Dell EMC

Integration Guide

ESKM

v8.54.0

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	2025-07-22
Status	PUBLISHED
Document No.	IG-2025-0040

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. This Integration Guide outlines the instructions for integrating Utimaco Enterprise Security Key Manager (ESKM) with Dell EMC Data Domain DD3300 using the KMIP Protocol. The integration enables secure and centralized management of encryption keys for Data Domain Systems, enhancing data protection and ensuring compliance with regulatory requirements.

This document details the necessary configuration process and validation steps required to integrate ESKM with DD3300.

1.1 About This Guide

This guide provides detailed instructions for integrating the Utimaco Enterprise Secure Key Manager (ESKM) with Dell EMC Data Domain DD3300 using the KMIP Protocol.

1.2 Target Audience

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

1.3 Purpose of the Integration

The purpose of this integration is to configure Dell EMC Data Domain DD3300 as a KMIP Client to use Utimaco Enterprise Secure Key Manager as External Key Management Server (KMS). This integration enables secure and centralized management of encryption keys, ensures that keys are stored separately from the data they protect, enhances data security, and helps to meet compliance requirements.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	ESKM Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol

Abbreviation	Meaning
DDVE	Data Domain Virtual Edition
DDOS	Data Domain Operating System
KMS	Key Management Server
CA	Certificate Authority

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **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 2: 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.

2 Product Overview

2.1 Dell EMC Data Domain DD3300

The Dell EMC Data Domain DD3300 is a backup storage appliance that reduces storage requirements through deduplication, eliminating duplicate data and improving storage efficiency.

In this integration, DD3300 connects to Utimaco ESKM, which acts as an external Key Management Server (KMS) using the KMIP Protocol. This setup allows DD3300 to manage encryption keys securely, enhance data protection, and ensure compliance with security standards.

2.2 Utimaco ESKM

The Utimaco Enterprise Secure Key Manager (ESKM) is a centralized key management solution that securely manages encryption keys. It acts as a Key Management Server (KSM) using KMIP protocol.

In this integration, ESKM manages the encryption keys for the Dell EMC Data Domain DD3300, ensuring that the keys are stored securely and managed separately from the data they protect. This enhances data security, simplifies key management, and supports compliance with data protection standards.

2.3 Joint Value Proposition

The Integration of Dell EMC Data Domain DD3300 with Utimaco ESKM provides a secure and efficient data protection solution. DD3300 offers reliable backup and storage with deduplication, while ESKM manages encryption keys centrally and securely using the KMIP protocol.

Together, this integration:

- Protects critical backup data with strong encryption.
- Ensures encryption keys are managed separately from the data for enhanced security.
- Simplifies compliance with data protection and regulatory requirements.
- Reduces storage needs through deduplication while maintaining data security.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Dell Data Domain OS Version	Utimaco ESKM Version
DDOS 8.3	8.54.0

Table 3: Tested Versions

3.2 Software Requirements

Software	Software Requirements
DDOS	DDOS 8.3 or later
Utimaco ESKM	8.54.0 or later

Table 4: Software Requirements

3.3 Prerequisites

- DDOS 8.3 or later.
- Utimaco ESKM version 8.54.0 or later.
- Admin access to both DDOS and ESKM.
- Network connectivity between DD3300 and ESKM over TCP port 5696.

3.4 Hardware Requirements

Hardware	Hardware Requirements
Filesystem in vSphere	500GB disk filesystem in vSphere

Table 5: Hardware Requirements

4 Installation and Configuration

4.1 Setting Up Utimaco ESKM

Configuring the ESKM is the initial step before proceeding with Dell EMC DD3300 Integration. For detailed configuration steps, refer to the "*ESKM_Installation and Replacement_Guide_8.54.0*".

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

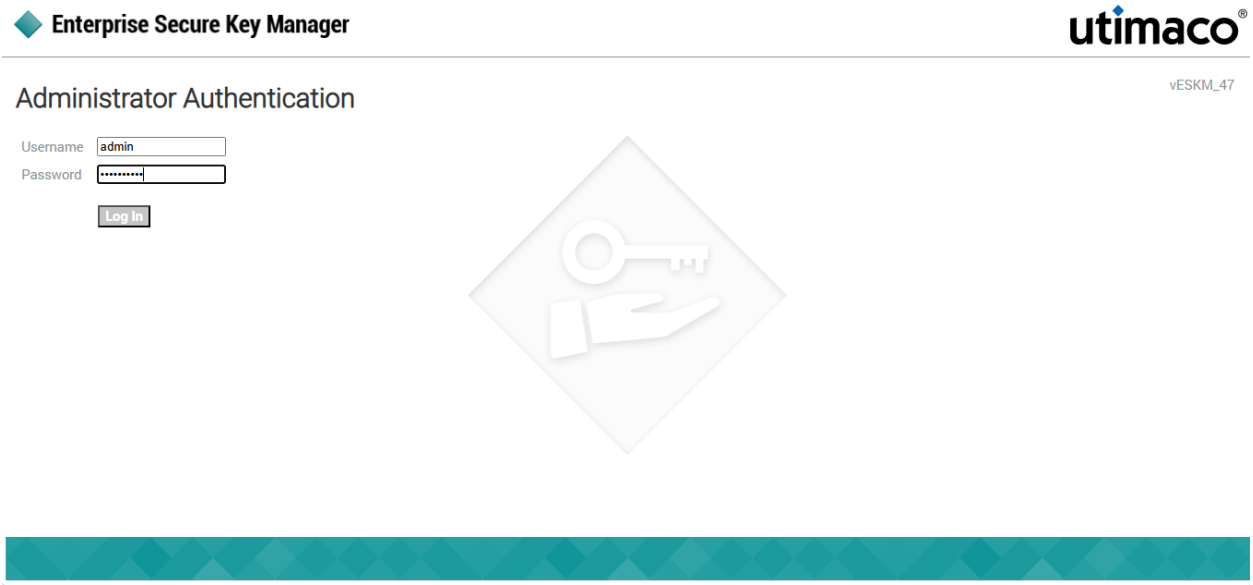

Figure 1 : ESKM Login Page

4.2 Setting UP Dell EMC Data Domain DD3300

Please refer to the installation and administration guide for setting up the Dell Data Domain: https://www.dell.com/support/home/product-support/product/emc-data-domain-dd3300/docs.

5 Integration Steps

5.1 Configuring on Utimaco ESKM

It is essential to configure Utimaco ESKM to ensure secure and efficient key management. This section guides you through the necessary steps to configure ESKM for Dell EMC DD3300 integration.

