# Using Self-Encrypting Drives (SEDs) with Dell EMC SC Series Storage

Abstract

This document provides a detailed description of the Dell Storage Secure Data solution including an overview on self-encrypting drives (SEDs), encryption features, and Key Manager Server (KMS) integration.

October 2017

A Dell EMC Reference Architecture

# Revisions

| Date | Description |
|---|---|
| May 2014 | Initial release |
| December 2014 | Added appendix B: Security KMS support |
| April 2016 | Minor updates; added rekey and rescue functionality |
| January 2017 | Added certificate creation for SafeNet KeySecure and Thales keyAuthority |
| October 2017 | Updated platforms and supported versions |

# Table of contents

# Executive summary

Data and intellectual property is the lifeblood for a company in the modern information-driven economy. The legal aspects of a data breach unprotected by encryption (safe harbor) could tarnish your business reputation, destroy consumer confidence, provoke customers to walk away, and at the very worst, wipe out your business completely.

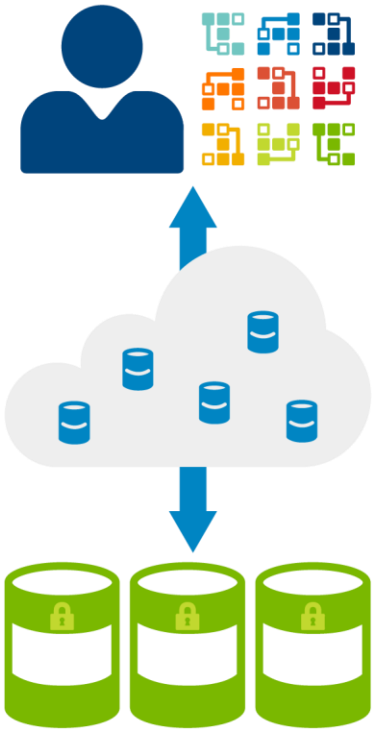
Although much money and effort have been spent protecting corporate networks from outside intrusion, many security analysts agree that there are still considerable vulnerabilities due to physical theft, misplacement, or inappropriate redeployment or disposal of hard drives from corporate computers and storage arrays. An effective solution to these problems is to employ self-encrypting drive (SED) technology. SEDs, coupled with Dell EMC™ SC Series arrays, provide a strong data-at-rest encryption solution for securing corporate data from hard drive loss or theft. This document provides a detailed description of the Dell Storage Secure Data solution including an overview on SEDs, encryption features, and Key Manager Server (KMS) integration.

# 1 Secure Data overview

With data security risks on the rise, an influx of government regulations for securing data have been mandated and are becoming an integral part of corporate business requirements. Regardless of government mandates, eliminating exposure of private data is now simply viewed as a sound business practice. This is a high priority for companies operating in the healthcare, federal or state government, financial, banking, education, and manufacturing spaces, just to name a few.

Dell EMC has always worked to provide companies like these with data storage solutions that are easy to manage and implement, both now and into the future. With non-disruptive deployment, these solutions allow customers to seamlessly grow with new requirements and regulations such as PCI DSS, GLBA, SOX, HIPAA, the HITECH Act, as well as the 45+ state laws requiring businesses to publicly disclose data breach incidents.

Before implementing data-security solutions, it is important for organizations to put a comprehensive security strategy in place. This requires understanding where data is at all times across the organization and securing it at each point. These points, or levels of security, can be broken down into three basic categories: data in use, data in motion, and data at rest.



| | |
|---|---|
| Data in use | User, OS, or application use of data (for example, print, copy, or move) |
| Data in motion | All data being transferred between two nodes across the network |
| Data at rest | Data recorded on the storage media |

Figure 1 Levels of data to be secured across an organization

The primary focus of this guide is securing data at rest (DAR). While each point in the storage infrastructure provides unique threat models, DAR presents one of the highest security vulnerabilities. Data, in fact, spends most of its life at rest on drives. When these drives eventually leave the data center for repair, retirement, relocation, or maintenance, the drives and their data are most vulnerable to being lost or stolen.

The emergence of full disk encryption technology and SEDs is timely for mitigating the security vulnerabilities of DAR. SEDs are also becoming a standardized technology across many of the world's top drive vendors, which allows for interoperability and ensures greater market competition and competitive pricing.

To further highlight the importance of SEDs, the Storage Networking Industry Association (SNIA) best practices recommends encryption as close to the information source as possible, which is the media where the data resides. In addition, many safe harbor laws, such as California state regulations CA 1798 (formerly SB-1386), protect organizations that store data in compliance with security encryption requirements. With safe harbor laws such as these, organizations might not have to notify customers of lost data if that data was stored and secured on SEDs. Current SEDs use the Advanced Encryption Standard (AES) algorithm as defined by the National Institute of Standards and Technology (NIST) and has been widely adopted as an encryption standard. SEDs selected for the Dell Storage product line are approved for use in applications requiring compliance with Federal Information Processing Standards (FIPS) 140-2 Level 2.

## 1.1 Securing data with SED technology on Dell SC Series arrays

As a leader in storage technologies, Dell EMC provides support and management capabilities that allow users to safely secure their DAR in SC Series arrays. This support is offered through a wide variety of SEDs with multiple capacities managed through Trusted Computing Group (TCG) protocols within the SC Series SAN. This solution is compatible with Key Management Interoperability Protocol (KMIP) v1.0 standards and customer-defined external KMS solutions.

The Secure Data support for DAR encryption in the SC Series arrays extends from encrypting the full array, multiple disk folders, or even at a volume level as tied to a separate secure data folder. SEDs and non-SEDs are supported separately, within the same array, with negligible performance impact on the system or applications. The encryption technology also works on legacy Compellent storage (with the addition of new SED drives). Figure 2 shows an SC Series array with both SEDs and non-SEDs as an example.

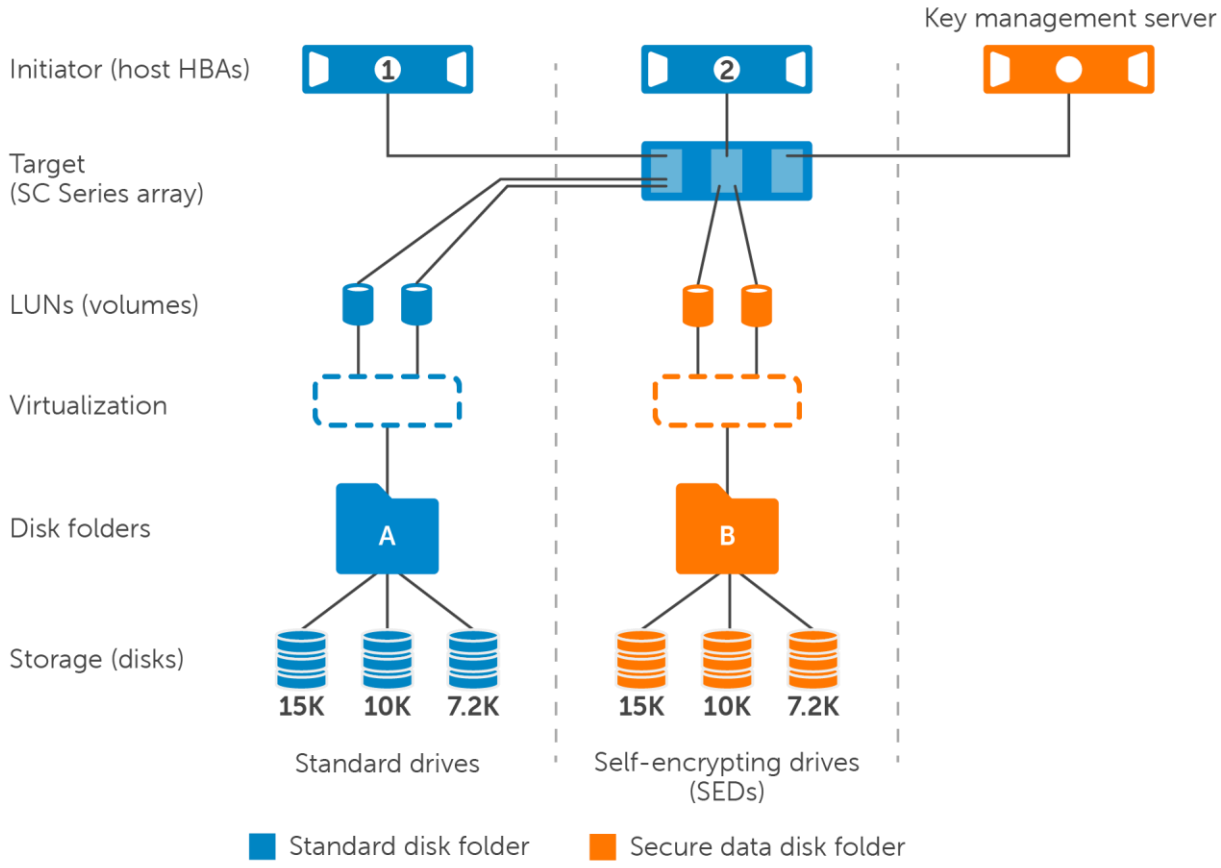



Figure 2 SC Series array with both SEDs and non-SEDs managed independently

Figure 3 FIPS 140-2 Level 2 tamper-evident drive

## 1.2 SED technology overview

An SED is a self-encrypting hard drive with an encryption/decryption function that performs like any other hard drive. Completely transparent to the user, the encryption is built into the disk drive controller chip, encrypting all data written to the magnetic media and decrypting all the data read from the media automatically. With the encrypting engine built into the drive hardware, there is no performance impact on the storage system as the SEDs encrypt constantly.

There are two primary functions of SED technology: To protect hard drive data from unauthorized access (secure DAR), and to provide cryptographic erase (CE). Also known as secure erase or crypto erase, CE is a mechanism to securely erase the data on the drive so that the drive can be repurposed or retired.

### 1.2.1 Security threats covered by SEDs

While using SEDs is fairly simple and transparent, it is important to understand what protection they do and do not provide. Secure Data provides data protection for threats including:

- Lost, transported, or stolen drives
- Theft of an entire enclosure
- Theft of an entire SC Series system

When a powered-on drive leaves the array (whether by failure, removal, or otherwise), the drive immediately locks itself. Its contents are inaccessible without the authority credential (AC). At the same time, the volumes with data on that drive will begin a RAID rebuild using the associated hot spare. If that drive is inserted into a different array, the drive will remain in a locked state. The administrator must explicitly bring the drive into service, which then will result in a CE of the SED. Furthermore, even if the platters were removed from the drive itself and placed on a spin stand, the data would be secure due to the AES-256 encryption used to write the bits.

### 1.2.2 Security scenarios not covered by SEDs

Secure Data does not provide data protection for threats including but not limited to:

- Insider attack: Any person who possesses the administrator password can access any volume on the array, or change SCOS user permissions to allow others to do the same. Similarly, a compromised host can access volumes that the host is authorized to access. SEDs cannot provide protection against improper access to an online data volume.
- Data-in-flight: SEDs are intended to solely provide protection for DAR, and thus provide no protection for data-in-flight on the network.
- Tampering with array hardware: Secure Data is not resistant to hardware probes, other snooping devices, or the removal of a drive without loss of power to that drive.
- Unauthorized access or theft of the KMS and the associated ACs saved in it.

## 1.3 Protecting data from unauthorized access

To protect the data from unauthorized access, SEDs use two sets of keys. One key is called the media encryption key (MEK). In the drive factory, each SED randomly generates an MEK that is encrypted and embedded within the drive. The MEK is never exposed outside the drive and requires no management by the user. The MEK functions as a secret password so that the encryption/decryption engine built into the drive will know how to decrypt the user data stored on the physical media. The encryption in the drive uses a symmetric key algorithm which means the MEK is the same for encrypting and decrypting the data on the disk. This MEK can be changed by CE, but the encryption can never be turned off.

The second required key is called the authority credential (AC), sometimes referred to as the locking key, credentials, authentication keys, or access key (AK). It is used to unlock and configure the SED. There is one AC for each SED. SC Series arrays automatically detect SED drives and will create the ACs when the array is initially configured with SEDs or when SEDs are added to a legacy system (requires an encryption software license and SCOS v6.7.40 or greater).

The AC is stored in a KMIP secret data object on the KMS. There is one valid secret data object for each SED that has been put into a lockable state. An SC Series array completes a KMIP register on this secret data object, and the secret data object keyblock contains the AC. The array also controls the contents of the secret data object. Once an SED has been configured with an AC, the AC must be provided to unlock the drive, and the drive remains unlocked only while powered on. The drive locks itself upon losing power or shutting down, and the AC must be provided again before the drive will unlock and participate in I/O operations.

The following steps and Figure 4 describe the process of how data is accessed on an SED during normal operation.

1. Upon boot, SCOS sends a series of commands to the drive to unlock it. One of those commands is an authentication request which carries the AC.
2. The drive electronics hash the AC from the storage controller and pull the stored hashed access key from the drive storage. The hashed keys are compared.
3. If the hashed keys do not match, no access is given to the data and a security error is passed back to the storage controller stating that the drive is locked and that the subsystem does not have authorization to access it. If the hashed keys match, a subsequent drive command is sent to unlock the drive.
4. During a request for data, the encrypting/decrypting circuit pulls the requested data from the drive and uses the MEK to decrypt the encrypted user data. The decrypted user data is then passed back to the storage controller.

The drive remains unlocked until the drive gets powered down.

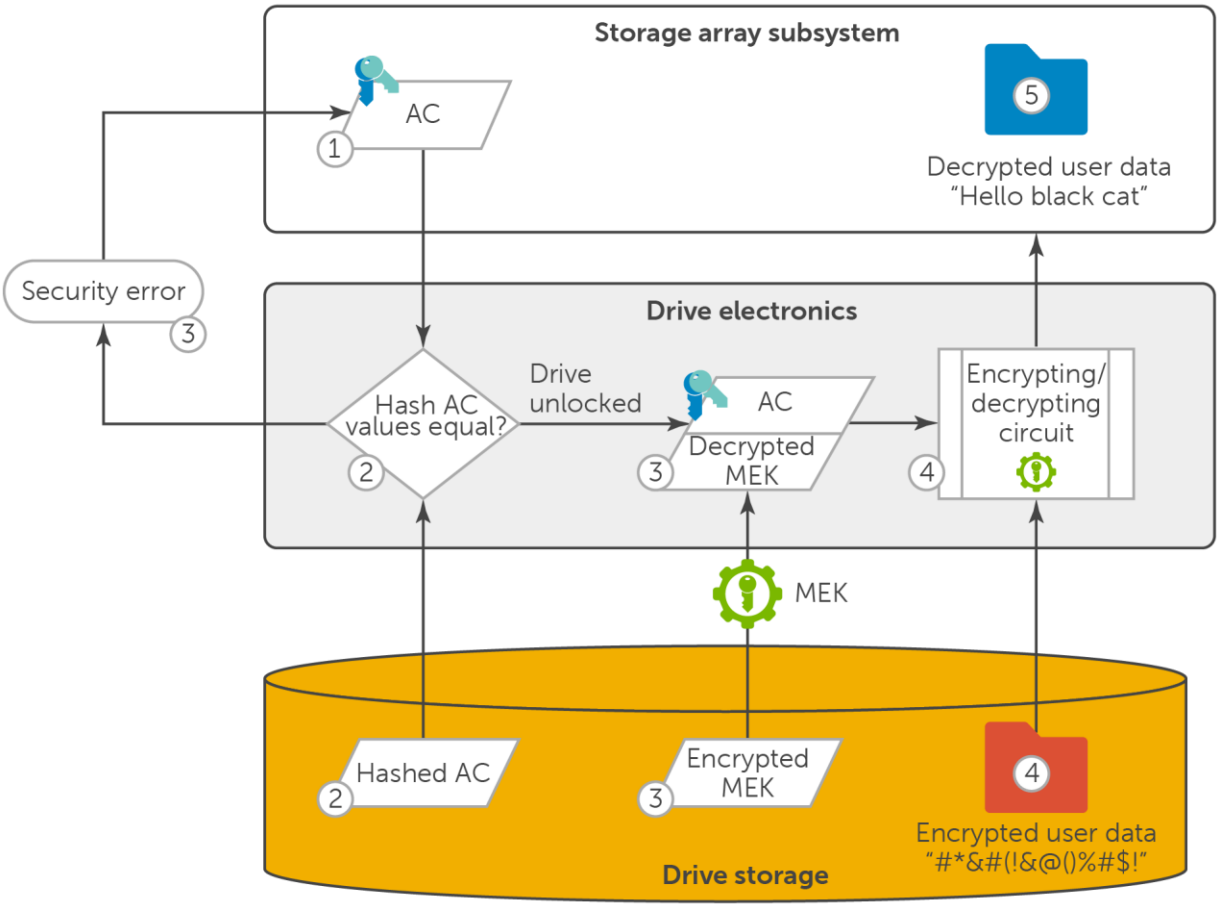



Figure 4 Accessing data on an SED

In summary, the true value of SEDs is realized when a drive is lost, removed, or stolen. In such an instance, the drive becomes locked and the data remains encrypted. Because an unauthorized user would not have the appropriate AC, the drive will remain locked and data will remain inaccessible to any attacker.

## 1.4 Cryptographic erase

Another security method available with SEDs is cryptographic erase (CE). CE simply replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data encrypted with the deleted key. Alternative methods, such as de-gaussing each drive or simply overwriting the data with zeros, are available to permanently erase this data; however, these methods often are expensive, slow, or do not completely erase the data.

A common use of CE is when a failing drive is preemptively copied to a spare SED drive and then removed from use (unmanaged) by the SC Series firmware. After the copy-to-spare operation occurs, the failing drive undergoes a CE so that it may be safely returned to the manufacturer under warranty. Through this process of unmanaging the drive out of a secure data folder, the CE function destroys the stored encrypted MEK, and if or when the drive is removed from the array, it will not lock when power is removed. At this point, a new, randomly-generated MEK is created by the drive and stored on the drive. Without the original MEK, there is no way to decode the already encrypted data on the drive. Drives that fail hard (head crash, unreadable, or other issues) do not undergo CE because they are not reachable, but they do lock when removed because their SED settings are still intact.

As shown in Figure 5 and Figure 6, CE prompts the SED to permanently erase the current media encryption key and replace it with a new key, randomly generated within the drive. When the media encryption key is changed, any data that has been written to the drive using the previous key cannot be decoded by the new media encryption key, which renders all of the data unusable. Thus, data that was encrypted with the previous media encryption key is now cryptographically destroyed.

