Dell

Data Domain

8.3.0

Integration Guide

ESKM

8.54.0

utimaco®

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	2025-07-24
Status	PUBLISHED
Document No.	IG-2025-0038

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. This guide details the integration of Utimaco ESKM with Dell Data Domain to enable secure and encrypted data archive and backup functionality. Together, Dell Data Domain and Utimaco ESKM deliver a comprehensive solution for secure, compliant, and resilient data protection.

The guide walks through the necessary steps to configure the integration.

1.1 About This Guide

This guide describes how to enable ESKM integration with Dell Data Domain to enable encryption during archiving. It equips users with the key data to facilitate effortless communication and authentication between ESKM and Dell Data Domain, implementing Key Management Interoperability Protocol (KMIP) and certificate-based Authentication.

1.2 Target Audience for This Guide

This integration guide is intended for administrators of Dell Data Domain and Utimaco ESKM systems.

1.3 Purpose of the Integration

Integration of Utimaco ESKM with Dell Data Domain enables and enhances secure and encrypted backup functionality. Dell Data Domain ensures reliable data archiving and recovery across virtual and physical environments. ESKM provides robust encryption key lifecycle management, including generation, storage, access control, and auditing.

The primary objective of this integration is to:

- Enhance data security by ensuring all archives are encrypted during storage and transmission.
- Leverage Dell Data Domain's encryption capabilities within the Utimaco ESKM environment.

1.4 Document Conventions

The following conventions are used in this guide:

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 find important safety information that should be followed.

Here, you find additional notes or supplementary information.

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

1.5 Abbreviations

The following abbreviations are used in this guide.

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol
CA	Certificate Authority
DD	Data Domain

Table 2: Abbreviations

2 Product Overview

2.1 Dell Data Domain

Dell Data Domain is a high-performance, disk-based data protection solution designed to streamline backup, archiving, and disaster recovery. It leverages advanced deduplication technology to minimize storage requirements, often reducing data footprints. With scalable architecture and support for cloud integration, Data Domain systems can handle massive data volumes while ensuring fast, reliable recovery. Built-in features like data integrity checks, encryption, and centralized management make it a trusted choice for enterprises seeking robust and secure data protection.

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, as well as custom integrations.

2.3 Joint Value Proposition

The integration of Dell Data Domain with Utimaco ESKM delivers a comprehensive and secure data protection solution that combines industry-leading data archive and recovery capabilities with advanced encryption key management. This joint solution empowers organizations to:

- Ensure end-to-end data security by encrypting backups both at rest and in transit.
- Simplify compliance with regulatory standards through centralized key lifecycle management, including generation, storage, access control, and auditing.
- Maximize operational efficiency by seamlessly leveraging Dell Data Domain’s encryption features within the ESKM environment.
- Strengthen resilience against data breaches and unauthorized access.

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 installed and configured the required software.

3.1 Tested Versions

The integration has been successfully tested with the Utimaco ESKM and Dell Data Domain.

Dell Data Domain OS Version	Utimaco ESKM Version
8.3.0	8.54.0

Table 3: Tested Versions

3.2 Supported Platforms

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

3.3 Software Requirements

Software	Software Requirements
Data Domain OS version	8.3.0
Utimaco ESKM version	8.54.0

Table 4: Software Requirements

3.4 Prerequisites

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

- Data Domain OS - Ensure the latest DDOS version is installed and properly configured.
- Licensing: A valid Dell Data Domain license that supports encryption with an external key manager.
- Utimaco ESKM: Ensure that the latest version of ESKM is available.

4 Installation and Configuration

4.1 Set Up ESKM

The initial phase involves configuring ESKM before proceeding to Dell Data Domain. For detailed configuration steps, see the *ESKM_Installation and Replacement_Guide_8.54.0.*

After successful installation and configuration, log in to ESKM.

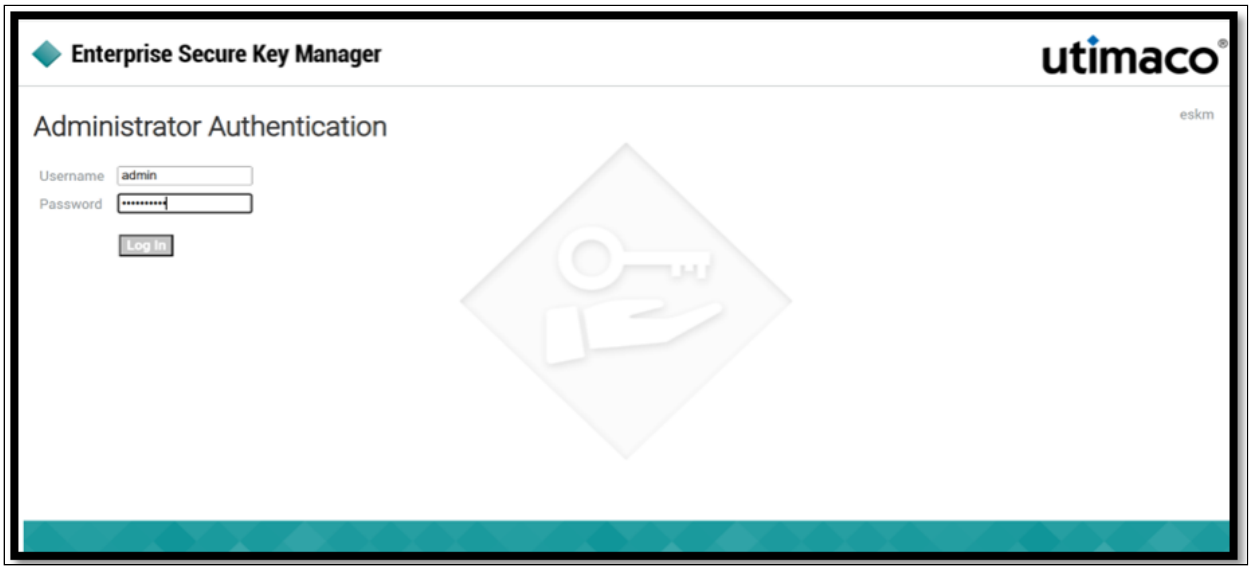


Figure 1 : ESKM Log in

Figure 2 : ESKM Home Page

4.2 Set Up Dell Data Domain

Please refer to the installation and administration guide for setting up the Dell Data Domain: *Dell Data Domain Manual*