5.1.1 Date & Time Configuration

1. Go to **Device** > **Date & Time**.
2. Set the **Time Zone & NTP**.

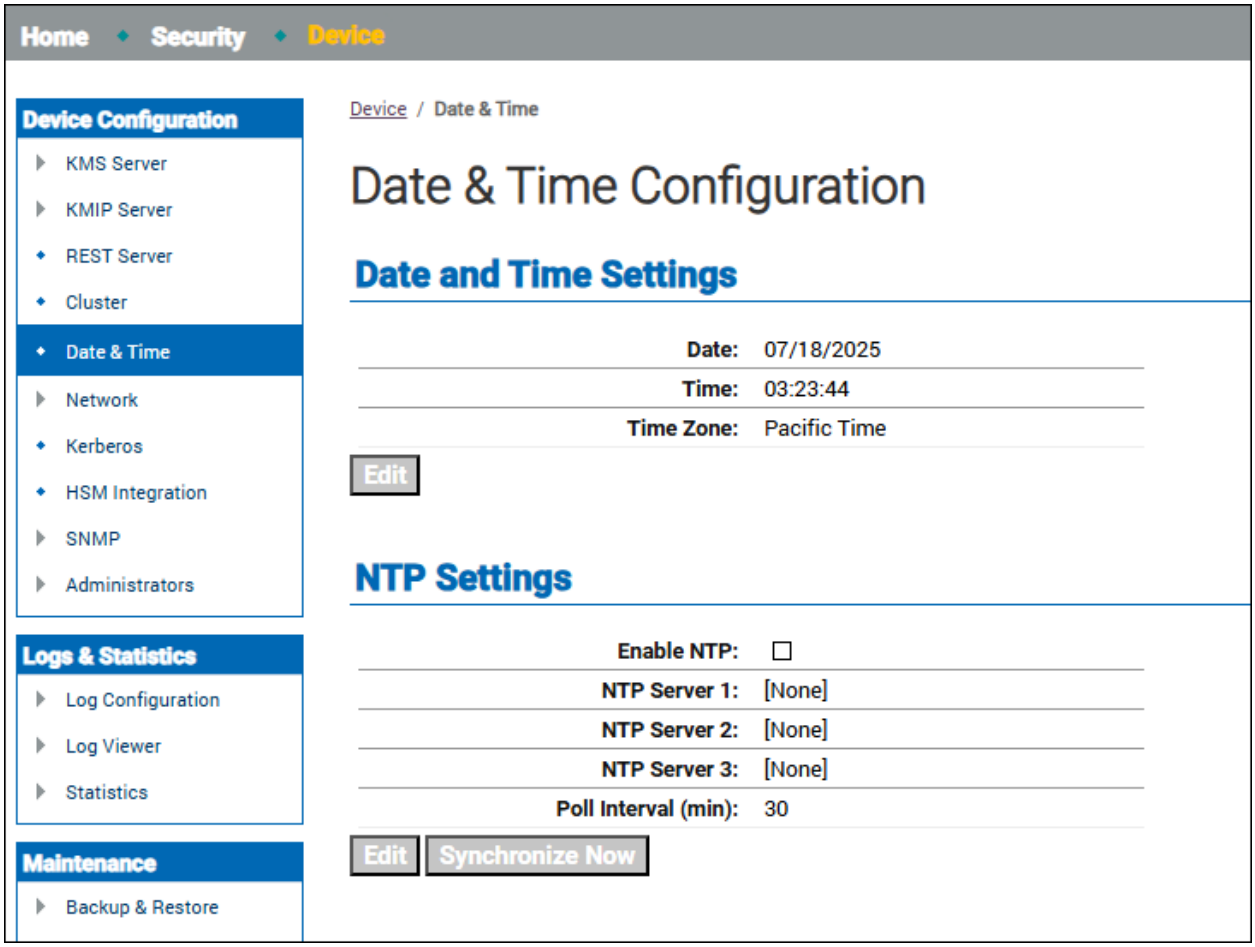

Figure 2 : Date and Time Configuration

5.1.2 Setting Up 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.**
2. Select the **Security** tab.
3. In **Certificates & CAs**, click **Local CAs**.
4. Scroll down to the **Create Certificate section**.
5. Enter a **Certificate Authority Name and Common Name**. These may have the same value, such as ESKM Local CA.
6. Enter your **Organizational** information.
7. Select the **Algorithm** (e.g., RSA-2048).
8. 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.
9. Click on **Create**.

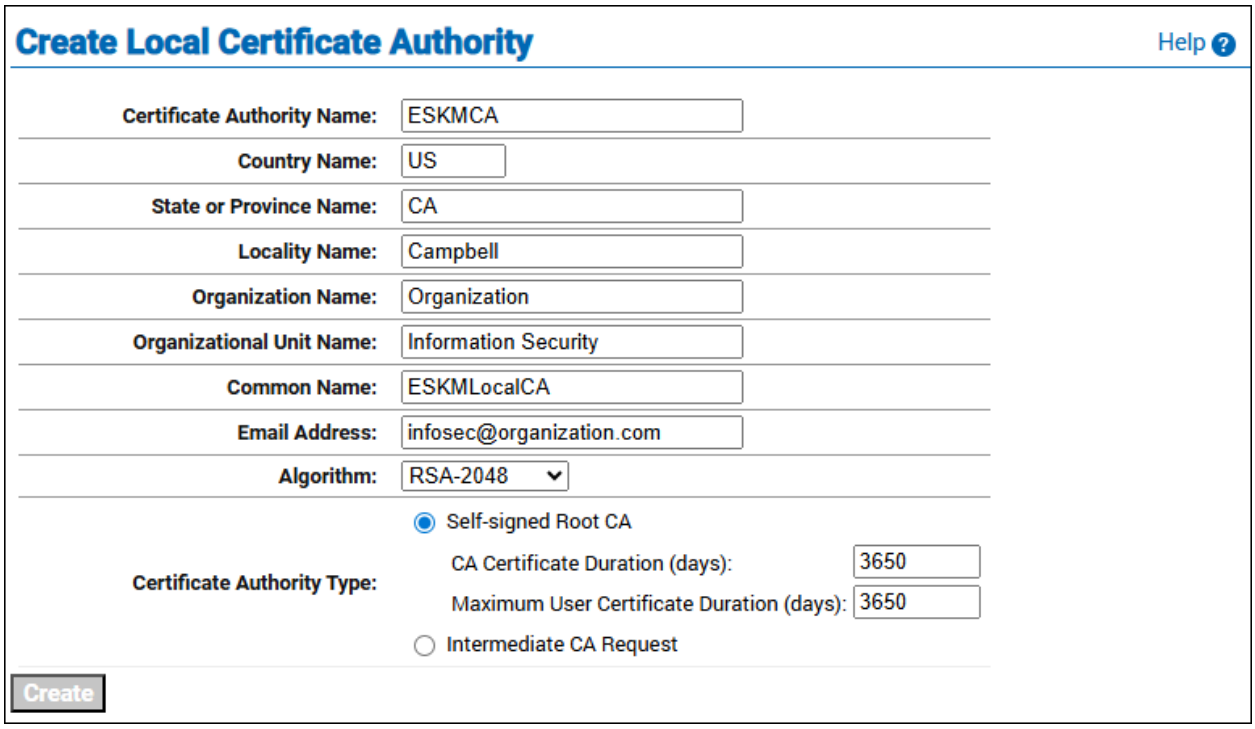

Figure 3 : Create Local CA

10. Select the created CA Certificate.
11. Click **Download** button to download the CA certificate.

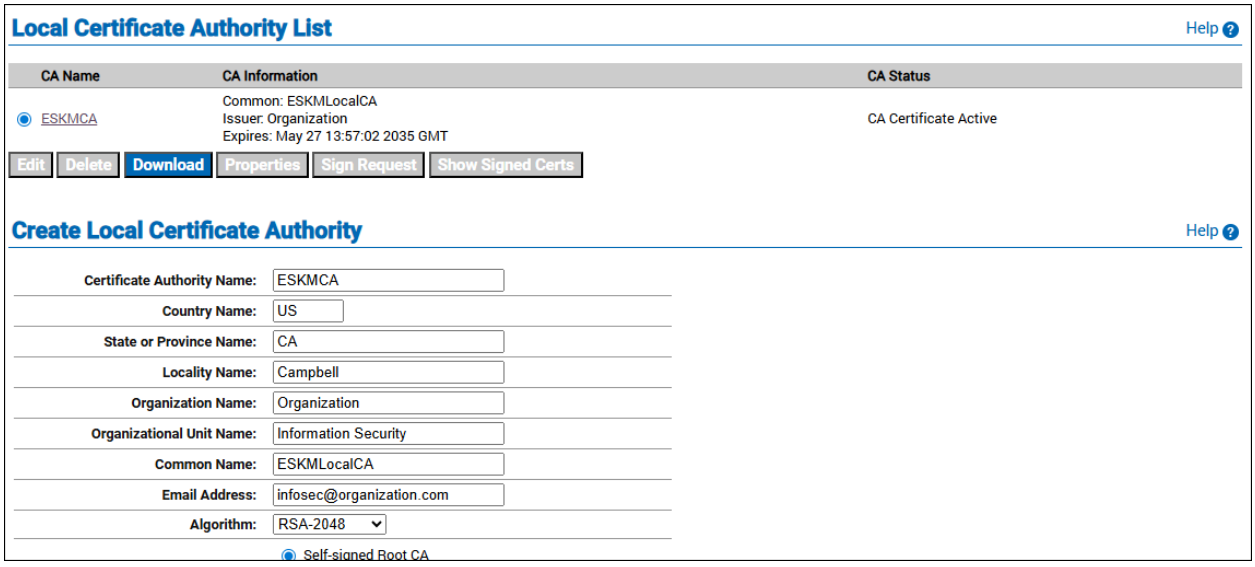

Figure 4 : Local CA

5.1.3 Setting Up ESKM Certificate

The ESKM Server Certificate is required to enable secure communication between DD3300 (KMIP Client) and ESKM (KMIP Server). It allows DD3300 to the authenticate the ESKM server during the TLS/SSL handshake, ensuring the connection is trusted and encrypted.