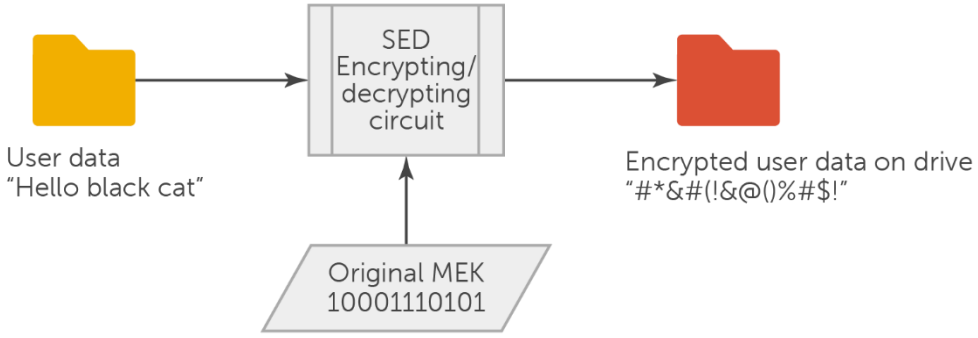



Figure 5 Before cryptographic erase

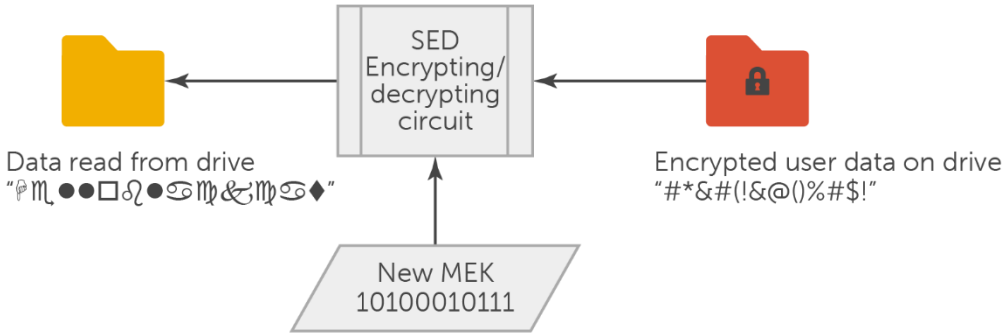



Figure 6 Reading data from the SED after cryptographic erase

# 2 Reference architecture

This section provides a reference architecture as a starting point for designing and implementing SED technology into your infrastructure.

## 2.1 Secure Data hardware requirements

Table 1 Controller support

| Controller model | Supported |
|---|---|
| SC9000 | Yes |
| SC8000 | Yes |
| SC7000 Series | Yes |
| SC5000 Series | Yes |
| SCv3000 Series | Yes |
| SC4020 | Yes |
| SCv2000 Series | No |
| Series 40 | Yes |

**Note:** Rekey and Rescue functionality is not available on the Series 40 controller.

Table 2 Enclosure support

| Enclosure model | Supported |
|---|---|
| SC200 / SC220 | Yes |
| SC280 | Yes |
| SC400 / SC420 | Yes |
| SC460 | Yes |
| SCv300 / SCv320 / SCv360 | Yes |
| Other enclosure models | No |

## 2.2 Secure Data software requirements

Table 3 SCOS versions

| SCOS | Supported |
|---|---|
| 6.7.40 (minimum) | Yes |
| 7.1.2+ recommended) | Yes |

**Note:** SCOS 7.1+ is required to use the rekey and rescue features. A Self-Encrypted Drive license must be applied to the SC array to enable SED functionality.

## 2.3 Reference architecture hardware

The hardware list and diagram for this environment are shown in Table 4 and Figure 7.

Table 4 Reference architecture hardware

| Model | Quantity |
|---|---|
| SC9000 controllers | 2 |
| SC420 disk enclosures | 4 |
| Dell EMC PowerEdge™ R630 rackmount server | 2 |
| Dell EMC Networking S3148 switch | 1 |
| Brocade® 6505 16Gb Fibre Channel switches | 2 |
| Gemalto SafeNet KeySecure™ K460 Key Management Server | 1 |
| Dell Enterprise Plus 600GB 15K SED | 48 |

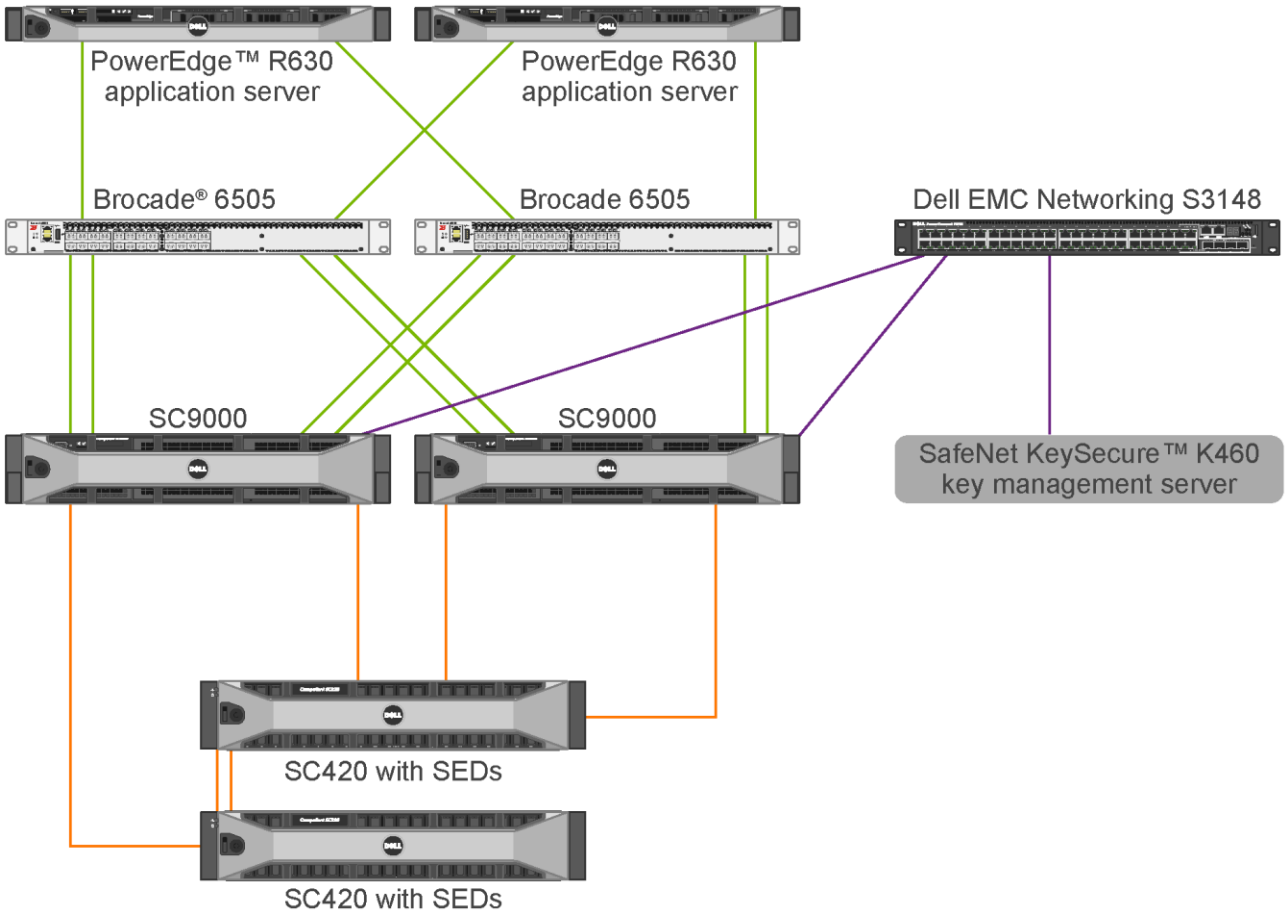


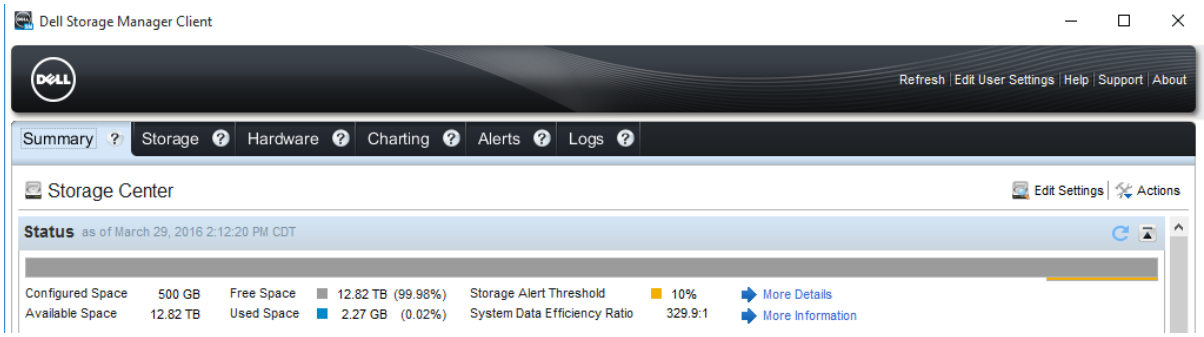

Figure 7 Reference architecture environment

## 2.4 Secure Data configuration

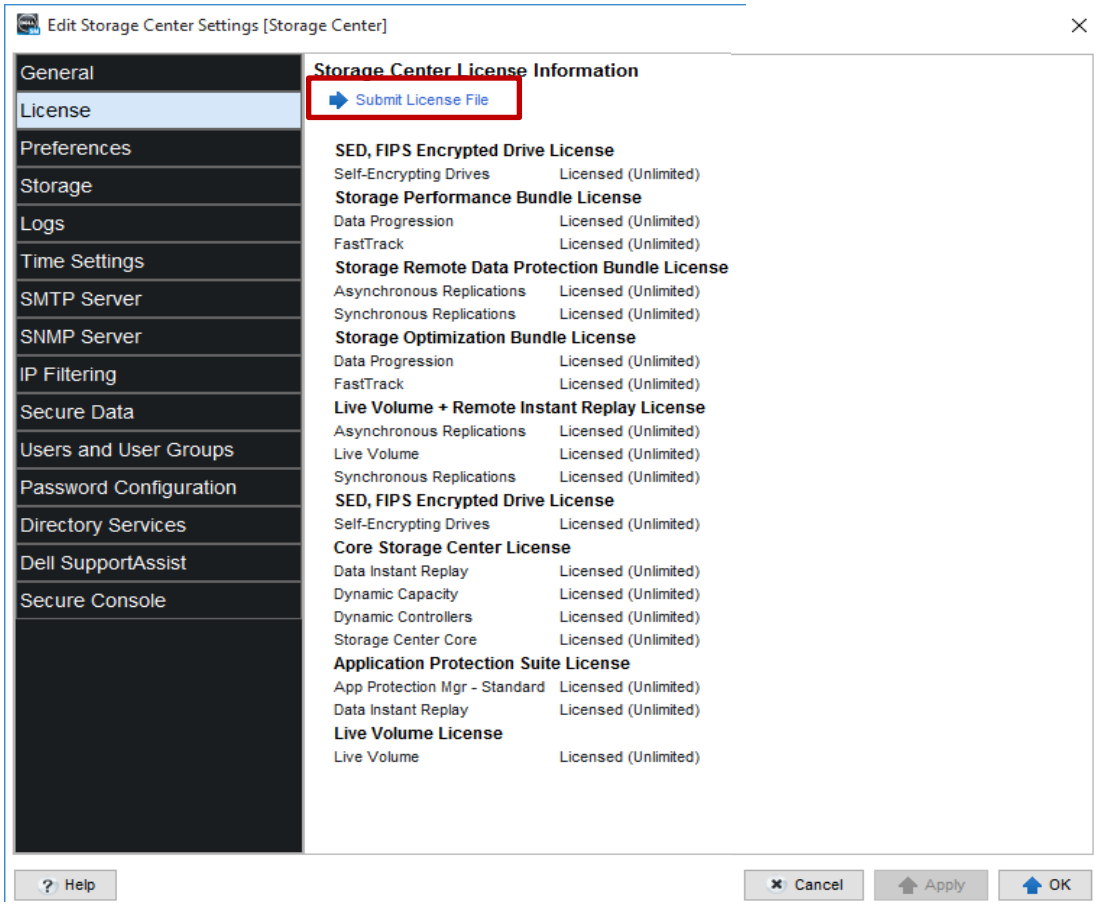
The Dell Secure Data implementation is simple to set up. The following steps outline how to configure SEDs on an SC Series array by setting up the KMS and adding drives to a secure data folder.

### 2.4.1 Apply license file

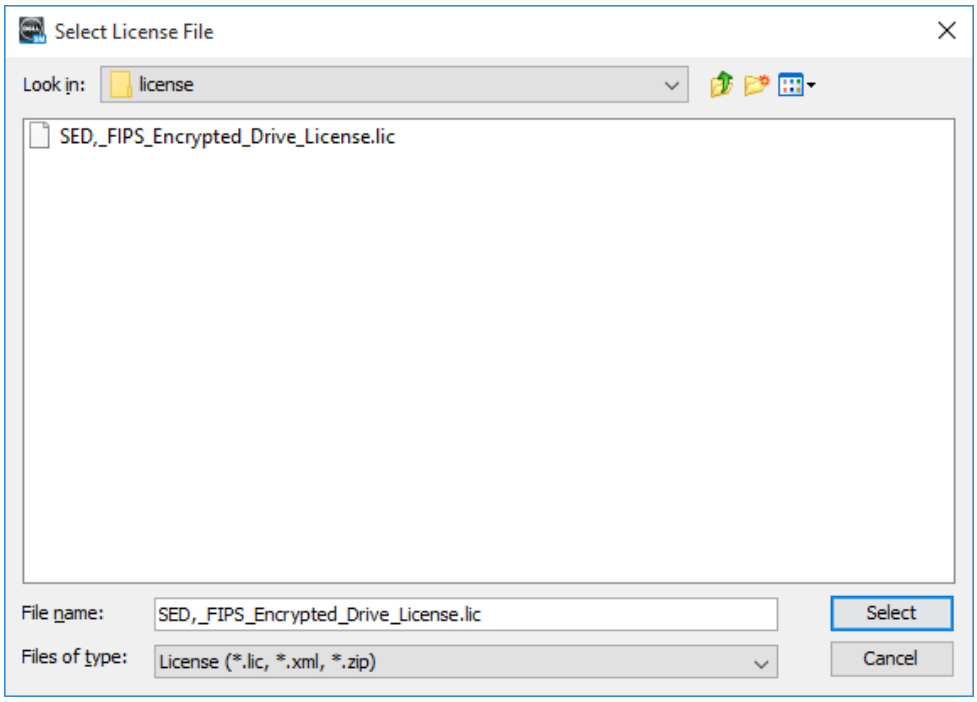
1. If the system does not already have a Self-Encrypting Drive license, one will need to be applied.
2. Using the Dell Storage Manager Client, click the Summary tab and click Edit Settings.



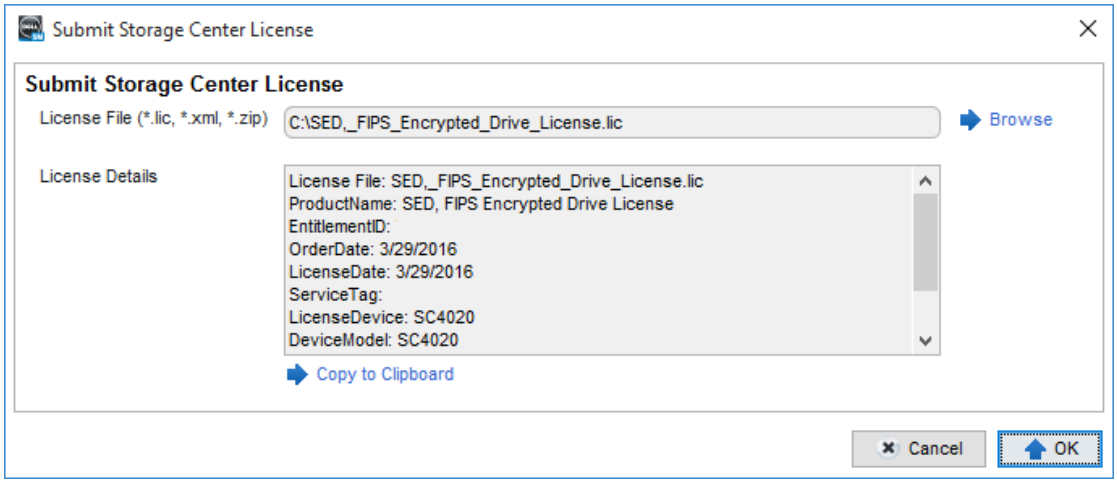

3. Click License and click Submit License File.



4. Locate the appropriate license file and click **Select**.




5. Review the **License Details** and click **OK**.



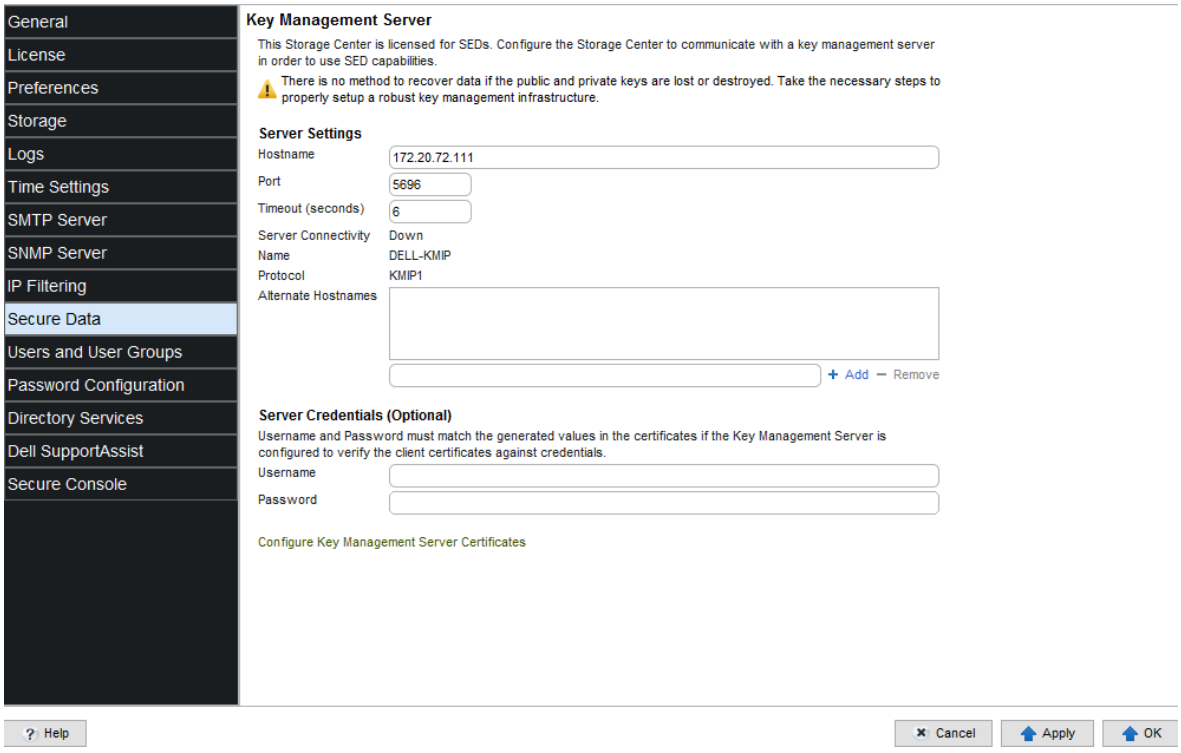
## 2.4.2 Configure KMS

By applying the license file, you can now configure a KMS.