Please note the following points while setting up the Dell Data Domain:

- Create the Security Officer role.
- Run the following commands after creating the Security Officer:

1. `authorization policy set security-officer enabled`
2. `system passphrase set`

- Create the file system by accessing the GUI:

Figure 3 : Dell Data Domain Log In Page

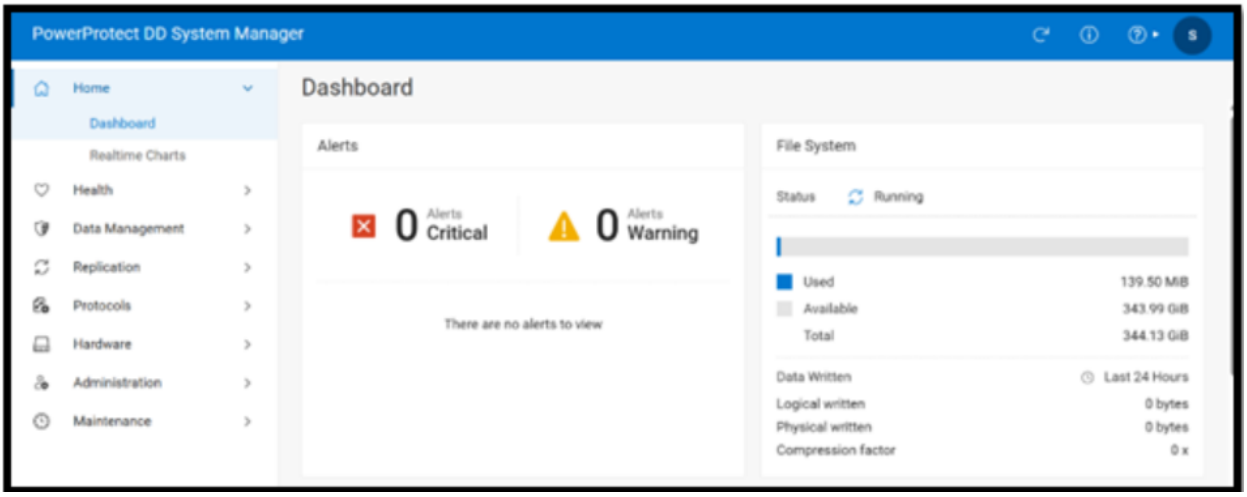


Figure 4 : Dell Data Domain Home page

```
[build@localhost ~]$ ssh sysadmin@10.222.55.126
EMC Data Domain Virtual Edition
Password:
Last login: Wed Jun 25 22:53:09 PDT 2025 from 10.222.17.153 on pts/0


Welcome to Data Domain OS 8.3.0.15-1161254
------------------------------------------
sysadmin@localhost#
```

Figure 5 : Dell Data Domain CLI screen

5 Integration Steps

5.1 Configuration on Utimaco ESKM

5.1.1 Create a Local CA

Within the ESKM Management Console, set up a local CA by following these steps:

1. Go to the **Security** tab.
2. Click on the **Certificates** option 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, such as 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**.

