj88MROR
BInxLX1pWyUGY6RpxXuutETUDVpesYTNENCVyZxs120haliskkY+rkJ3/rz8tXTE
+K97cUhRAwbfzRHNlwqsTnL5fA0KCPLrNuP6valsqZjdm/eOmEgndoWfg676/F19
60Q8qOFJhPWmrycrPuPt9CduFopnENkHymyeUzwdfNJJxs7ggid8mGDOIrPTbDGu
L8khTy+GdM9wk+cQRuX3s/vqvXtrMm/khF6+Kv7gGqATVkLRzFuPkk913Y3+uNMB
wawEqwIDAQABozEwLzAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDAPBgNV
HREECDAGhwQKLN+RMA0GCSqGSIb3DQEBCwUAA4IBAQB6Au7gYfLtHgrqwkME4A9r
gIYtaAL2OJeV12j1VjNsGcW8uJWJ1Zdd5oWyI0YjQuf6LtxiIc5kBXQMuFV5fhMh
F0zfmAETBW1idsKVh2o0J497brE+NzbRg6doUomj61IA4NxUGtDvUIHhGz39hk63
kNBaojJt8Q8g+i6Fht7oGKBo+iE6wCArVOepiEOZR05PwLB+wA6aZuwP5pxW64G2
kNyJHXgR8C3JQcYMKwXeqAteLooVoo2ls5pTcpeTF2m/ETmHhaYOW/kxNDd6SE3+
mLZfuaMoT1swmsQvmr43FYQj7Qs+kdveTXc14z8pP1geq6HCfi+ap4BU49ZqJNXR
-----END CERTIFICATE-----
Download
Install Certificate
Back

Figure 12 : Certificate Information window

8. After signing the certificate request with a local CA, click on Download to download the file.
9. Save as the correct name; in this case, /var/lib/mysql/mysql-keyringokv/ssl/cert.pem.

5.4.3 Exporting Certificate with Private Key from ESKM

1. Enter the password to export the key.

Figure 13 : Export Certificate with Private Key window

2. Converting PKCS#12 key into PEM using OpenSSL.

›_ Console

```
# openssl pkcs12 -in <key name.p12> -nodes -nocerts | openssl rsa -out key.pem
```

6 Creating KMIP User and Password

Create the user — an individual (client) on the ESKM server, in this case, KMIP_client.

A client license is required for each user created on the ESKM server. Refer to the ESKM

Installation and Replacement Guide for information about how to request and install the license pack.

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

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

4. Select “permissions” for this user.
5. Click the Enable KMIP option.
6. If required, from the drop-down lists, select the User and Object group to which the user belongs. In this case, Company-group_user and Company-group.
7. Paste the signed client certificate request, still on your clipboard from Step 8 above, into the KMIP Client Certificate field. (If it isn’t on your clipboard, open KMIP_client.pem and recopy it).

