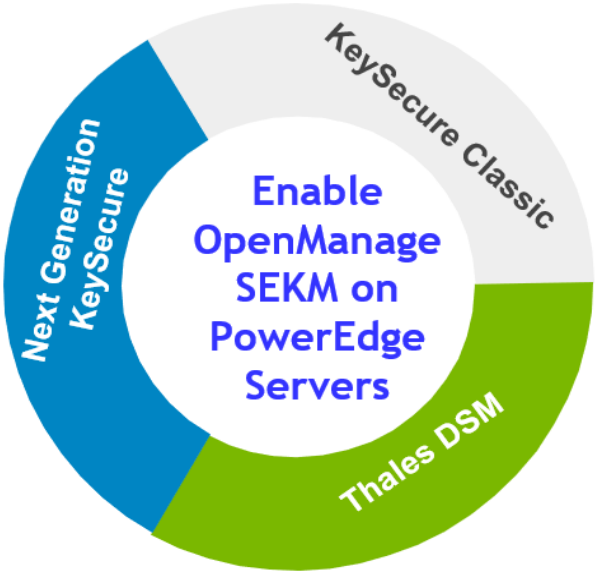
DELL Technologies

Configuration and Deployment Guide

# Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

This Dell EMC Configuration and Deployment Guide describes the process of enabling the SEKM feature on PowerEdge servers. Key tips and troubleshooting techniques for using SEKM are also discussed.





## Abstract

Keeping your business-critical operations and IT infrastructure safe and secure is key to providing seamless services. Dell EMC provides the OpenManage Secure Enterprise Key Manager (SEKM) that assists iDRAC (the Dell EMC PowerEdge server BMC) in locking and unlocking storage devices on a PowerEdge server. This Configuration and Deployment Guide provides step-by-step procedure to set up SKEM on KeySecure Classic, Vormetric Data Security Manager, Next Generation Key Manager (branded as CipherTrust Manager at the time of release of this guide, but change will not show in a shipping product until Sept 2020), iDRAC, and PERC. Also, a few important tips and troubleshooting steps are provided to help you effectively use this SEKM on your PowerEdge servers.


October 2021

# Revisions

| Date | Description |
|---|---|
| July 2019 | Initial release |
| June 25, 2020 | Added procedures related to KeySecure Classic, Thales Data Security Manager (DSM), and CipherTrust Manager (previously branded as Next Generation KeySecure) |
| September 2020 | Added extra information about including IP information during setup and configuration |

# Acknowledgements

This Configuration and Deployment Guide was produced by the following members of the Dell EMC Enterprise Server Solutions team:

Author—Sanjeev Dambal, Texas Romer, Xavier Conley, and Craig Phelps

# Contents

# Executive summary

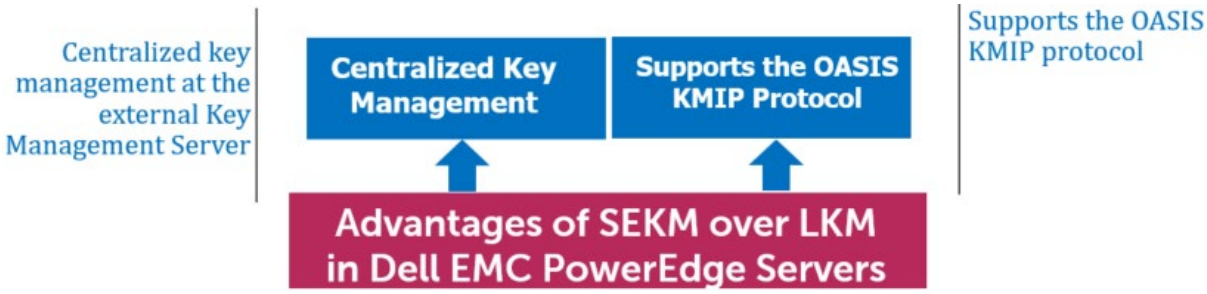



Figure 1 Advantages of SEKM over LKM in Dell EMC PowerEdge servers

The OpenManage SEKM enables you to use an external Key Management Server (KMS) to manage keys that can then be used by iDRAC to lock and unlock storage devices on a Dell EMC PowerEdge server. iDRAC requests the KMS to create a key for each storage controller, and then fetches and provides that key to the storage controller on every host boot so that the storage controller can then unlock the SEDs.

The advantages of using SEKM over Local Key Management (LKM) are:

- In addition to the LKM–supported “Theft of an SED” use case, SEKM protects from a “Theft of a server” use case. Because the keys used to lock and unlock the SEDs are not stored on the server, attackers cannot access data even if they steal a server.
- Centralized key management at the external Key Management Server.
- SEKM supports the industry standard OASIS KMIP protocol thus enabling use of any external third party KMIP server.

# 1 KeySecure Classic (k150v)

## 1.1 Prerequisites for KeySecure Classic

Before you start setting up iDRAC SEKM support, you must first ensure that the following prerequisites are fulfilled. Else, you cannot successfully set up SEKM.

**PowerEdge Server Prerequisites**

- iDRAC SEKM license installed
- iDRAC Enterprise license
- iDRAC updated to the firmware version which supports SEKM
- Supported storage devices updated to the firmware version which supports SEKM

**Key Management Server (KMS) Prerequisites**

- Set up a valid CA to sign iDRAC CSR
- A user account that represents the iDRAC on the KMS (For Gemalto, this means having the associated connector license)
- Authentication settings on the KMIP Service of the KMS

## 1.2 Set up SEKM on KeySecure Classic

This section describes the Gemalto KeySecure features that are supported by iDRAC. For information about all other KeySecure features, see the *KeySecure Appliance Administration Guide* available on the Gemalto support site: https://support.thalesgroup.com.

**SSL Certificate**

When creating an SSL certificate request, you must include the IP address of the key management server in the Subject Alternative name field.

The IP address must be given in the format listed below:

IP:xxx.xxx.xxx.xxx

**Users and groups**

It is recommended that you create a separate user account for each iDRAC on the KMS. This enables you to protect the keys created by an iDRAC from being accessed by another iDRAC. If the keys require to be shared between iDRACs then it is recommended to create a group and add all iDRAC usernames that must share keys to that group.

**Authentication**
The authentication options supported by the KeySecure KMS are as shown in the sample screen shot:


Figure 2 Authentication settings on Gemalto

**Password authentication**
It is recommended that you set this setting to “Required (most secure)”. When set to this option, the password for the user account that represents the iDRAC on the KMS must be provided to iDRAC as explained later in Set up SEKM on iDRAC.

**Client certificate authentication**
It is recommended that you set to “Used for SSL session and username (most secure)”. When set to this option, the SSL certificates must be set up on iDRAC as explained later in Set up SEKM on iDRAC.

**The Username field in client certificate**
It is recommended to set this option to one of the iDRAC supported values:

- CN (Common Name)
- UID (User ID)
- OU (Organizational Unit)

When set to one of these values, the iDRAC username on the KMS must be set up on the iDRAC as explained later in Set up SEKM on iDRAC.

**Require client certificate to contain source IP**

Set up SEKM on iDRAC.

## 1.3 Set up SEKM on iDRAC

**Licensing and firmware update**
SEKM is a licensed feature with the iDRAC Enterprise license as a pre-requisite. To avoid an additional iDRAC firmware update, it is recommended that the SEKM license is installed first and then the iDRAC firmware updated to a version that supports SEKM. This is because an iDRAC firmware update is always required after the SEKM license is installed irrespective of whether the existing firmware version supports SEKM or not. The existing interface methods for installing license and firmware update can be used for SEKM.

**Set up SSL certificate**
The SEKM solution mandates two-way authentication between the iDRAC and the KMS. iDRAC authentication requires generating a CSR on the iDRAC and then getting it signed by a CA on the KMS and

uploading the signed certificate to iDRAC. For KMS authentication, the KMS CA certificate must be uploaded to iDRAC.

**Generate iDRAC CSR**
Though most of the CSR properties are standard and self-explanatory, here are a few important guidelines:

- If the “Username Field in Client Certificate” option on the KMS is enabled then ensure that the iDRAC account user name on the KMS is entered in the correct field (CN or OU or KMS User ID) that matches the value selected in the KMS.
- If the **Require Client Certificate to Contain Source IP** field is enabled on the KMS then enable the “iDRAC IP Address in CSR” field during the CSR generation.

## 1.4 Configure SEKM by using the iDRAC GUI

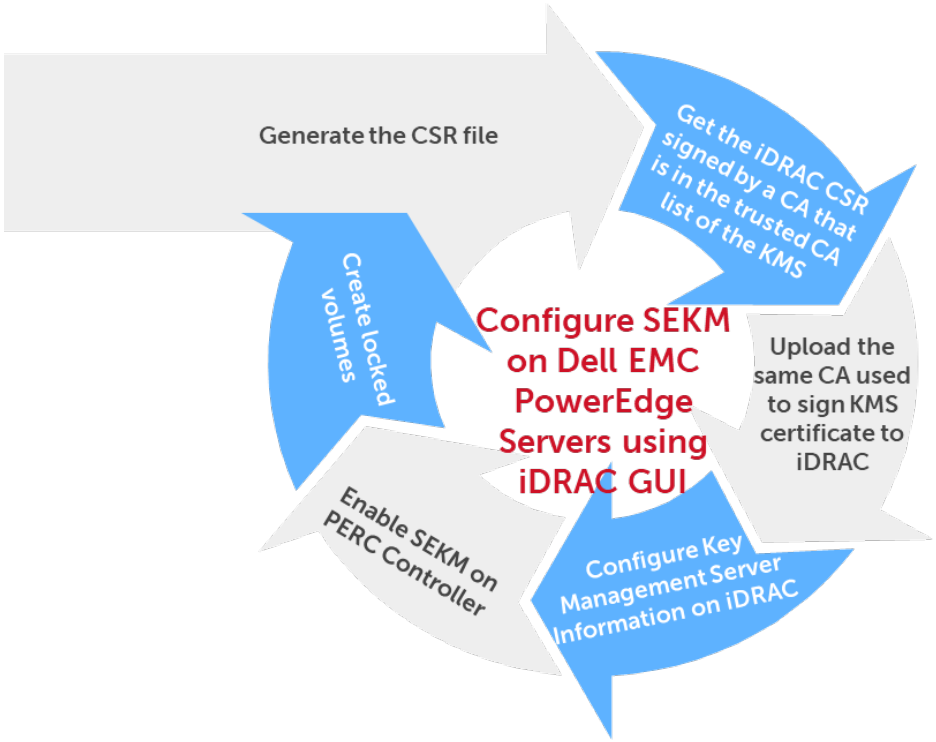



Figure 3 Key processes in configuring SEKM on PowerEdge servers by using iDRAC GUI

For the Key Management Server, this workflow will be using Gemalto KeySecure as the Key Management Server.

1. Start iDRAC by using any supported browser.
2. Click **iDRAC Settings** → **Services**.

3. Expand the **SEKM Configuration** menu and click **Generate CSR**.


Figure 4 Generate CSR by using the iDRAC GUI

4. In the **Generate Certificate Signing Request (CSR)** dialog box, select or enter data.
5. Click **Generate**.
   The CSR file is generated.
6. Save it to your system.

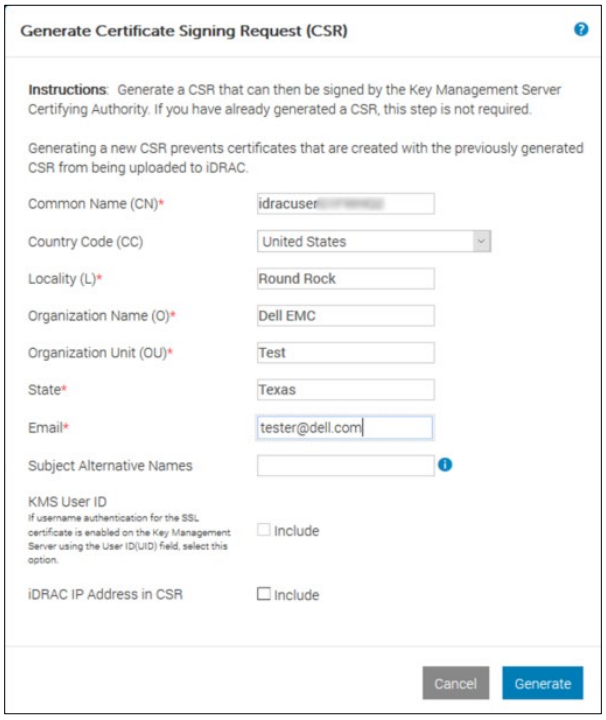



Figure 5 Enter or select data in the CSR dialog box of iDRAC

7. Get the full CSR file contents signed on Gemalto. See Get the CSR file signed on Gemalto.
8. Download the signed image file, and then upload it to iDRAC.

### 1.4.1 Get the CSR file signed on KeySecure Classic

-----BEGIN CERTIFICATE REQUEST-----

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV
i/OyLyeJ7l1SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB2l6UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=

-----END CERTIFICATE REQUEST-----

1. Log in to Gemalto.
2. Click **Security Tab → Local CAs**.
3. Click **Sign Request**.

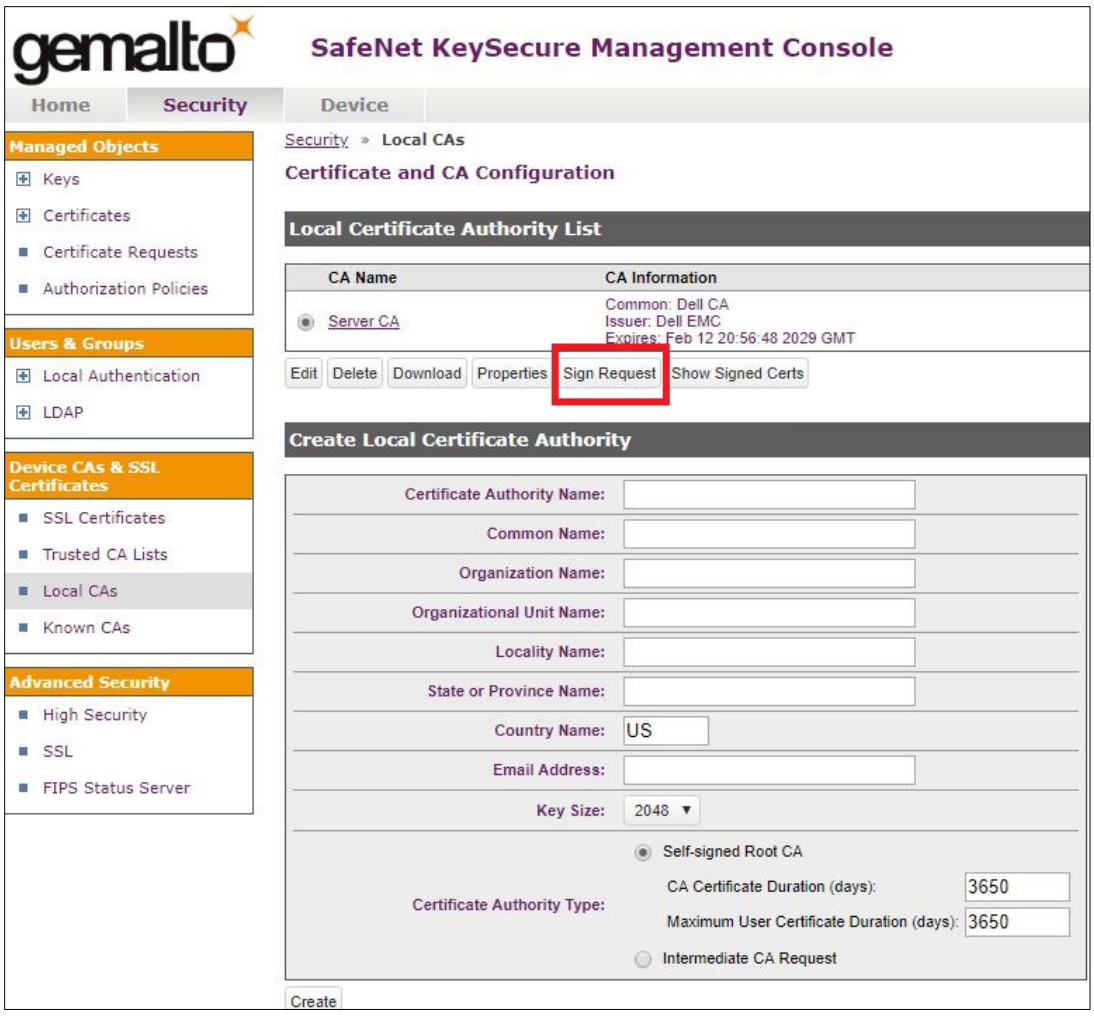



Figure 6 Enter or select data in the Select Request section of Gemalto

4. Select **Client** as the purpose of generating the certificate.
5. Paste the complete CSR content in the **Certificate Request** box.
6. Click **Sign Request**.