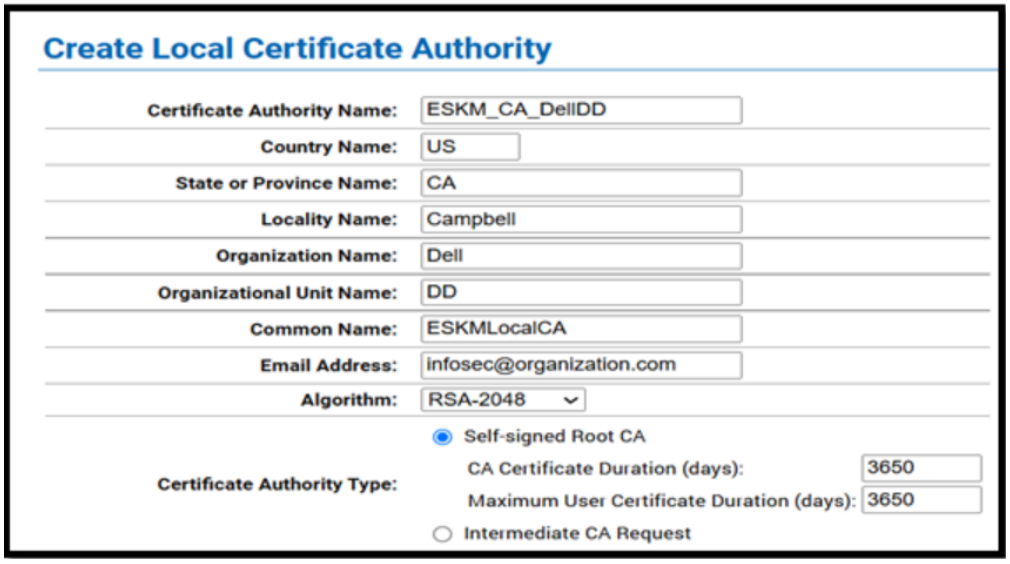


Figure 6 : Local CA Creation Page

9. Select the recently created CA Certificate.
10. Click on the **Download** button to download the CA certificate.

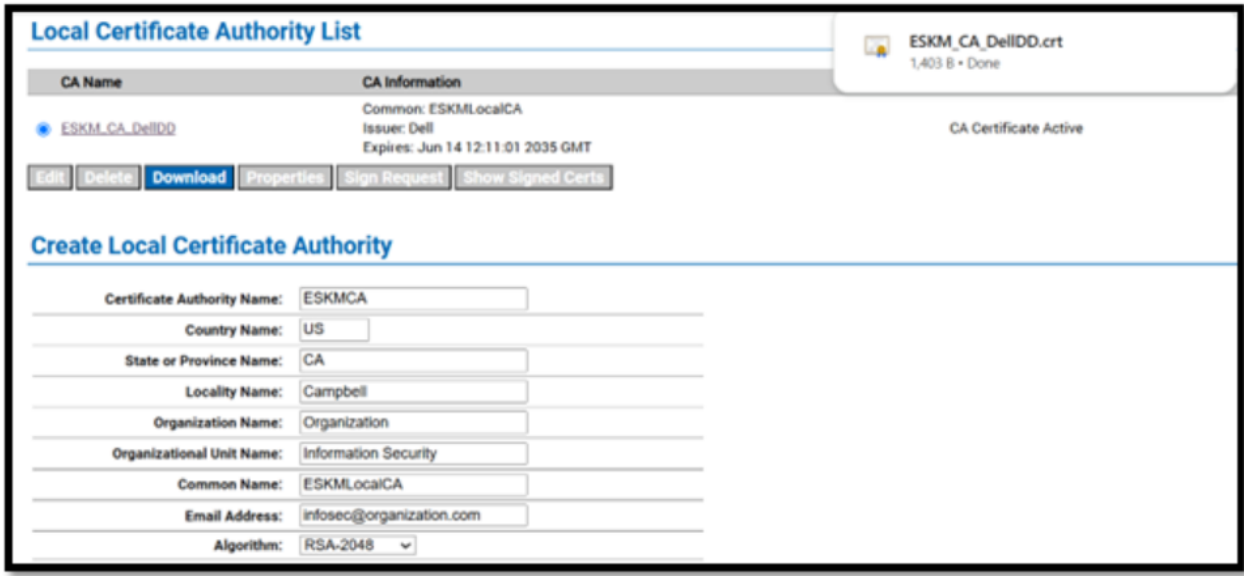


Figure 7 : Local CA details

5.1.2 Generate a Server Certificate

1. Go to the **Security** tab.

2. Click on the **Certificates** option 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** dropdown list.
7. Select Server from the **Certificate Purpose** dropdown list.
8. Click on the **Create** button.

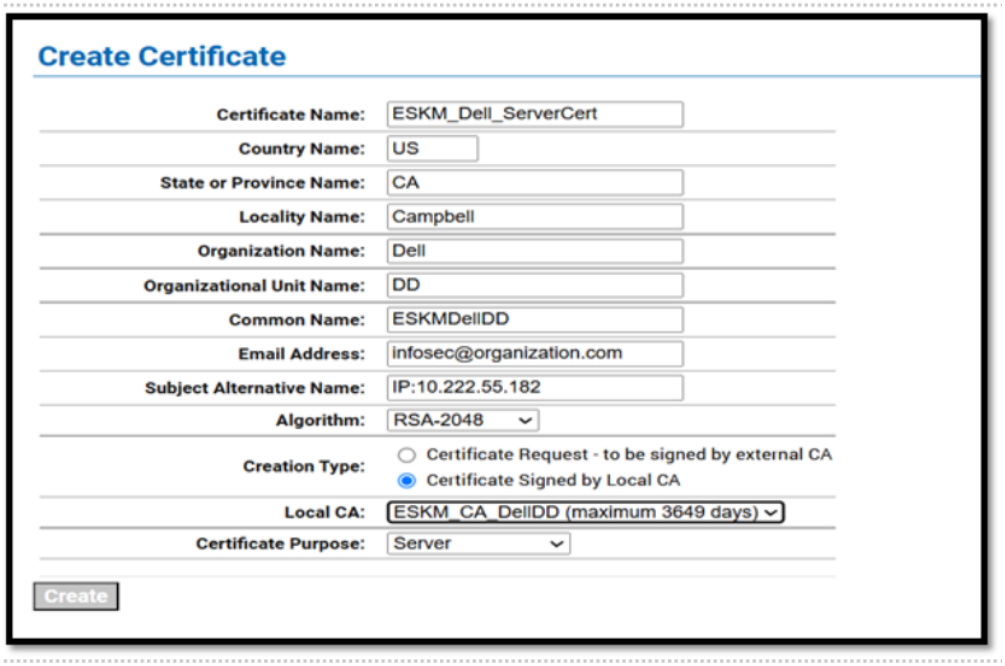


Figure 8 : Server Certificate

5.1.3 KMIP Server Configuration

1. Go to the **Device** tab.

2. From the left side panel, click on the **KMIP Server** option under **Device Configuration**.
3. Click the **Edit** button on the main page.
4. Choose the created server certificate as the server certificate for the KMIP server.
5. Click the **Save** button.