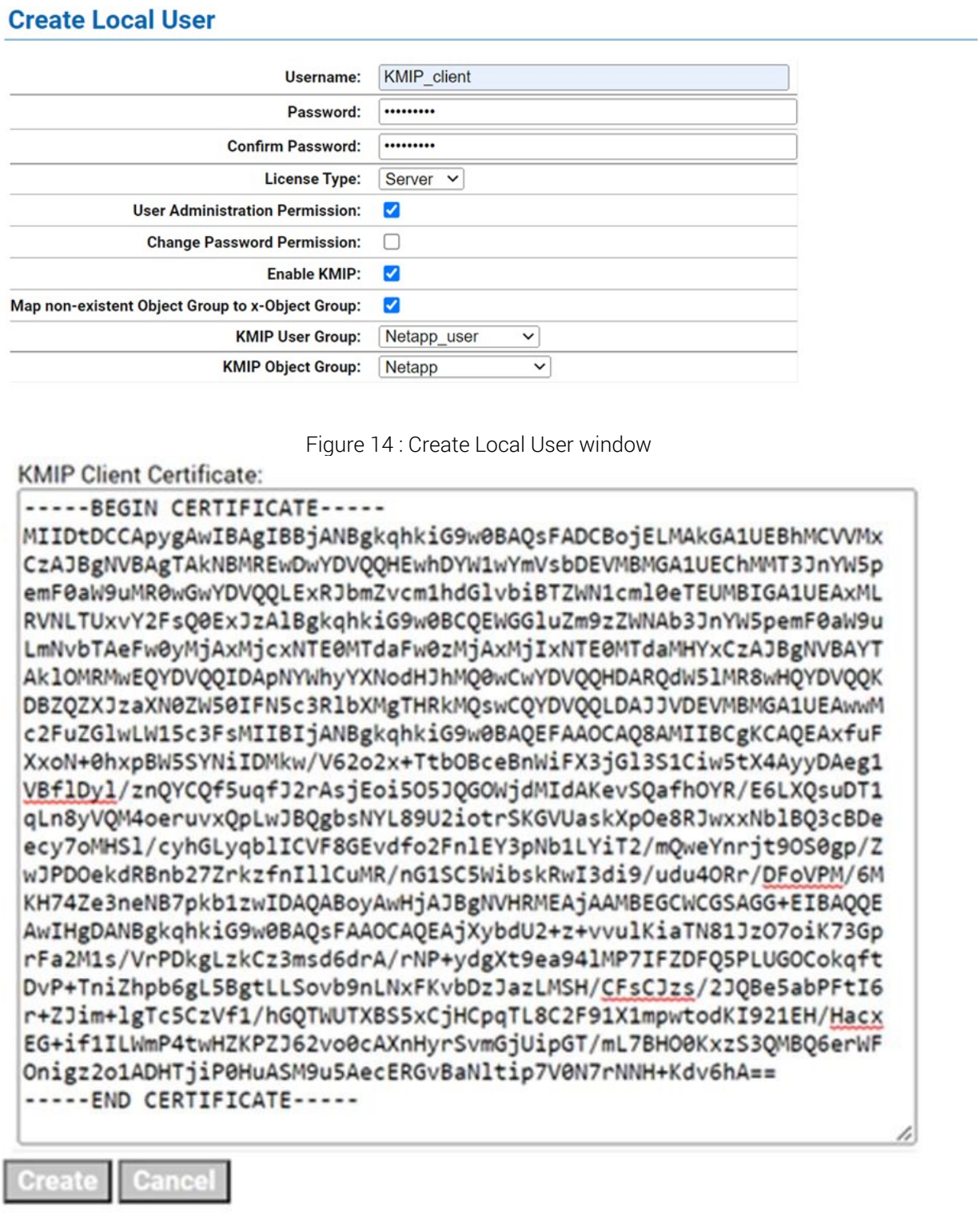


Figure 14 : Create Local User window

8. Click Create.

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

The configuration of the ESKM server is now complete.

7 Installing NetApp ONTAP using Simulate ONTAP

Skip this section if you already have NetApp ONTAP deployed. For demonstration purpose Simulate ONTAP has been used. You can download Simulate ONTAP ova file from https://mysupport.netapp.com/ and deploy it by importing the ova file on VMware Workstation Pro, VMware Workstation Player or VMware Fusion.

7.1 Deploying and Configuring a Two Node Cluster

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

1. Create the first Simulate ONTAP virtual machine and name it node1 using .ova file.
2. After a few minutes from starting the virtual machine, you receive a message to log in to System Manager to complete cluster setup. This message includes an IP address. Copy this IP address and paste it 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