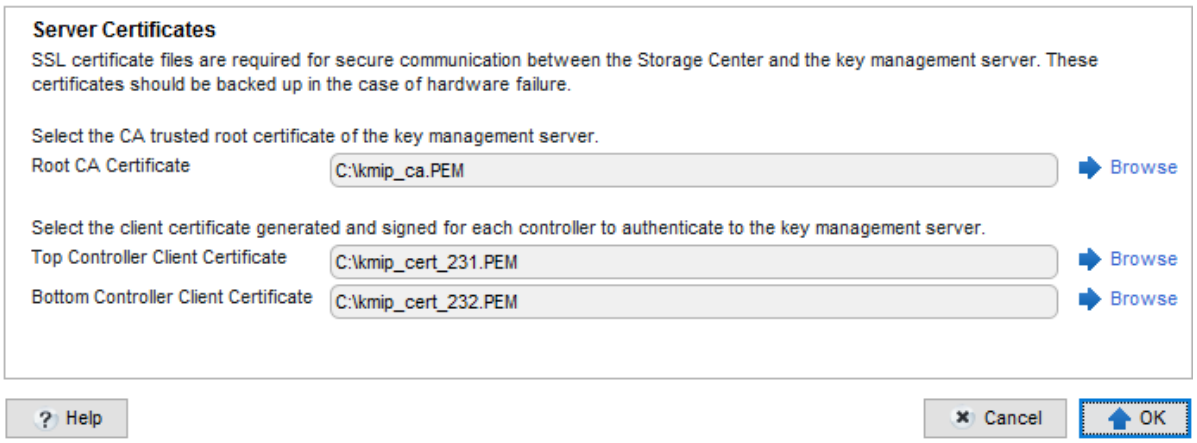
1. In the Dell Storage Manager Client, click Edit Settings. In the next window, click Secure Data.
2. Enter the **Hostname** or IP of the KMS and the **Timeout**.
3. If you have a clustered KMS configuration you can add other member hostnames or IP addresses in the **Alternate Hostnames** field.

**Note**: Alternate hostnames should be added to the configuration after all drives in the system have initially been managed and fully secured. The alternate hostname provides the SC Series array with alternate KMS servers to communicate with for key retrieval in the event that the primary KMS is offline. To ensure optimized access times during initial key creation, alternate hosts should only be added after the drives in the SC Series array have been initially managed and fully secured.

4. If applicable, enter the KMS authentication under **Server Credentials**.
5. Click Configure Key Management Server Certificates.

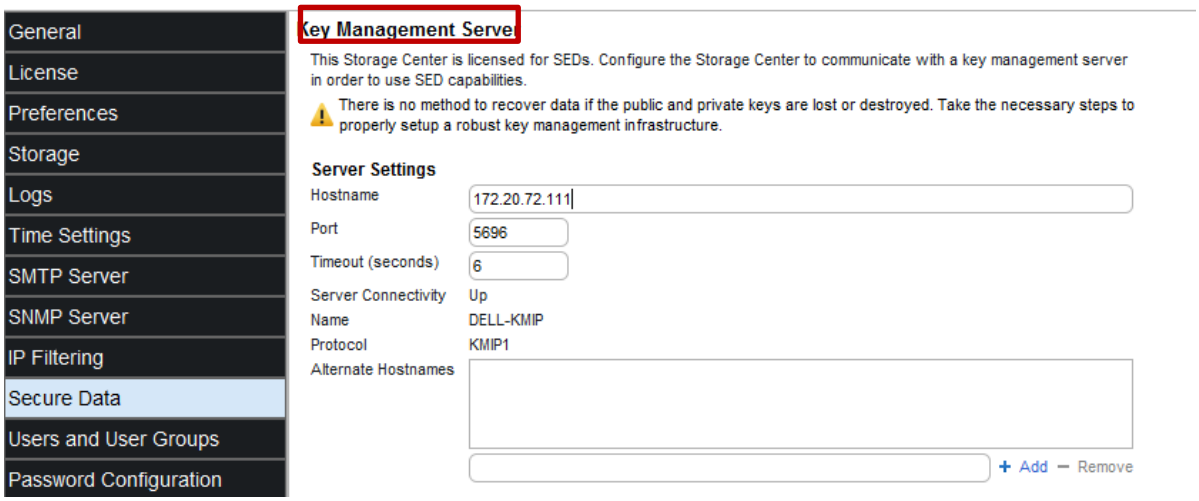


6. Click **Browse**, select the **Root CA Certificate** for the KMS, and select the client certificates. Click **OK**.



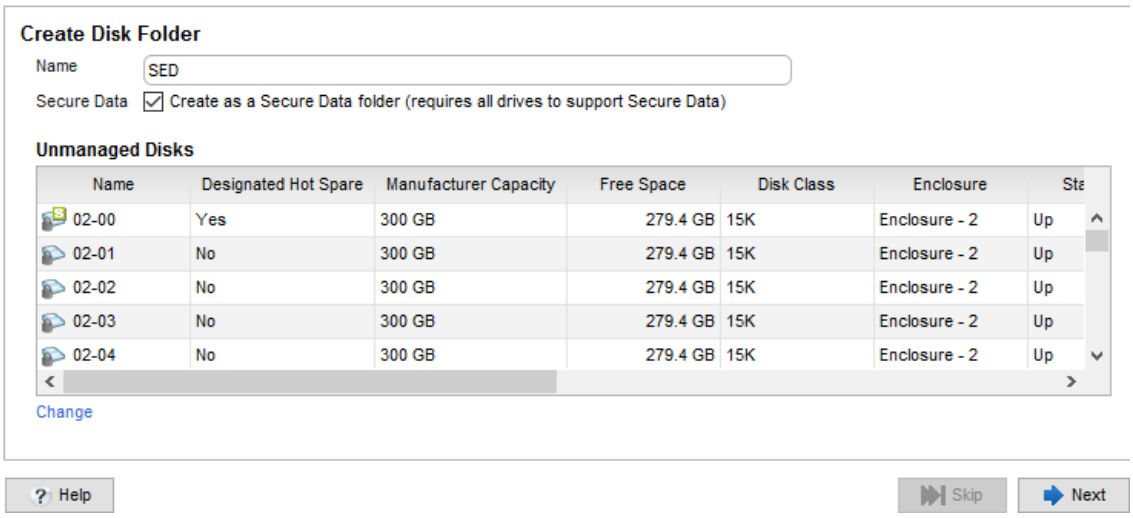

7. Returning to the **Edit Storage Center Settings** screen, click **Apply**.

   The Server Connectivity should be up, indicating that the SC Series array is now communicating with the KMS.

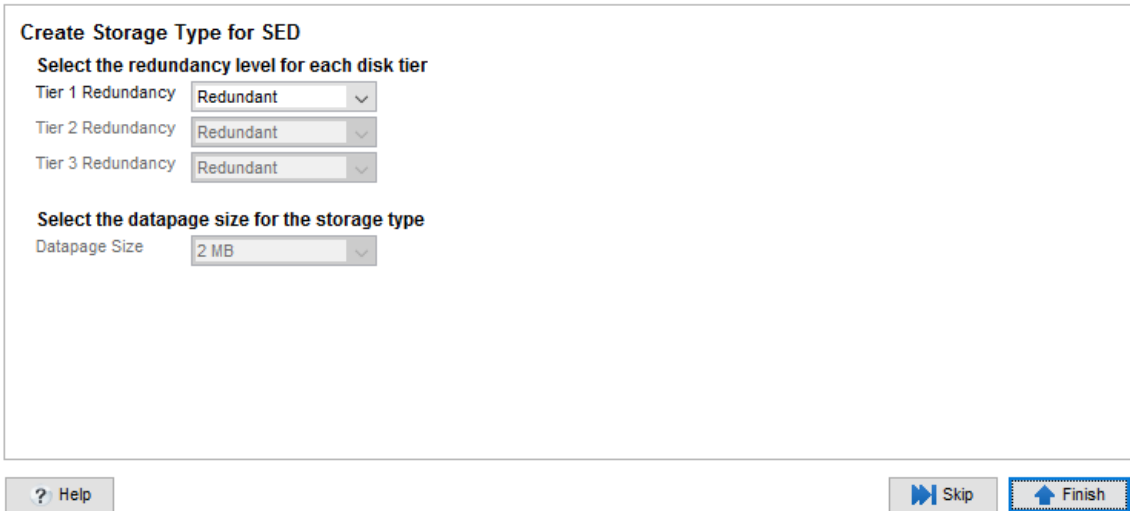


### 2.4.3 Add SEDs to a new secure data folder

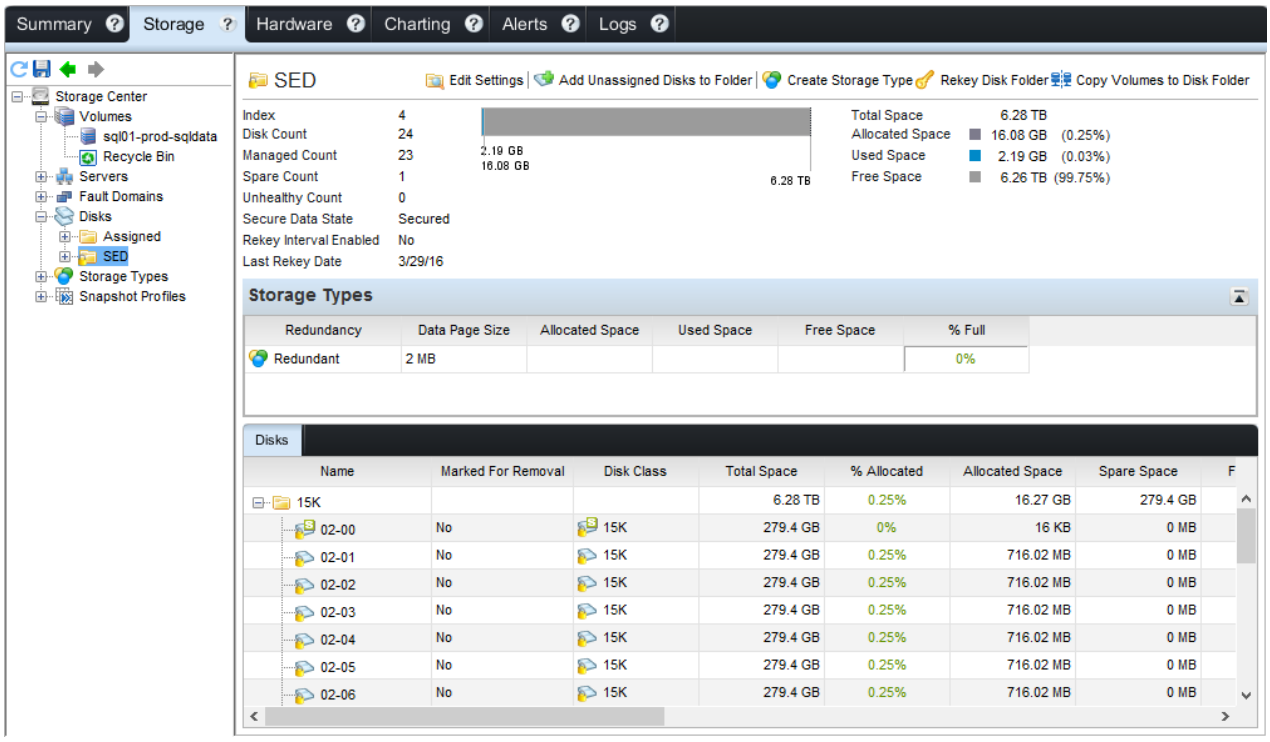
1. In the Dell Storage Manager Client, click the Storage tab, right-click Disks, and select Create Disk Folder.
5. The next window displays the settings to creating a secure data folder with SED drives. The KMS is set up and the SC Series array recognizes the drives so it defaults to **Create as a Secure Data folder**. Click **Next** to continue.




6. Select the redundancy level and datapage size and click **Finish**.




The SC array has created the Secure Data folder. The **Secure Data State** option indicates that the disk folder is **Secured** and the drives are now required to use the KMS to be unlocked. The yellow lock icon on the disk folder and drive indicates the drives are now encrypting data.




**Note**: If drives fail to add to the Secure Data folder, do not delete keys from the KMS appliance and engage support immediately.

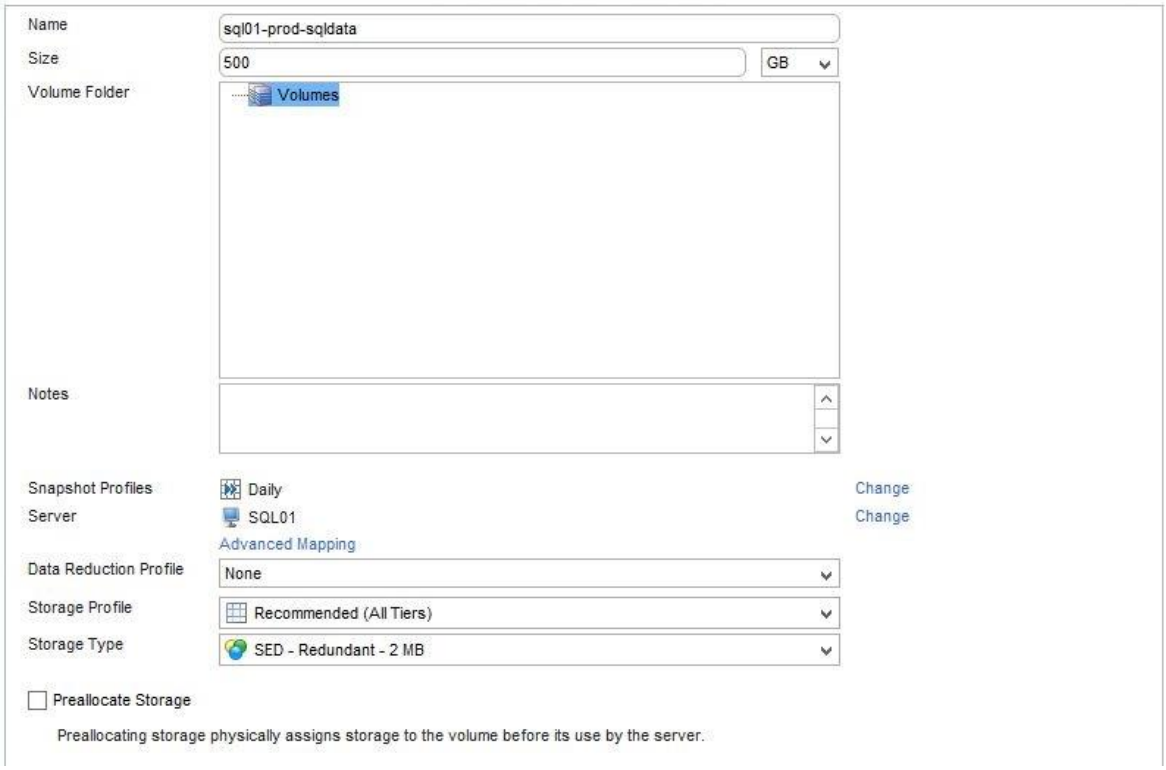
### 2.4.4 Create volume

1. In the Dell Storage Manager Client, click the Storage tab, and right-click Volumes. Select Create Volume.
2. Enter the volume information:

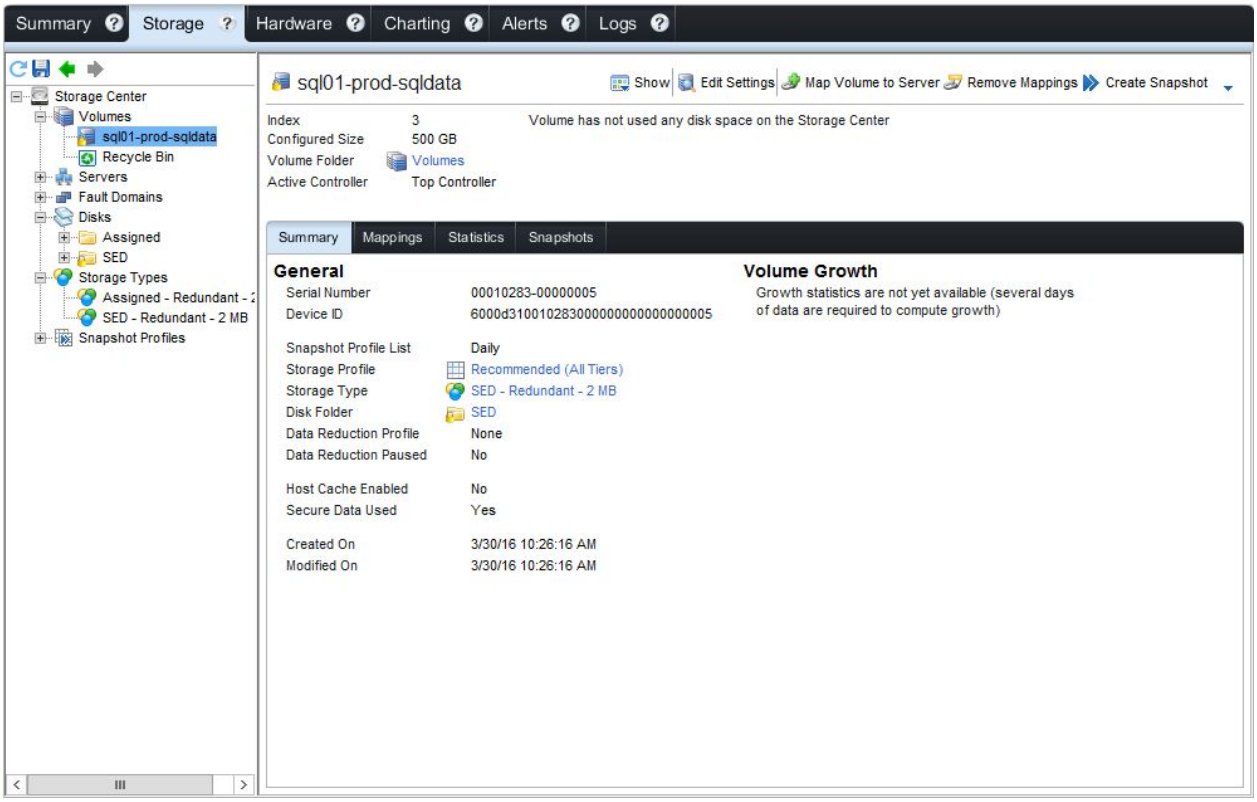
   a. Provide details for the **Name**, **Size**, and **Volume Folder**.
   b. Change the settings for **Snapshot Profiles**, **Server**, **Data Reduction Profile**, **Storage Profile**, and **Storage Type** as necessary.

   For the Storage Type, **SED – Redundant – 2MB** was selected to create the volume in the **SED** Secure Data Disk folder.

   c. Select **OK** once the volume is ready to be created.



The volume is now created and is on a secure data disk folder. The authority credential is now stored on the KMS. If a drive needs to be unlocked, the authority credential from the KMS will be requested.