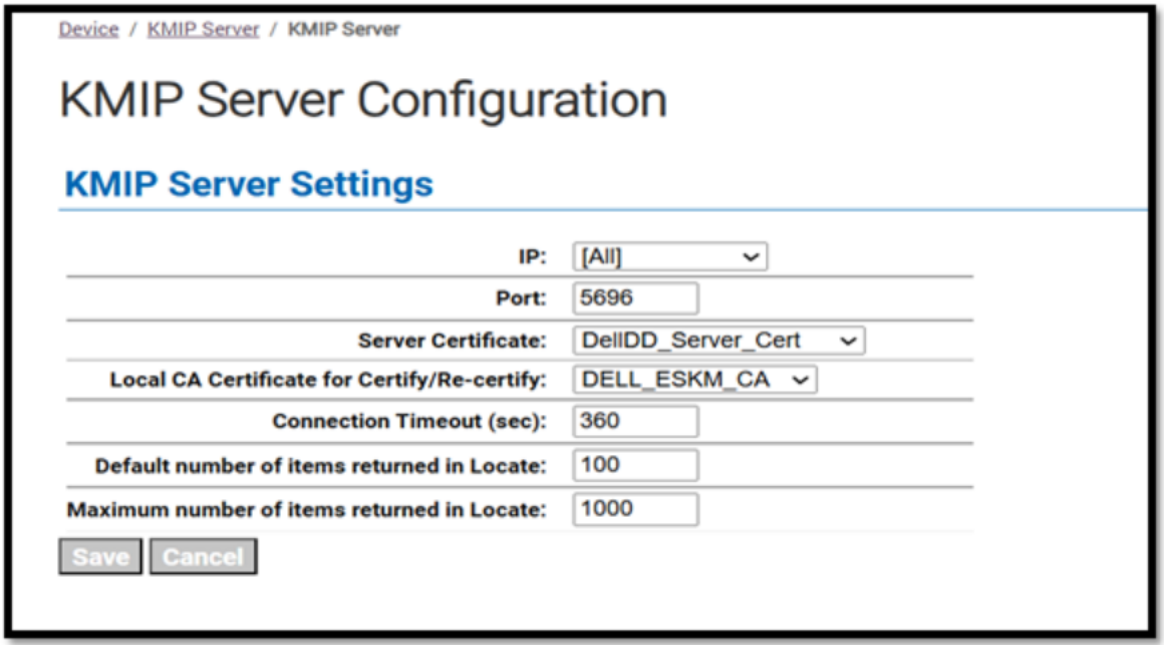


Figure 9 : KMIP Server Configuration

5.1.4 Sign the Host Certificate using ESKM

See section Create a Data Domain Host Certificate and complete all related steps before performing the steps below.

1. Copy the host certificate signing request (`CertificateSigningRequest.csr`) from the Dell DD for signing with the ESKM local CA. The following command can copy the CSR to a Linux machine.

```
    $scp sysadmin@<DDServerIP>:/ddvar/certificates/
CertificateSigningRequest.csr
```

2. Open the ESKM Management Console, click the **Security** tab, and then click on the **Local CAs** link in the Certificates & CAs section.
3. Select the previously created CA certificate name from the Sign with Certificate Authority.

4. Select the radio button **Client** in the **Certificate Purpose** section.
5. Copy the host certificate content to the **Certificate Request** box.