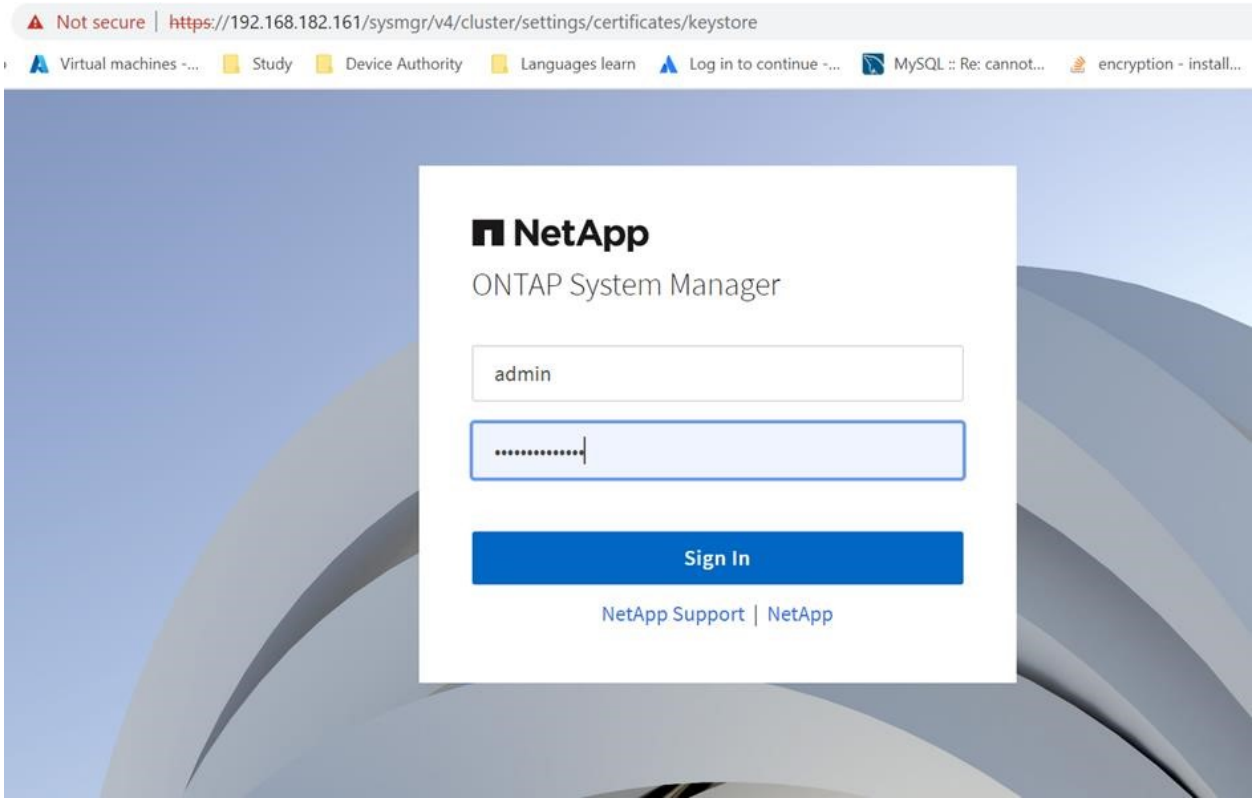


Figure 15 : NetApp ONTAP Login window

6. Back in the VMware Workstation Player window, log in with the username admin and the password.

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 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: https://mysupport.netapp.com.
    a. Click to downloaded latest image for example “Download Latest Release [9.11.1P4]”.
    b. Click I read the EULA. Click Accept and Continue.
    c. Click Download ONTAP 9.11.1P4 with NetApp Volume Encryption for FAS [2.31 GB].
    d. Save the file and make it accessible via a web server.

›_ Console

```
cluster1::>  cluster image package get -url
http://192.168.182.176/9111P4_q_image.tgz
cluster1::>  cluster image package show
cluster1::>  cluster image update -version 9.11.1P4 -nodes cluster1-01
cluster1::>  cluster image show-update-progress
cluster1::>  security login unlock -username diag
cluster1::>  security login password -username diag
```

11. Create the second Simulate ONTAP virtual machine and name it node2.
12. Power on the node2 virtual machine.
13. Change the system ID and serial number of the second node before joining the cluster as shown in the following steps.

14. Press the space bar when the *Hit [Enter] to boot immediately, or any other key for command prompt. Booting in 10 seconds…* message is displayed in the console of node2.
15. You should see a VLOADER> prompt.
16. Change the serial number and system ID for this node:

›_ Console

```
VLOADER> setenv SYS_SERIAL_NUM 4034389-06-2
VLOADER> setenv bootarg.nvram.sysid 4034389062
```

17. Verify that the information was saved correctly:

›_ Console

```
VLOADER> printenv SYS_SERIAL_NUM
VLOADER> printenv bootarg.nvram.sysid
```

18. Enter the boot command to boot the node:
    a. Type boot and press Enter to boot the node.
    b. You will receive a message that System Initialization has completed successfully, and then the Node Management IP has been assigned. It may take several minutes for the messages to appear.
19. Log in with the username admin and a blank password. Then create a password for the admin account with the command.

›_ Console

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

Enter your current password: Leave blank and hit Enter.

Enter a new password for example: Utimaco@123.