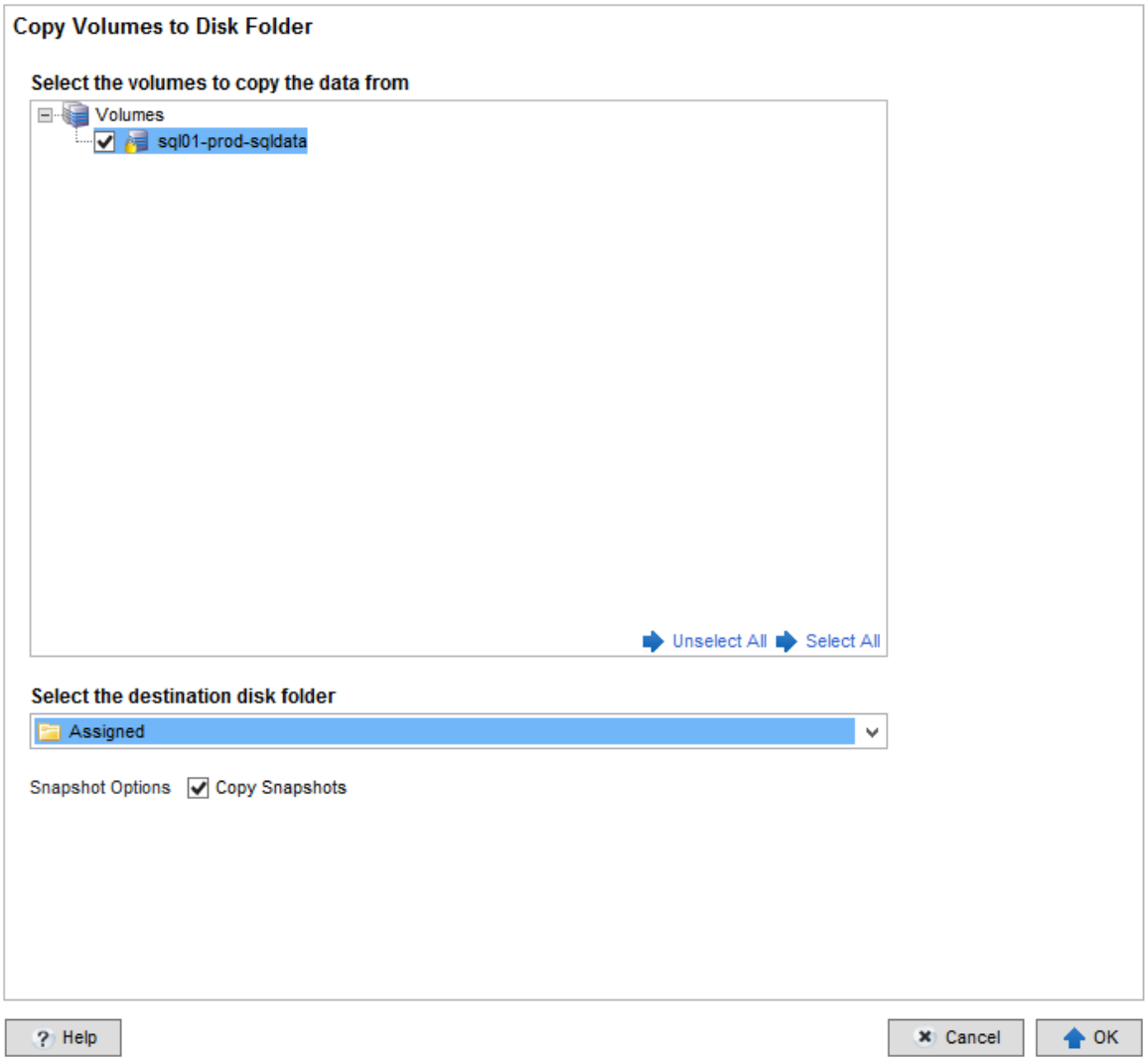



## 2.4.5 Rescue

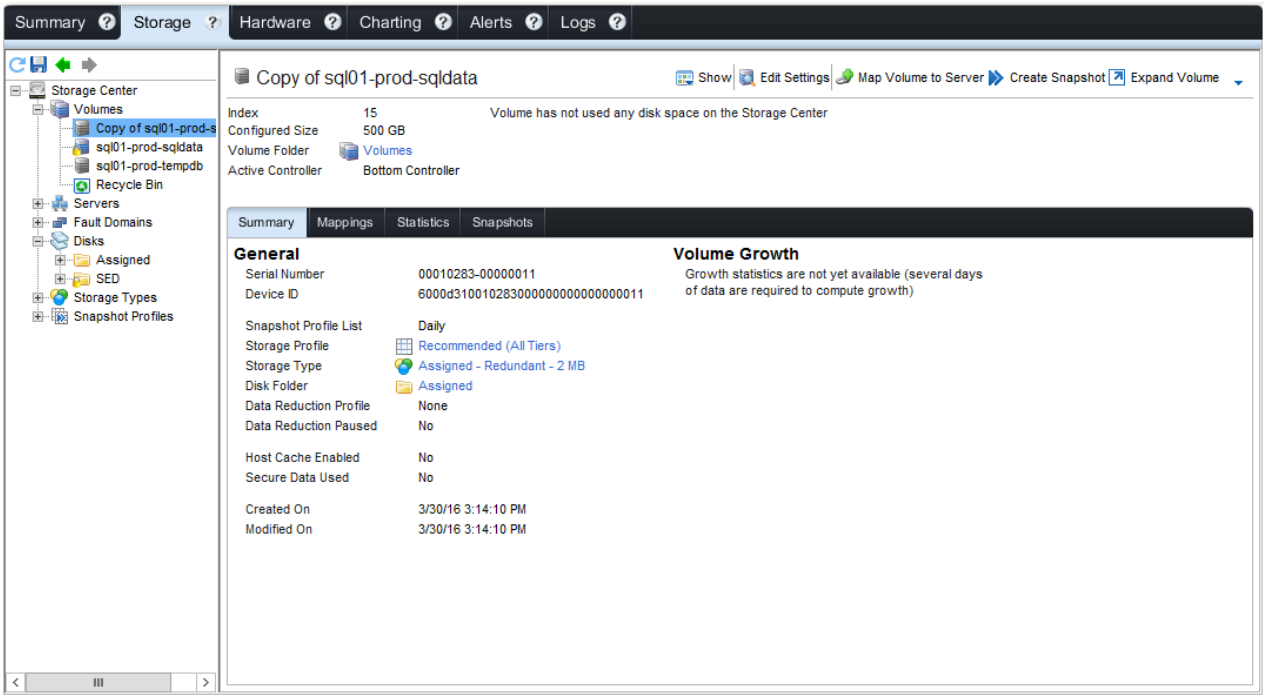
The rescue feature allows a storage administrator to quickly and easily copy a volume off a secure data folder in an event such as losing the keys or an issue with the KMS. It can also be used to migrate a volume from one disk folder to another (from a secure data folder to a normal disk folder or the other way) during normal operation.

There are a couple of considerations to make when using this feature. If you intend to use this volume after the copy, unmap the volume to the server first. Also, any changes made to the volume after the copy has started will not be copied to the destination volume.

1. To copy a volume from one disk folder to another, in the **Storage** tab, right-click the disk folder that contains the volume you want to move, and select **Copy Volumes to Disk Folder**.
2. Select the volumes to copy the data from and select the destination disk folder. If the snapshots should be copied, check the **Copy Snapshots** option.



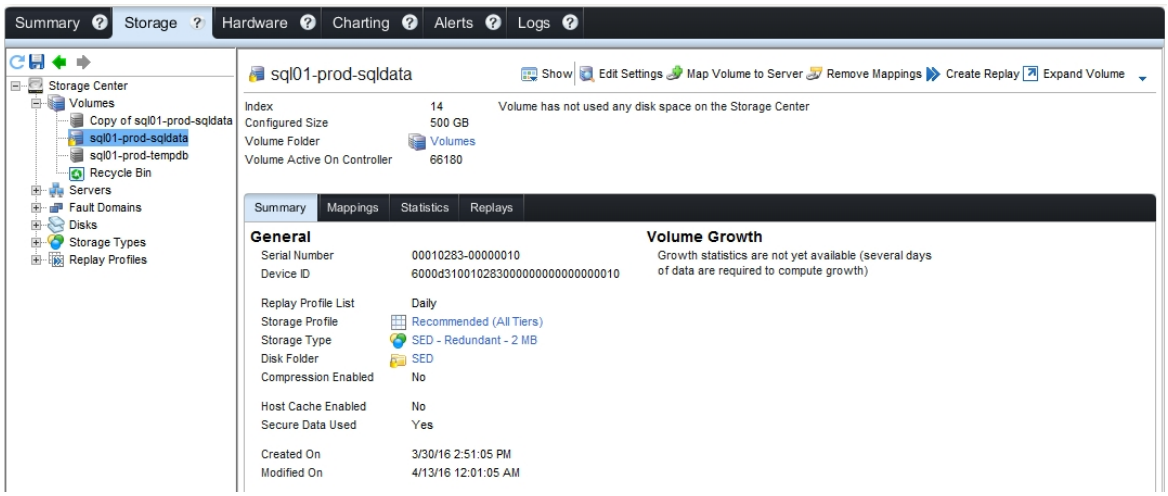
The volume is then copied from the SED secure data disk folder to the assigned disk folder. It there is an event with the KMS that prevents access to the volumes on the secure data folder, there will be a second volume available.



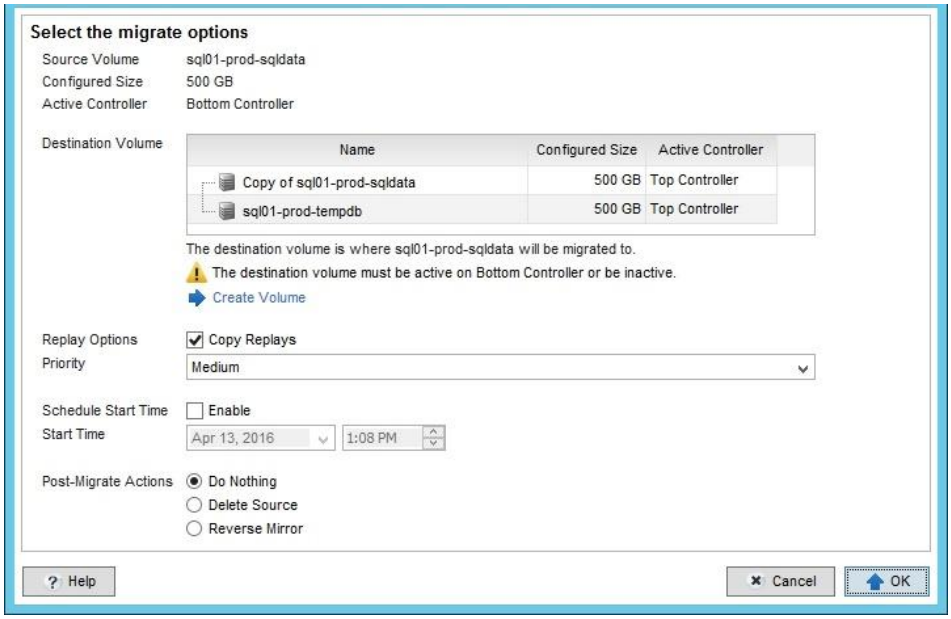
### 2.4.6 Rescue with migrate volume

The rescue feature allows you to create a copy of the volume in an event such as losing the keys or an issue with the KMS. To perform a copy and keep the volume accessible to I/O, the preferred method is to use the migrate volume option. This will create an exact duplicate of the volume and then seamlessly migrate to the new volume on a non-secure data folder, allowing for zero downtime.

1. In the **Dell Storage Manager Client**, click the **Storage** tab, right-click the volume you would like to migrate, click **Local Copy**, and click **Migrate Volume**. This example migrates the **sql01-prod-sqldata** volume that is currently on a secure data folder to a non-secure data folder.




7. Click Create Volume.

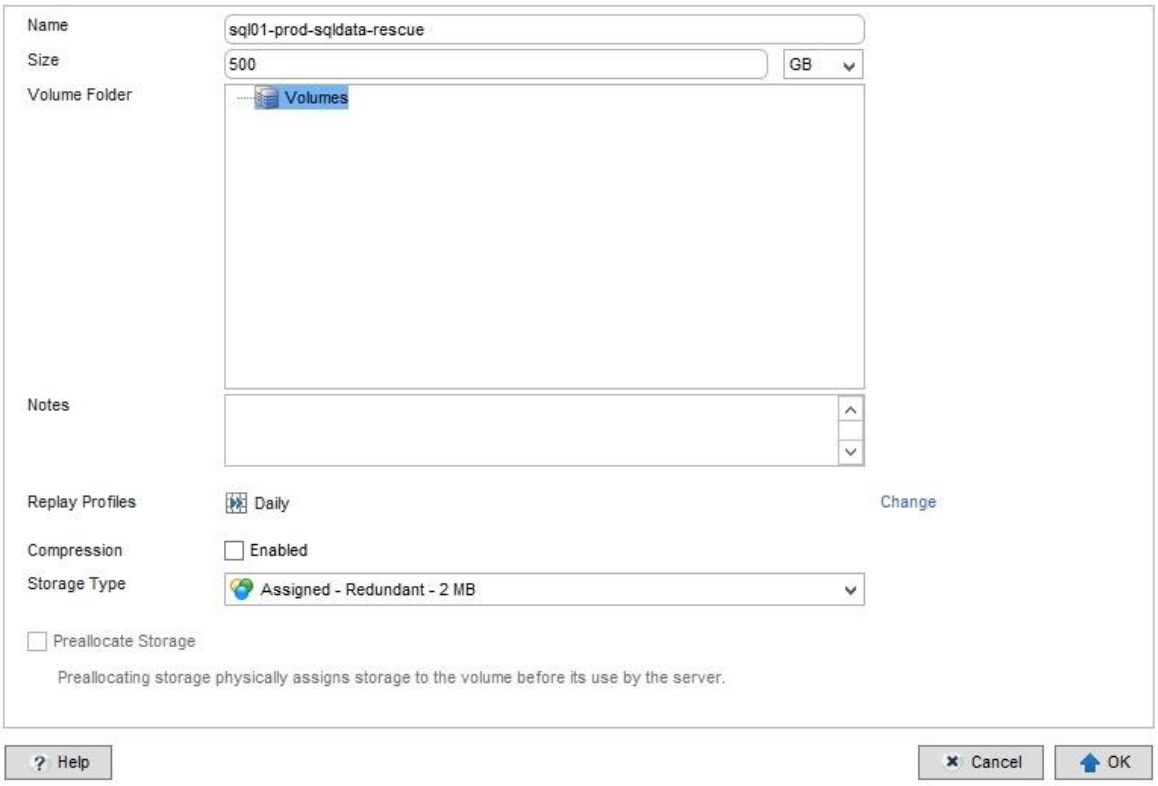



8. Enter the volume information:

   a. Provide details for the **Name**, **Size**, and **Volume Folder**.
   b. Change the settings for **Replay Profiles, Compression,** and **Storage Type** as necessary.

For the **Storage Type**, **Assigned – Redundant – 2MB** was selected to create the volume in the **Assigned** non-secure data disk.

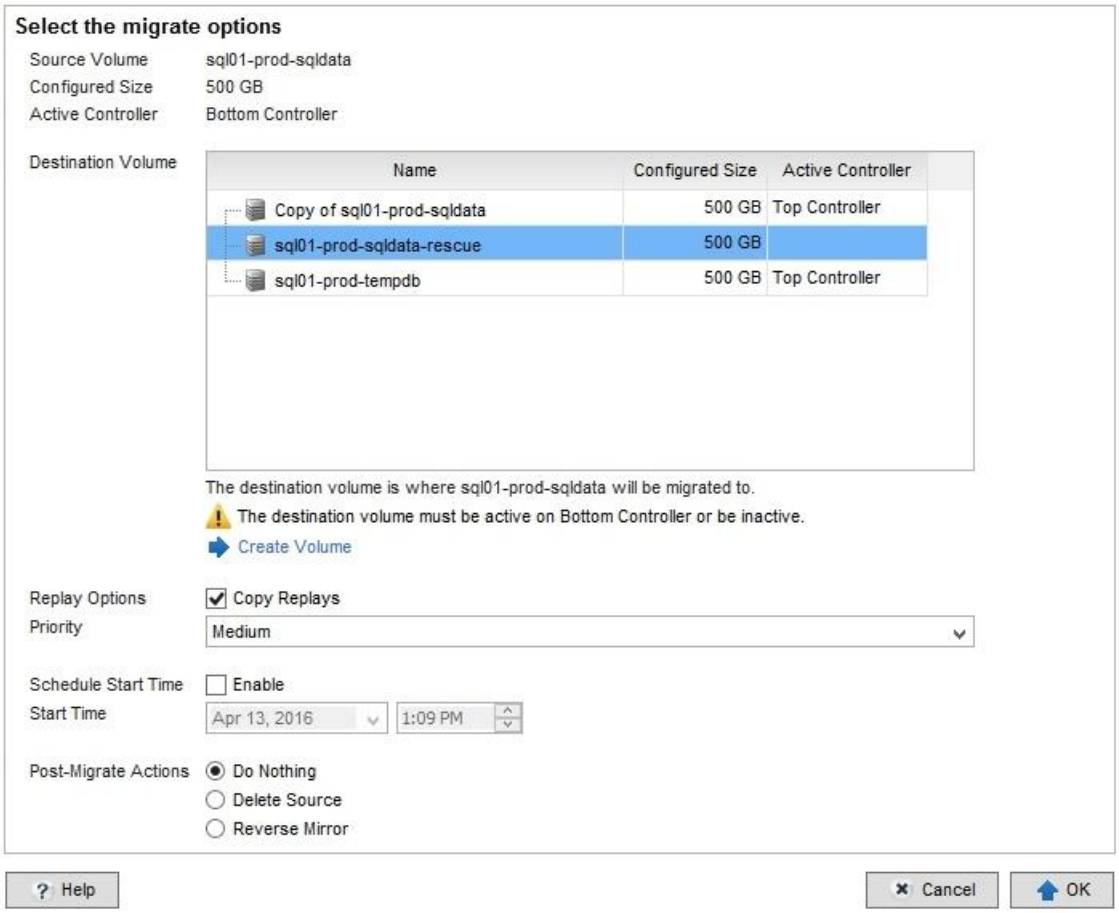
c. Click **OK** once the volume is ready to be created.0



2. Select the migrate options:

   a. Select a destination volume.
   b. Change the settings for **Replay Options, Priority, Schedule Start Time, Start Time,** and **Post-Migrate Actions** as necessary.
   c. Click **OK** once the volume is ready to be migrated.

   Depending on the size of the volume, it can take several minutes or longer to complete the migration.

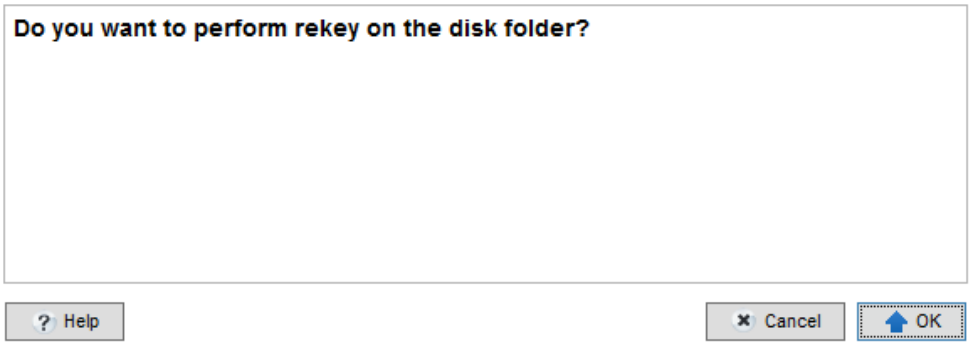



Once the volume is created, the **Summary** tab shows the Disk Folder as **Assigned**. If there is an event with the KMS, this would allow for the volume to be copied and still remain available to service volume I/O.