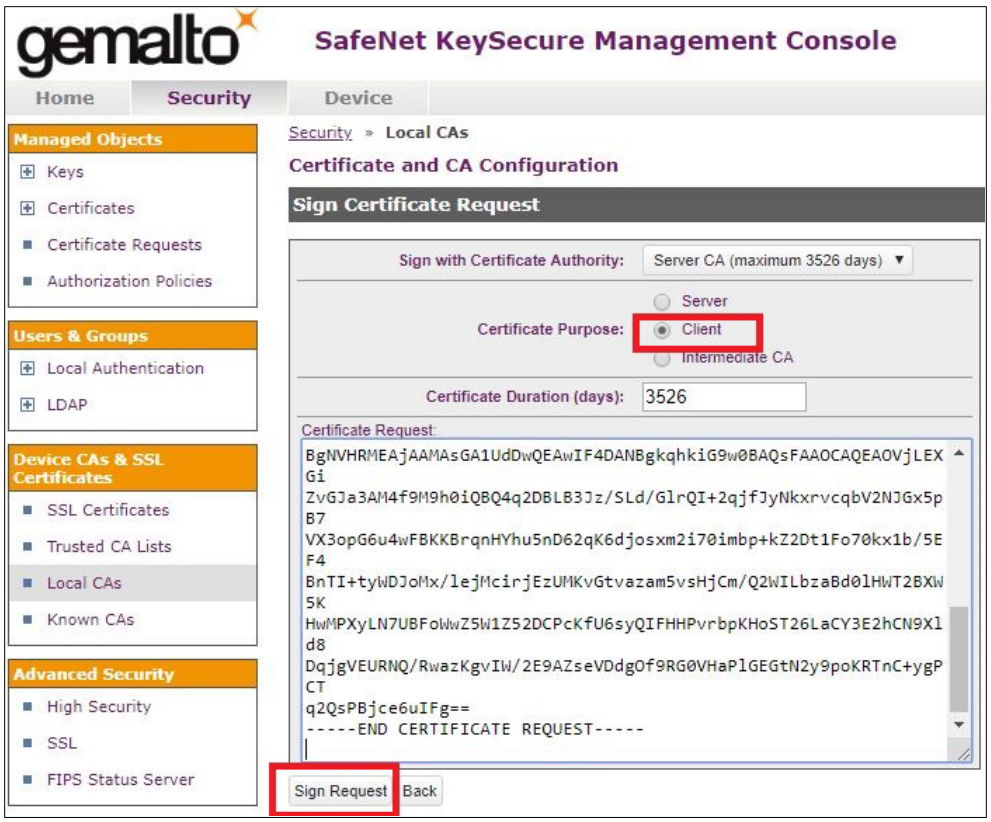



Figure 7 Request for certificate signing on Gemalto

7. After the request is signed, click **Download**, to save the signed CSR file to your system.

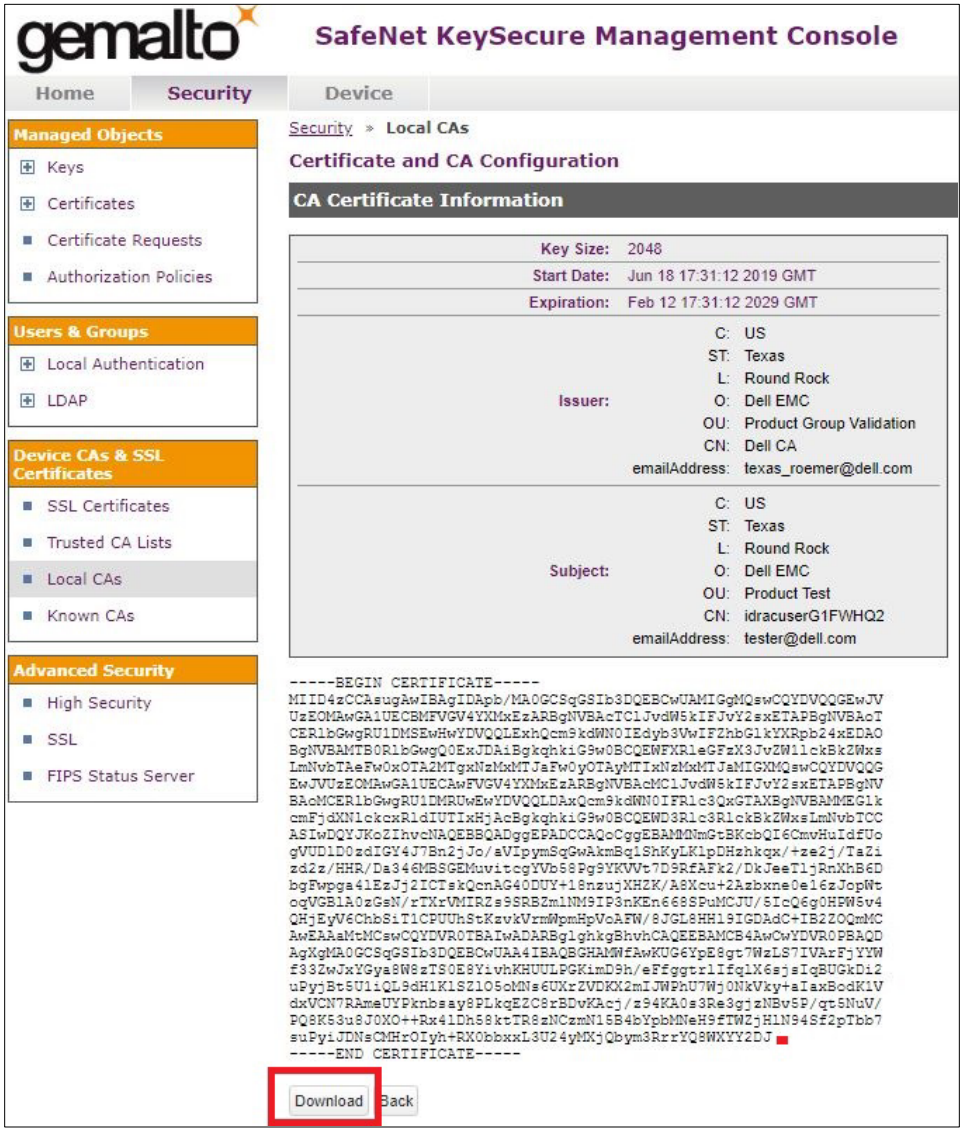



Figure 8 Download and save the CSR file on Gemalto

8. To upload the file that you just got signed on Gemalto, access the iDRAC GUI, go to the **SEKM Certificate** page, and click **Upload Signed CSR**.

   A message is displayed to indicate the successful upload.

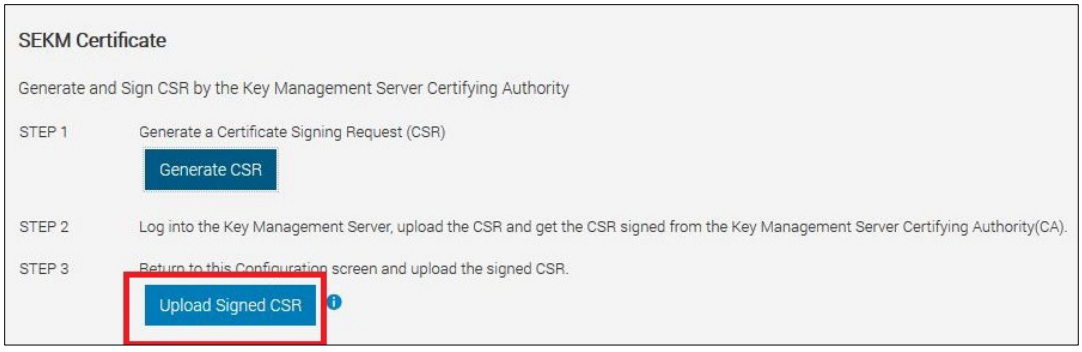



Figure 9 Upload the signed CSR certificate by using iDRAC GUI

## 1.4.2 Download the server CA file from KeySecure Classic and upload to iDRAC

1. On the Gemalto GUI, click **Security Tab → Local CA**.
2. Select the Server CA you are using and click **Download**.

   The file is saved to your local system.

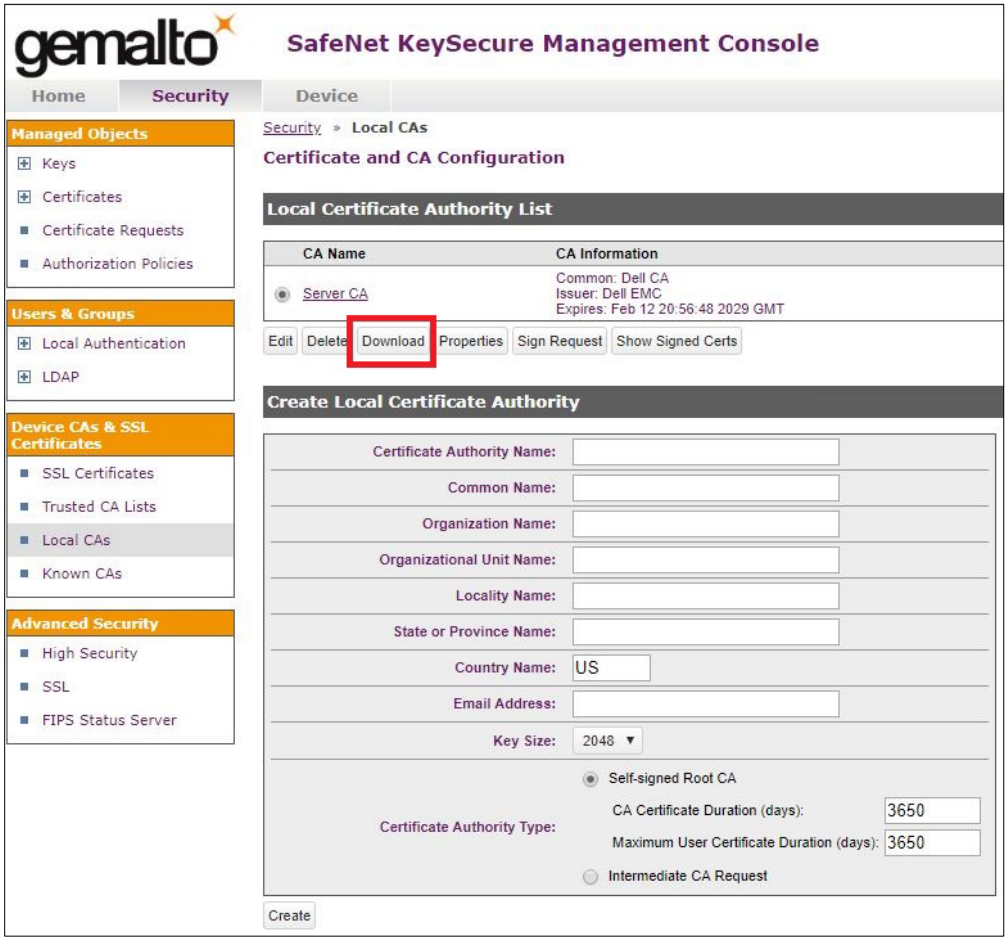



Figure 10 Download the server CA file from Gemalto

3. On the iDRAC GUI, in the **KMS CA Certificate** section, click **Upload KMS CA Certificate**.
4. Upload the Server CA you just downloaded from Gemalto.

   A message is displayed to indicate the successful upload.

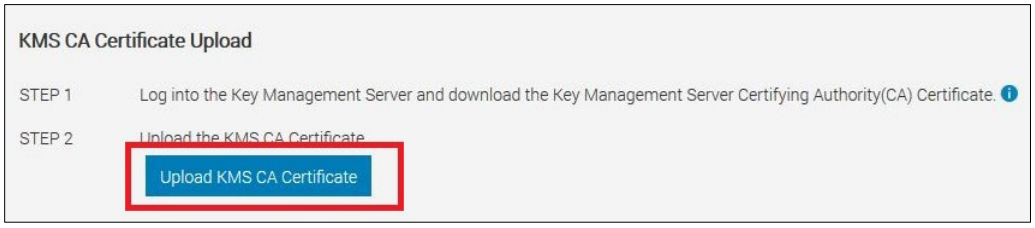



Figure 11 Upload the CA certificate to iDRAC

### 1.4.3 Configure the Key Management Server (KMS) settings on iDRAC

1. Enter or select data in the fields, and then click **Apply**.

IMPORTANT—Make sure you already have a user created on the KMS you will be using for key exchange with the iDRAC. For the user name, ensure it matches the exact value in the CSR certificate property you selected for the Gemalto KMIP **Username field in client certificate** Authentication Settings

For example, in the signed CSR Certificate on iDRAC used in this experiment, the Common Name property is set to “idracuserG1FWHQ2”. On the Gemalto server, in the KMIP Authentication Settings, the “Username field in client certificate” field is set to “Common Name”. For creating a username on Gemalto, you must create a user with the name “idracuserG1FWHQ2”. This is the user which iDRAC will be using for key exchange.

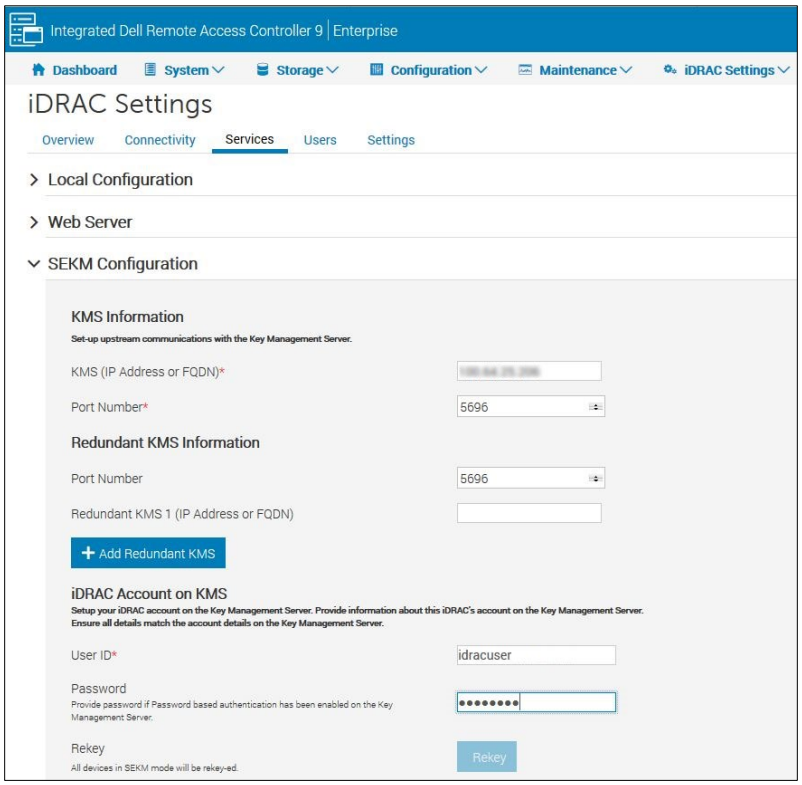



Figure 12 Configure the KMS properties on iDRAC GUI

A message is displayed indicating that a job ID has been created.

2. Go to the **Job Queue** page and ensure that the job ID is marked as successfully completed.

3. If you see any job status failures, view Lifecycle Logs for more information about the failure.

iDRAC SEKM configuration is now complete.