20. Back to the VMware Workstation Player window for Cluster 1 Node 1, and enter the command.

›_ Console

```
cluster1::> network interface show
```

Note the IP address of the first interface cluster1-01_clus1. It is 169.254.181.219.

```
CLuster1::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
CLuster1
            CLuster1-01_mgmt
                       up/up    192.168.182.163/24 CLuster1-01   e0c     true
            CLuster1-01_mgmt_auto
                       up/up    192.168.182.159/24 CLuster1-01   e0c     true
            cluster_mgmt up/up    192.168.182.161/24 CLuster1-01   e0c     true
Cluster
            CLuster1-01_clus1
                       up/up    169.254.181.219/16 CLuster1-01   e0a     true
            CLuster1-01_clus2
                       up/up    169.254.181.229/16 CLuster1-01   e0b     true
            CLuster1-02_clus1
                       up/up    169.254.58.202/16  CLuster1-02   e0a     true
            CLuster1-02_clus2
                       up/up    169.254.58.212/16  CLuster1-02   e0b     true
7 entries were displayed.
```

Figure 16 : Network Interface IPs

21. Back in the VMware Workstation Player window for Cluster 1 Node 2, enter the command.

›_ Console

```
cluster join -clusteripaddr <cluster1-01_clus1 IP>, where <cluster1-
01_clus1 IP>
Example:
cluster1::>  cluster join -clusteripaddr 169.254.181.219
```

169.254.181.219 is the IP address you just noted on Node 1. This will join Node 2 to Cluster 1.

22. Add all existing disks to Cluster 1 Node 2 with the command.

›_ Console

```
cluster1::> storage disk assign -all true -node cluster1-02
```

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

23. 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_02
```

```
cluster1::> storage aggregate add-disks -diskcount 8 -aggregate aggr0_cluster1_02

Warning: Aggregate "aggr0_cluster1_02" is a root aggregate. Adding disks to the root aggregate is not
recommended. Once added, disks
             cannot be removed without re-initializing the node.
Do you want to continue? {y|n}: y

Info: Disks would be added to aggregate "aggr0_cluster1_02" on node "cluster1-02" in the following
manner:

        First Plex

          RAID Group rg0, 16 disks (block checksum, raid_dp)
                                                                  Usable Physical
            Position     Disk                      Type           Size     Size
            ---------- ------------------------ ---------- -------- --------
            data         NET-2.1                   FCAL        1000MB   1.00GB
            data         NET-2.26                  FCAL        1000MB   1.00GB
            data         NET-2.2                   FCAL        1000MB   1.00GB
            data         NET-2.27                  FCAL        1000MB   1.00GB
            data         NET-2.3                   FCAL        1000MB   1.00GB

          RAID Group rg1, 3 disks (block checksum, raid_dp)
                                                                  Usable Physical
            Position     Disk                      Type           Size     Size
            ---------- ------------------------ ---------- -------- --------
            dparity      NET-2.4                   FCAL              -        -
            parity       NET-2.28                  FCAL              -        -
            data         NET-2.5                   FCAL        1000MB   1.00GB

        Aggregate capacity available for volume use would be increased by 5.27GB.

Do you want to continue? {y|n}: y
```

Figure 17 : Adding disks to aggregate

24. Set the root volume to a new size.

›_ Console

```
cluster1::>  volume modify -size 7.47GB -volume vol0 -vserver cluster1-02
```

```
cluster1::> volume modify -size 7.47GB -volume vol0 -vserver cluster1-02
Volume modify successful on volume vol0 of Vserver cluster1-02
```

Figure 18 : Modifying size of volume

25. Install the VE license for a node:

›_ Console

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

26. 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
                                                 2/13/2023 08:00:00
```

Figure 19 : NVE License Show

27. Add all the licenses for the ONTAP simulator via SM web GUI.

```
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
                                                  2/13/2023 08:00:00

Serial Number: 1-81-0000000000000004034389062
Owner: CLuster1-02
Installed License: Legacy Key
Capacity: -
Package           Type     Description           Expiration
----------------- -------- --------------------- --------------------
NFS               license  NFS License           -
CIFS              license  CIFS License          -
iSCSI             license  iSCSI License         -
FCP               license  FCP License           -
SnapRestore       license  SnapRestore License   -
SnapMirror        license  SnapMirror License    -
FlexClone         license  FlexClone License     -
SnapVault         license  SnapVault License     -
SnapLock          license  SnapLock License      -
SnapManagerSuite  license  SnapManagerSuite License
                                                  -
SnapProtectApps   license  SnapProtectApp License
                                                  -
Insight_Balance   license  OnCommand Balance     -

Serial Number: 1-81-0000000000000004082368507
Owner: CLuster1-01
Installed License: Legacy Key
Capacity: -
Package           Type     Description           Expiration
----------------- -------- --------------------- --------------------
NFS               license  NFS License           -

Serial Number: 1-81-0000000000000004082368507
Owner: CLuster1-01
Installed License: Legacy Key
Capacity: -
Package           Type     Description           Expiration
----------------- -------- --------------------- --------------------
CIFS              license  CIFS License          -
iSCSI             license  iSCSI License         -
FCP               license  FCP License           -
SnapRestore       license  SnapRestore License   -
SnapMirror        license  SnapMirror License    -
FlexClone         license  FlexClone License     -
SnapVault         license  SnapVault License     -
SnapLock          license  SnapLock License      -
SnapManagerSuite  license  SnapManagerSuite License
                                                  -
```