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

1. Click the **Security** tab.
2. In **Certificates and CAs**, select **Certificates**.
3. Enter **Certificate Name, Country Name, State and Province Name, Locality Name, Organization Name,** and **Organization Unit Name**.
4. Select **RSA-2408** from the **Algorithm** dropdown list.
5. Select the previously created CA certificate name from the **Local CA** dropdown list.
6. Select Server from the **Certificate Purpose** dropdown list.
7. Click **Create**.

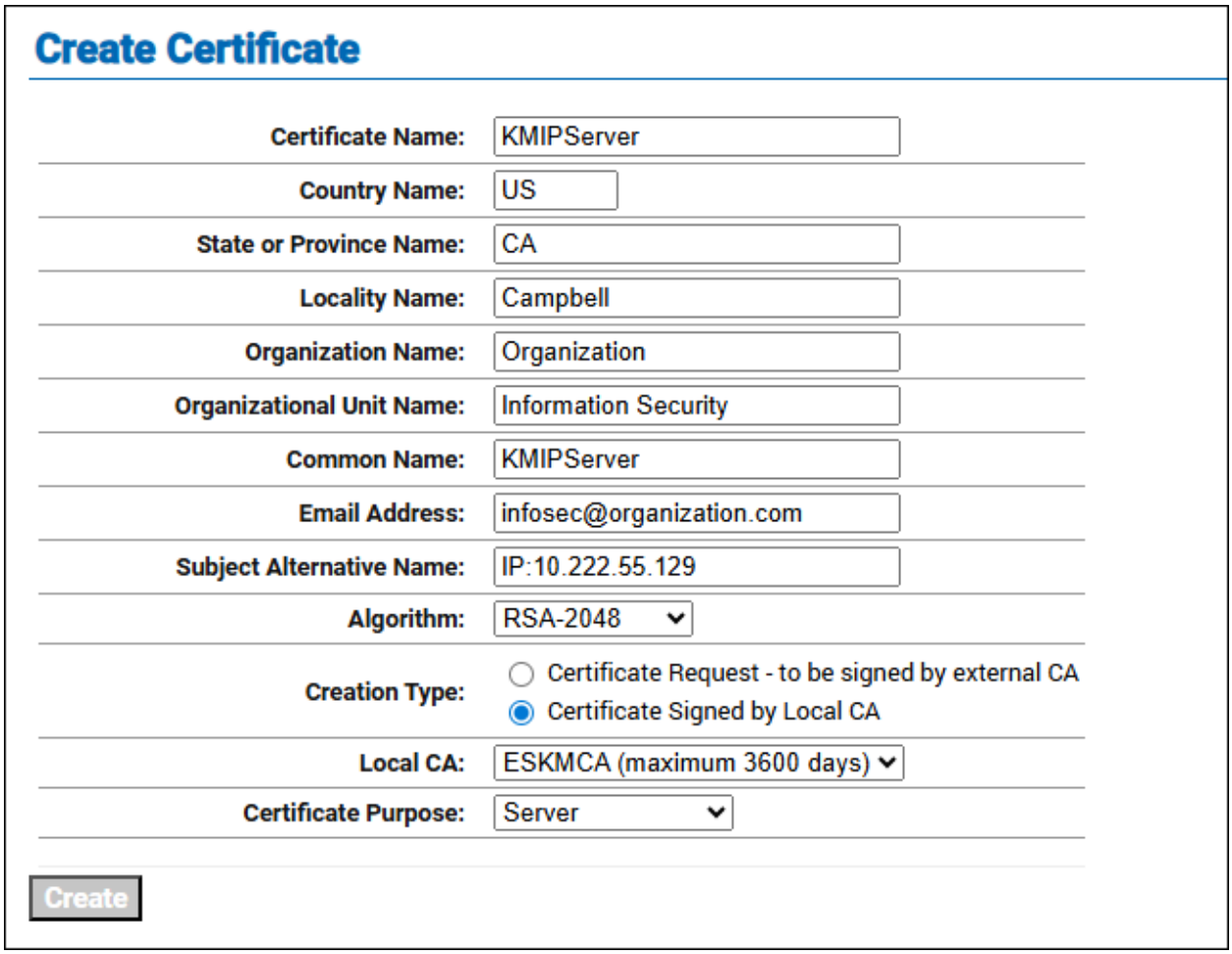

Figure 5 : Create Certificate

5.1.4 KMIP Server Configuration

1. Login to the **ESKM Management Console**
2. In the **Device**, select **KMIP Server** > **KMIP Server**.
3. Select relevant KMIP **Port**.
4. Select the created server certificate as the **Server Certificate** for the KMIP server
5. Select **Local CA** from the drop-down list.
6. Click **Save**.

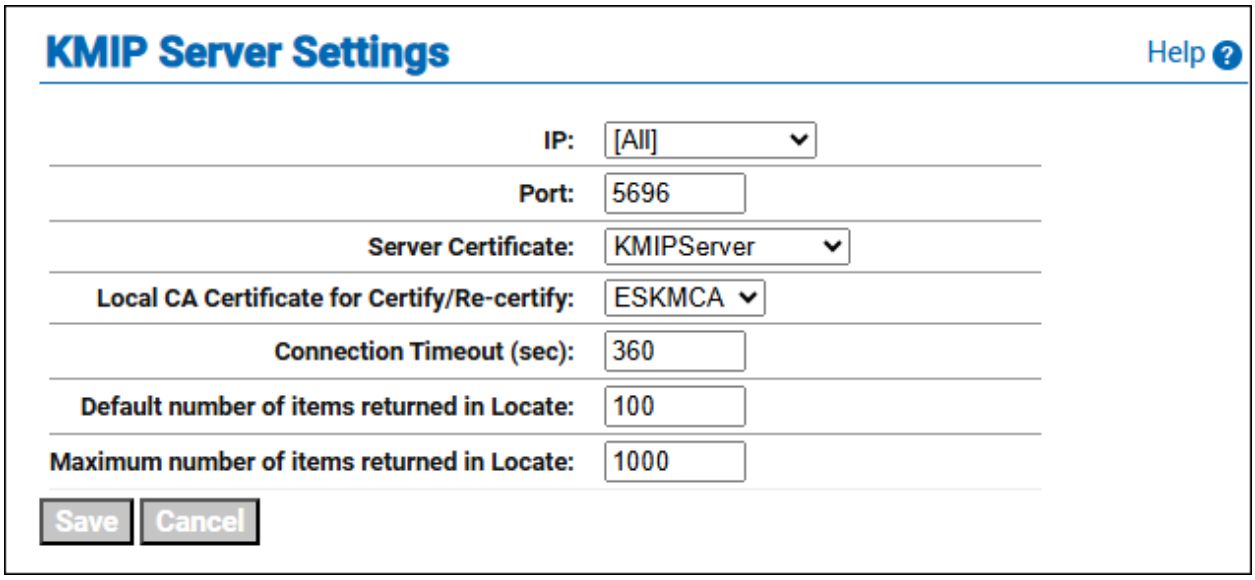

Figure 6 : KMIP Server Settings

5.1.5 KMIP Interoperability Configuration

1. In the **Device**, select **KMIP Server** > **KMIP Interoperability**.
2. Grant appropriate KMIP role interaction permissions. Click **Save**.