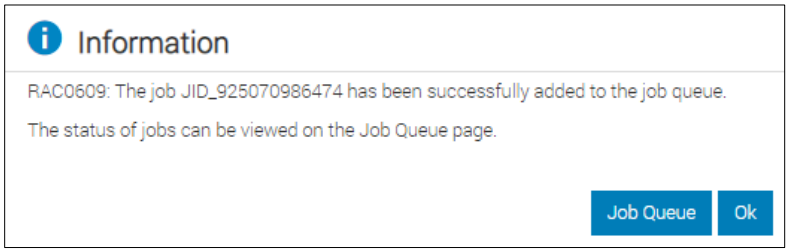



Figure 13 A job is created on iDRAC for configuring KMS on iDRAC

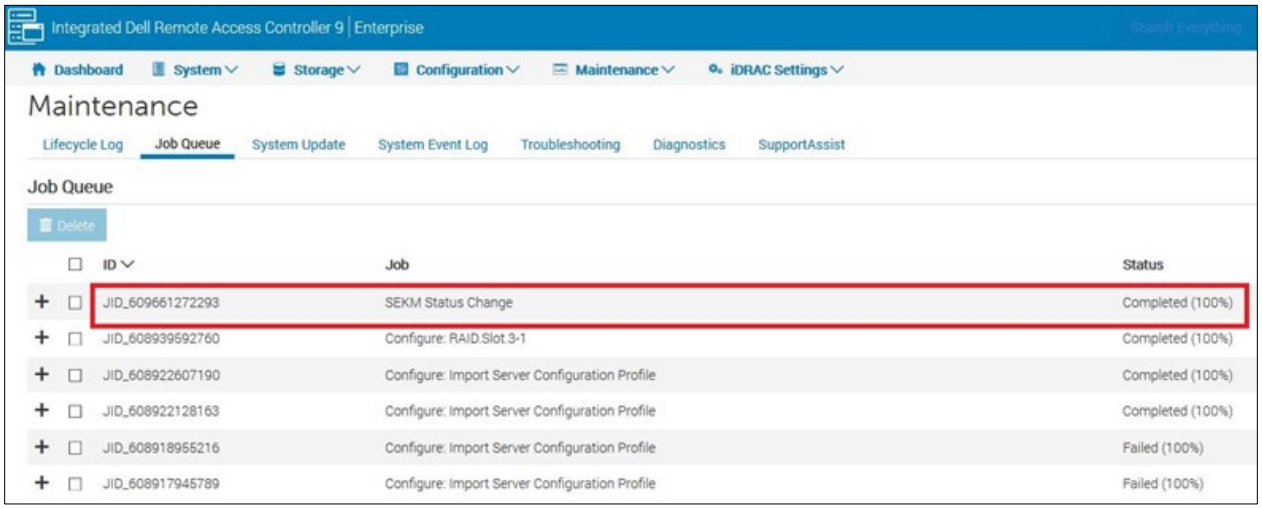



Figure 14 iDRAC SEKM is successfully configured

# 2 Enable SEKM by using the iDRAC PERC

1. On the iDRAC GUI, click **Configuration** → **Storage Configuration**.
2. Select your storage controller.
3. Expand **Controller Configuration**.
4. From the **Security (Encryption)** down-down menu, select **Secure Enterprise Key Manager**.
5. Click **Add to Pending Operations**.

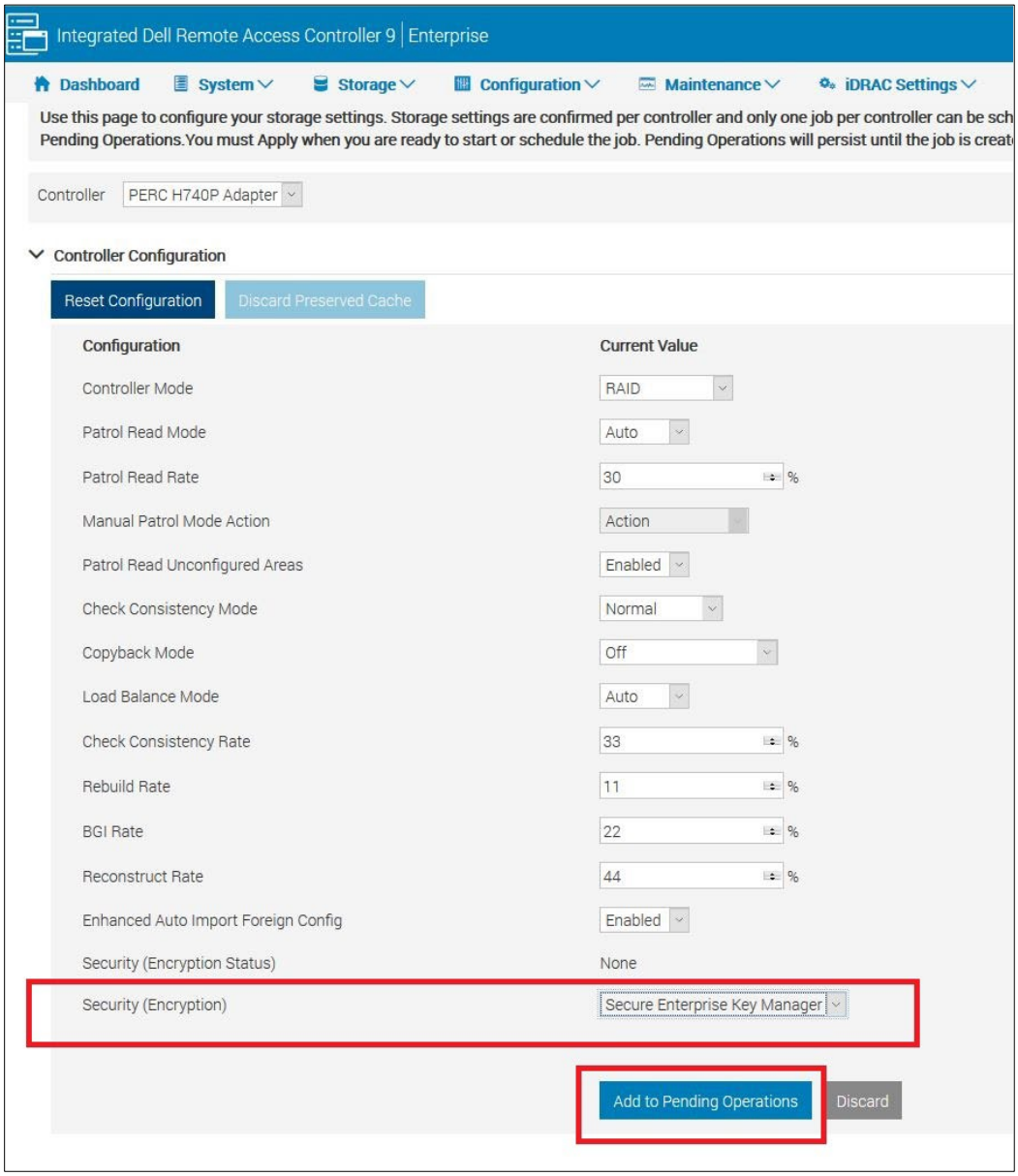



Figure 15 Enable SEKM on iDRAC PERC

6. Select **At Next Reboot**.

   A message is displayed indicating that the job ID is created.
7. Go to the **Job Queue** page and ensure that this job ID is marked as **Scheduled**.

8. Restart the server to run the configuration job.

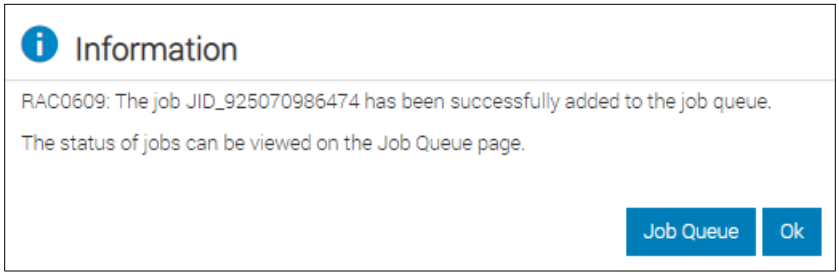



Figure 16 A job is created to enable SEKM on IDRAC PERC

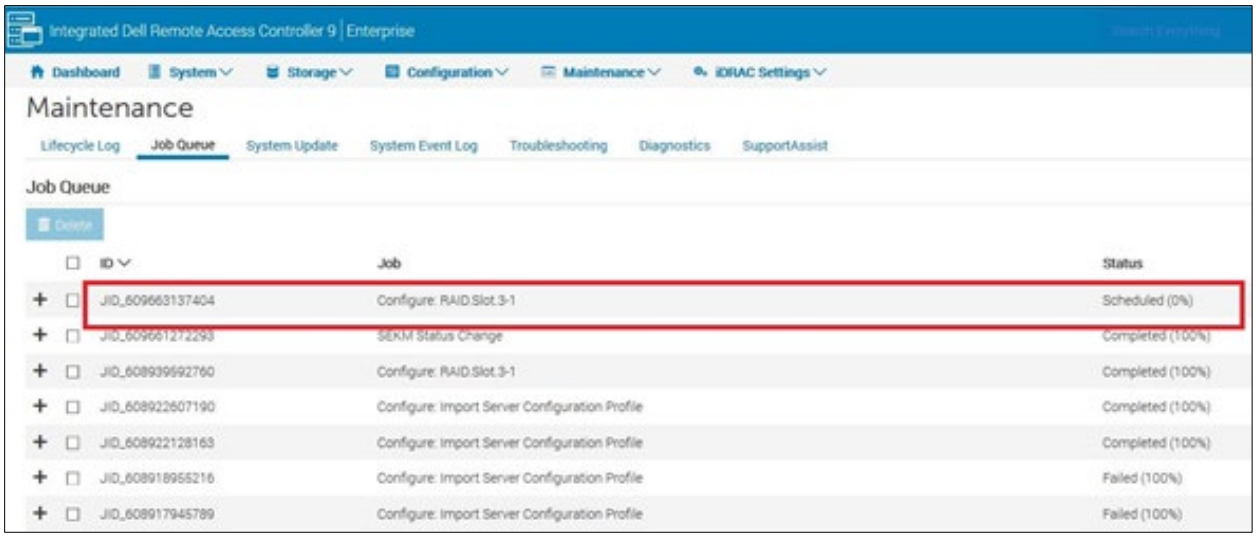



Figure 17 A job is scheduled to enable SEKM on iDRAC PERC

After restarting the server, the configuration job is run in the Automated Task Application to enable SEKM on the PERC. The server is automatically restarted.

9. After the POST or Collecting Inventory operation is completed, ensure that the job ID has been marked as “Completed” on the Job Queue page.

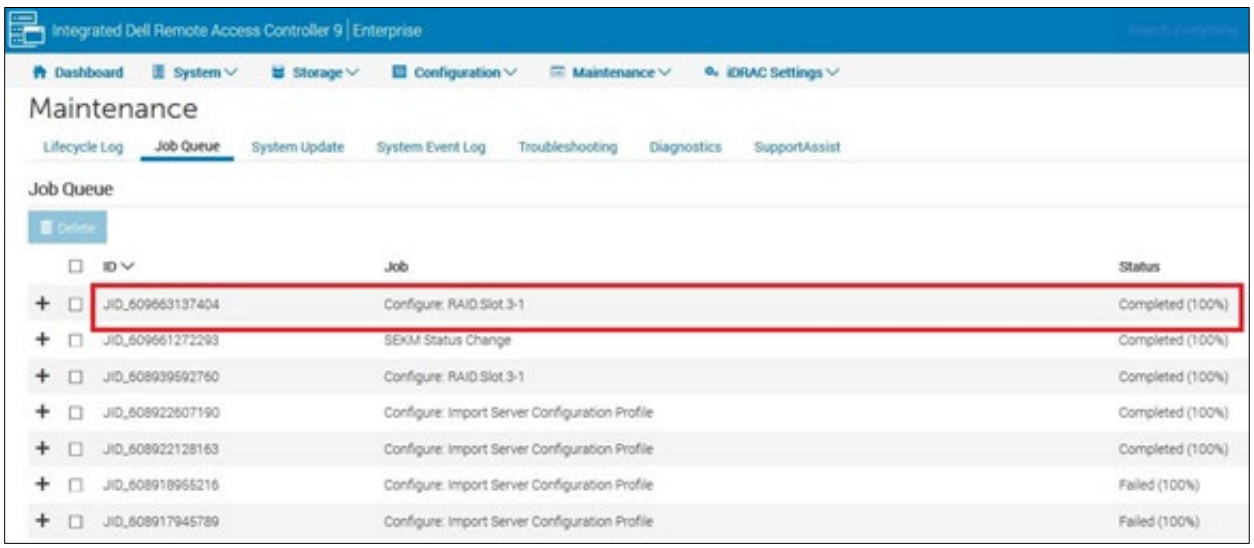



Figure 18 A job successfully run to enable SEKM on iDRAC PERC

## 2.1 Ensure that SEKM is enabled on iDRAC PERC

1. On the iDRAC GUI, click **Storage** → **Overview**.
2. Expand your storage controller and ensure the following statuses:
   - **Security Status** = Security Key Assigned
   - **Encryption Mode** = Secure Enterprise Key Manager

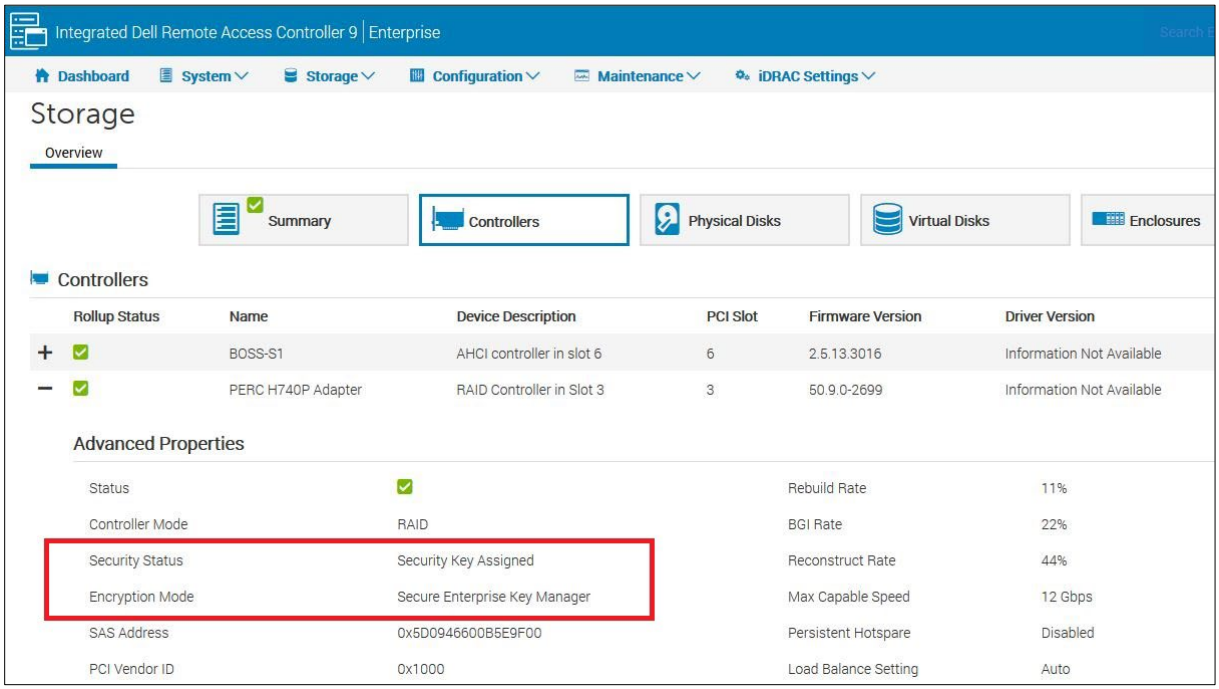



Figure 19 Ensure that SEKM is enabled on your controller

# 3 Thales Data Security Manager (DSM)

## 3.1 Prerequisites for Thales Data Security Manager (DSM)

Before you start setting up iDRAC SEKM support, you must first ensure that the following prerequisites are fulfilled. If these prerequisites are not fulfilled, you will not be able to successfully set up SEKM.