Figure 20 : All Licenses Output

8 Configuring ONTAP to use Utimaco ESKM

8.1 Importing the Client Certificate to ONTAP

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

You have to import the following files:

a) A <cert_name>.pem file that includes both the client certificate and the private key. You will have to paste two sections from this the file into the corresponding prompts from ONTAP.

The client certificate section of the <cert_name>.pem file includes all the encrypted text and the BEGIN and END lines:

```
"-----BEGIN CERTIFICATE-----"
some text
"-----END CERTIFICATE-----"
```

Figure 21 : Client cert.pem

The private key section of the <cert_name>.pem file includes all the encrypted text and the BEGIN and END lines:

```
"-----BEGIN PRIVATE KEY-----"
some text
"-----END PRIVATE KEY-----".
```

Figure 22 : Client cert.pem

b) A cacert.pem file, which is the root certificate for the KMIP cluster. It is always named cacert.pem.

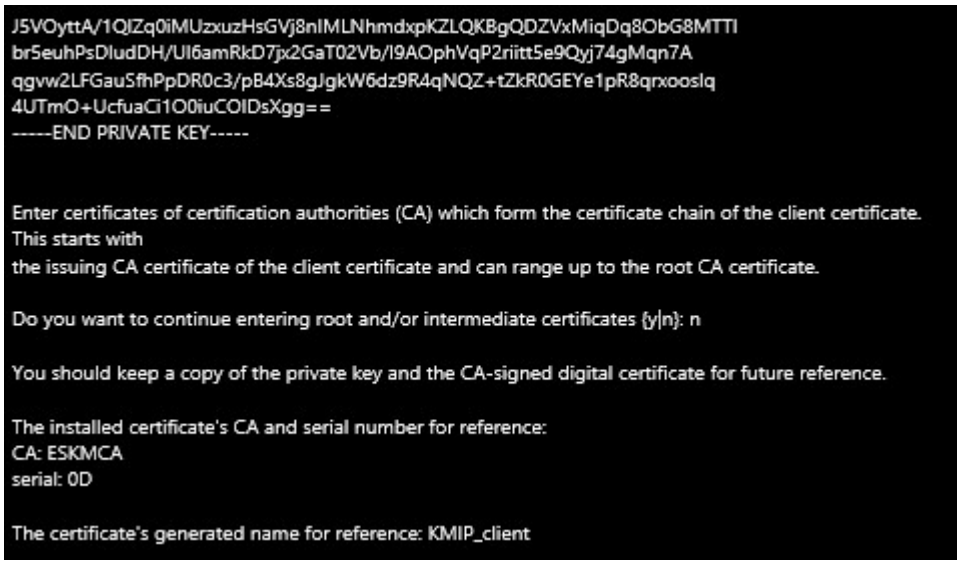
1. Run the security certificate install command as described in the ONTAP 9 NetApp Encryption Power Guide https://docs.netapp.com/us-en/ontap/index.html.
2. Install the NetApp cluster's KMIP client certificate:

›_ Console

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

You will be prompted to paste the certificate and private key content from <cert_name>.pem.

Figure 23 : Client Certificate & Private Key Installation



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

Run below command to install the certificate.