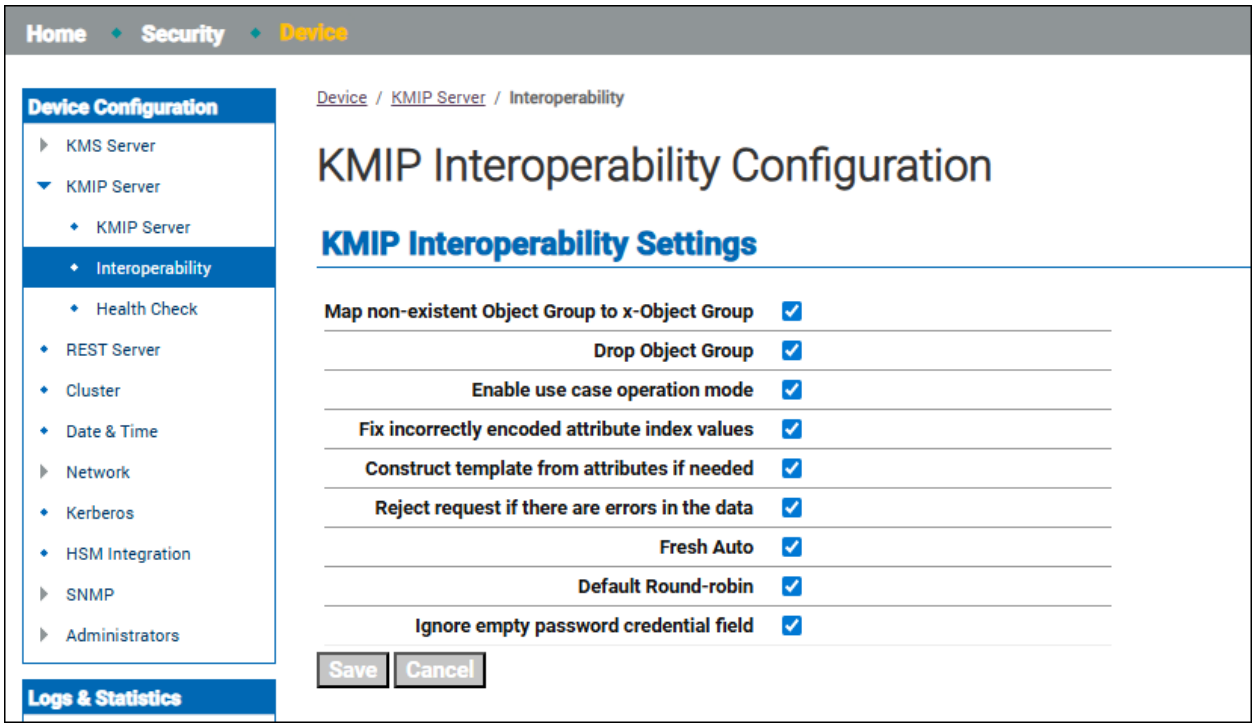

Figure 7 : KMIP Interoperability Configuration

5.1.6 Sign the Host Certificate using ESKM

Refer to steps 5 to 7 in Configuring on Dell Data Domain DD3300 and ensure that all the steps are completed before proceeding with the steps below.

1. Copy the host certificate signing request (**CertificateSigningRequest.csr**) from the Dell DD3300 for signing with the ESKM local CA.
2. Go to **ESKM Management Console** > **Security** > **Certificates & CAs** > **Local CAs** .
3. Select the previously created CA certificate name from the Sign with Certificate Authority.
4. Select **Client** in the Certificate Purpose section.
5. Copy the host certificate content to the Certificate Request box.