**PowerEdge Server Prerequisites**

- iDRAC SEKM license installed
- iDRAC Data Center or Enterprise license
- iDRAC updated to the firmware version which supports SEKM
- Supported storage devices updated to the firmware version which supports SEKM

**Thales Vormetric DSM Prerequisites**

- Set up a valid external certificate authority to sign the iDRAC CSR.
- Create a host that represents the iDRAC on the KMS.
- Ensure a KMIP—enabled license is applied to the DSM. If applying a new KMIP enabled license to an existing DSM for the first time, restart the DSM after applying the license.

## 3.2 Set up SEKM on Thales DSM

This section describes the Thales Vormetric Data Security Manager features that are supported by iDRAC. For information about all other Thales features, see the *Thales Appliance Administration Guide*.

### 3.2.1 Add a new host in Thales Vormetric Data Security Manager

1. Log in to Thales as an administrator.
2. Switch to the domain where the keys will be managed. Click **Domains** → **Switch Domains** → Select desired Domain → **Switch to Domain**.

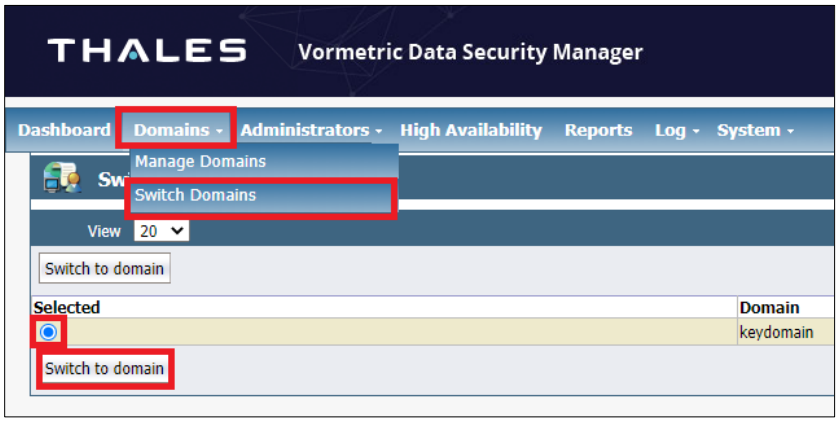



Figure 20 Switch to Domain where keys will be managed

3. To add a new host, click **Hosts → Hosts → Add**.

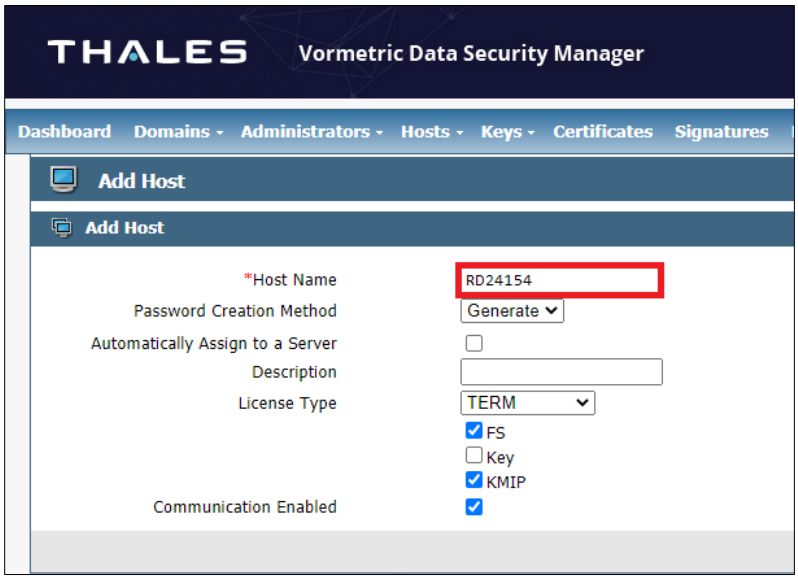



Figure 21 Adding a new host in Thales Vormetric Data Security Manager

Note—The host name must match the Common Name (CN) in the iDRAC SSL certificate, otherwise certificate import will fail. In the example shown above, the system service tag is used as the host name.

## 3.2.2 Set up SEKM on iDRAC

See Set up SEKM on iDRAC.

## 3.2.3 Configure SEKM by using the iDRAC GUI

See Configure SEKM by using the iDRAC GUI.

Note—For the Key Management Server, this workflow will be using Thales Vormetric Data Security Manager (DSM) as the Key Management Server.