›_ Console

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

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC4zCCAoqgAwIBAgIBADAKBggqhkjOPQQDAjCBhjELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEQMA4GA1UEChMHVXRpbWFjbzEQ
MA4GA1UECxMHVXRpbWFjbzEPMA0GA1UEAxMGRVNLTUNBMSIwIAYJKoZIhvcNAQkB
FhNzdXBwb3J0QFV0aW1hY28uY29tMB4XDTIzMDEwMTE4NTcxNloXDTMyMTIzMDE4
NTcxNlowgYYxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTERMA8GA1UEBxMIQ2Ft
cGJlbGwxEDAOBgNVBAoTB1V0aW1hY28xEDAOBgNVBAsTB1V0aW1hY28xDzANBgNV
BAMTBkVTS01DQTEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBVdGltYWNvLmNvbTBZ
MBMGByqGSM49AgEGCCqGSM49AwEHA0IABC/qUNvmajo3OpRpDDF1ut3meWDn2Af9
q0jcZkzRnXjkZUF60f4DltmUyWUtnDnGPvuZgLBoqxf2NXh6u4erkAejgeYwgeMw
HQYDVR0OBBYEFDO29v5lMoRNfGhjF5x8VdTJTswsMIGzBgNVHSMEgaswgaiAFDO2
9v5lMoRNfGhjF5x8VdTJTswsoYGMpIGJMIGGMQswCQYDVQQGEwJVUzELMAkGA1UE
CBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRAwDgYDVQQKEwdVdGltYWNvMRAwDgYD
VQQLEwdVdGltYWNvMQ8wDQYDVQQDEwZFU0tNQ0ExIjAgBgkqhkiG9w0BCQEWE3N1
cHBvcnRAVXRpbWFjby5jb22CAQAwDAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNH
ADBEAiBc0qOuMpdmA2qajJO77mWBVRPezDZgYH6B9Rb/T1huLQIgaORFUNwZEk8M
k9BQsGcgUwJrhNOgZOG/lz7MxpXgPPc=
-----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: ESKMCA
serial: 00

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

Figure 24 : Server CA Certificate Installation

8.3 Adding the Utimaco ESKM as Key Control Nodes on ONTAP

Run below command enable external key manager.

›_ Console

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

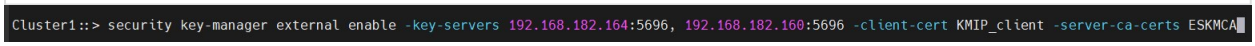


Figure 25 : Adding Key Managers nodes

8.4 Verifying the communication between the external Key Manager and the cluster (ONTAP)

Run below command to show the status of key managers.

›_ Console

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

```
CLuster1::> security key-manager show -status

Node                  Port    Registered Key Manager       Status
--------------------  ------  --------------------------   ---------------
CLuster1-01           5696    192.168.182.160              available
CLuster1-01           5696    192.168.182.164              available
CLuster1-02           5696    192.168.182.160              available
CLuster1-02           5696    192.168.182.164              available
4 entries were displayed.
```

Figure 26 : Key Manager Status

9 Performing NetApp Volume Encryption

9.1 Enabling Aggregate-level Encryption

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE. ONTAP automatically “pushes” an encryption key to the Utimaco ESKM server when you encrypt a volume.

Note: 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
```

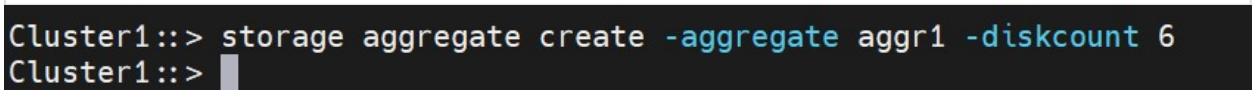


Figure 27 : Creating a new aggregate and enabling aggregate-level encryption

2. Verify that the aggregate 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
aggr0_CLuster1_02 false
aggr1             true
3 entries were displayed.
```

Figure 28 : Verifying encryption on aggregate

9.2 Enabling Encryption on a New Volume

1. Create a new volume and specify 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:

›_ Console

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

Example
Cluster1::> volume create -vserver svm1 -volume vol0 -aggregate aggr1
```

```
Cluster1::> volume create -vserver svm1 -volume vol0 -aggregate aggr1
[Job 121] Job succeeded: Successful
```

Figure 29 : Creating a new volume

2. View the newly created NAE volume.

›_ Console

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

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

                                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: 1051
                   Volume Master Data Set ID: 2157968616
                                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: 18.57MB
                              Filesystem Size: 20MB
                    Total User-Visible Size: 19MB
                                  Used Size: 436KB
                              Used Percentage: 2%
           Volume Nearly Full Threshold Percent: 95%
                  Volume Full Threshold Percent: 98%
                               Maximum Autosize: 24MB
                               Minimum Autosize: 20MB
```