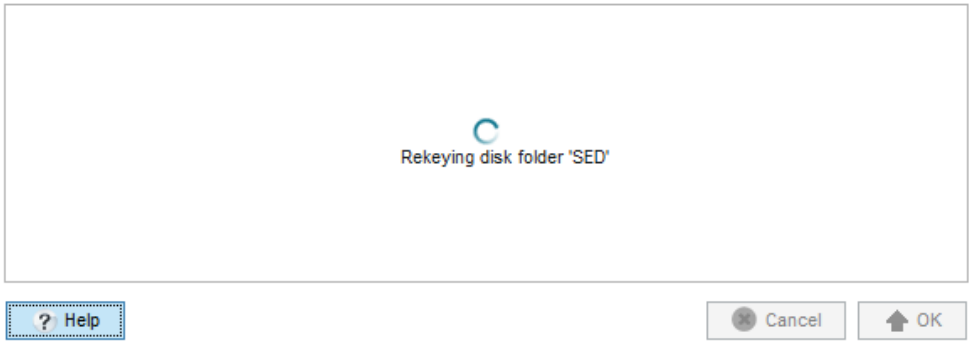
### 2.4.7 Rekey

The rekey feature allows you to change the key (or authority credential) for an SED. Certain organizations may be required to rekey or may perform this as part of a corporate security policy. The key can be changed using two methods: on-demand (disk folder or specific drives), or interval (disk folder only).

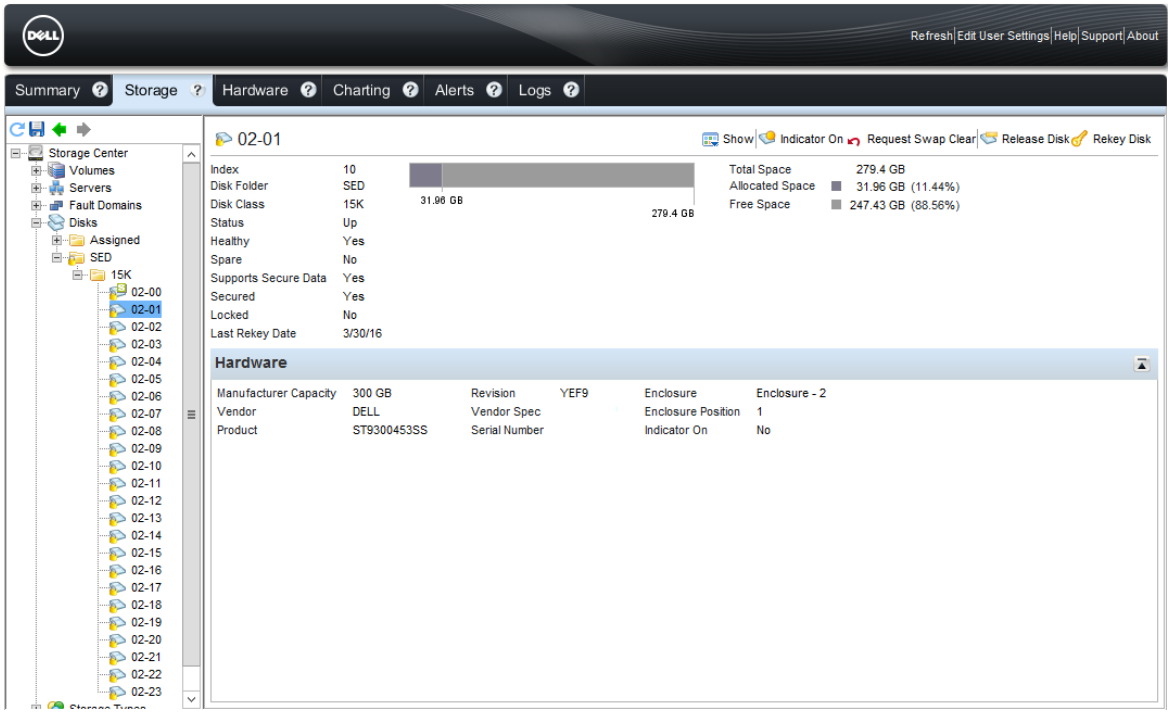
1. To rekey a drive or disk folder on demand inside the Dell Storage Manager client, select the **Storage** tab, expand **Disks,** right-click the secure data folder, and select **Rekey Disk Folder**. This will perform a rekey on all of the drives in the disk folder.
2. Click **OK** to start the rekey on the disk folder.




3. The rekey may take several minutes to complete.

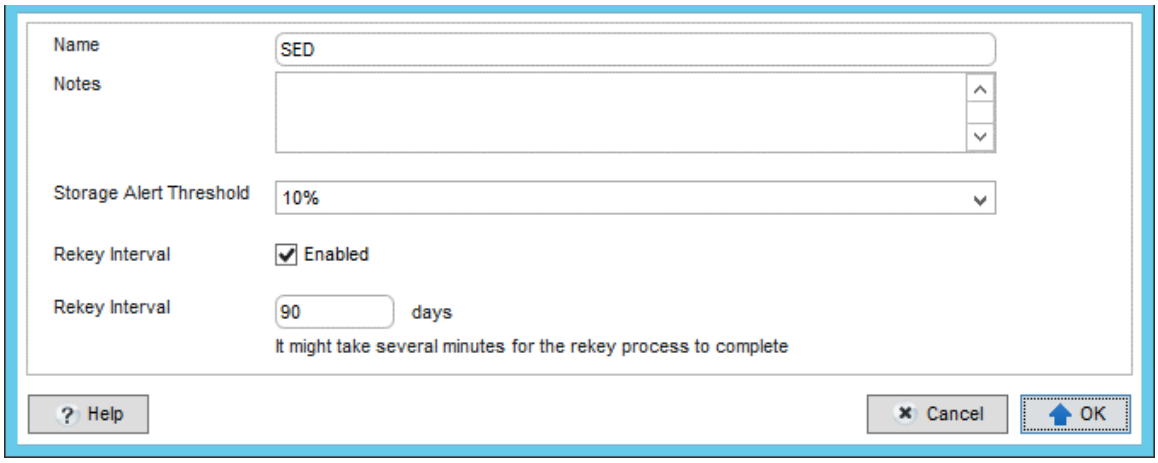


Once completed, view the properties of a drive and review the **Last Rekey Date**. The KMS will also have a different creation time, among other properties.

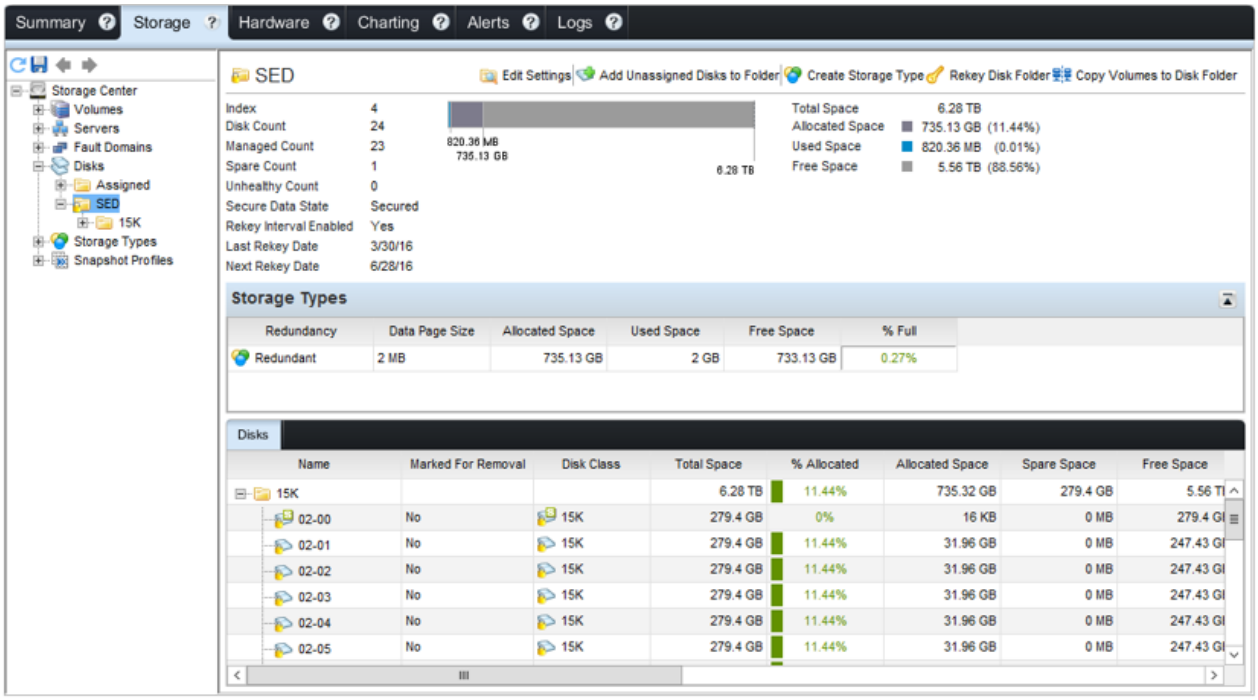



4. To set up a rekey interval, inside the **Dell Storage Manager Client**, click the **Storage** tab, expand **Disks**, right-click the secure data folder, and select **Edit Settings**.

5. Next to **Rekey Interval**, check **Enabled**. For the **Rekey Interval**, specify the number of days to wait between a rekey and click **OK**.




9. Review the **Next Rekey Date** to see when the drive folder will rekey next, which reflects the interval change specified in step 5 (90 days).



# 3 Certificate Creation with SafeNet KeySecure

**Disclaimer**: This procedure is an example procedure and the process of creating certificate files should be completed by a professional with expert knowledge of the process. The fields and information should be changed based on the organization and department in accordance with corporate security policies.

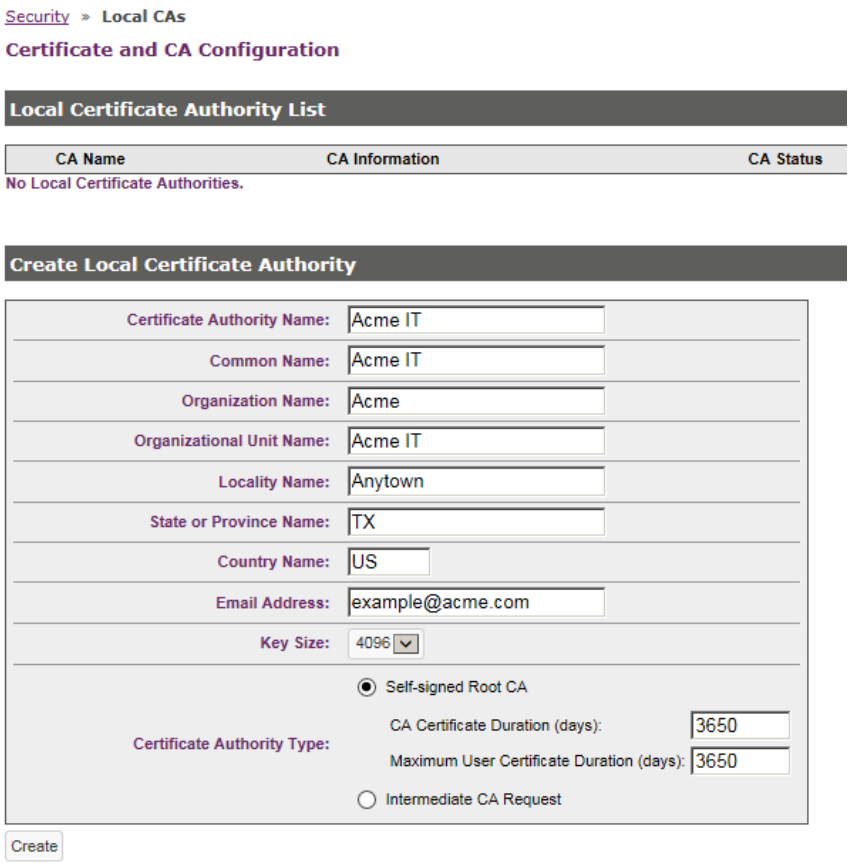
**Note**: This guide assumes that the SafeNet KeySecure appliance has already been configured correctly. For a reference architecture and step-by-step documentation on configuring the SafeNet appliance, refer to SafeNet's documentation for deploying and configuring the appliance.

**Note**: If the KeySecure K150v virtual appliance is being used to hold the keys of an SC Series array, it is important to NOT place the K150v on the same SC Series array that contains SED drives as this may result in the keys not being available during the array boot.

**Note**: The filenames listed are examples. Replace *sn111111* and *sn111112* with the Controller ID of the specific system where the files are created.

## 3.1 Generate the KeySecure Local Certificate Authority (CA)

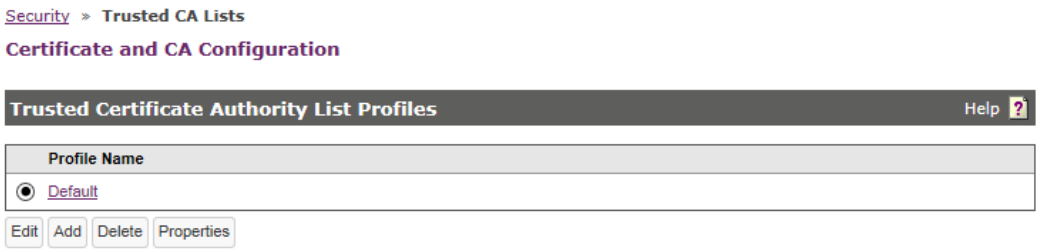
1. In the KeySecure Web UI, select the **Security** tab and select **Local CAs** from the left navigation menu.
2. Based on your organization, fill in the fields for the **Create Local Certificate Authority** section and select **Create**.




3. Verify the Certificate Authority has been created and select **Download**. It will be downloaded as Certificate Authority Name.crt, in this example Acme IT.crt. Change the name on your computer to remove spaces and change the extension from .crt to .cer. The resulting file should be AcmeIT.cer.

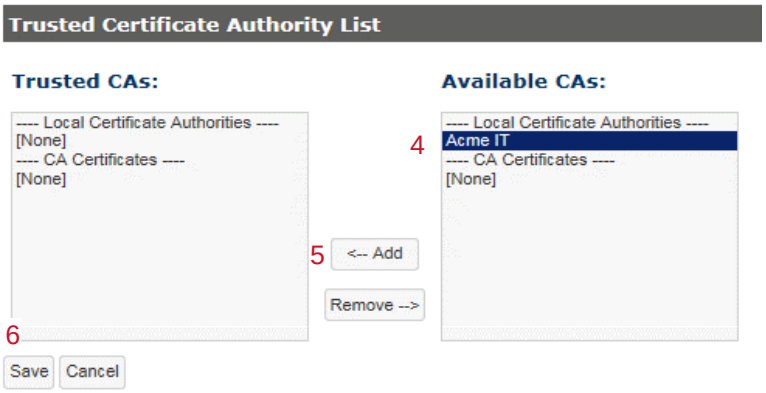
## 3.2 Add the Certificate Authority (CA) to the Trusted CA list

1. In the KeySecure Web UI, select the **Security** tab and select **Trusted CA Lists** from the left navigation menu.
2. Select the profile being used. In this example, we are using the profile name **Default**. Click **Properties** after selecting the Profile Name.




3. Below Trusted Certificate Authority List, select Edit.

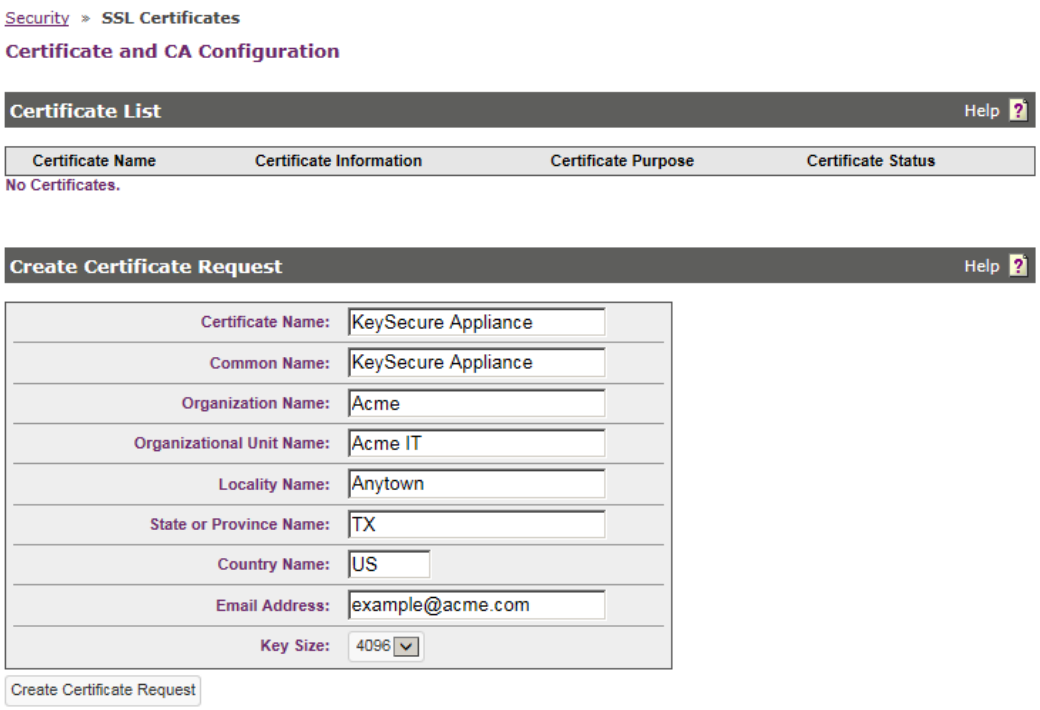

4. Select the CA in the **Available CAs** list, in this case “Acme IT”.
5. Select **Add** to add to the Trusted CAs list
6. Select **Save** to save the changes.