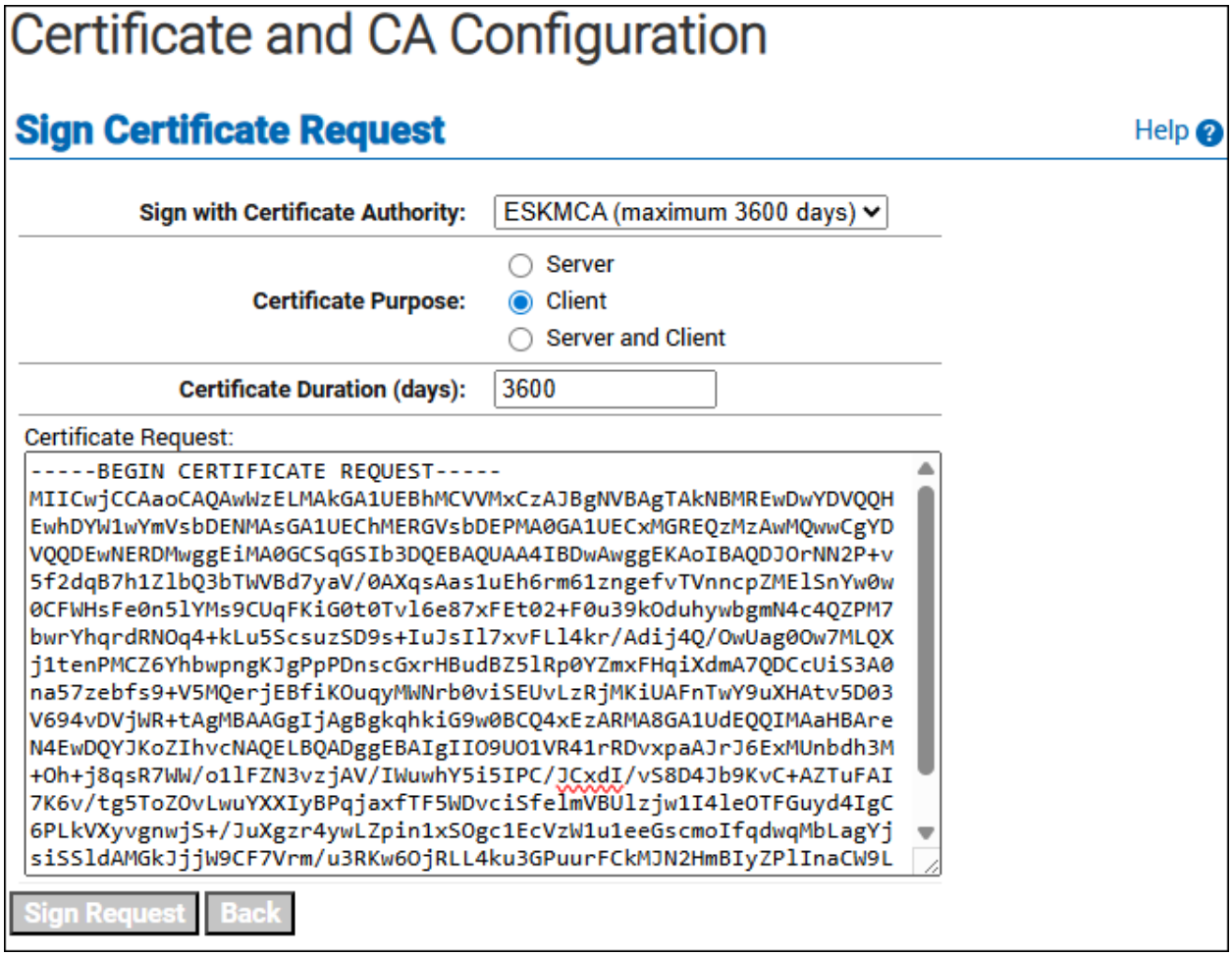

Figure 8 : Sign Certificate Request

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

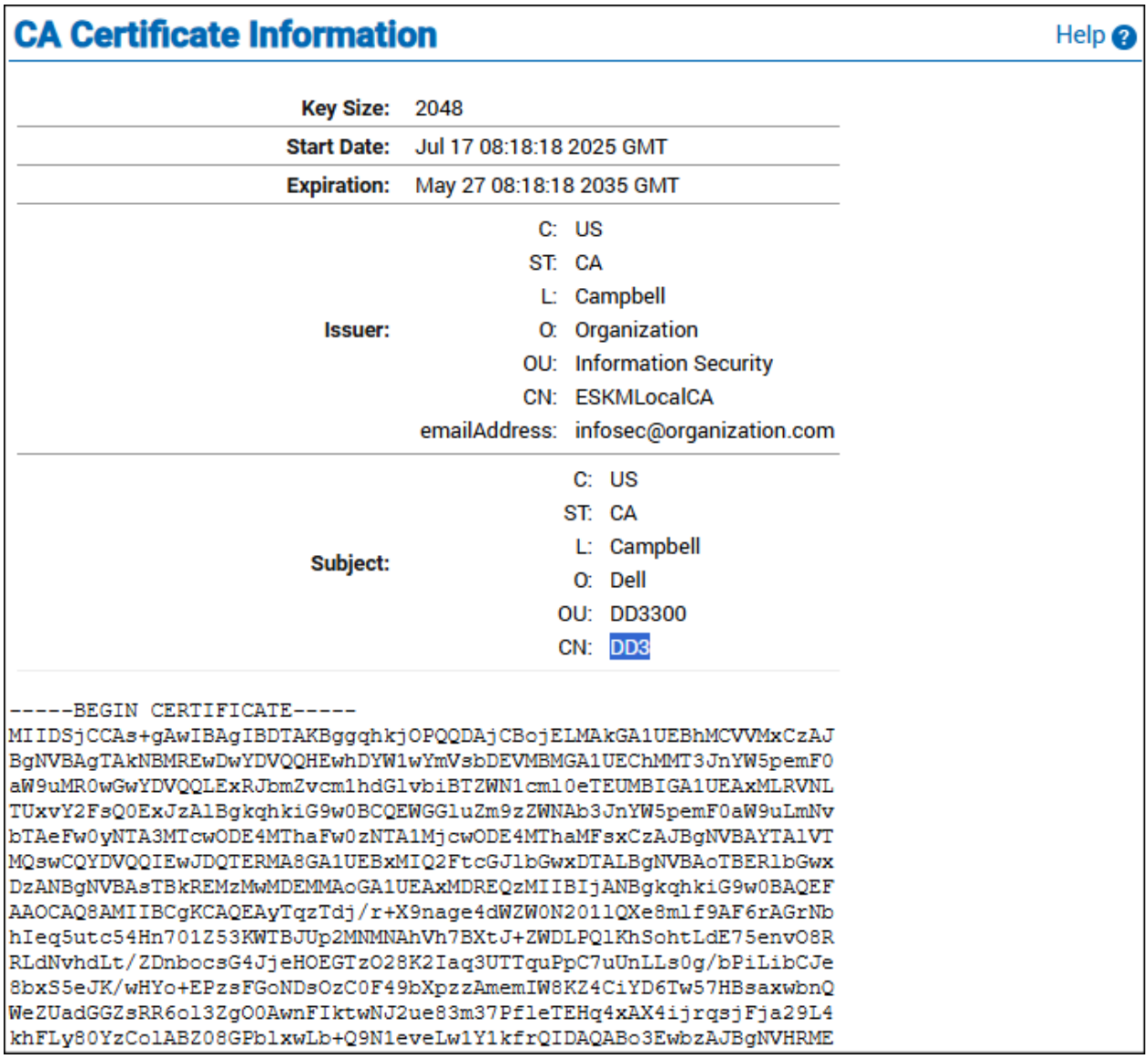

Figure 9 : CA Certificate Information

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

5.1.7 Create KMIP user

1. Login to **ESKM Management Console**,
2. In the **Security** tab, select **Users & Groups** > **Local Users & Groups** > **Local Users**.

3. 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 (refer Setting Up ESKM Certificate) in KMIP Client Certificate.

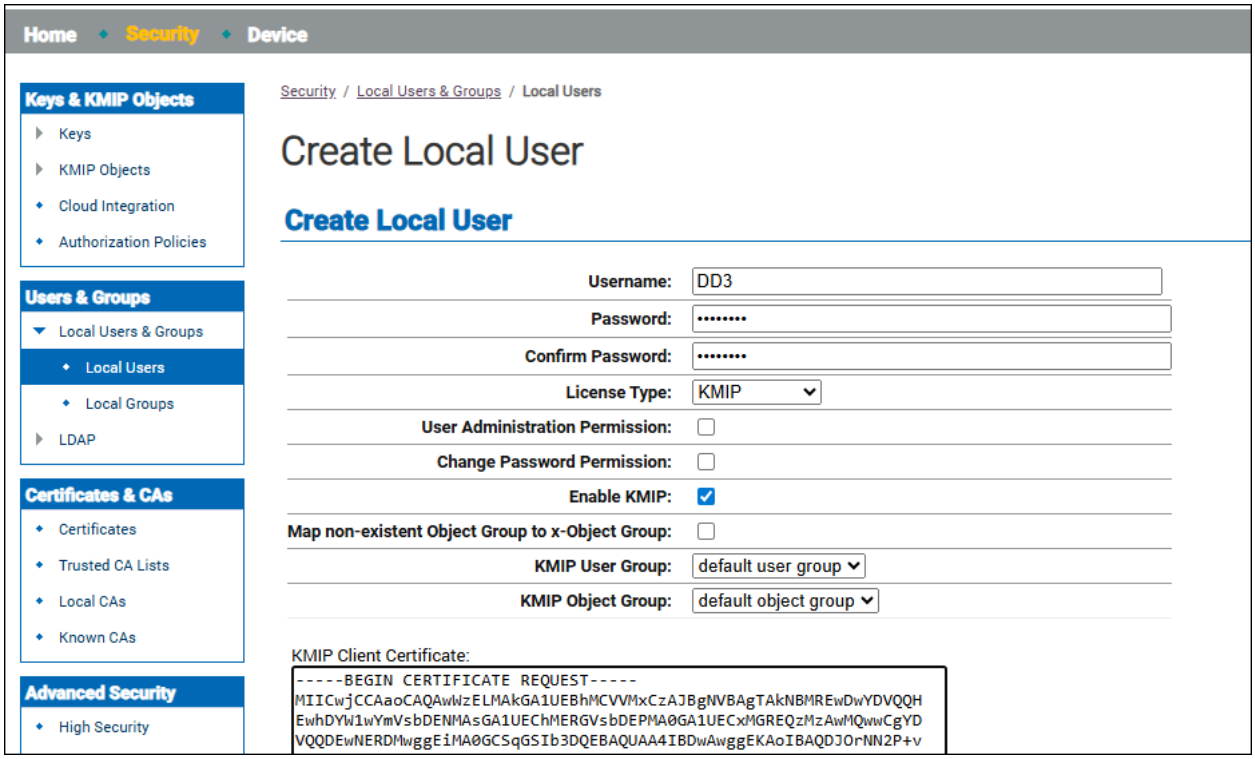

Figure 10 : Create KMIP User

8. Click **Create**.

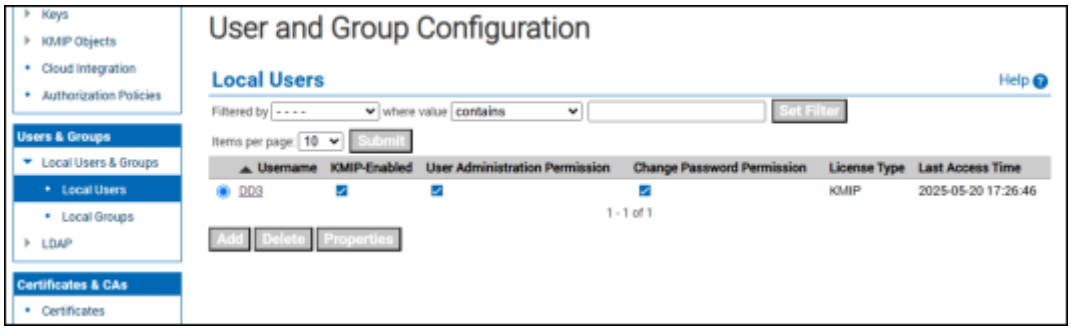

Figure 11 : KMIP User

5.2 Configuring on Dell Data Domain DD3300

1. Login to DD System Manager using the admin credentials.
2. Go to **DD3300** > **Protocols** > **CIFS** and verify that the certificate folder is enabled.