Figure 30 : Volume show output

3. Create an NVE volume.

›_ Console

```
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
```

```
CLuster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -encrypt true
[Job 122] Job succeeded: Successful
```

Figure 31 : Creating an NVE volume

4. View the newly created NVE Volume.

›_ Console

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

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

                                    Vserver Name: svm1
                                     Volume Name: vol1
                                  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: 1048
                      Volume Master Data Set ID: 2157968617
                                  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: 18.62MB
                                Filesystem Size: 20MB
                       Total User-Visible Size: 19MB
                                     Used Size: 392KB
                                Used Percentage: 2%
          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
           Total Files (for user-visible data): 566
```

Figure 32 : Volume show output

5. Verify that volumes are enabled for encryption.

›_ Console

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

```
Cluster1::> volume show -is-encrypted true
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
CLuster1-01
          vol0         aggr0_CLuster1_01
                                    online     RW       7.47GB     2.78GB   60%
svm1      svm1_root    aggr1        online     RW         20MB    18.51MB    2%
svm1      vol0         aggr1        online     RW         20MB    18.57MB    2%
svm1      vol1         aggr1        online     RW         20MB    18.62MB    2%
svm1      vol10        aggr2        online     RW         20MB    18.56MB    2%
svm1      vol2         aggr1        online     RW         20MB    18.55MB    2%
svm2      vol11        aggr2        online     RW         20MB    18.56MB    2%
svm2      vol12        aggr2        online     RW         20MB    18.55MB    2%
svm2      vol3         aggr2        online     RW         20MB    18.61MB    2%
9 entries were displayed.

Cluster1::>
```

Figure 33 : Verifying encrypted volumes

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

1. Convert an existing volume (plain text volume) to encrypted volume by running below command.

›_ Console

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

Example:
Cluster1::> volume encryption conversion start -vserver svm2 -volume vol5
```

```
Cluster1::> volume encryption conversion start -vserver svm2 -volume vol5

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 "vol5". Run "volume encryption conversion show -volume vol5 -vserver svm2" to see the status of t
his operation.

Cluster1::> volume encryption conversion show -volume vol5 -vserver svm2

       Vserver Name: svm2
        Volume Name: vol5
         Start Time: 1/11/2023 02:13:52
             Status: running
```

Figure 34 : Converting to encrypted volume

2. 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%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
CLuster1-01
          vol0         aggr0_CLuster1_01
                                    online     RW       7.47GB     2.75GB   61%
svm1      svm1_root    aggr1        online     RW         20MB    18.39MB    3%
svm1      vol0         aggr1        online     RW         20MB    18.49MB    2%
svm1      vol1         aggr1        online     RW         20MB    18.50MB    2%
svm1      vol10        aggr2        online     RW         20MB    18.44MB    2%
svm1      vol2         aggr1        online     RW         20MB    18.42MB    3%
svm2      vol11        aggr2        online     RW         20MB    18.44MB    2%
svm2      vol12        aggr2        online     RW         20MB    18.43MB    3%
svm2      vol3         aggr2        online     RW         20MB    18.49MB    2%
svm2      vol5         aggr2        online     RW         20MB    18.70MB    1%
10 entries were displayed.
```

Figure 35 : Verifying encrypted volumes

9.4 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

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

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

Figure 36 : Moving an NAE volume to an NVE volume

2. 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 -destinationaggregate
aggr1 -encrypt-with-aggr-key true
Cluster1::> volume move show -vserver svm1 -volume vol0
```