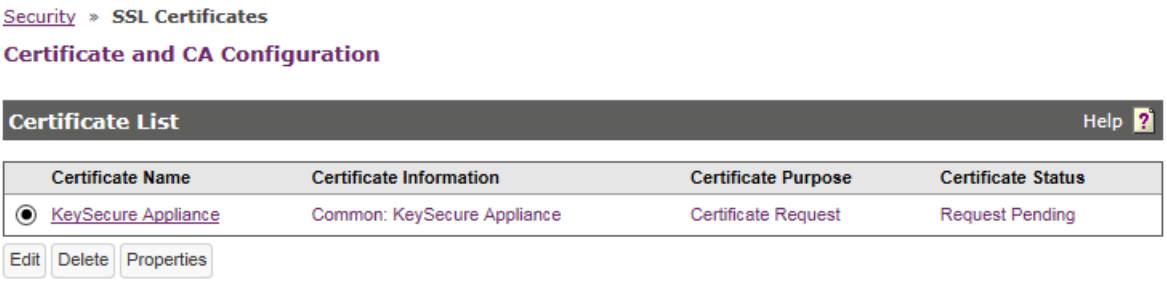

7. Verify that the Acme IT Local CA appears in the Trust Certificate Authority List.

## 3.3 Generate a KeySecure SSL certificate and sign with Local CA

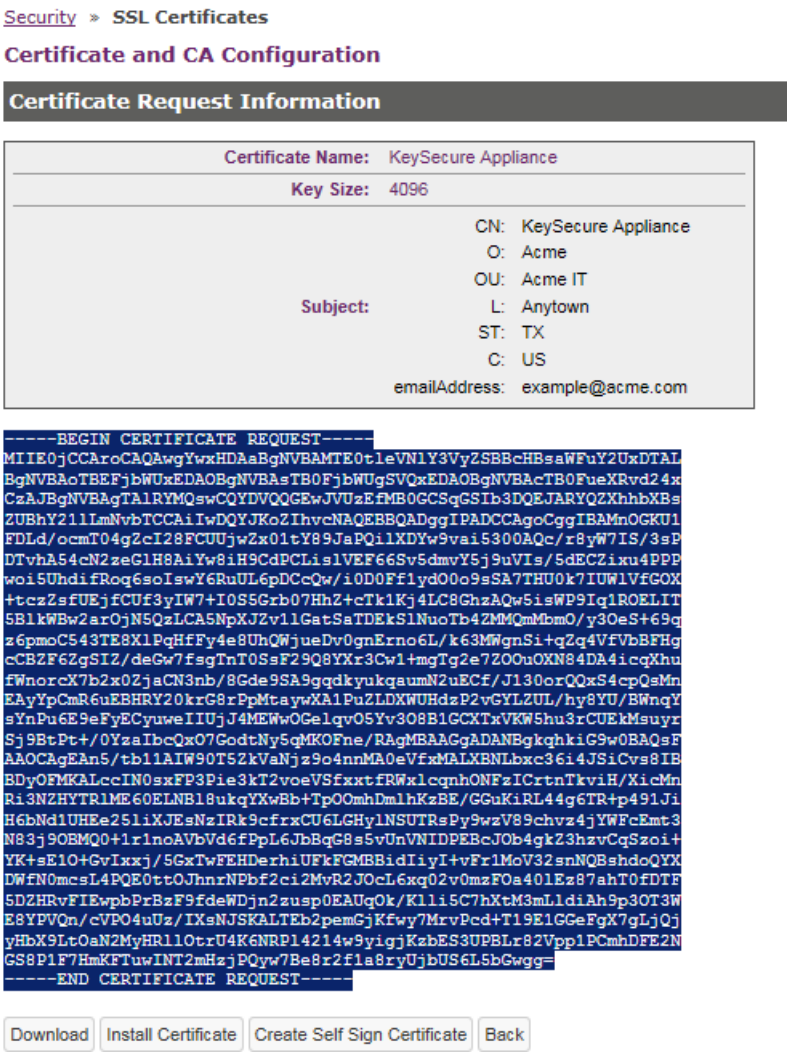
1. In the KeySecure Web UI, select the **Security** tab and select **SSL Certificates** from the left navigation menu.
2. Based on your organization, fill in the fields for the **Create Certificate Request** section and select **Create Certificate Request**




3. Verify in the **Certificate List** that the **KeySecure Appliance** Certificate Signing Request (CSR) has been created and has a **Certificate Status** of **Request Pending**.
4. Select the certificate and select **Properties**.



5. Copy the Certificate Signing Request (CSR) including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines.

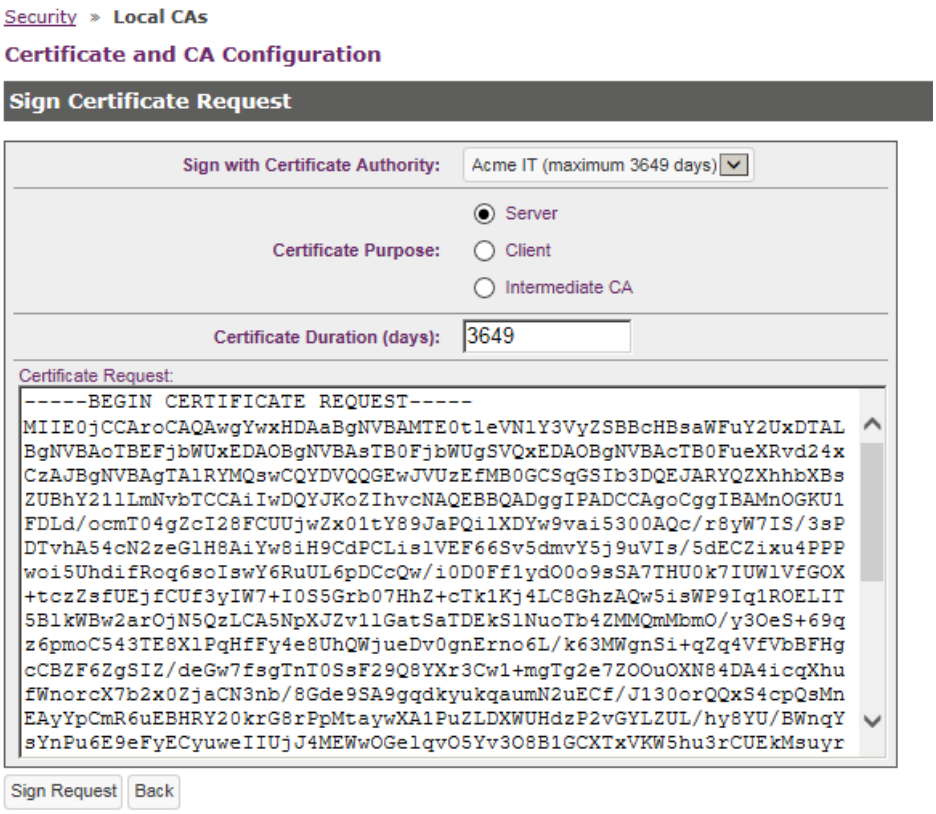



## 3.4 Sign the certificate

1. In the KeySecure Web UI, select the **Security** tab and select **Local CAs** from the left navigation menu.
2. Select the Acme IT CA that was created previously, and select **Sign Request**.


3. Paste the Certificate Signing Request from Step 3.1.3 into the Local CA **Certificate Request** window.

4. Select Server for the Certificate Purpose and then click Sign Request.

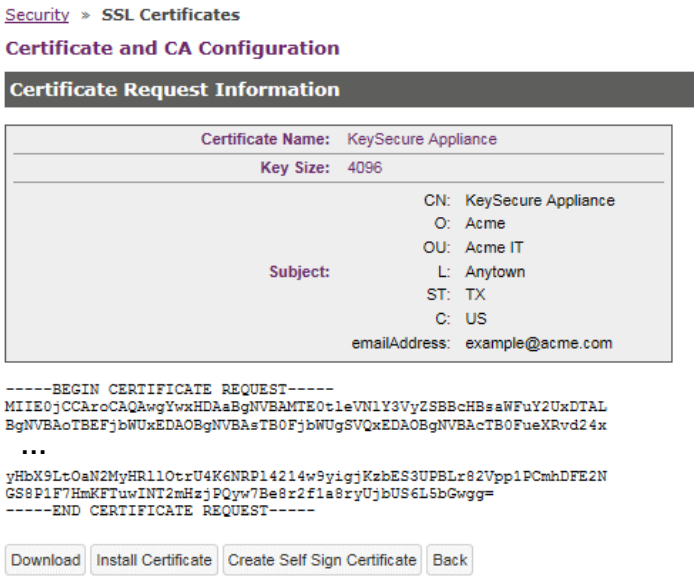



Sign Request Back

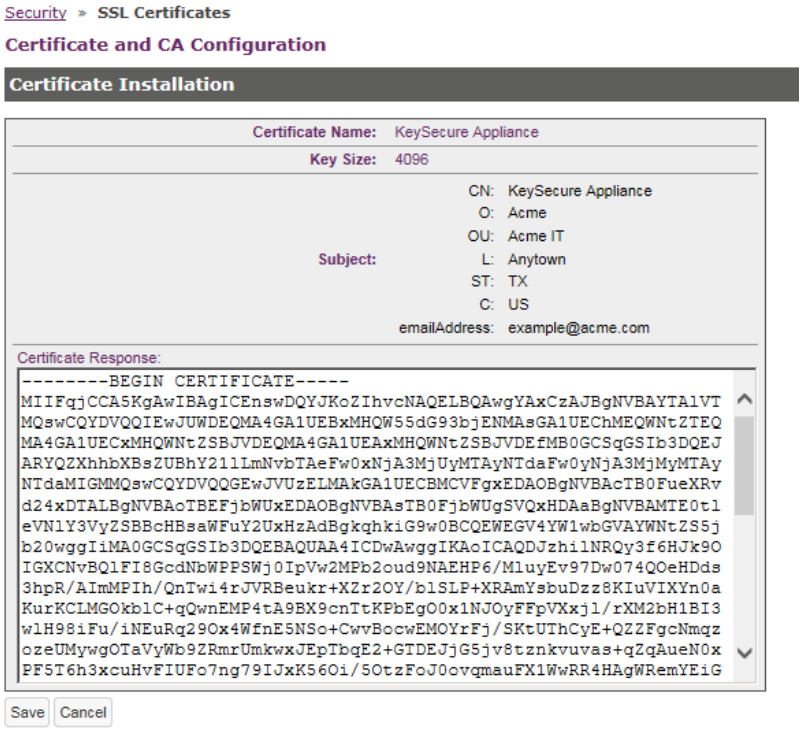
5. Copy the signed certificate, including the BEGIN CERTIFICATE and END CERTIFICATE lines.


Download Back

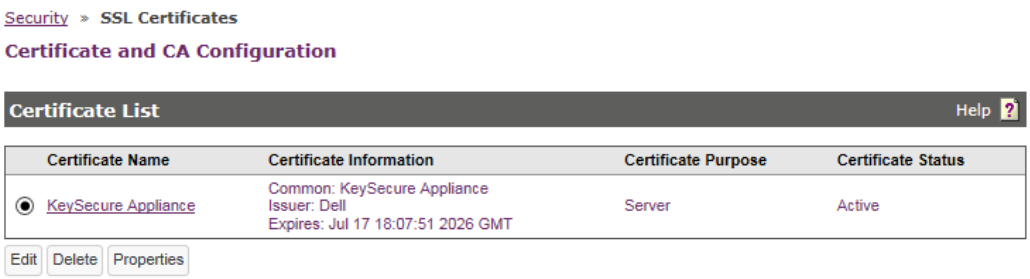
6. In the UI, open the **Secrity** tab and then click **SSL Certificate**.
7. Select the **KeySecure Appliance** SSL certificate and click **Properties**.
8. Click Install Certificate.




9. Paste the signed certificate from **Step 3.1.5** into the **Certificate Response** window and click **Save**

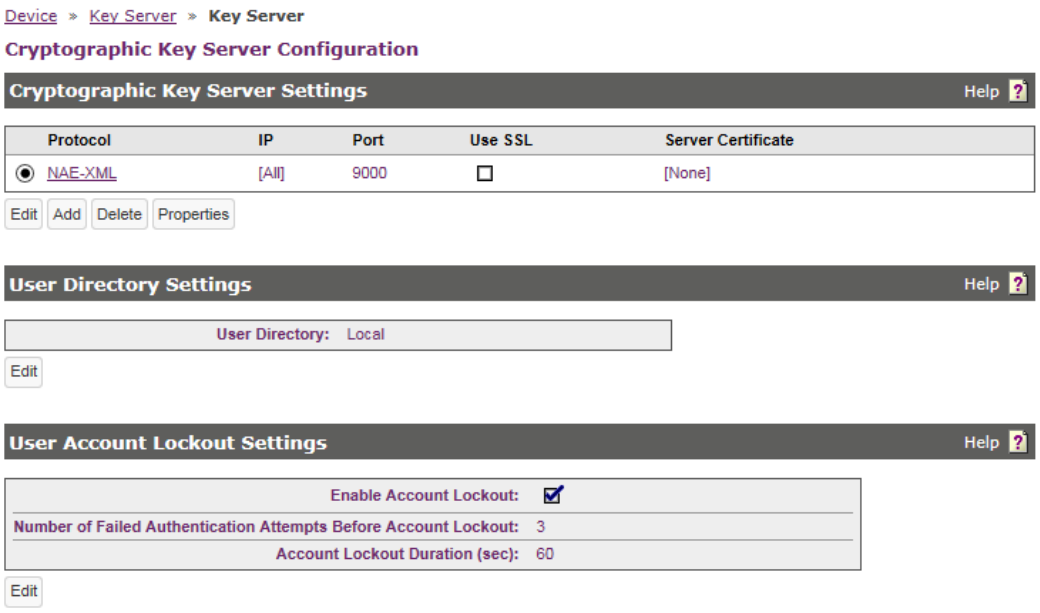


10. Verify that the Certificate Status is Active.




## 3.5 Generate the KMIP key server

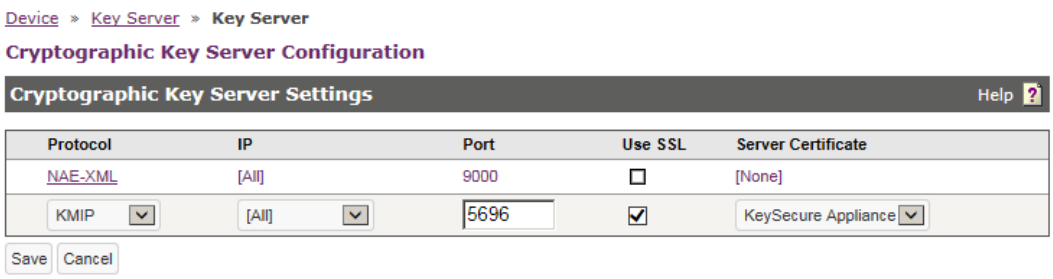
1. In the KeySecure Web UI, select the **Device** tab and select **Key Server** from the left navigation menu.
2. Select **Add** to create a new key server entry



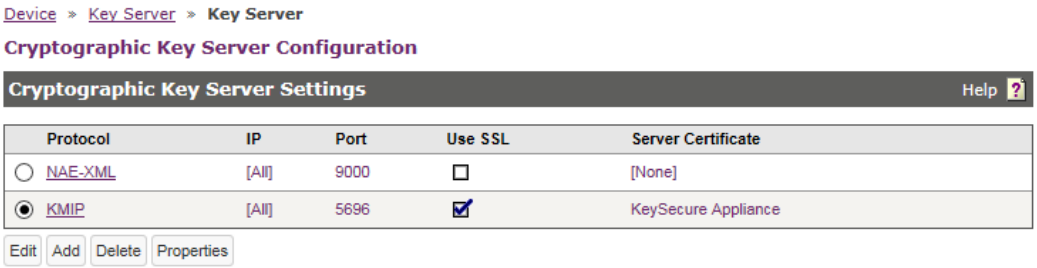

3. Set the following parameters:

   a. **Protocol** = KMIP
   b. **Port** = 5696
   c. Select **Use SSL**
   d. Select the KeySecure Appliance certificate that was previously signed.

4. Click **Save** to retain the new key server configuration.

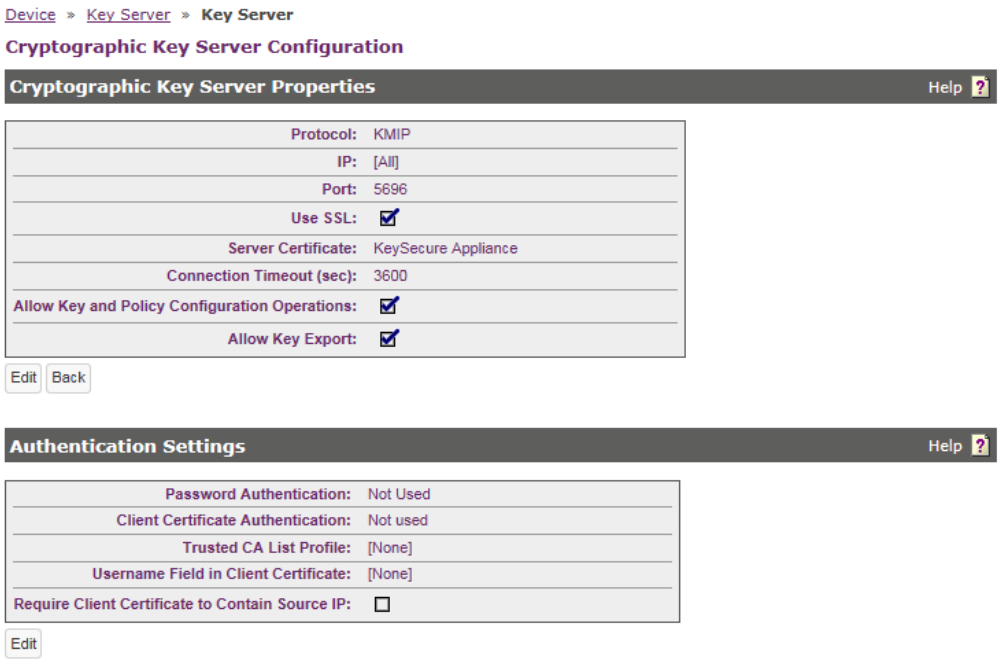



5. Review the settings.




## 3.6 Change authentication settings for the SC Series array and KMS to negotiate

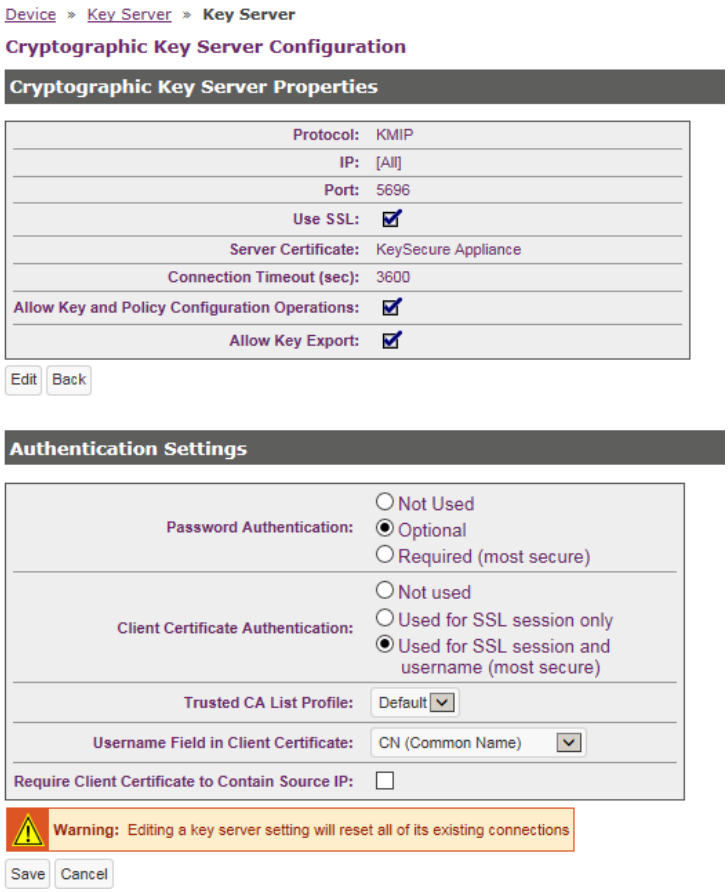
1. In the KeySecure Web UI, select the **Device** tab and select **Key Server** from the left navigation menu.
2. Select the radio button for the newly created **Key Server** KMIP and select **Properties**.