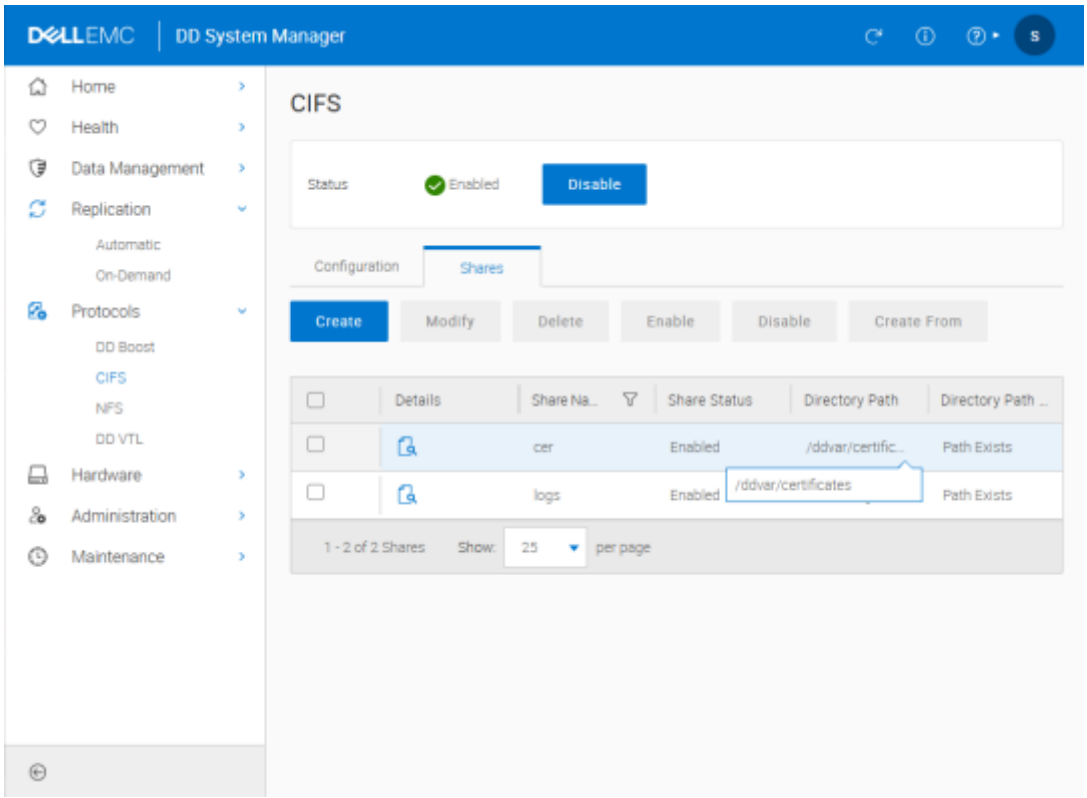

Figure 12 : DD System Manager

3. After enabling CIFS setup, you can access the certificate folder from Windows using the configured CIFS credentials.

- Path: `\\<ipaddress>\cer`
- **Username:** sysadmin
- **Password:** xxxxxxxxx

4. Log in to the DD3300 console using an SSH tool to create the certificate request file. The DD3300 (KMIP Client) will use this certificate later.
5. Generate a host certificate signing request (CSR) Format by using the below command.

```
adminaccess certificate cert-signing-request generate [key-strength {1024bit | 2048bit | 3072bit | 4096bit}] [country country-code] [state state] [city city] [orgname organization-name] [org-unit organization-unit] [common-name commonname] [subject-alt-name value]
```

6. After entering the command, the generated request file (.csr) can be found at the `\\<ipaddress>\cer` path.
7. After obtaining the generated .csr file and having it signed by ESKM (refer to the Sign the host certificate using ESKM chapter and complete all related steps before performing this step), place the signed certificate file in PEM format into the DD3300 certificate directory. Once the file is placed, run the appropriate command in the DD3300 console to import and apply it as the DD3300 Host CA.

5.2.1 Import the host certificate & CA to the Data Domain System

> The authentication method varies depending on the application type. When integrating with ESKM, select **GKLM** for the Import CA application type.

1. Run the `adminaccess certificate import` command on the DD system to import the host certificate.
   `adminaccess certificate import host application gklm file signed.pem`

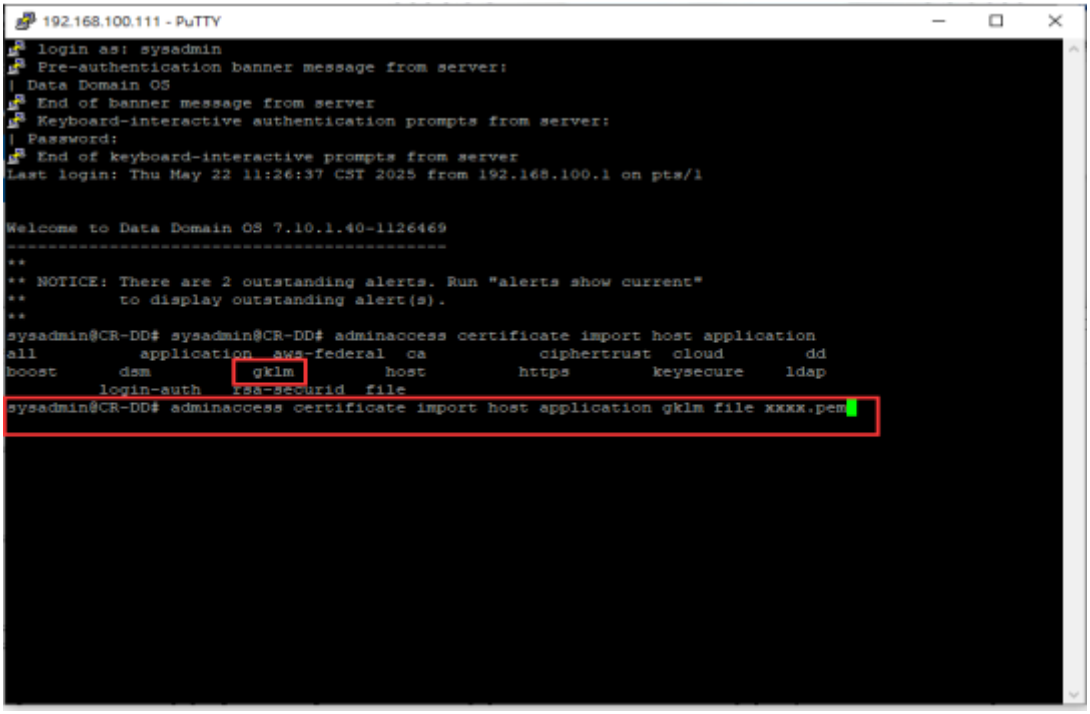

Figure 13 : Import the host application GKLM file

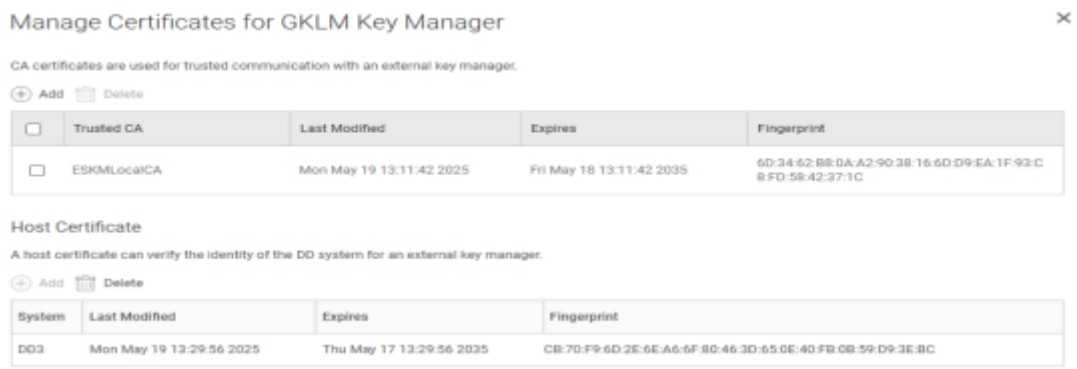

Figure 14 : Manage Certificates

2. Go to **Security > Local CAs**, download the ESKM (KMIP Server) Local CA, and then import it into the DD3300 (KMIP Client) to establish trust.
3. Since DD3300 only accepts .pem format, the .crt certificate file downloaded from ESKM can be converted via OpenSSL.
4. After opening the command prompt, navigate to the file directory and run the following command:
   `openssl x509 -in DD3signed.crt -out DD3signed.pem`

5. Place the ESKM Local CA into the DD3300 certificate folder, then enter the command and complete the import of ESKM CA.
   `adminaccess certificate import ca application gklm file xxxx.pem`
6. Go to DD3300 Web GUI > **Data Management** > **File System** > **DD Encryption.**
7. Enable encryption and connect key management.