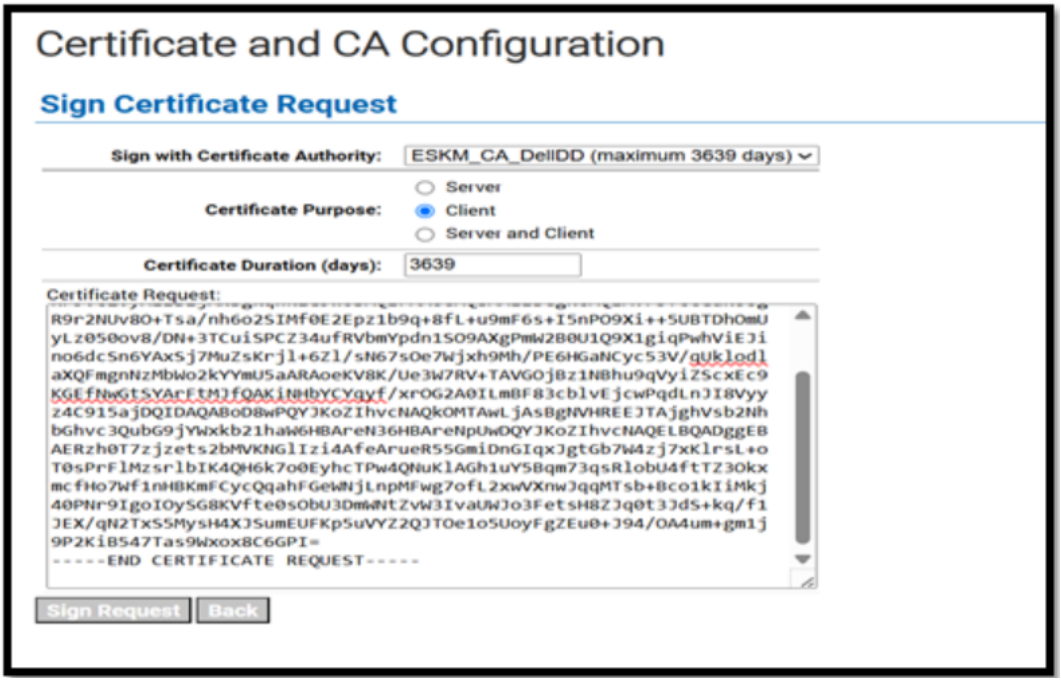


Figure 10 : Sign Certificate Request

6. Click on the **Sign Request** button.

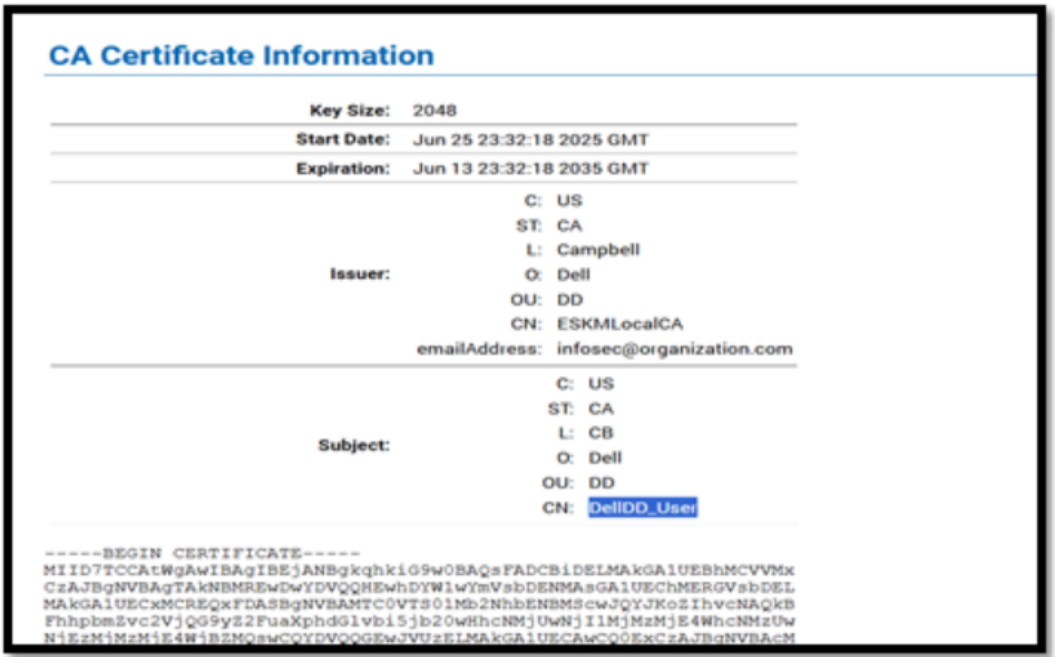


Figure 11 : Signed Host Certificate Details

7. Note down the common name and copy the signed certificate content to create a KMIP user.
8. Click on the **Download** button to download the signed host certificate file.

5.1.5 Create a Local User in ESKM

Perform the following steps to create a local user in the ESKM:

1. Go to the **Security** tab.
2. In **Users & Groups** > **Local Users and Groups**, select **Local Users**.
3. Scroll down and click **Add**.
4. Enter the **Username** in the same way as the common name provided during host certificate creation.
5. Select **Enable KMIP**.
6. Select KMIP as **License Type**.
7. Paste the downloaded client certificate in **KMIP Client Certificate** .
8. Click **Create**.

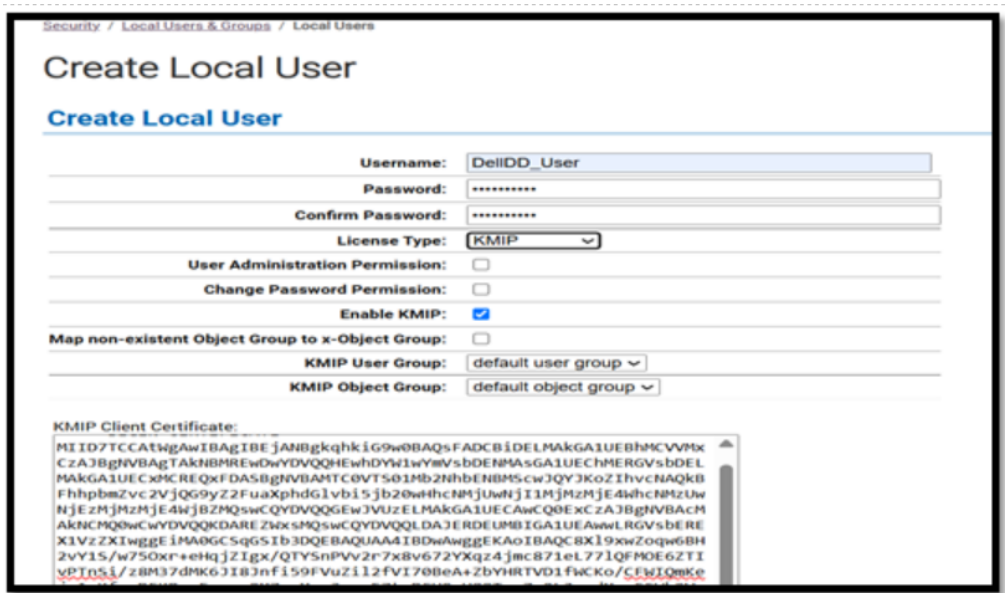


Figure 12 : Local User Creation

Figure 13 : Created Local User details

5.2 Configuration on Dell Data Domain Side

5.2.1 Create a Data Domain Host Certificate

Run the `adminaccess certificate cert-signing-request generate` command in DD system to generate a host certificate.

```
# adminaccess certificate cert-signing-request generate key-strength 2048bit country US state <state> city <city> org-name Dell org-unit DD common-name <username>
```

The `.csr` file will be generated in `/ddr/var/certificates/CertificateSigningRequest.csr`.