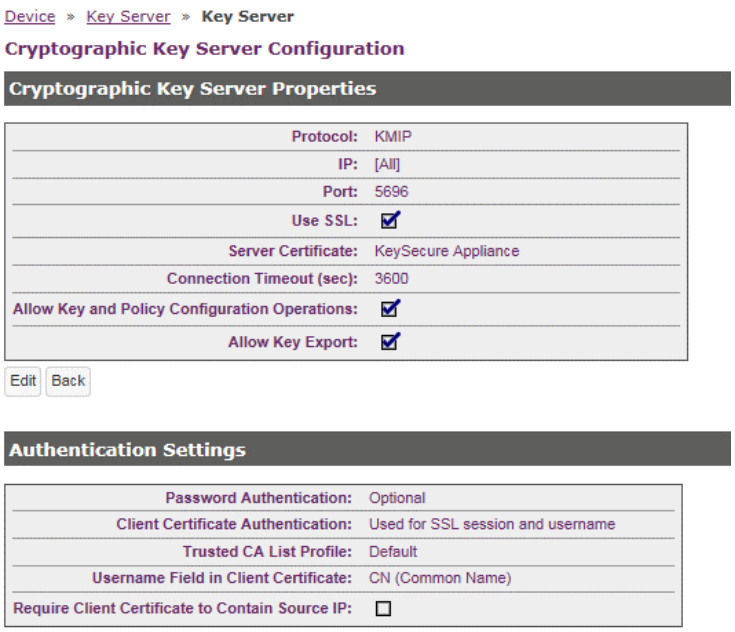
3. Click **Edit** below **Authentication Settings** and change the following settings

   a. Password Authentication = Optional
   b. Client Certificate Authentication = Used for SSL session and username (most secure)
   c. Trusted CA List Profile = Default
   d. Username Field in Client Certificate = CN (Common Name)

4. When finished, click **Save**.

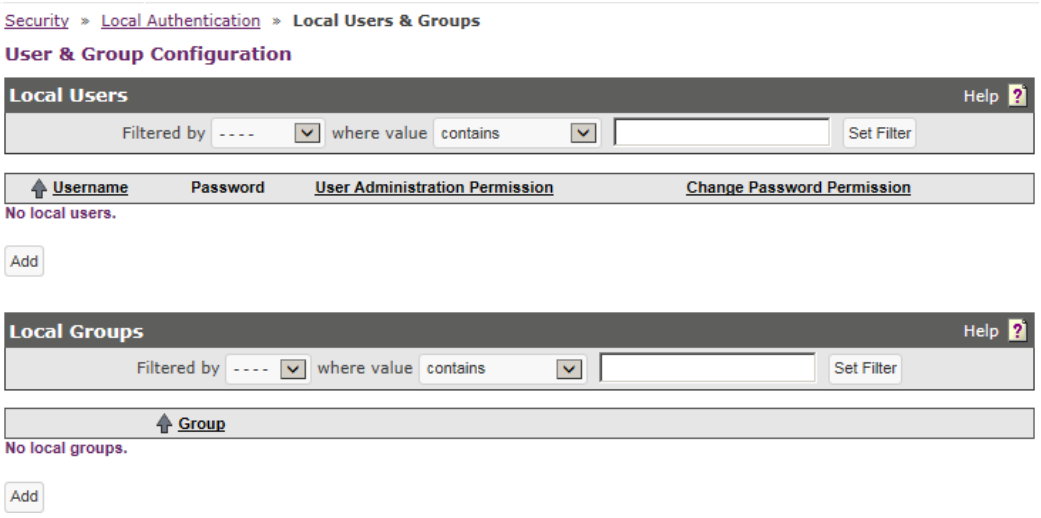


5. Review the settings




## 3.7 Add the common name to the KeySecure local users directory

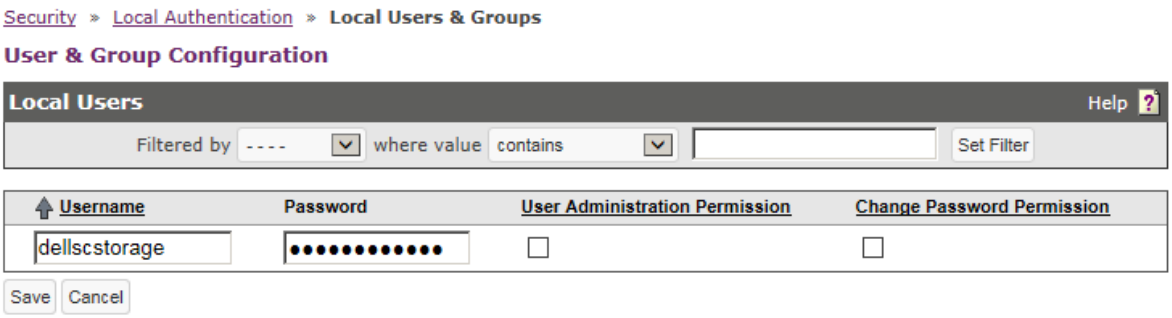
1. In the KeySecure Web UI, select the **Security** tab and select **Local Authentication** from the left navigation menu.



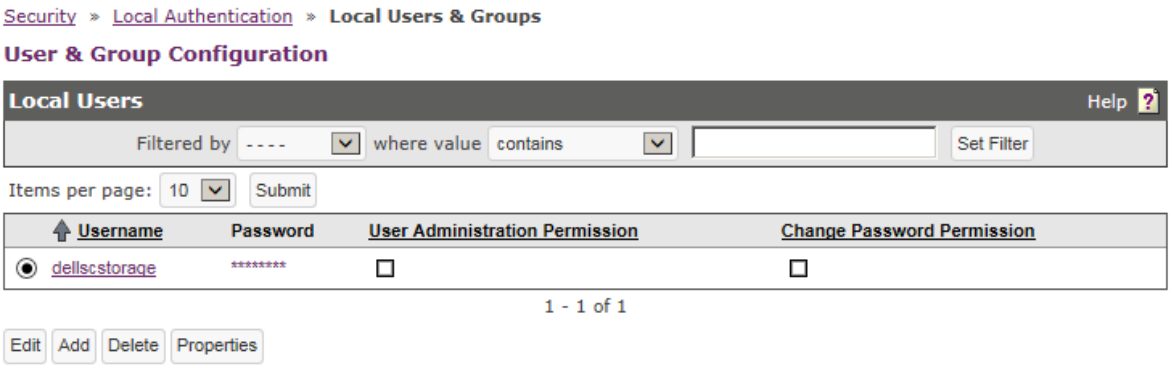

2. Select **Add** to create the authentication user
3. Enter in the following details:

   a. The username that corresponds to the CN field from the SC Series certificate.
   b. The password field cannot be left blank, however, it is not used for further authentication.

4. Select **Save** to retain the user settings.




5. The username should appear in the Local Users list.




**Note**: If you are connecting multiple SC Series arrays to a KeySecure KMS it is recommended to create and utilize a local authentication user that is uniquely named for each SC Series array. This will ensure that a single array can only access keys that belong it, and that access times are optimized and as quick as possible.

## 3.8 Generate an RSA key pair for the SC Series arrays

SC Series arrays allow creating one client certificate and using it on multiple controllers as well as creating separate client certificates for each controller. The standard practice is to use OpenSSL to create the client certificate request and the private key file. Once the client certificate request(s) (CSR files) are created, they need to be signed by the KeySecure CA as client certificates.

1. Using OpenSSL, enter the following command and provide the necessary details (based on the specific organization for the certificates) to create key pair for the first controller. The CN field for the certificate should be the same as defined in Step 3.4. An example of the entire process is listed below.

   ```
   openssl req -out sn111111_4096.csr -new -newkey rsa:4096 -nodes -keyout
   sn111111_4096.key
   ```

2. Using OpenSSL, enter the following command and provide the necessary details (based on the specific organization for the certificates) to create the key pair for the second controller. The CN field for the certificate should be the same as defined in Step 3.4. An example of the entire process is listed below.

```
openssl req -out sn111112_4096.csr -new -newkey rsa:4096 -nodes -keyout
sn111112_4096.key
```

```
[root@localhost ~]# openssl req -out sn111111_4096.csr -new -newkey rsa:4096 -nodes -keyout sn111111_4096.key
Generating a 4096 bit RSA private key
.....................................................++
.....................................................................................................................
writing new private key to 'sn111111_4096.key'
-----
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) [XX]:US
State or Province Name (full name) []:TX
Locality Name (eg, city) [Default City]:Anytown
Organization Name (eg, company) [Default Company Ltd]:Acme
Organizational Unit Name (eg, section) []:Acme IT
Common Name (eg, your name or your server's hostname) []:dellscstorage
Email Address []:example@acme.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:dellscseries
An optional company name []:
[root@localhost ~]# openssl req -out sn111112_4096.csr -new -newkey rsa:4096 -nodes -keyout sn111112_4096.key
Generating a 4096 bit RSA private key
..........++
................++
writing new private key to 'sn111112_4096.key'
-----
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) [XX]:US
State or Province Name (full name) []:TX
Locality Name (eg, city) [Default City]:Anytown
Organization Name (eg, company) [Default Company Ltd]:Acme
Organizational Unit Name (eg, section) []:Acme IT
Common Name (eg, your name or your server's hostname) []:dellscstorage
Email Address []:example@acme.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:dellscseries
An optional company name []:
[root@localhost ~]#
```

3. The result will be four files and the AcmeIT.cer file from Step 3.1.

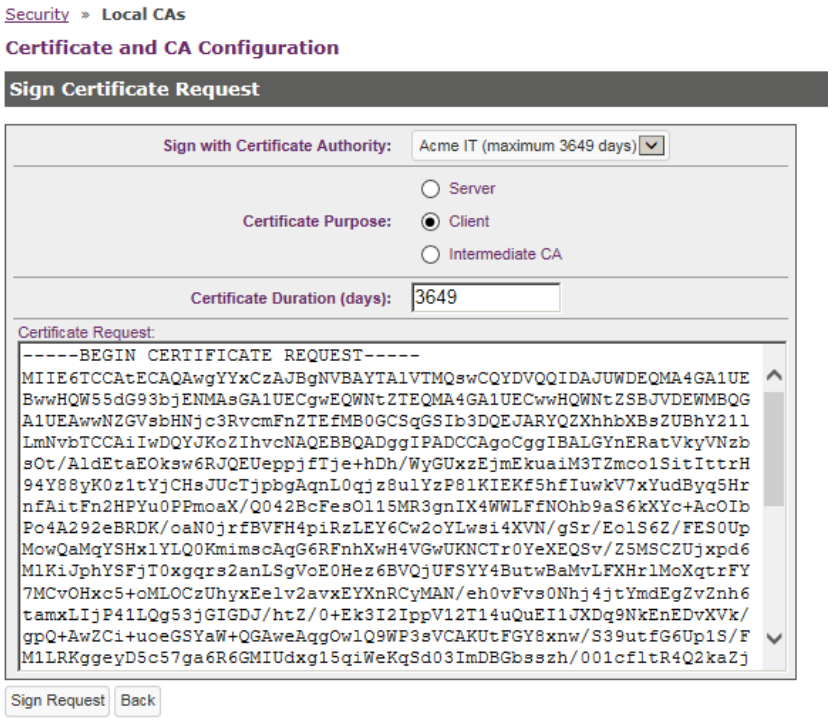
   sn111111_4096.csr
   sn111111_4096.key
   sn111112_4096.csr
   sn111112_4096.key

**Note**: The CN field for both certs use the same entry.

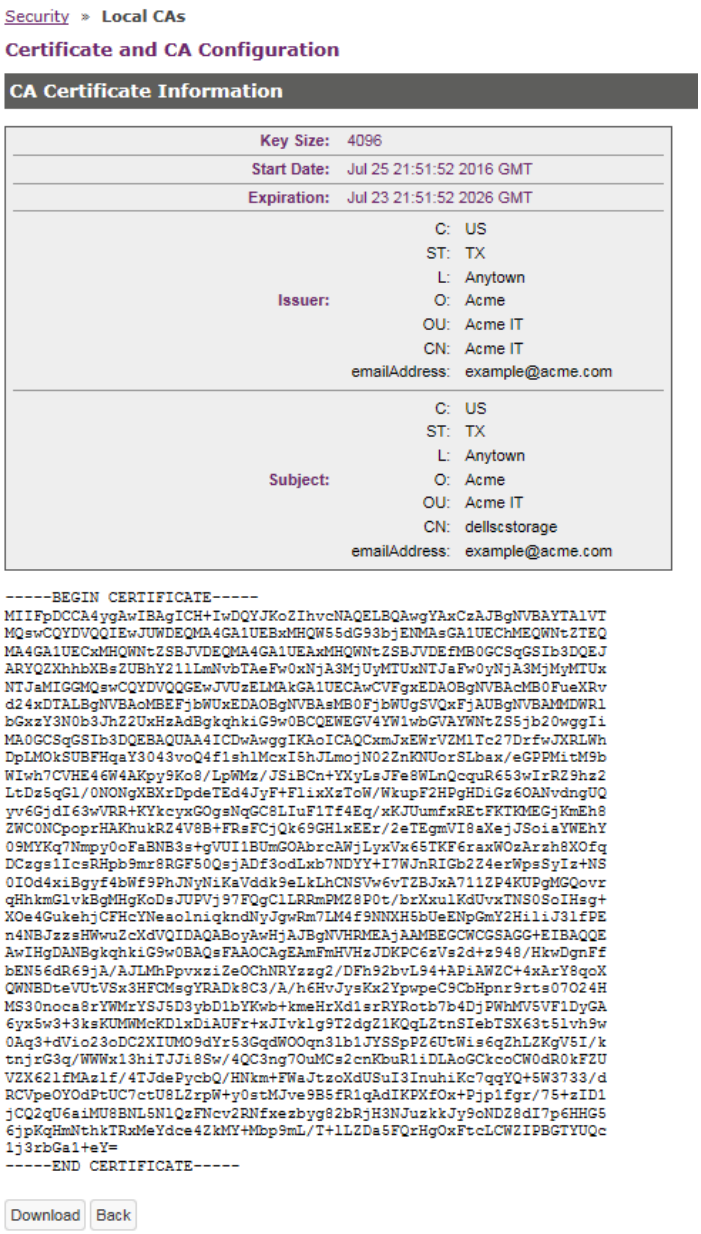
## 3.9 Sign the .csr key pair files

1. In the KeySecure Web UI, select the **Security** tab and select **Local CAs** from the left navigation menu.
2. Click Sign Request.


3. Open the sn111111_4096.csr file in a text editor, then copy and paste the contents including the BEGIN and END lines into **Certificate Request** field.
4. Change the Certificate Purpose to Client and click Sign Request.




5. Click **Download** to save the certificate.



Security » Local CAs

**Certificate and CA Configuration**

**CA Certificate Information**

| | | |
|---|---|---|
| **Key Size:** | 4096 | |
| **Start Date:** | Jul 25 21:51:52 2016 GMT | |
| **Expiration:** | Jul 23 21:51:52 2026 GMT | |
| **Issuer:** | C: | US |
| | ST: | TX |
| | L: | Anytown |
| | O: | Acme |
| | OU: | Acme IT |
| | CN: | Acme IT |
| | emailAddress: | example@acme.com |
| **Subject:** | C: | US |
| | ST: | TX |
| | L: | Anytown |
| | O: | Acme |
| | OU: | Acme IT |
| | CN: | dellscstorage |
| | emailAddress: | example@acme.com |

```
-----BEGIN CERTIFICATE-----
MIIFpDCCA4ygAwIBAgICH+IwDQYJKoZIhvcNAQELBQAwgYAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJUWDEQMA4GA1UEBxMHQW55dG93bjENMAsGA1UEChMEQWNtZTEQ
MA4GA1UECxMHQWNtZSBJVDEQMA4GA1UEAxMHQWNtZSBJVDEfMB0GCSqGSIb3DQEJ
ARYQZXhhbXBsZUBhY211LmNvbTAeFw0xNjA3MjUyMTUxNTJaFw0yNjA3MjMyMTUx
NTJaMIGGMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxEDAOBgNVBAcMB0FueXRv
d24xDTALBgNVBAoMBEFjbWUxEDAOBgNVBAsMB0FjbWUgSVQxFjAUBgNVBAMMDWRl
bGxzY3N0b3JhZ2UxHzAdBgkqhkiG9w0BCQEWEGV4YW1wbGVAYWNtZS5jb20wggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCxmJxEWrVZMlTc27DrfwJXRLWh
DpLMOkSUBFHqaY3043voQ4flshlMcxI5hJLmojN02ZnKNUorSLbax/eGPPMitM9b
WIwh7CVHE46W4AKpy9Ko8/LpWMz/JSiBCn+YXyLsJFe8WLnQcquR653wIrRZ9hz2
LtDz5qGl/0NONgXBXrDpdeTEd4JyF+FlixXzToW/WkupF2HPgHDiGz6OANvdngUQ
yv6GjdI63wVRR+KYkcyxGOgsNqGC8LIuF1Tf4Eq/xKJUumfxREtFKTKMEGjKmEh8
ZWC0NCpoprHAKhukRZ4V8B+FRsFCjQk69GH1xEEr/2eTEgmVI8aXejJSoiaYWEhY
09MYKq7Nmpy0oFaBNB3s+gVUI1BUmGOAbrcAWjLyxVx65TKF6raxWOzArzh8XOfq
DCzgs1IcsRHpb9mr8RGF50QsjADf3odLxb7NDYY+I7WJnRIGb2Z4erWpsSyIz+NS
0IOd4xiBgyf4bWf9PhJNyNiKaVddk9eLkLhCNSVw6vTZBJxA711ZP4KUPgMGQovr
qHhkmGlvkBgMHgKoDsJUPVj97FQgClLRRmPMZ8P0t/brXxulKdUvxTNSOSoIHsg+
XOe4GukehjCFHcYNeaolniqkndNyJgwRm7LM4f9NNXH5bUeENpGmY2HiliJ3lfPE
n4NBJzzsHWwuZcXdVQIDAQABoyAwHjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQE
AwIHgDANBgkqhkiG9w0BAQsFAAOCAgEAmFmHVHzJDKPC6zVs2d+z948/HkwDgnFf
bEN56dR69jA/AJLMhPpvxziZeOChNRYzzg2/DFh92bvL94+APiAWZC+4xArY8qoX
QWNBDteVUtVSx3HFCMsgYRADk8C3/A/h6HvJysKx2YpwpeC9CbHpnr9rts07O24H
MS30noca8rYWMrYSJ5D3ybD1bYKwb+kmeHrXd1srRYRotb7b4DjPWhMV5VF1DyGA
6yx5w3+3ksKUMWMcKDlxDiAUFr+xJIvklg9T2dgZ1KQqLZtnSIebTSX63t5lvh9w
0Aq3+dVio23oDC2XIUMO9dYr53GqdWOOqn3lb1JYSSpPZ6UtWis6qZhLZKgV5I/k
tnjrG3q/WWWx13hiTJJi8Sw/4QC3ng7OuMCs2cnKbuR1iDLAoGCkcoCW0dR0kFZU
VZX62lfMAzlf/4TJdePycbQ/HNkm+FWaJtzoXdUSuI3InuhiKc7qqYQ+5W3733/d
RCVpeOYOdPtUC7ctU8LZrpW+y0stMJve9B5fR1qAdIKPXfOx+Pjp1fgr/75+zID1
jCQ2qU6aiMU8BNL5N1QzFNcv2RNfxezbyg82bRjH3NJuzkkJy9oNDZ8dI7p6HHG5
6jpKqHmNthkTRxMeYdce4ZkMY+Mbp9mL/T+lLZDa5FQrHgOxFtcLCWZIPBGTYUQc
1j3rbGa1+eY=
-----END CERTIFICATE-----
```

Download Back

6. Rename as sn111111_signed_4096.cer in the operating system.
7. Repeat Steps 1 – 6 for the sn111112_4096.csr file and rename it to sn111112_signed_4096.cer in the operating system

## 3.10 Create the Dell client certificate bundle.

1. Consolidate the signed certificate files into one folder. The files listed below are an example of what should be located in the folder.

   sn111111_4096.csr
   sn111111_4096.key
   sn111111_signed_4096.cer
   sn111112_4096.csr
   sn111112_4096.key
   sn111112_signed_4096.cer

2. Create the final client certificate file bundle by concatenating the certificate signing request, the private key and the signed client certificate file to create the final client certificate.