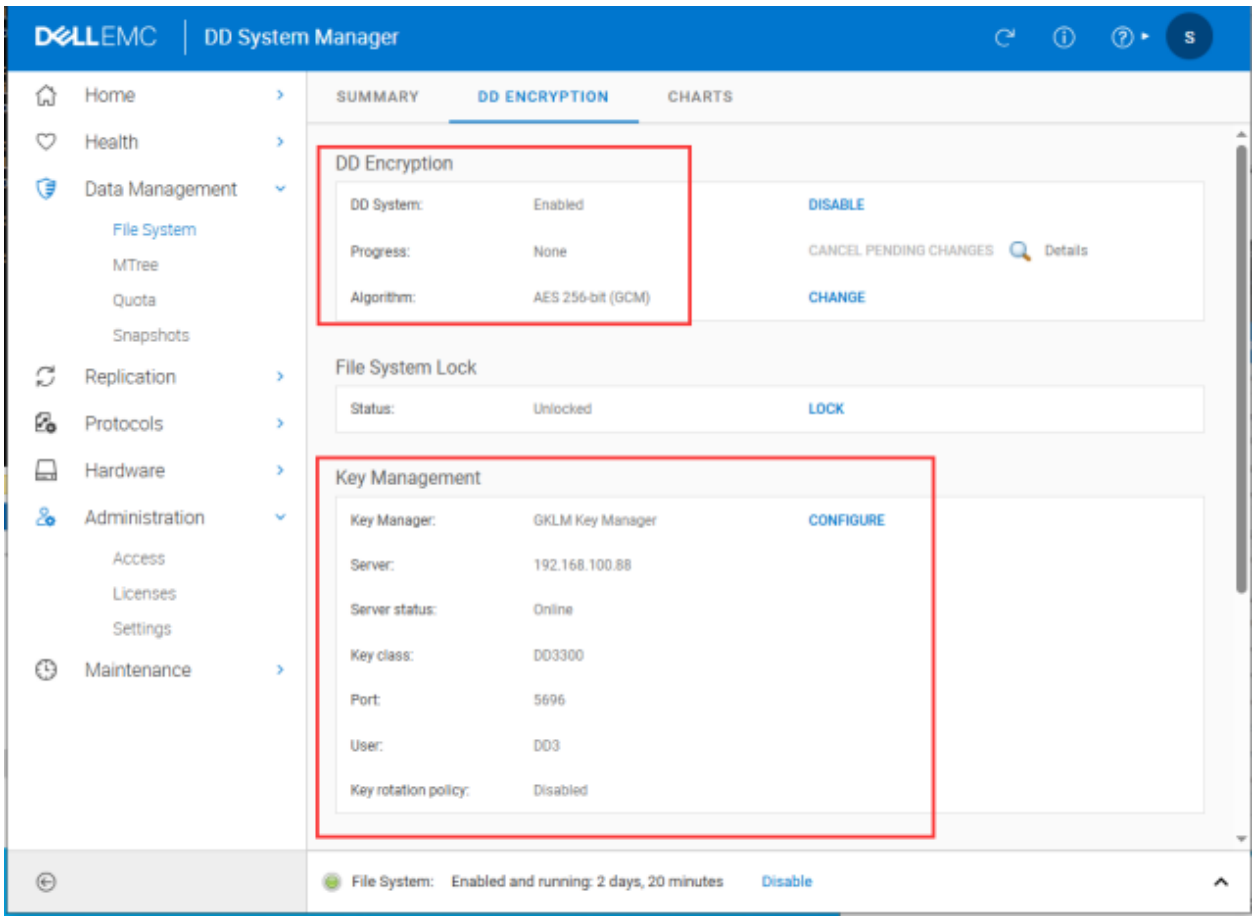

Figure 15 : DD Encryption and Key Management

8. Go to **Key Management** > **Settings.** Input relevant information to complete the integration with ESKM (KMIP Server).

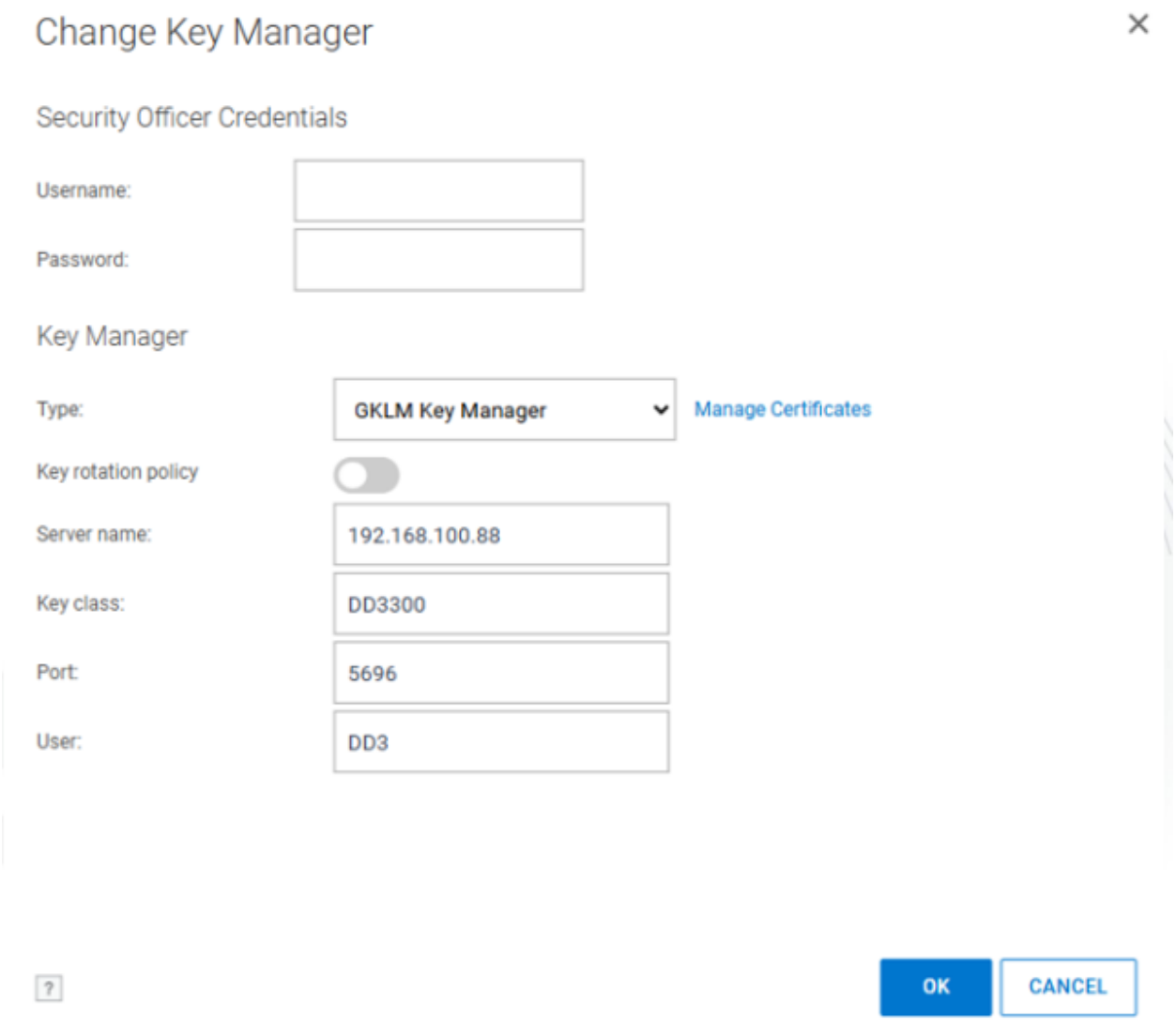

Figure 16 : Change Key Manager

When integrating with ESKM, select **GKLM** as the application type.

9. After selecting the application type, click **Manage Certificates** to confirm whether the certificate previously imported in the Console command is successfully displayed.

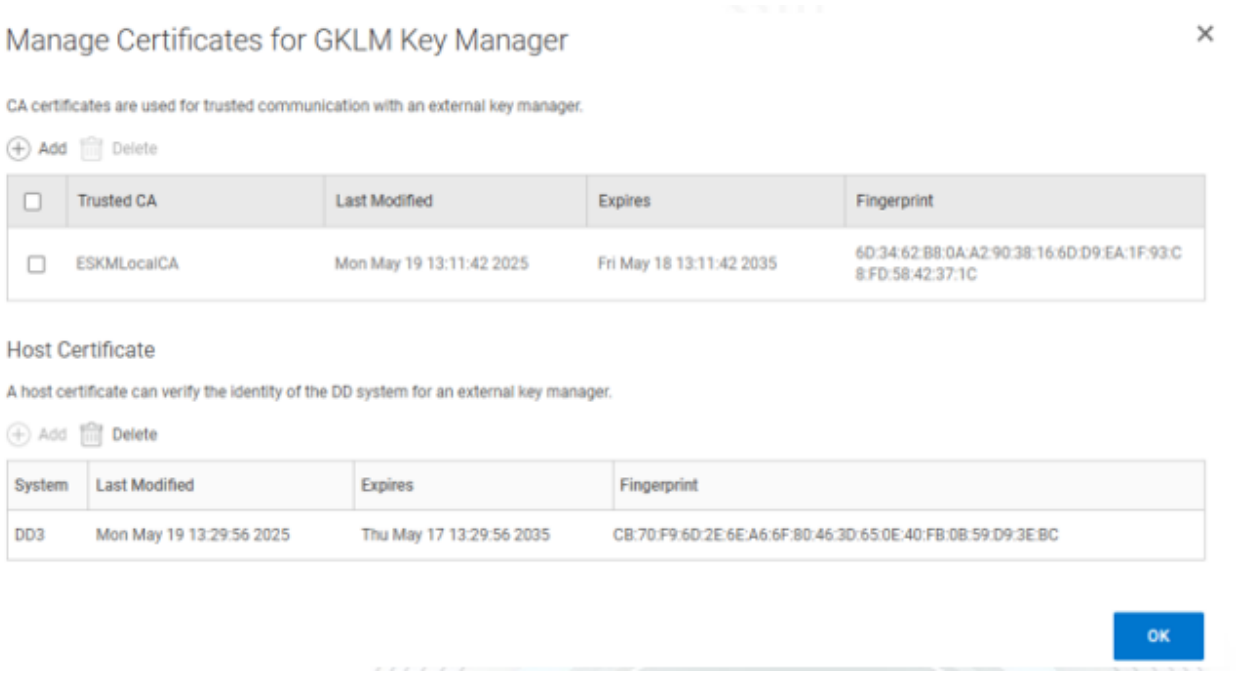

Figure 17 : Manage Certificates for GKLM Key Manager

10. If DD3300 (KMIP Client) and ESKM (KMIP Server) are successfully integrated, the interface will display the key management (ESKM) information, and the KMIP key activation status will be visible.