Figure 14 : Host Certificate

5.2.2 Import the CA and Host Certificates to Dell DD System

See Sign the host certificate using ESKM and complete all related steps before performing the steps below:

1. Copy the downloaded ESKM local CA certificate and signed host certificate to the `ddr/var/Certificates` folder in the Dell DD system. The following `scp` command can be used to copy ESKM local CA certificate and the signed host certificate to a Linux machine.

- `scp signed.crt <username>@<DDServerIP >:/ddr/var/Certificates`
- `scp ESKM_CA_DellDD.crt<username>@<DDServerIP>:/ddr/var /Certificates`

2. Run the `adminaccess certificate import` command on the DD system to import the host certificate and the CA certificate.

- `adminaccess certificate import host application gklm file <hostfilename>.crt`

```
sysadmin@localhost# adminaccess certificate import host application gklm file signed.crt

The SHA1 fingerprint for the imported host certificate is:
9D:23:F7:ED:A3:F4:8A:D7:76:8F:7B:F4:7B:59:4E:BD:7C:D3:74:A3

       Do you want to import this certificate? (yes|no) [yes]: yes
Host certificate imported for applications(s) : "gklm".
```

Figure 15 : Host certificate imported

- `adminaccess certificate import ca application file <cacertificate>.crt`

```
sysadmin@localhost# adminaccess certificate import ca application gklm  file ESKM_CA_DellDD.crt

The SHA1 fingerprint for the imported CA certificate is:
16:C4:47:E4:18:A3:9F:D1:40:A4:04:28:B0:9F:C0:FA:F5:43:5A:E0

       Do you want to import this certificate? (yes|no) [yes]: yes
CA certificate imported for application(s) : "gklm".
```

3. Run the `adminaccess certificate show` command to verify the host and CA certificates are present.

```
sysadmin@localhost# adminaccess certificate show
Subject                Type           Application   Valid From                Valid Until               Fingerp
nt
--------------------   ------------   -----------   -----------------------   -----------------------   -------
-------------------------------------------------
localhost.localdomain  host           https         Sun May 04 01:46:57 2025  Thu Jun 04 01:46:57 2026  08:54:8
9C:F1:FA:79:1B:AA:D5:10:ED:F9:A2:A2:47:BF:96:43:00
localhost.localdomain  ca             trusted-ca    Tue Jun 04 01:46:57 2024  Mon Jun 03 01:46:57 2030  85:BD:D
3F:00:8A:92:39:69:DB:BB:09:44:9C:74:B1:E3:CD:6D:A7
DellDD_User            imported-host  gklm          Sun Jun 15 11:23:54 2025  Sun Jun 10 11:23:54 2035  9D:23:F
ED:A3:F4:8A:D7:76:8F:7B:F4:7B:59:4E:BD:7C:D3:74:A3
ESKMLocalCA            imported-ca    gklm          Sun Jun 15 05:11:01 2025  Thu Jun 14 05:11:01 2035  16:C4:4
84:18:A3:9F:D1:40:A4:04:28:B0:9F:C0:FA:F5:43:5A:E0
--------------------   ------------   -----------   -----------------------   -----------------------   -------
-------------------------------------------------
Certificate signing request (CSR) exists at /ddr/var/certificates/CertificateSigningRequest.csr
sysadmin@localhost# sysadmin@localhost#
```

Figure 16 : Certificate Details

5.2.3 Set ESKM as Key Manager

1. Run `the filesys encryption key-manager set command` to configure the system to use ESKM as key manager.

- `$filesys encryption key-manager set server <IP> port 5696 key-class <class name> server-type gklm kmip-user <username>`.

```
sysadmin@localhost# filesys encryption key-manager set server 10.222.55.182 port 5696 key-clas
s NA server-type gklm kmip-user DellDD_User
The current key-manager configuration is:
Key Manager:                            Disabled
Server Type:                            GKLM
Server:                                 10.222.55.182
Port:                                   5696
Status:                                 Online
Key-class:                              NA
KMIP-user:                              DellDD_User
Key rotation period:                    not-configured
Last key rotation date:                 N/A
Next key rotation date:                 N/A
sysadmin@localhost# sysadmin@localhost#
```

Figure 17 : ESKM set as Key manager in Dell Data Domain

2. Run the `filesys encryption key-manager enable` command to enable key management with ESKM , if key manager is disabled.

```
sysadmin@localhost# sysadmin@localhost# filesys encryption key-manager enable
Key manager is enabled.
sysadmin@localhost#
```

Figure 18 : Key Manager enabled in Dell Data Domain

3. Run the `filesys encryption key-manager show` command to verify key management is enabled.

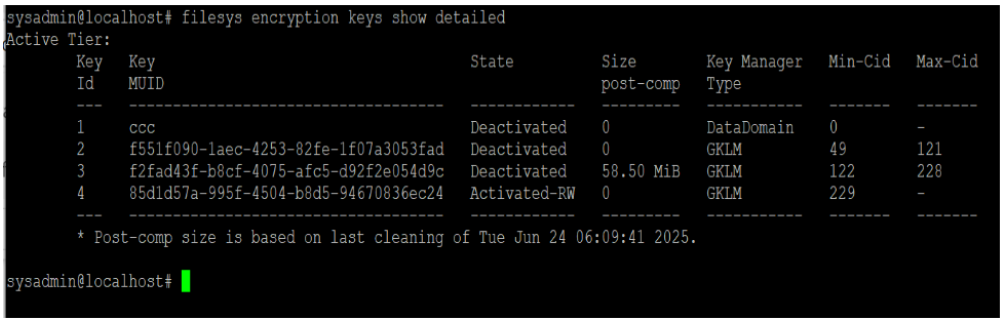
```
sysadmin@localhost# filesys encryption key-manager enable

Key manager is already enabled.

sysadmin@localhost# filesys encryption key-manager show
The current key-manager configuration is:
Key Manager:                            Enabled
Server Type:                            GKLM
Server:                                 10.222.55.182
Port:                                   5696
Status:                                 Online
Key-class:                              NA
KMIP-user:                              DellDD_User
Key rotation period:                    not-configured
Last key rotation date:                 N/A
Next key rotation date:                 N/A
sysadmin@localhost# sysadmin@localhost#
```