### 3.2.4 Generate a CSR file to be signed by an external certificate authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KKKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV
i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y
kjw+SxEOs6JnYpI9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=
-----END CERTIFICATE REQUEST-----
```

Figure 22 CSR signed by external certificate authority

Note—The Microsoft CA below was specifically configured for our testing purposes. Your external certificate authority may vary. It is not required to use a Microsoft CA; just a valid 3rd party certificate signer is sufficient. For more information, see the *Thales Vormetric Administration Guide*.

1. Go to your Certificate Authority and sign the CSR.

   Note—If you are using a Microsoft CA, the template used here to sign the CSR was configured manually and may not be available by default.

2. On the **Certificate Authority** welcome page, select **Request a certificate**.

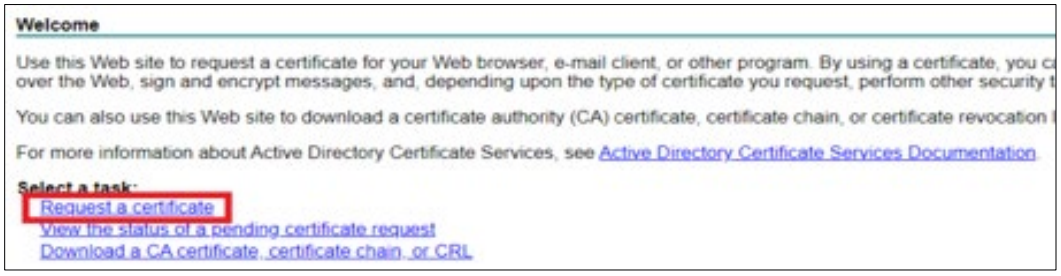



Figure 23 Request for a certificate from your Certificate Authority

3. Select **Advanced certificate request**.
4. Paste the CSR text data in the saved request box.
5. Click **Submit**.
6. After the certificate is issued to you, select **Base 64 encoded**.

7. To save the signed CSR file to your system, click **Download Certificate**.

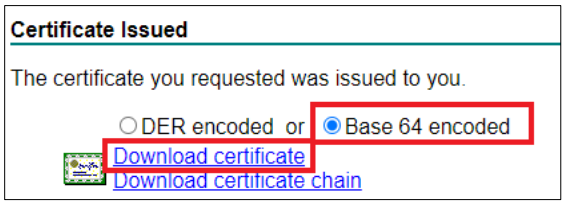



Figure 24 Download certificate

8. On the iDRAC GUI, on the SEKM Certificate page, click **Upload Signed CSR** to upload the file you just got signed by your Certificate Authority. A message is displayed to indicate the successful upload.

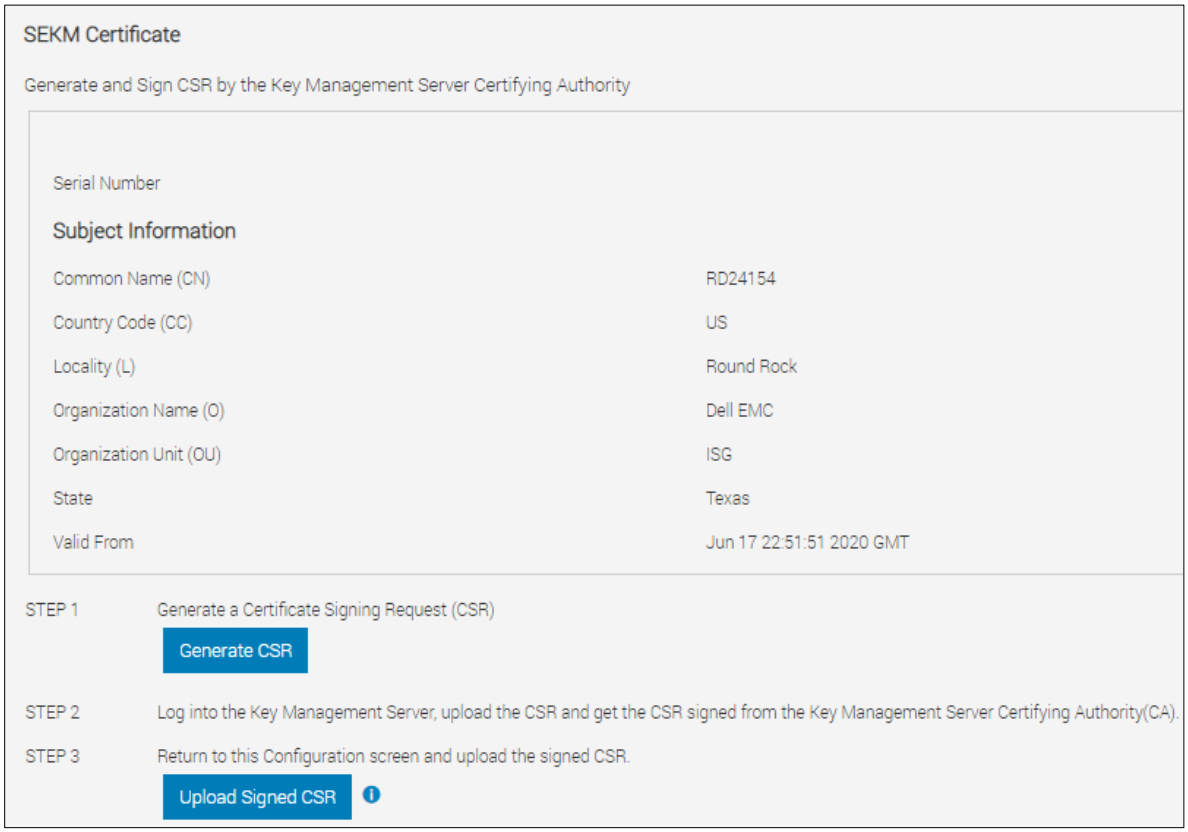



Figure 25 Upload the signed CSR certificate on iDRAC GUI

### 3.2.5 Upload the signed CSR to Thales DSM

1. Select your host.

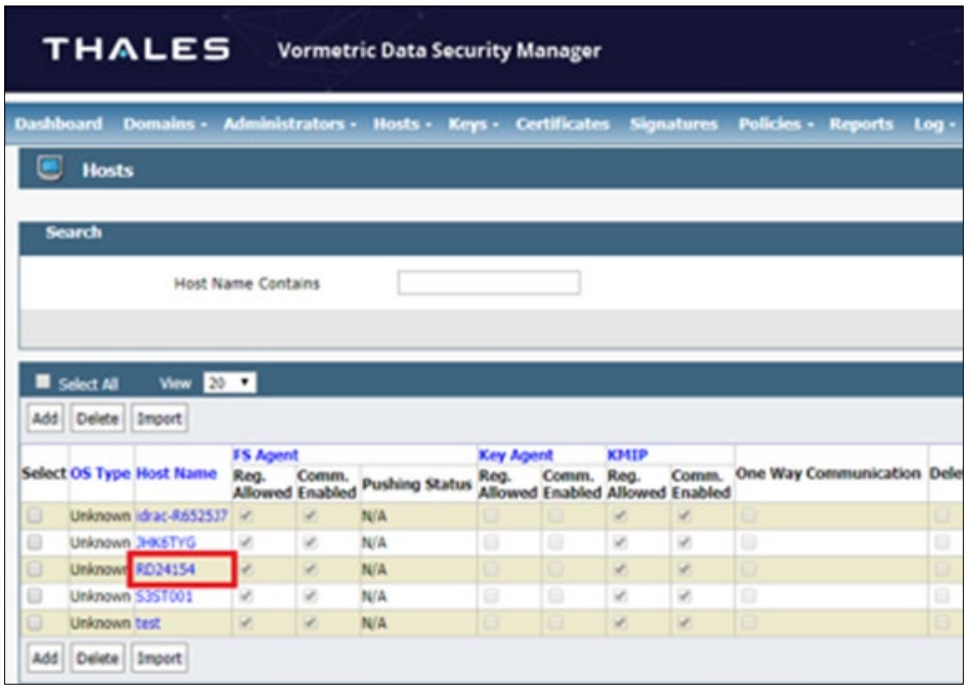



Figure 26 Select your host on Thales Vormetric Data Security Manager

2. Import the KMIP certificate. Import the CSR that was signed by your Certificate Authority.
3. Click **Ok**. After you import the KMIP certificate, a message and the certificate fingerprint are displayed.
4. Click **Apply**.

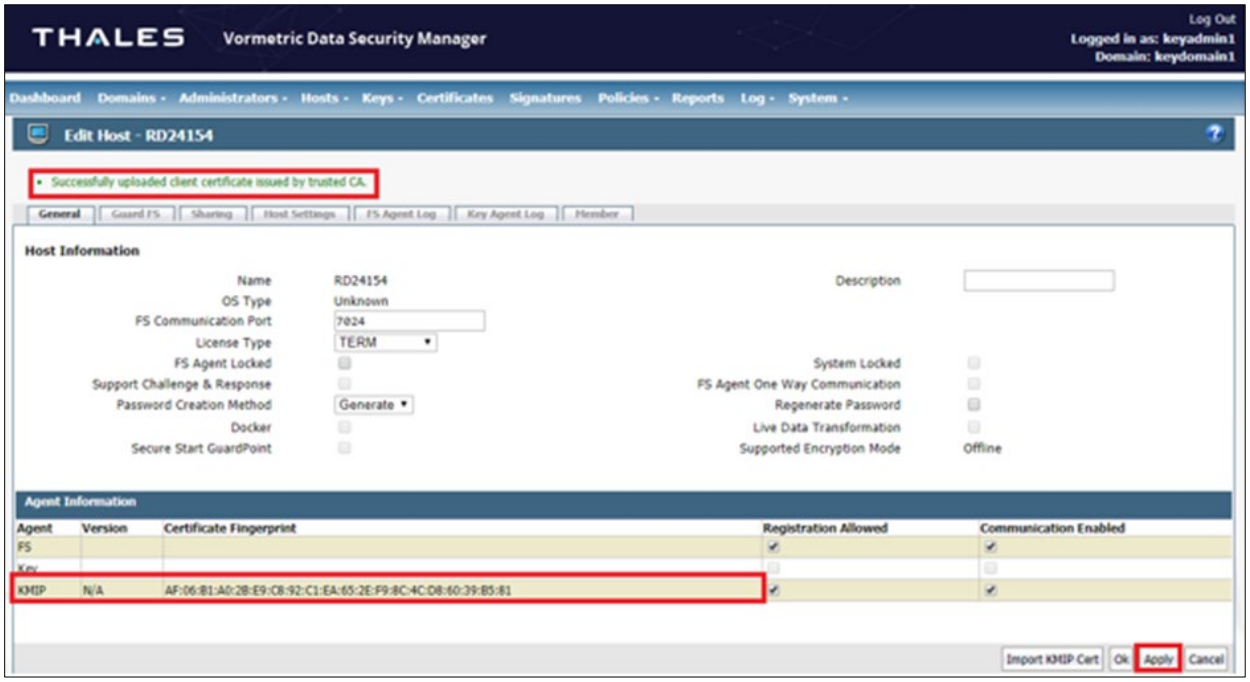



Figure 27 Success message and certificate fingerprint displayed after importing KMIP certificate

### 3.2.6 Download the Root CA that has signed the Thales DSM appliance and upload to iDRAC

1. From the Thales web interface, download the Root CA. Chrome browser is used in this example. Process may vary based on the browser type you use.
2. Click **Not Secure → Certificate (Invalid)**.

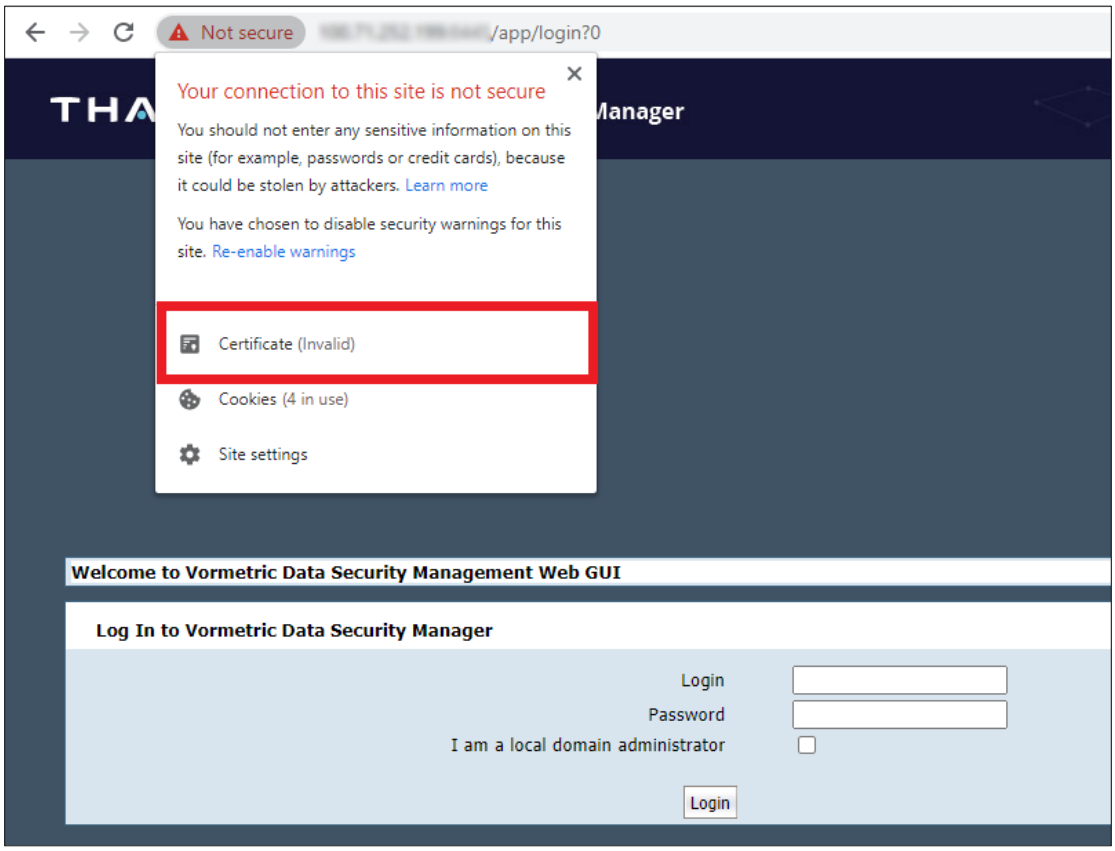



Figure 28 Click Certificate (Invalid)

3. Select **Certification Path → CG CA S on XXX.XXX.XXX.XXX** (this is the Root CA).
4. Click **View Certificate**.

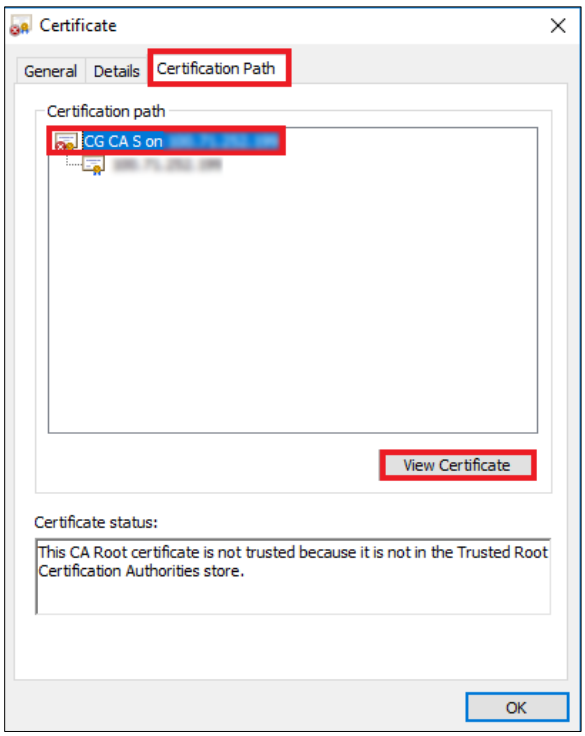



Figure 29 View Root CA

5. Click **Details → Copy to File → Next**.
6. Select **Base-64 encoded X.509 (.CER)**.
7. Click **Next**.
8. Enter a file name the file, click **Save**, and then click **Finish**.

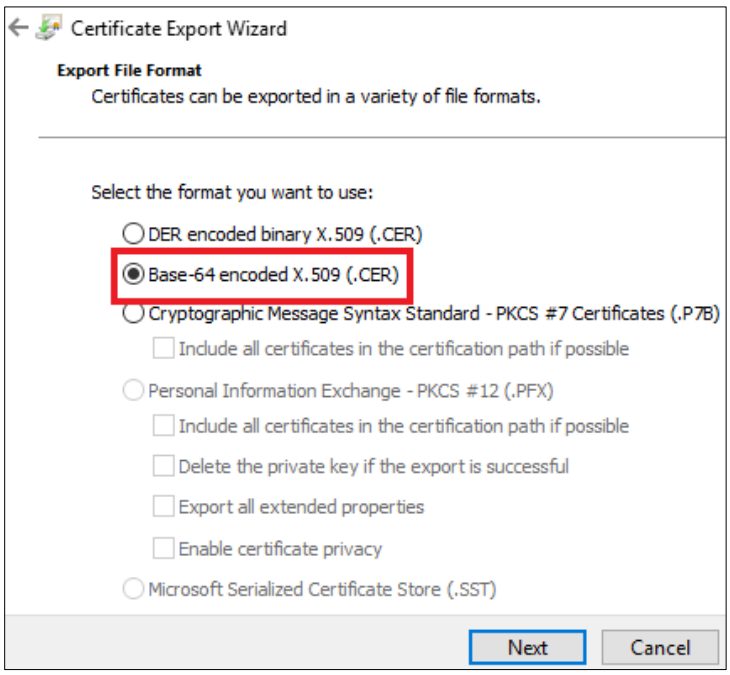



Figure 30 Export Root CA

9. Upload the file you just saved by using it as the KMS CA Certificate on the iDRAC. A message is displayed to indicate the upload was successful.

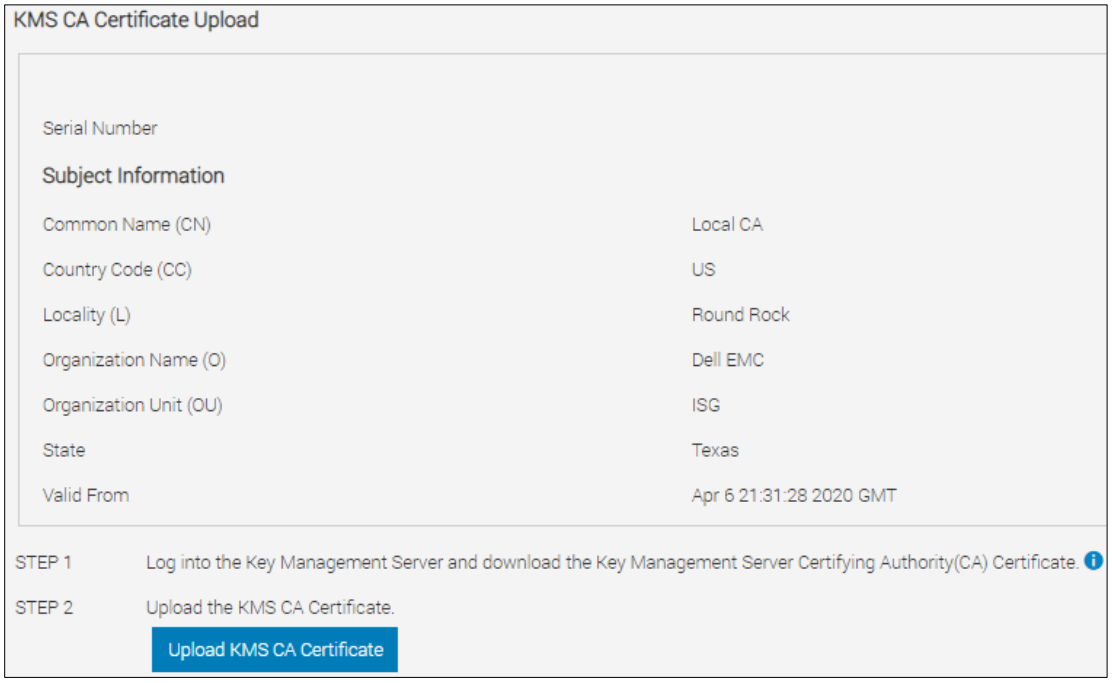



Figure 31 Upload the KMS CA certificate to iDRAC

## 3.3 Configure the Key Management Server (KMS) settings on iDRAC

1. Enter or select data in the fields, and then click **Apply**.


Figure 32 Configure the KMS properties on the iDRAC GUI

Note—User Authentication is not supported on Thales Vormetic Data Security Manager, so the User ID and Password fields on iDRAC GUI are not required.

2. Go to the Job Queue page and ensure that the job ID is marked as successfully completed.
3. If you see any job status failures, view Lifecycle Logs for more information about the failure.

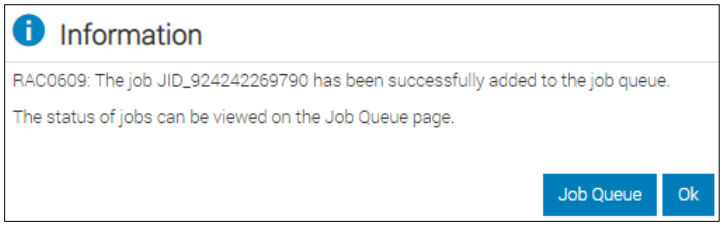



Figure 33 A job is created on iDRAC for configuring KMS on iDRAC

The iDRAC SEKM configuration is now complete.

### 3.3.1 Enable SEKM on the iDRAC PERC

1. On the iDRAC GUI, click **Configuration** → **Storage Configuration**.
2. Select the storage controller.
3. Expand **Controller Configuration**.

5. Click **Add to Pending Operations**.

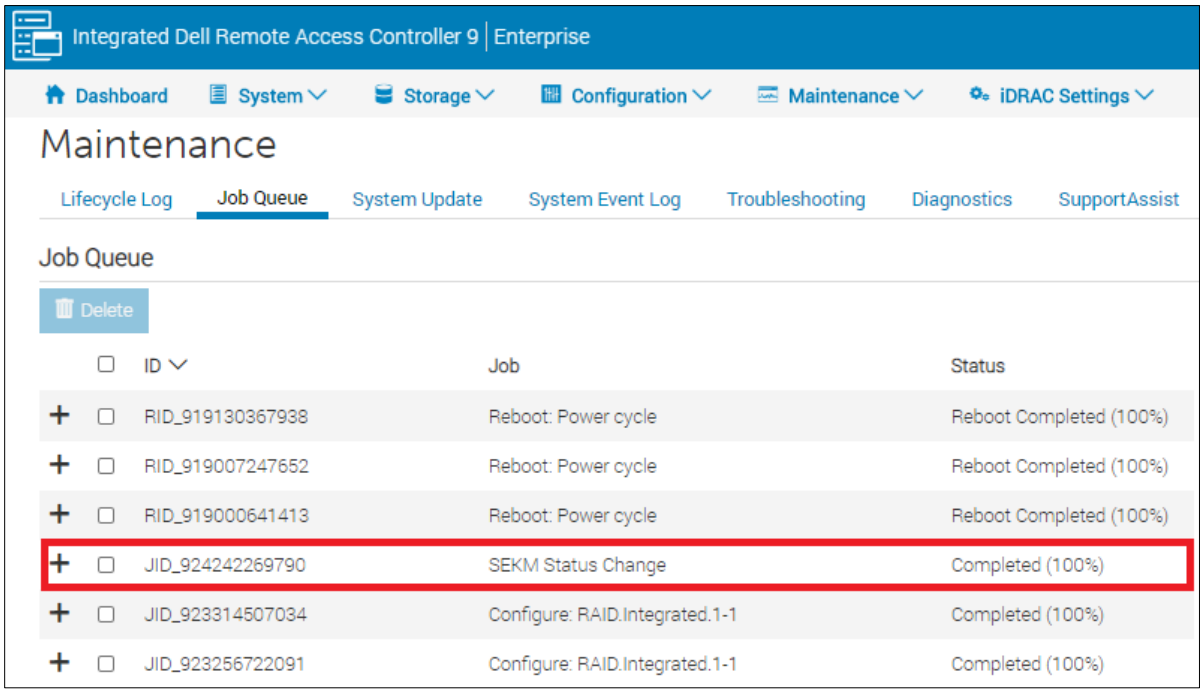



Figure 34 A job to enable SEKM is successfully completed

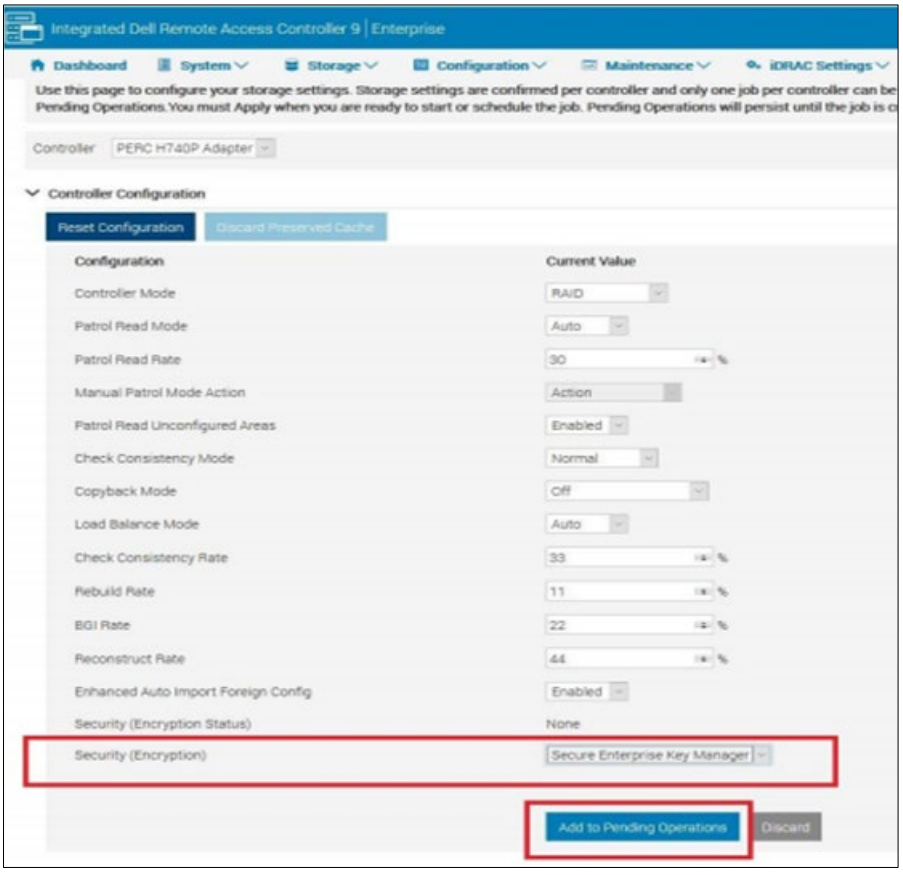



Figure 35 Enable SEKM on iDRAC PERC

6. Select **At Next Reboot**.
   A message is displayed indicating that the job ID is created
7. Go to the Job Queue page and ensure that this job ID is identified as **Scheduled**.
8. Restart the server to run the configuration job.

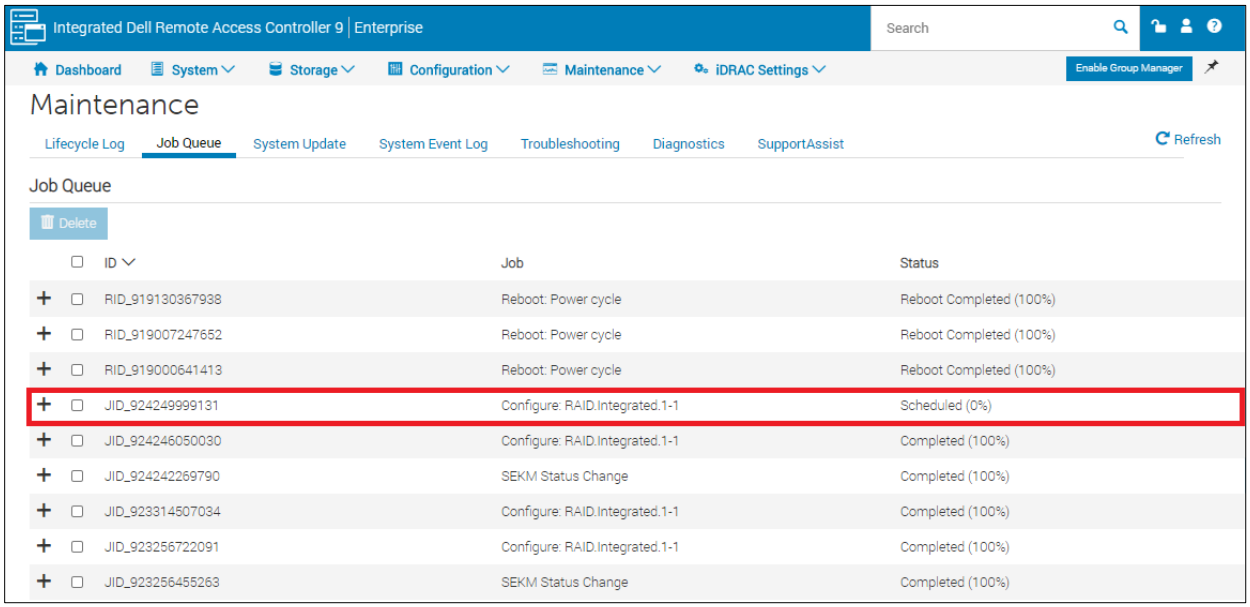



Figure 36 A job is now scheduled to enable SEKM on iDRAC PERC

After restarting the server, the configuration job is run in the Automated Task Application to enable SEKM on the PERC. The server is automatically restarted.

10. After the POST or Collecting Inventory operation is completed, ensure that the job ID is identified as **Completed** on the Job Queue page.

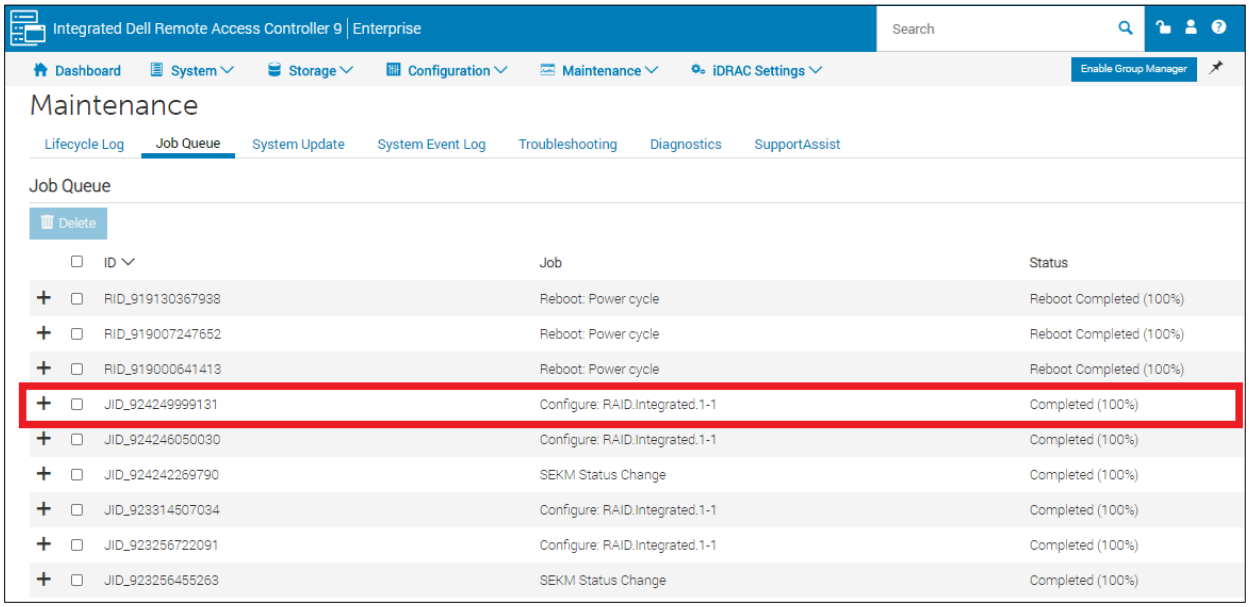



Figure 37 A job successfully ran to enable SEKM on iDRAC PERC

## 3.3.2 Ensure SEKM is enabled on iDRAC PERC

1. On the iDRAC GUI, click **Storage → Overview**.
2. Expand your storage controller and ensure the following statuses:

- Security Status = Security Key Assigned
- Encryption Mode = Secure Enterprise Key Manager

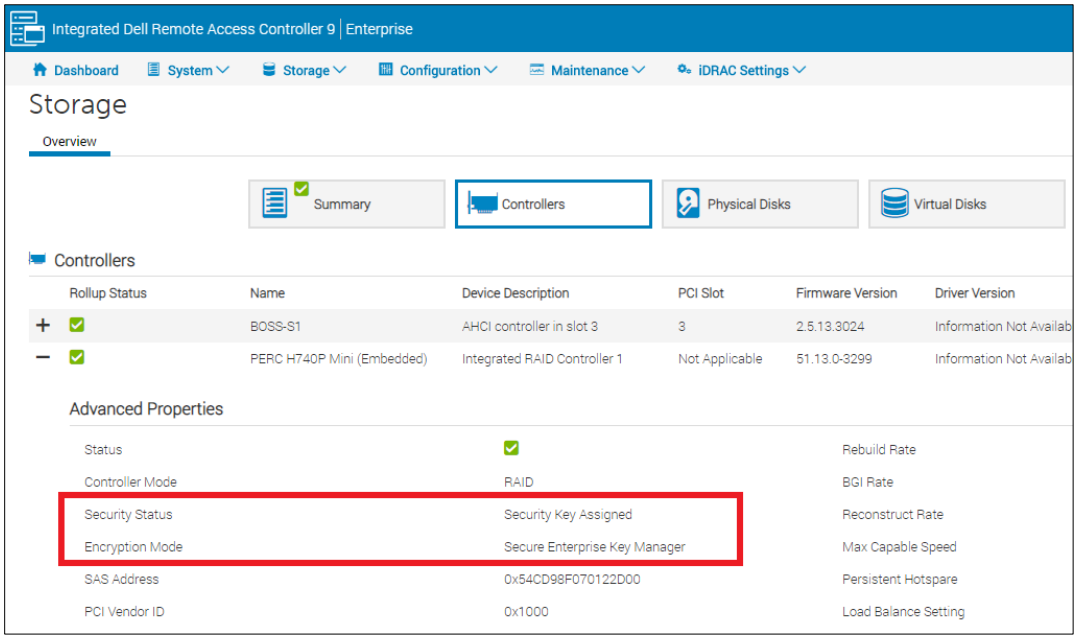



Figure 38 Ensure that SEKM is enabled on your controller

## 3.3.3 Viewing Key ID on Thales DSM

1. Log in to Thales as an Administrator.
2. Switch to the domain where your keys are being managed.
3. Click **Keys → KMIP Objects**.