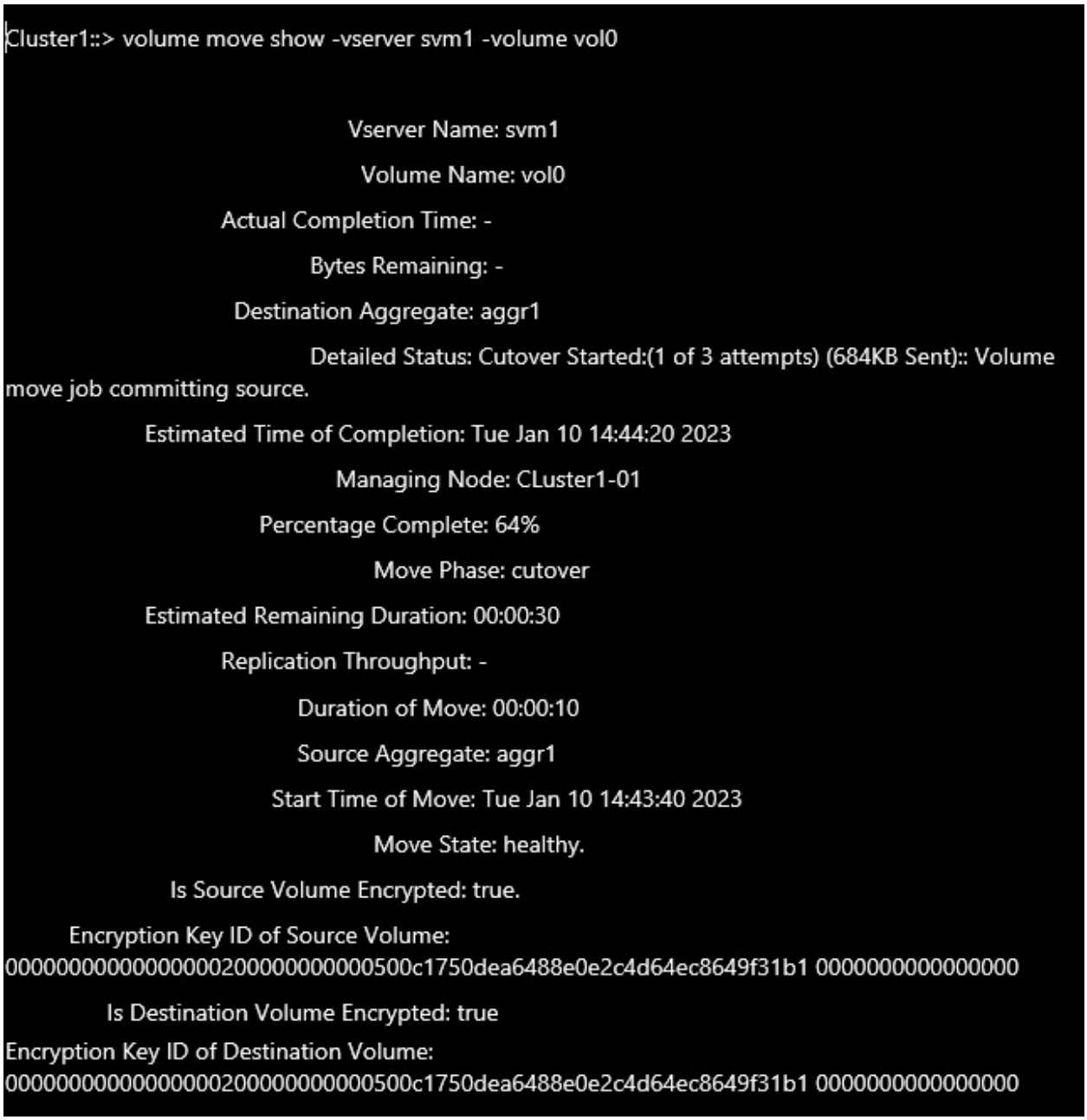


Figure 37 : Moving an NVE volume to an NAE volume

10 Managing the Client and CA Certificates on ONTAP

10.1 Deleting Certificates

Before you begin to install 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 192.168.182.160
```

Figure 38 : Key Manager Status

2. Remove all certificates for the cluster:

›_ Console

```
Cluster1::> security certificate delete -vserver Cluster1 -common-name KMIPCert
-ca KMIPCert -type client -serial 17391C189F77D0C5
```

Figure 39 : Delete Certificates Output

The old certificates were deleted. You can install the new ones.

10.2 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 step mentioned in section Creating and Exporting a Client Certificate using ESKM.

This completes the integration of NetApp ONTAP with Utimaco ESKM.

11 Troubleshooting

Error	Diagnosis
CLuster1::> volume move start -vserver svm1 volume svm1_root -destination-aggregate aggr1 -encrypt-with-aggr-key false Error: 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. CLuster1::> storage aggregate create -aggregate aggr2 -diskcount 6 -encrypt-with-aggr-key false

Table 7: Errors and their Diagnoses

12 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

13 References

Reference	Title/Company
[ESKMIRG]	ESKM_Installation and Replacement_Guide.pdf
[ESKMUG]	ESKM_User_Guide.pdf

Table 8: References

14 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
Germanusstr. 4
52080 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.