Figure 19 : Key manager configuration details

4. Run the `filesys encryption keys show detailed` command to view the ESKM keys created on the system.



```
sysadmin@localhost# filesys encryption keys show detailed
Active Tier:
        Key   Key                                  State         Size        Key Manager   Min-Cid   Max-Cid
        Id    MUID                                               post-comp   Type
        ---   ----------------------------------   -----------   ---------   -----------   -------   -------
        1     ccc                                  Deactivated   0           DataDomain    0         -
        2     f551f090-1aec-4253-82fe-1f07a3053fad Deactivated   0           GKLM          49        121
        3     f2fad43f-b8cf-4075-afc5-d92f2e054d9c Deactivated   58.50 MiB   GKLM          122       228
        4     85d1d57a-995f-4504-b8d5-94670836ec24 Activated-RW  0           GKLM          229       -
        ---   ----------------------------------   -----------   ---------   -----------   -------   -------
        * Post-comp size is based on last cleaning of Tue Jun 24 06:09:41 2025.

sysadmin@localhost#
```

Run the `filesys restart` command to activate the key if it is in a deactivated state.

6 Verification and Testing

6.1 Logs and Validation Steps

1. In ESKM Management Console, click on **Security tab**
2. Click on **KMIP Objects** link in **Keys & KMIP Objects**

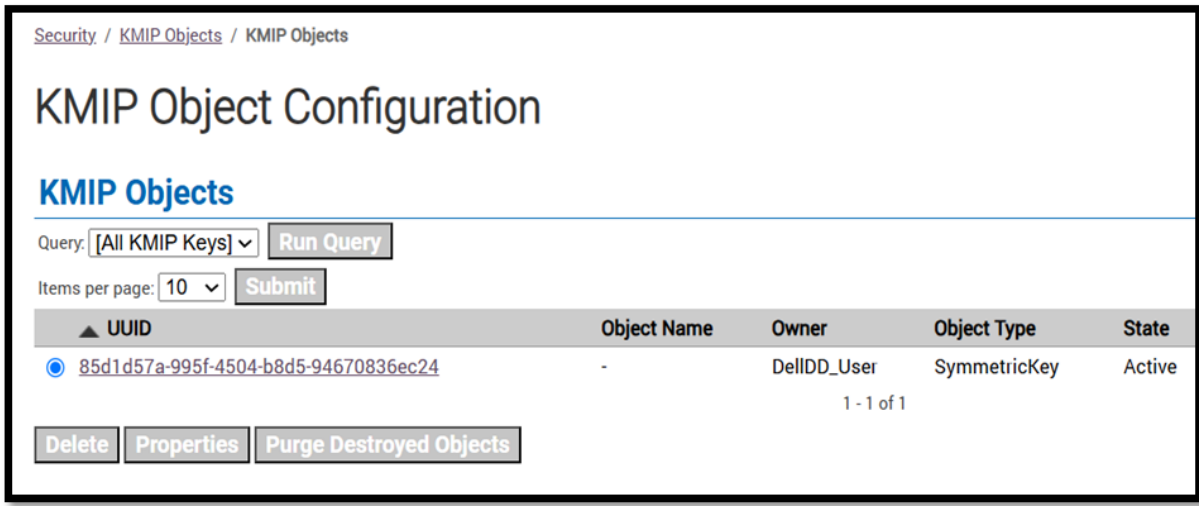


Figure 20 : Key details displayed in ESKM

3. Open ESKM Management Console and click on **Device** tab.
4. Click on **Log Viewer** under Logs & Statistics.
5. Click on **KMIP** under Log Viewer.