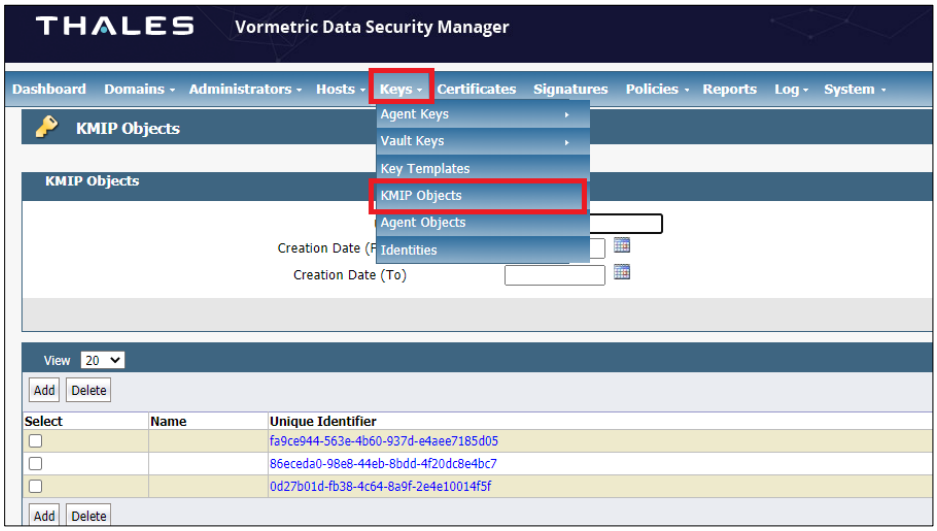



Figure 39 Set up SEKM on Thales

The SEKM setup operation is complete. You can now start creating locked RAID volumes and perform key exchanges.

# 4 CipherTrust Manager (k170v)

## 4.1 Prerequisites for CipherTrust Manager

Before you start setting up iDRAC SEKM support, you must first ensure that the following prerequisites are fulfilled. If these prerequisites are not met, you will not be able to successfully set up SEKM.

### PowerEdge Server Prerequisites

- iDRAC SEKM license installed
- iDRAC Data Center or Enterprise license
- iDRAC updated to the firmware version which supports SEKM
- Supported storage devices updated to the firmware version which supports SEKM

### CipherTrust Manager Prerequisites

- Configure Auto-Client registration
- Configure KMIP interface
- Create a user that represents the iDRAC on the KMS

## 4.2 Set up SEKM on CipherTrust Manager

This section describes the CipherTrust Manager features that are supported by iDRAC. For information about all other CipherTrust features, see the CipherTrust Appliance Administration Guide.

### 4.2.1 Configure Auto-Client Registration

1. Log in to the CipherTrust appliance and click **KMIP (OASIS Key Management Interoperability)**.

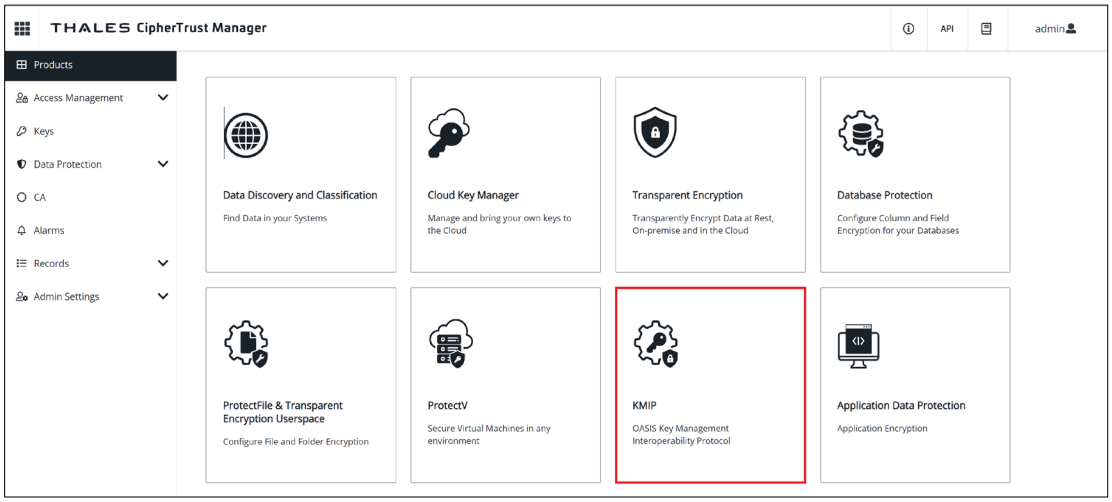



Figure 40 Start the OASIS Key Management Interoperability (KMIP) application

2. Click **Client Profile → Add Profile**.


Figure 41 Add Client Profiles in KMIP

3. Enter or select data in the Add Profile dialog box.

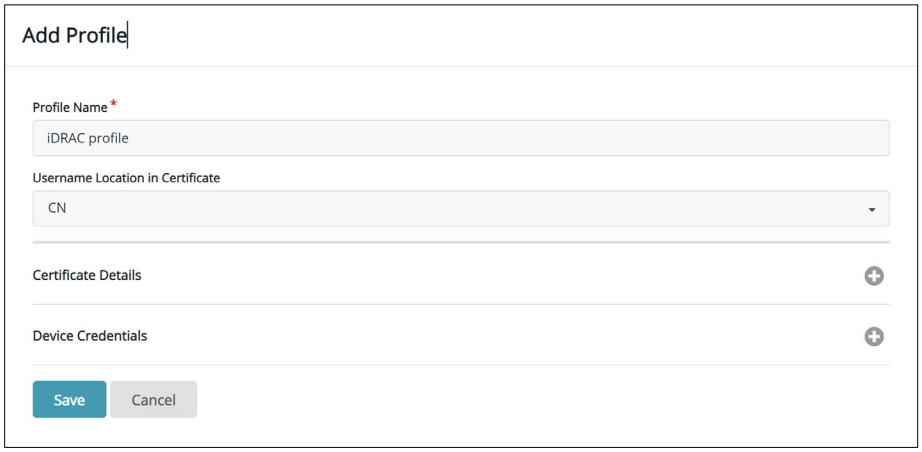



Figure 42 Add profile information on KMIP

Note—CN is required for “Username Location in Certificate”.

Certificate Details and Device Credentials are not required for this step.

If you are using an older version of the k170v (versions 1.10 and below), you will need to specify the Common Name field in the certificate to add a profile. A user with this name must already exist on the KeySecure appliance. This user does not need to be added to a group.

4. Click Registration Token → New Registration Token.


5. Enter the prefix name of the registration token. For example, iDRAC token.

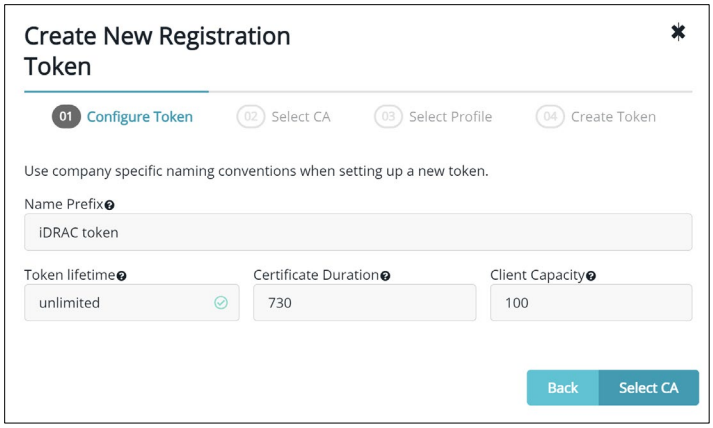



Figure 44 Enter the token prefix name while creating a new registration token

6. Select **Local CAs** as the certification authority, and then click **Select Profile**.

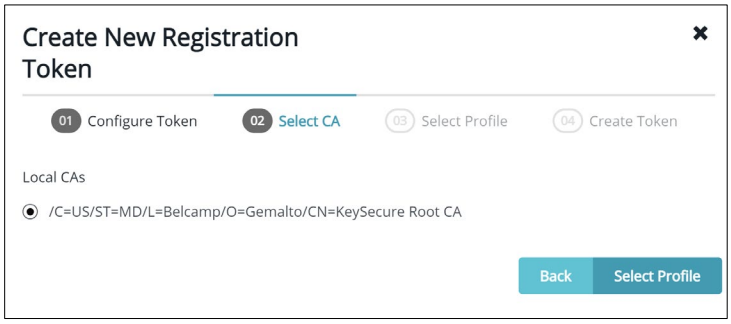



Figure 45 Select CA as the certification authority while creating a new registration token

7. Select the profile you created, and then click **Create Token**.

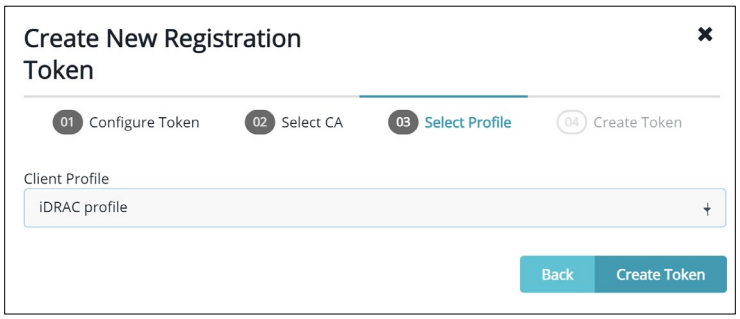



Figure 46 Select a profile for creating a new registration token

8. Copy the registration token.

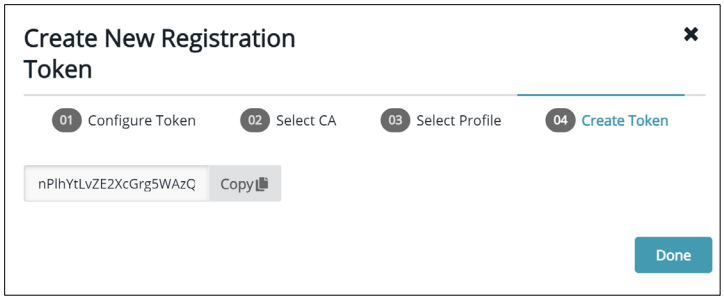



Figure 47 Copy registration token

9. Navigate back to CipherTrust home page, click Admin settings
10. Click Interfaces -> Click Ellipses next to KMIP interface -> click Edit.
11. Select the **Auto Registration** check box.
12. Paste the token that you copied into the **Registration Token** box.
13. Select Enable hard delete

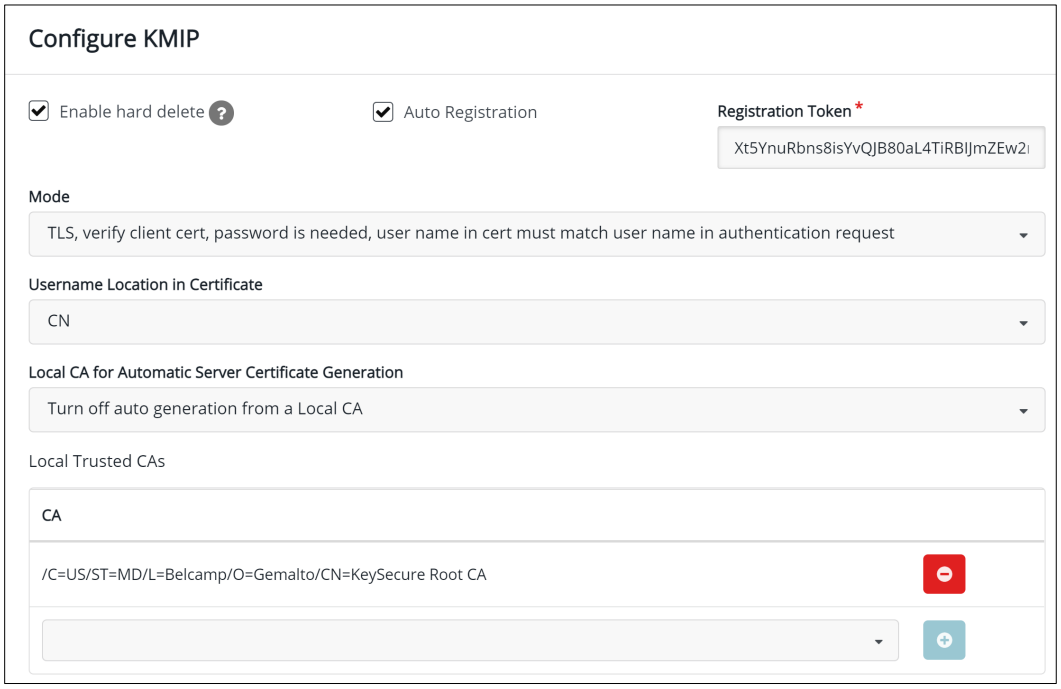



Figure 48 Paste the token and configure KMIP

Note—Ensure that you disable automatic generation from a Local CA on the **Configure KMIP** page. If this option is not disabled, the KeySecure k170v will replace the KMIP server certificate with a new certificate after rebooting. This option is available under **Local CA for Automatic Server Certificate Generation** in the **Edit** section.

If you are using an older version of the k170v (versions 1.10 and below), you will need to restart KMIP services. Go to system -> Services -> Restart KMIP

## 4.2.2 Configure KMIP Interface

1. Click **CA → Create CSR**.
   The save **csr** and **save private key** buttons are enabled.

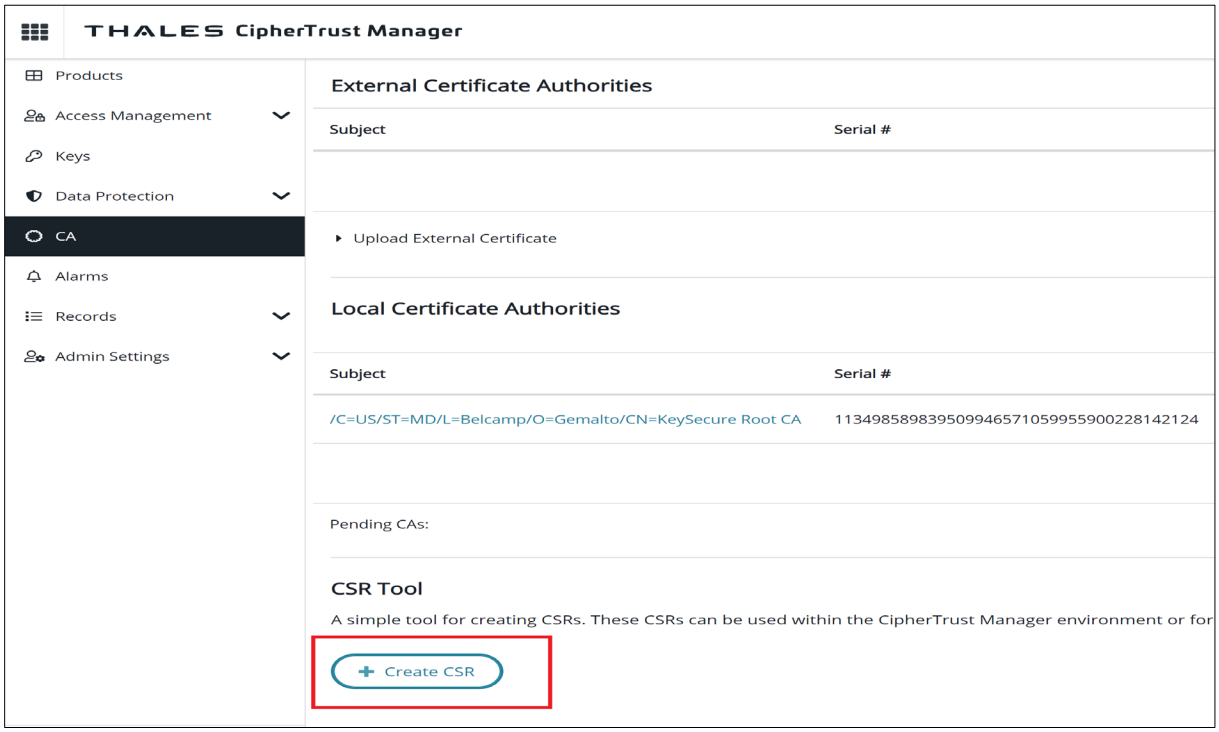



Figure 49 Create CSR on Thales

Note—By default, the Local Certificate Authority shown in the image is available. If you are using a newer version of CipherTrust (version 2.3 and above), click Local CA -> Issue Certificate and follow steps below.

2. Enter or select the settings in the **Create CSR** section.

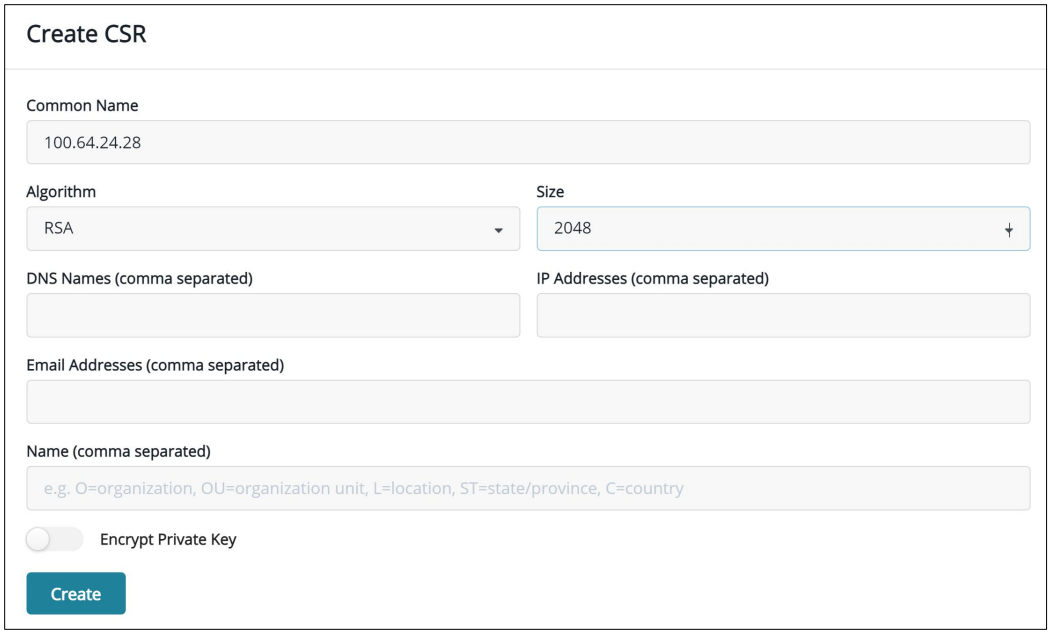



Figure 50 Enter setting to create CSR on Thales

Note—If you have used an older version of Gemalto (KeySecure 150v), the "**Subject Alternative Name**" field has been split into two separate fields—**DNS Names** and **IP addresses.**

In the example above, we have included the IP address of the Next Generation KeySecure in the **Common Name** box.

- Algorithm—RSA
- Size—2048

3. Click both the buttons.

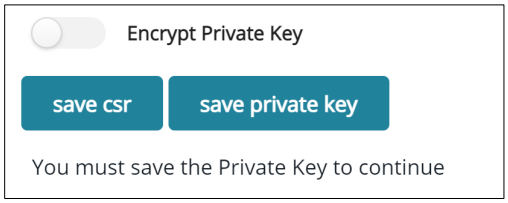



Figure 51 Saving CSR and Private Key

4. Copy the contents of your CSR and get it signed by your Certificate Authority. In this example, we will use the certificate authority that is available by default.
(**CA → Local Certificate Authority**)

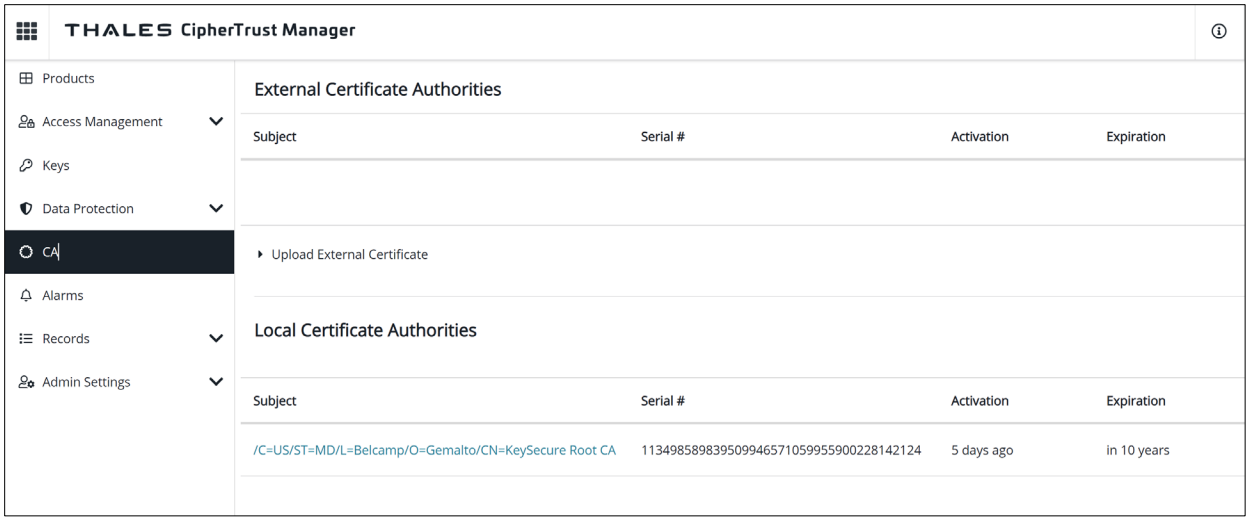



Figure 52 Copy CSR content on Gemalto

5. Select the Certificate Authority (CA).
6. After you select the CA, the Create New Certificate and Upload and Sign CSR buttons are displayed.
7. Select Upload and Sign CSR, and then upload the contents from the CSR you generated in the above steps.


Figure 53 Upload and Sign CSR on CipherTrust

8. Upload the externally generated CSR.

**Note**—For **Certificate Purpose**, make sure you select **server**.


Figure 54 Issue certificate on CipherTrust

After you click “**Issue Certificate**”, the certificate becomes available for download on the same page under “**Subject**”.

10. Take the private key you downloaded in the earlier steps and append it to the signed certificate you just downloaded. An example private key is shown in the screen shot here:

```
-----BEGIN CERTIFICATE-----
MIIDrDCCAZSgAwIBAgIQLaa47JRqlqWA8KnM9L3pZTANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO
BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx
MTAwOTIwNDIxOVoXDTIyMTAwOTIwNDIxOVowFzEVMBMGA1UEAxMMMTAwLjY0LjI0
LjI4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCGo3baZiLf2xdymghU18P
0qKluOYHhOA+7eLfOze7P9MQLf9SysbhAkvBSx41JuAgpbmIWQpGu1etUzclTSm3
9pHi+itI3I5nS4WBfN/yMHXjc0tdpgdgQfozlNhR3ftgKO7ZeU7FjxcovOoykDWm
e1tBDxkQX5Xf97SX0UrM6wIDAQABozUwMzAOBgNVHQ8BAf8EBAMCA4gwEwYDVR0l
BAwwCgYIKwYBBQUHAwEwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAgEA
MsdPI1TMbsfPD9xH3yltRYM2FVEjnwziu708PyJ89rjLfY8463l7Wg2A0oej9uHn
LiCn0b+1k+OIHRbJtJ6UZ6h/TL57x/cJ06g1S/VNhxHi2HRUrDAlgQXLfiBbpqEb
pS0EbfoBJH+0MGbibGnBsLcLBDS5hvEVvHXs2cwWUICrhdRt0VTP8xXKQfmPsoYR
Lj1FF4Rfc1QZ5kEG1U9y8nV+huOjQ8Nt4fDrNbm/ZR10aN1+3VR8oNtAYrUNaVxa
8hShsa6H0rfo2cEbxLpkOgae4nnzEjLqh1hxbaoB9cVJXtzG4aDDG0DwLSCFgl/u
01P2p/sF1TpPU0EwC8EigHf5SKPkeXlufQb4SFmWQceP0S+Pb3x8dZyLe0Zl+VYf
VtOzjS8cKtUjnOKU8cmlm/SxjiBaZyE2sX4mIkO5xJdz1xvzIztQWv6/ss60OCGl
R3Y+3UZDH6mP96P1VtWWQqkYGysfzN5wmh9ohjmrqnP1wHyjDmm6JfVMutsvf0du
kt/SMck6AS4lWCHtC9BNdn5MB07aLEv25dzJHmC3SSREv2fKow5qXjlcAq44cE6n
b3H1eaBRkl78HFCyxcg3eEf5vwe6aF8XoPdJ37bUuctqrpHo8mizDBL/aL6jeP7m
u310T6PjK27/PVonV6tyYxruVGoidiG85Fzxejh0Rm8=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDCGo3baZiLf2xdymghU18P0qKluOYHhOA+7eLfOze7P9MQLf9S
ysbhAkvBSx41JuAgpbmIWQpGu1etUzclTSm39pHi+itI3I5nS4WBfN/yMHXjc0td
pgdgQfozlNhR3ftgKO7ZeU7FjxcovOoykDWme1tBDxkQX5Xf97SX0UrM6wIDAQAB
AoGBAJ4ajw33lz+ZTSWgZu0uQbJbugwO7Z+WRio8Dp4SWDT3qe316ZEAhrpk6lvJ
2hMlVU6Cbvt2u34dvy75J2QE1EMO/MU6xNjbHLKQlyPSwB36pnM367QeVWNBY26r
dm99uUIWAQwzCc8GFxlIU5q2WZMKWMv9DGtVPi7/MiOF/9MRAkEA5xYlCHNSKX9y
LlvVVPQVzqNu8OhmeMedMKWhNC88YRweBCXSXfa4wHEM5rX6sWiNR2jOBkAOvJfZ
bmsdYjekFQJBANcHtL0jlr+xNtO0b8oF9vmXiWW0TwhL3jxpM8jOecN1yMoHBkz8
+xe5V5yhIfbQ93YWzuQD7ObreZOhar3v7P8CQEz7C4stH4nDcv4OiZqrVThpKWQH
h1tk4/B4vKLtuWeAPl+TWekDb7hr8KhKpyDCe432U+uxGzeoPj6SYE9/yaECQAzQ
1sLXFisCouPnQyplRJ0HnRbEslkqPGqZUo7LT5KIuJjh5kw8X7LARyp8qAuP1M/i
+B265im1Kx/TZQtA+30CQEZyflA2wHm0WXJhWjcBHa/kTxEgobDTzeYkkPixztdt
/Gr4pmbnBtwSNwlFCmpoysZ7w85ZSd25LYoivP4PBDQ=
-----END RSA PRIVATE KEY-----
```

Figure 55 Appending the private key on CipherTrust

11. Save this file and upload it to the KMIP interface.
12. Upload signed certificate and private key to KMIP interface.
    a. Click **Admin Settings -> Interfaces**
    b. Click the ellipses symbol next to KMIP interface, and then click Edit
    c. After you click Edit, the Configure KMIP screen is displayed

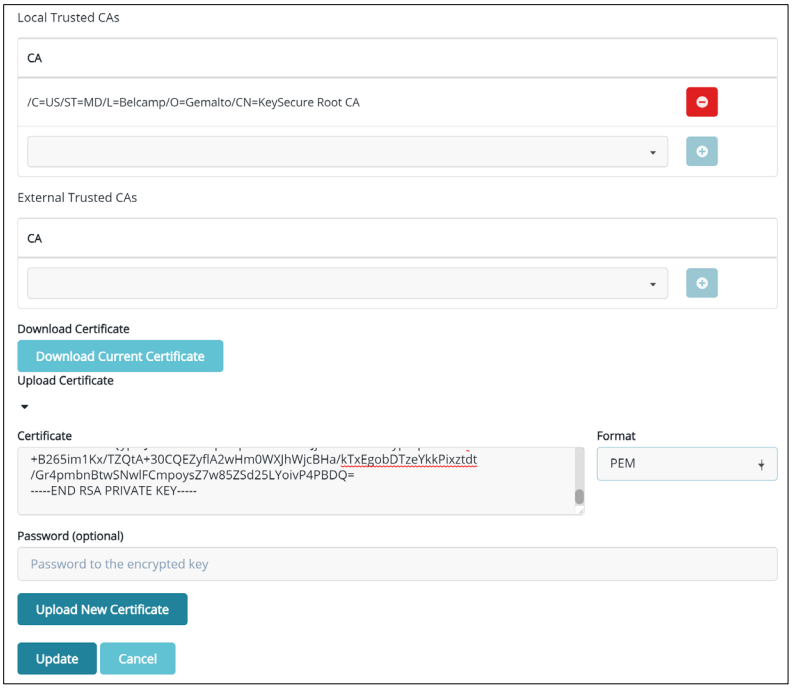



Figure 56 Edit and upload new certificate on Gemalto

- **Certificate**—Contains the signed certificate contents along with the appended private key.
- **Format**—PEM

13. Click **Upload New Certificate**.
14. Click **Update**

---

Note—A green check mark is displayed after uploading the new certificate.

If you are using a older version of the k170v (versions 1.10 and below), you will need to restart the KMIP services.

Go to System -> Services -> Restart KMIP

---

### 4.2.3 Create a user that represents the iDRAC on CipherTrust Manager

1. Click Users → Create New User.

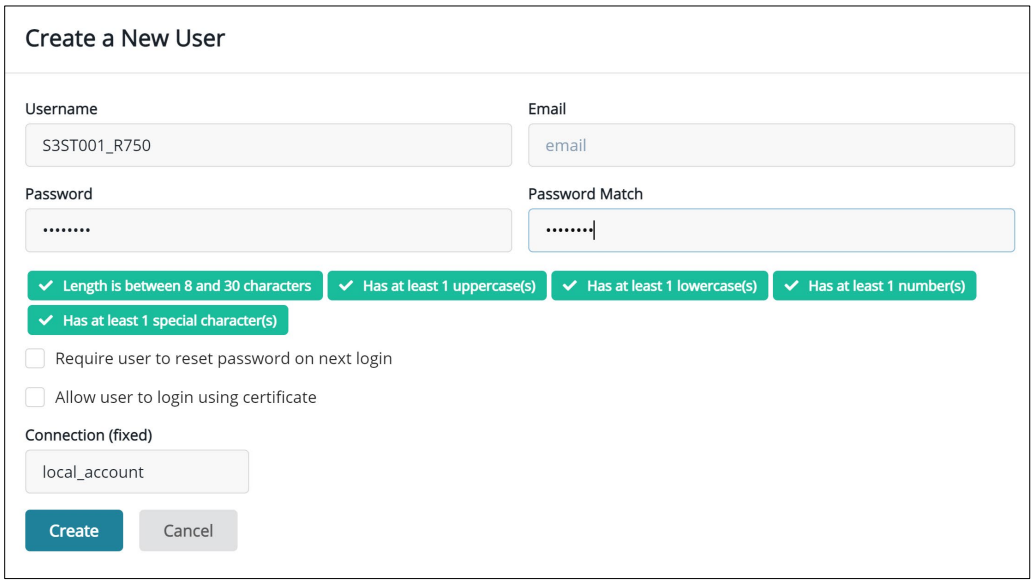



Figure 57 Create iDRAC user on CipherTrust Manager

Note—The username must match the Common Name field in the iDRAC CSR.

2. After you create this user, add this user to the Key Users group:
   a. Click Access Management -> Groups -> search for “Key Users”.
   b. Add your newly created user to the group.

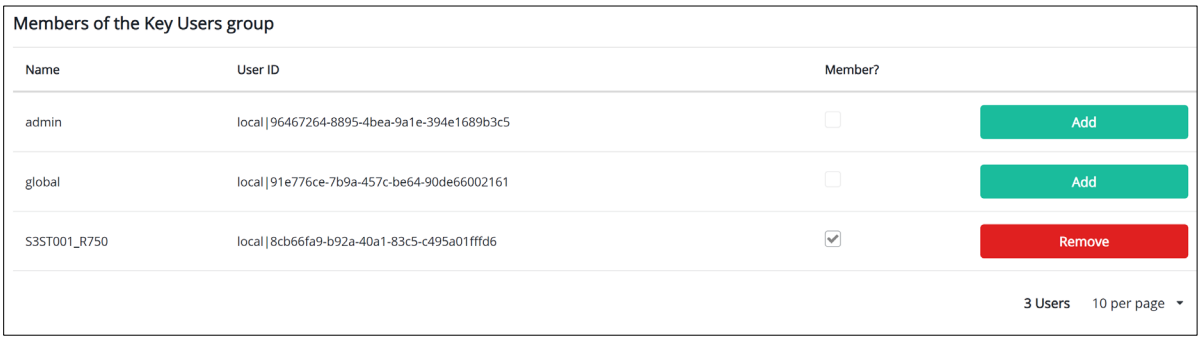



Figure 58 Add new user to the group on CipherTrust Manager

## 4.3 Set up SEKM on iDRAC

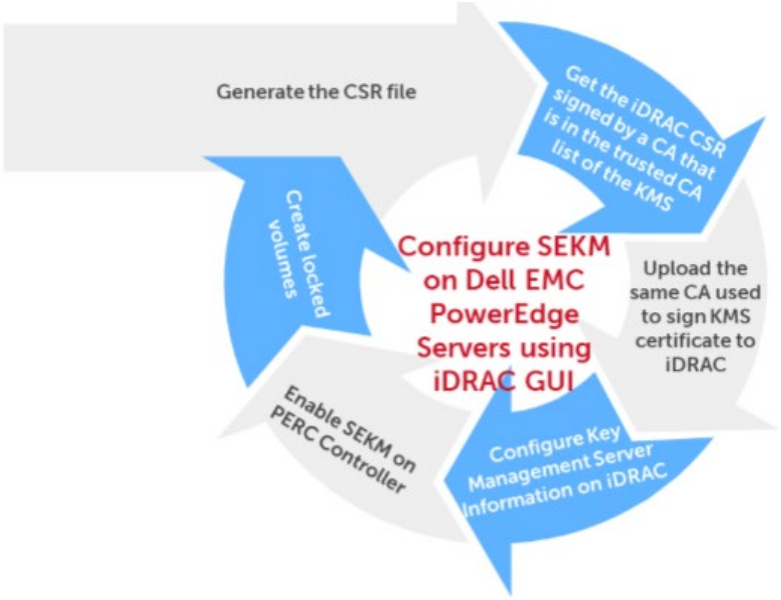
**Licensing and firmware update**

SEKM is a licensed feature with the iDRAC Enterprise or Data Center license as a pre-requisite. To avoid an additional iDRAC firmware update, it is recommended that the SEKM license is installed first and then the iDRAC firmware updated to a version that supports SEKM. This is because an iDRAC firmware update is always required after the SEKM license is installed irrespective of whether the existing firmware version supports SEKM or not. The existing interface methods for installing license and firmware update can be used for SEKM.

**Set up SSL certificate**

The SEKM solution mandates two-way authentication between the iDRAC and the KMS. iDRAC authentication requires generating a CSR on the iDRAC and then getting it signed by a CA on the KMS and uploading the signed certificate to iDRAC. For KMS authentication, the KMS CA certificate must be uploaded to iDRAC.

## 4.4 Configure SEKM by using the iDRAC GUI




For the Key Management Server, this workflow will be using the CipherTrust Manager as the Key Management Server (KMS).

1. Start iDRAC by using any supported browser.
2. Click iDRAC **Settings** → **Services**.

3. Expand the SEKM Configuration menu and click **Generate CSR**.

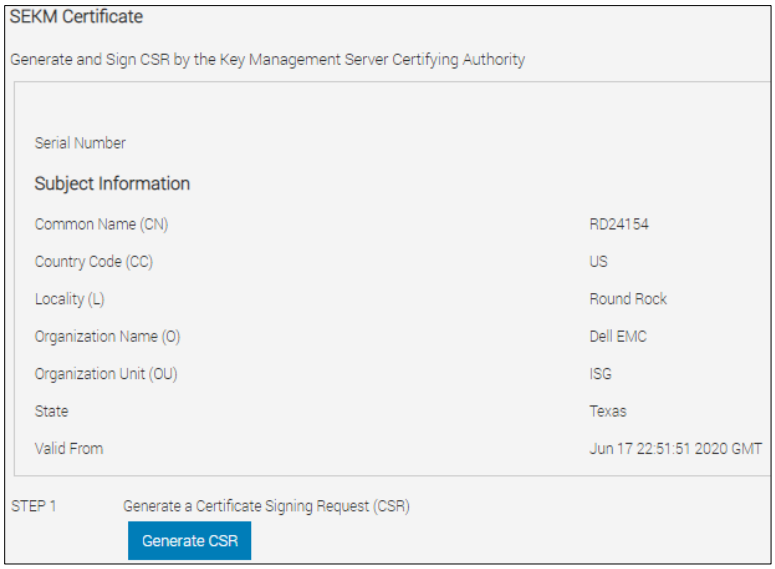



Figure 59 Generate CSR on iDRAC

4. In the **Generate Certificate Signing Requests (CSR)** dialog box, enter the certificate information.
5. Click **Generate**.
   The CSR file is generated.
6. Save it to your system.

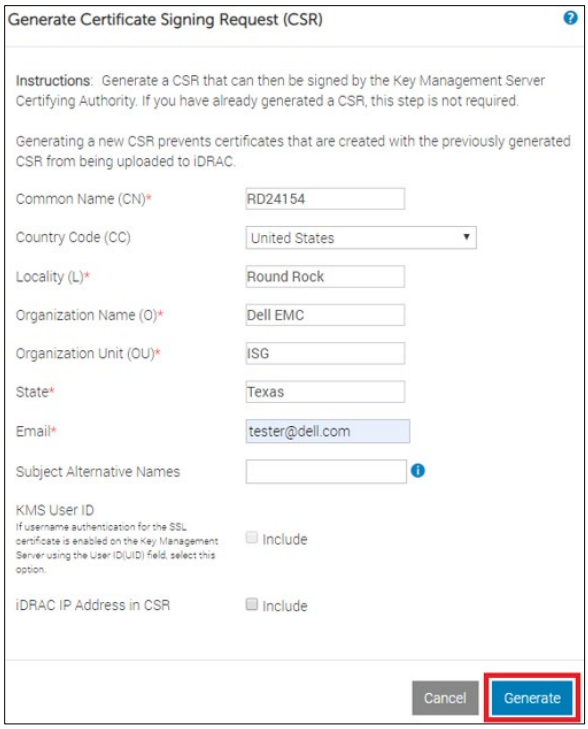



Figure 60 Specify CSR properties on iDRAC GUI

7. Get the full CSR file contents signed on the CipherTrust Manager.
8. Download the signed image file, and then upload it to iDRAC.

## 4.5 Get the CSR file signed by CipherTrust Manager