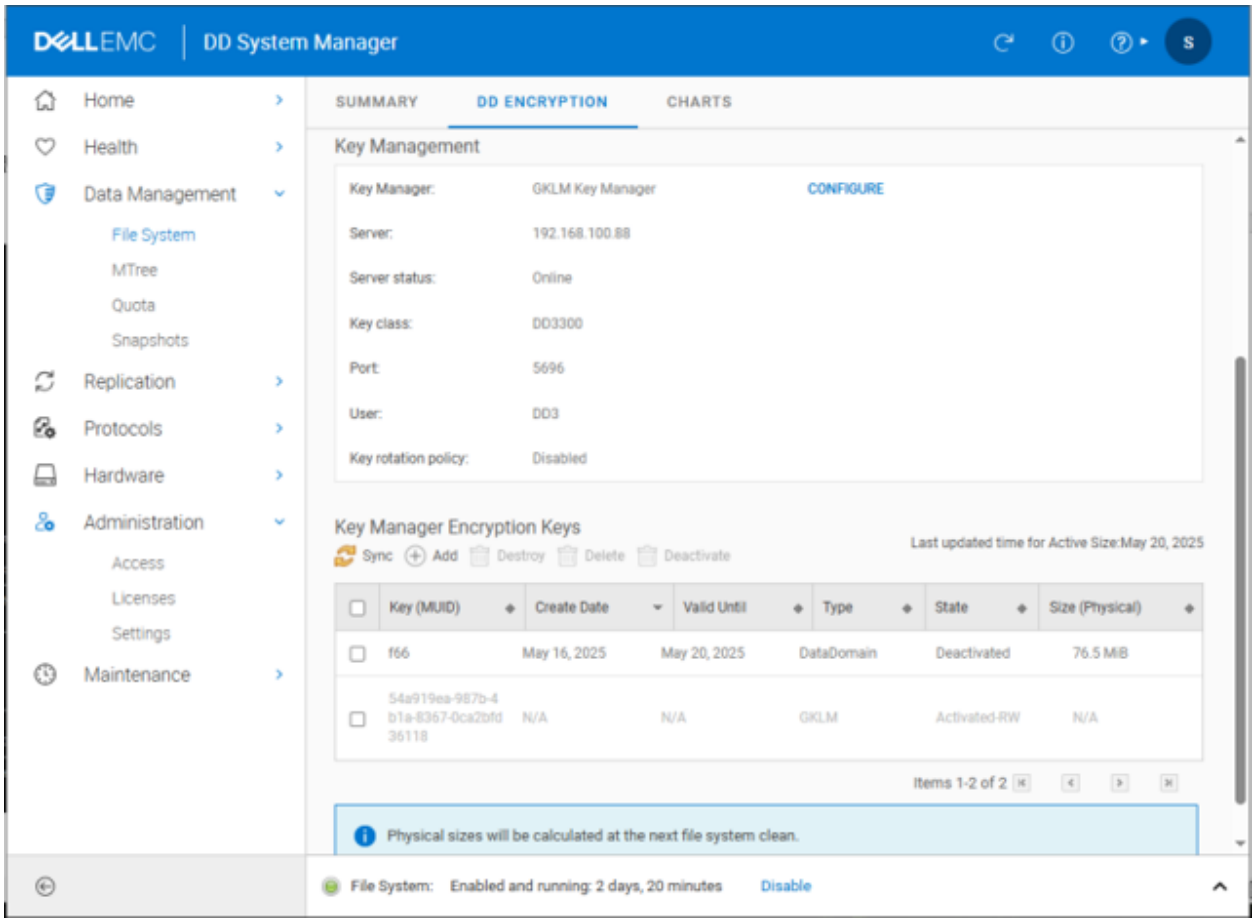

Figure 18 : DD Encryption

11. Enter the relevant commands in the DD3300 console to verify again that the KMIP integration is successful and that the KMIP key is activated.

Figure 19 : KMIP Key Activation Status

6 Verification and Testing

6.1 Logs and Validation Steps

1. In the **ESKM Management Console** > Click **Security** > **KMIP Objects**. Confirm that the **key Type**, **UUID**, **Owner** and other attributes are correct.

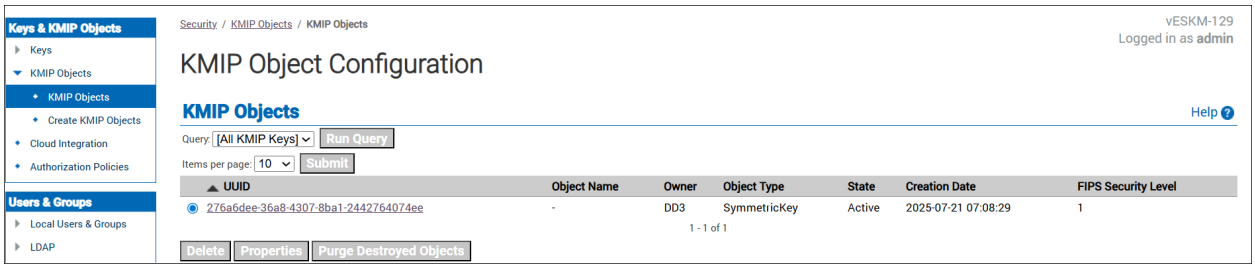

Figure 20 : KMIP Objects

2. In the **ESKM Management Console**, click **Device** > **Logs & Logistics** > **Log Viewer** >> **KMIP**. The KMIP logs are displayed.

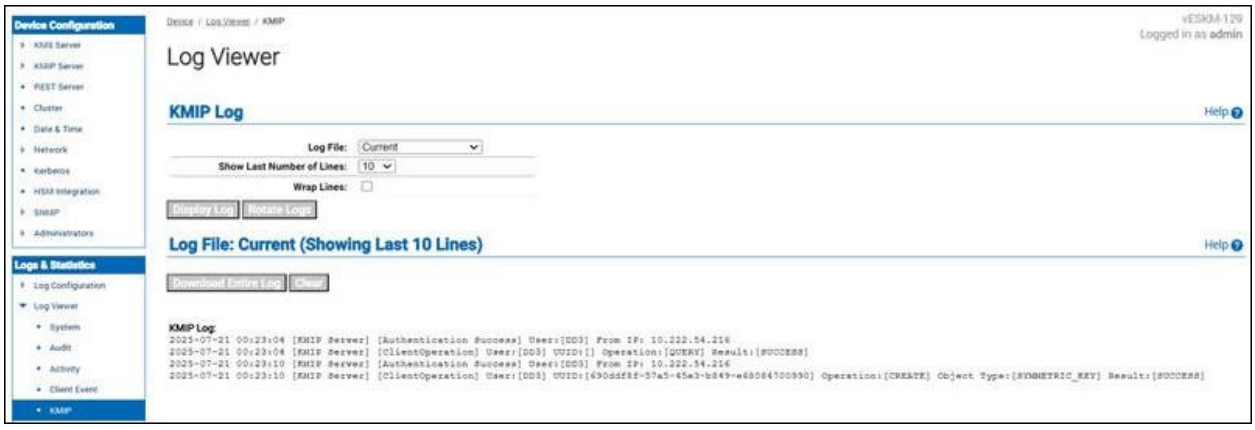

Figure 21 : KMIP Logs

7 Troubleshooting

7.1 Log Locations and Interpretation

Verify the Utimaco ESKM logs by following the steps below:

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **KMIP**.
2. Review logs related to operations performed on the Dell EMC DD3300.

8 Contact and Support Information

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

Utimaco IS GmbH
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.

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*.