   ```
   cat sn111111_4096.csr sn111111_4096.key sn111111_signed_4096.cer >
   sn111111_4096.pem

   cat sn111112_4096.csr sn111112_4096.key sn111112_signed_4096.cer >
   sn111112_4096.pem
   ```

## 3.11 Validating the Certificates

1. Before attempting to connect the SC Series array to the KeySecure appliance you can use the OpenSSL command shown below to validate the SSL connection to the KeySecure is working. Use the example commands below to verify validity.

   ```
   openssl s_client -tls1 -connect 10.10.10.10:5696 -verify 10 -showcerts -
   cert sn111111_4096.pem –CAfile AcmeIT.cer

   openssl s_client -tls1 -connect 10.10.10.10:5696 -verify 10 -showcerts -
   cert sn111112_4096.pem –CAfile AcmeIT.cer
   ```

2. The results at the end of the command should show the following lines:

   ```
   Start Time: 1471622451
   Timeout   : 7200 (sec)
   Verify return code: 0 (ok)
   ```

# 4 Certificate creation with keyAuthority

**Disclaimer**: This procedure is an example procedure and the process of creating certificate files should be completed by a professional with expert knowledge of the process. The fields and information should be changed based on the organization and department in accordance with corporate security policies.

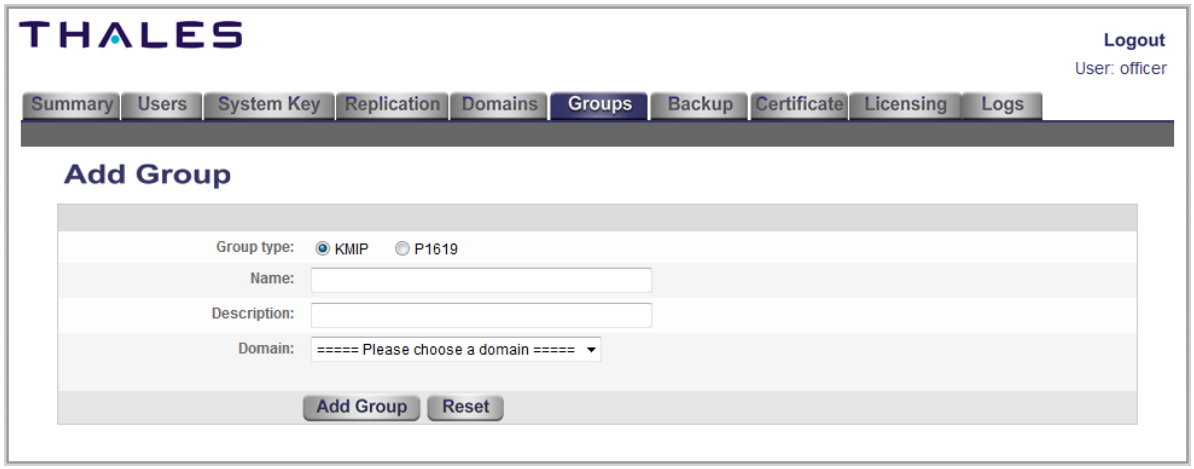
**Note**: This guide assumes that the Thales® keyAuthority® appliance has already been configured correctly. For reference architecture and step-by-step documentation on configuring the keyAuthority appliance refer to the Thale documentation for deploying and configuring the appliance.

**Note**: The filenames listed are examples. Replace *sn111111* and *sn111112* with the specific system controller ID.

## 4.1 Adding a group for your clients

In order to add the Controller(s) as a keyAuthority client you will need to have configured a valid domain name and a group that will contain the controller or controllers. As an officer user, you may need to login and verify that a group or groups exist for the controllers or add them as shown below.

1. In the keyAuthority Web UI, select the **Groups** tab.
2. Click Add Group.

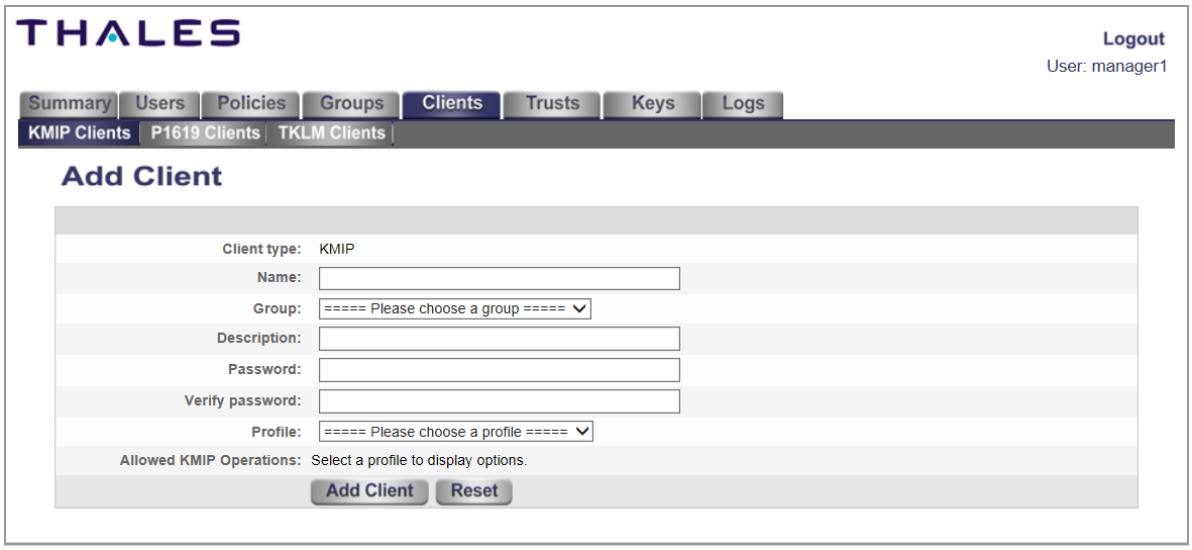



## 4.2 Adding the controller as a KMIP Client

Once the group is added, the officer will need to add group management rights to the appropriate group manager user ID's at which point an assigned group manager will login and add the device as a client as shown below.

1. In the keyAuthority Web UI, open the **Clients** tab.
2. Enter in values for **Name**, **Description**, **Password** and **Verify password** fields.
3. Select the **Group** created in Step 4.1.
4. For Profile, select Generic Profile.

5. Click Add Client.




## 4.3 Generate an RSA key pair for the SC Series array

SC Series arrays allow creating one client certificate and using it on multiple controllers as well as creating a separate client certificate for each controller. The standard practice is to use OpenSSL to create the client certificate request and the private key file. Once the client certificate request(s) (CSR files) are created, they need to be signed by the keyAuthority CA client certificate(s).

1. Using OpenSSL, enter the following command and provide the necessary details (based on the specific organization the certificates are being generated for) to create key pair for the first controller. The CN (Common Name) does not have to match the configured client name in keyAuthority as the keyAuthority operates as a closed PKI system, but should match for consistency.

   ```
   openssl req -out sn111111_4096.csr -new -newkey rsa:4096 -nodes -keyout
   sn111111_4096.key
   ```

2. Using OpenSSL, enter the following command and provide the necessary details (based on the specific organization the certificates are being generated for) to create key pair for the second controller. The CN (Common Name) does not have to match the configured client name in keyAuthority as the keyAuthority operates as a closed PKI system, but should match for consistency.

   ```
   openssl req -out sn111112_4096.csr -new -newkey rsa:4096 -nodes -keyout
   sn111112_4096.key
   ```

```
[root@localhost ~]# openssl req -out sn111111_4096.csr -new -newkey rsa:4096 -nodes -keyout sn111111_4096.key
Generating a 4096 bit RSA private key
.....................................................................++
.....................................................................................................................................+
writing new private key to 'sn111111_4096.key'
-----
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) [XX]:US
State or Province Name (full name) []:TX
Locality Name (eg, city) [Default City]:Anytown
Organization Name (eg, company) [Default Company Ltd]:Acme
Organizational Unit Name (eg, section) []:Acme IT
Common Name (eg, your name or your server's hostname) []:
Email Address []:example@acme.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@localhost ~]# openssl req -out sn111112_4096.csr -new -newkey rsa:4096 -nodes -keyout sn111112_4096.key
Generating a 4096 bit RSA private key
.....................................................................................................++
..........................++
writing new private key to 'sn111112_4096.key'
-----
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) [XX]:US
State or Province Name (full name) []:TX
Locality Name (eg, city) [Default City]:Anytown
Organization Name (eg, company) [Default Company Ltd]:Acme
Organizational Unit Name (eg, section) []:Acme IT
Common Name (eg, your name or your server's hostname) []:
Email Address []:example@acme.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3. The result will be four files.

   sn111111_4096.csr
   sn111111_4096.key
   sn111112_4096.csr
   sn111112_4096.key

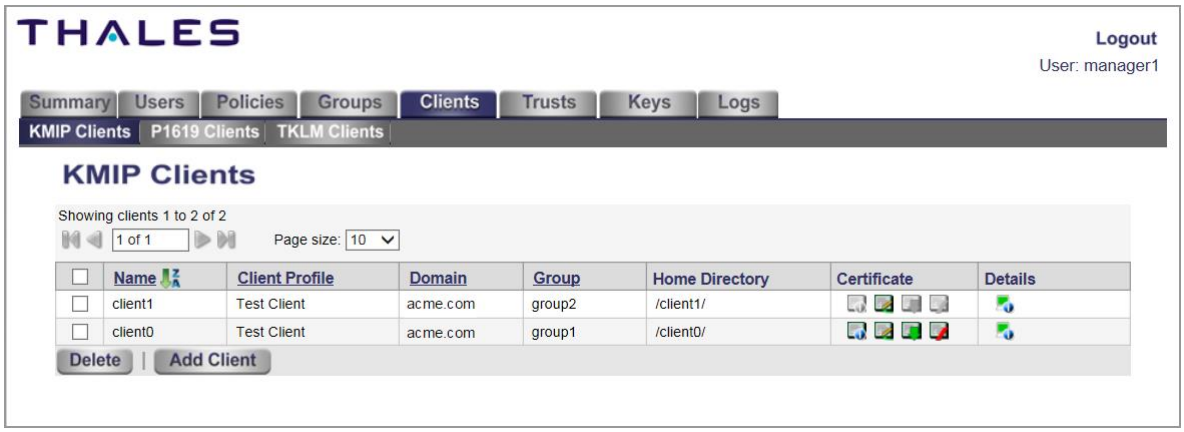
## 4.4 Sign the .csr key pair files

Take the generated CSR(s) (sn111111_4096.csr and sn111112_4096.csr) and use the KMIP client created in step 3.1 to sign the requests.

1. In the keyAuthority Web UI, open the **Clients** tab and locate the KMIP Client created in step 4.2.

**Note**: The example below shows two clients, but for simplicity there would be one client for both controllers.

2. Select the **Sign Request** button (second icon in the Certificate column). Refer to Figure 4 below.




3. The CSR files created earlier can be imported individually or cut and paste the text from the CSR file.
4. Enter the number of days the certificate needs to be valid (the default is 730 days or approximately two years). Ensure you select the proper radial button next to **From file** or **From text** based on how you enter the CSR as shown below.


**Note**: When the certificate expires or is revoked, the controller will no longer be able to access keyAuthority to get keys. Proper planning for certificate validity is critical for the long term accessibility and functionality of the system.

5. Click **Sign** to download and save the certificate.

## 4.5 Create the SC Series client certificate bundle

1. Consolidate the certificate files into one folder. The files listed below are an example of what should be located in the folder.

   sn111111_4096.csr
   sn111111_4096.key

sn111111_signed_4096.cer
sn111112_4096.csr
sn111112_4096.key
sn111112_signed_4096.cer

2. Create the final client certificate file bundle by concatenating the certificate signing request, the private key and the signed client certificate file to create the final client certificate.

```
cat sn111111_4096.csr sn111111_4096.key sn111111_signed_4096.cer >
sn111111_4096.pem

cat sn111112_4096.csr sn111112_4096.key sn111112_signed_4096.cer >
sn111112_4096.pem
```

## 4.6 Download the keyAuthority Client Root CA

1. In the keyAuthority Web UI, select the **Clients** tab and locate the KMIP Client created in step 3.1.
2. Click **Export Certificate** (third icon in the certificates column). Refer to screenshots in section 4.4.
3. The web browser will prompt you to download and save the file. The name of the certificate will default to the name of your KMIP client. The default file format will be .pem; you can also save the file in the .cer format. Save the file in the same folder as the certificates in step 4.4.

**Note**: All examples that follow will assume that the KMIP Client Root CA is named AcmeIT.cer.

## 4.7 Validating the Certificates

Before attempting to connect the SC Series array to the KeySecure appliance, use the OpenSSL command shown below to validate the SSL connection to the KeySecure.

```
openssl s_client -tls1 –connect <IP of Appliance Data Interface>:<KMIP
Port> -verify 10 -showcerts -cert <Client Cert Filename> –CAfile <KMIP
Client Root CA>
openssl s_client -tls1 -connect 10.10.10.10:5696 -verify 10 -showcerts -
cert sn111111_4096.pem –CAfile AcmeIT.cer
openssl s_client -tls1 -connect 10.10.10.10:5696 -verify 10 -showcerts -
cert sn111112_4096.pem –CAfile AcmeIT.cer
```

The results at the end of the command should show:

```
Start Time: 1471622451
Timeout   : 7200 (sec)
Verify return code: 0 (ok)
```

# 5 Best practices

The following SED best practices are recommended:

**Volume migration using Copy/Mirror/Migrate to a secure data disk folder:** The Dell Fluid Data™ architecture allows volumes to be moved from one disk folder to another. It is expected that volumes may be moved from a non-secure to a secure data disk folder when attaching SED drives to a system. When completing this, make sure there is enough RAID10 space allocated in Tier 1 space.

**SC Series design guidance with SEDs:** There is no performance difference between non-SEDs and SEDs. When designing an SC Series system, follow standard design guidance.

**Using cryptographic erase (CE):** There is no CE button in the system. In the necessary situation, such as marking a drive as failed or repurposing a drive into a new array, the controller firmware will perform a CE as part of the process when unmanaging out of a secure data folder. During a Crypto-Erase the Media Encryption Key is changed.

**Mixing drive types in the same disk folder**: SED and non-SED drives can be used in the same array. In order to securely lock and manage the SED drives for DAR protection, the SED drives will be managed in their own disk folder.

# A Frequently asked questions

**What is the difference between a locked drive and a securely-erased drive**?

Data that is locked is inaccessible without the authority credential. Data that is securely erased has been cryptographically destroyed.

**What if the entire array is stolen?**

The data will be protected as long as the thieves are not able to steal and access the KMS and compromise the ACs to unlock all of the SED drives in the array.

**Is it safe to discard or return a locked SED?**

Yes. Any data that was written to the drive will be locked and inaccessible. When you return a drive to Dell, the only information that remains readable are its operating statistics (S.M.A.R.T. data), the RAID type that the drive was used in, and drive hardware error logs.

**Can I turn on encryption at a later date?**

Dell Enterprise Plus SED HDD & SSD's are always encrypting. By using the Secure Data license and a Key Management Server you enable the ability for the drives to be unlocked using an Authority Credential. Without the Secure Data license and the Key Management Server they operate like non-SED drives and provide no additional benefits.

# B Security KMS support

Table 5 provides KMS detailed support information. For the latest information on supported KMS products, refer to the *Dell Storage Compatibility Matrix*.

Table 5 KMS support

| Vendor | KMS solution | KMS version | SCOS version |
|---|---|---|---|
| Gemalto | SafeNet KeySecure k150 | 6.6.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | | 8.1.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | SafeNet KeySecure k150v | 8.0.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | | 8.1.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | SafeNet KeySecure k250 | 6.6.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | | 8.1.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | SafeNet KeySecure k460 | 6.6.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| | | 8.1.x | 6.5.x, 6.6.x, 6.7.x, 7.1.x |
| Thales | EMS 200 | 4.0.2 | 6.5.x, 6.6.x, 6.7.x, 7.1.x, 7.2.x |

# C Glossary

**256-bit Advanced Encryption Standard (AES) encryption**: AES is a specification established by the U.S. National Standards of Institute and Technology (NIST).

**Authority credential (AC)**: Sometimes referred to as the locking key, credentials, authentication keys or access key (AK). It is used to unlock and configure the SED. There is one AC for each SED. See Table 6 for a comparison of media encryption key and AC.

**Cryptographic erase (CE)**: This feature permanently changes the media encryption key so the drive can be reused or repurposed. After the CE is performed, the data previously written to the drive becomes unreadable. CE is also known as secure erase or crypto-erase.

**Data at rest (DAR) encryption**: Protection of data written on the storage media using symmetric encryption/decryption keys.

**Data in motion**: Data in transit between two nodes. This is also known as data in flight.

**Data in use**: Data being used by a person, an application, or an operating system.

**Disk folder**: A logical pool of storage disks with multiple disk drives, RAID levels, and volumes managed with a virtualization layer for application and user efficiencies.

**FIPS 140-2 Level 2**: Provides certification for the cryptographic module and tamper-evident labels/seals around the drive to show physical access to the inside.

**Key management server (KMS)**: An external appliance that manages (stores and serves up) authority credentials to lock/unlock SEDs.

**Key Management Interoperability Protocol (KMIP) v1.0**: The standards-based protocol used to communicate between a KMS and a storage device.

**Locked drive**: An SED in which security has been enabled and the drive has been unexpectedly removed from the storage array, or powered down. Data on the drive cannot be read from or written to until the appropriate AC is provided.

**Media encryption key (MEK)**: Functions as a secret password so that the encryption/decryption engine built into the drive will know how to decrypt the user data stored on the physical media. Generated in the drive factory, the MEK is encrypted and embedded within the drive and is never exposed outside the drive. See Table 6 for a comparison of MEK and authority credential.

**Re-purpose**: Changes the drive from a secured state to an unsecured state so that it can be safely used for another purpose. This task is accomplished using the CE feature.

**RevertSP function**: Reverts the drive to factory default condition.

**Self-encrypting drive (SED)**: A drive with a dedicated ASICs encryption engine built in to encrypt/decrypt all data to the media transparently, without user intervention.

**Secure Data**: The Dell term for the DAR encryption solution in Dell and Dell EMC arrays.

**TCG**: Trusted Computing Group.

**Unlocked**: Data on a drive is accessible for all read and write operations.

Table 6 Comparison of MEK and AC

| Term | Definition and usage | Location and management | How is it generated |
|---|---|---|---|
| Media encryption key (MEK) | Required to encrypt and decrypt data | Resides and managed by the drives<br><br>Never leaves the drives<br><br>Unique MEK for every drive | Generated by the drive at the manufacturer |
| Authority credential (AC) | Needed to unlock a drive | Managed by the SC Series firmware and stored on KMS | Created by a random number generator in the drive |

# D Additional resources

## D.1 Technical support

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell software, hardware and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC storage platforms.

## D.2 Referenced or recommended documentation

Referenced or recommended publications and resources:

- *Best Practices for Securing Dell Storage Center*
- *Guidelines for Media Sanitation*
- *Best Practices for Key Management for Secure Storage*
- SNIA Guidance and Best Practices

Brocade offers in-flight encryption available in the Brocade 6510, Brocade 6520 and Brocade DCX-8510. Using this feature will provide additional security for frames between switches.

The following resources describe two options for host-based transparent file-system level encryption for DAS, SAN and NAS for additional protection and security.

- SafeNet ProtectFile
- Vormetric Transparent Encryption