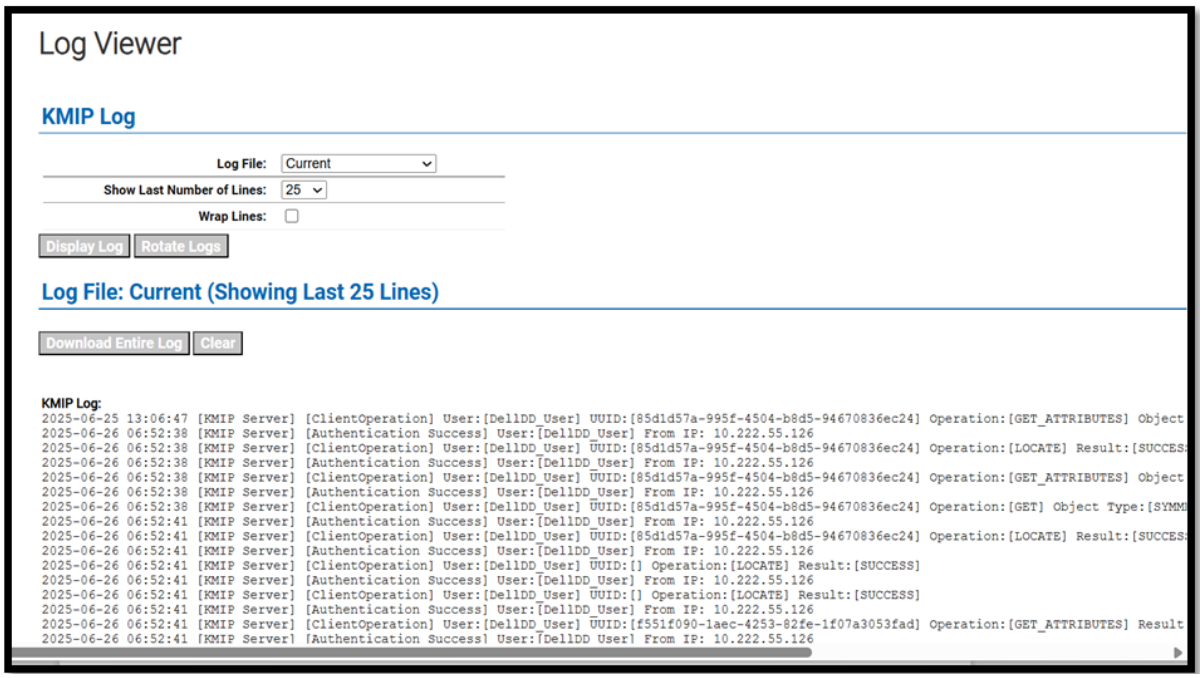


Figure 21 : Log details displayed in ESKM

7 Troubleshooting

7.1 Log Locations and Interpretation

Verify the Utimaco ESKM logs by following the steps below:

1. Open the ESKM Management Console and click on the **Device** tab.
2. Click on **Log Viewer** under **Logs & Statistics**.
3. Click on **KMIP** under **Log Viewer**
4. Review logs related to operations performed on the Dell Data Domain.

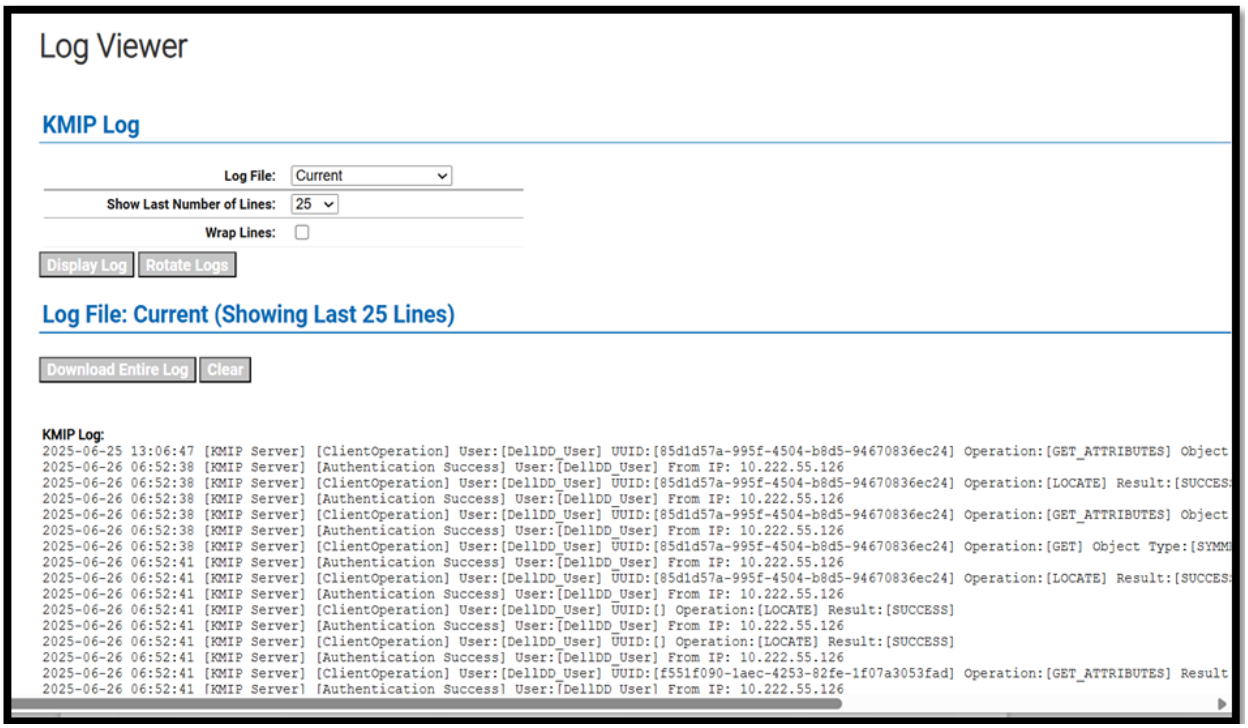


Figure 22 : Log details displayed in ESKM

8 Contact for Support

8.1 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:

Technical support registration number or NonStop system number (if applicable)

1. Service Agreement ID number (SAID)
2. Product serial numbers
3. Error messages
4. Software version number

8.2 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 Dell Data Domain.

For more information on other Utimaco products and offerings, please visit the official Utimaco website. *Utimaco Portal* .

9.2 Command Summary

DDOS Commands Used	Purpose
`#adminaccess certificate cert-signing-request generate`	To generate a host certificate
`# adminaccess certificate import`	To import a certificate (CA and Host) into the system.
`# adminaccess certificate show`	To view all the certificates available in the system.
`# filesys encryption key-manager enable`	To enable the key manager.
`# filesys encryption key-manager show`	Verify whether key management is enabled.
`# filesys encryption keys show detailed`	To view the keys created on the system.

Table 5: List of Commands Used