```
-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEG1kcmFjdXN1ckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV
i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB2l6UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=
-----END CERTIFICATE REQUEST-----
```


Figure 61 CSR certificate signed by CipherTrust Manager

1. Log in to CipherTrust Manager.
2. Click **CA → Local Certificate Authority**.

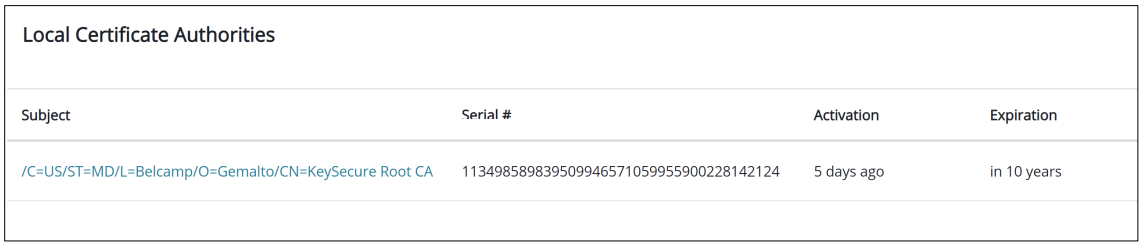



Figure 62 Copy Local Certificate properties

3. Click Upload and Sign CSR.

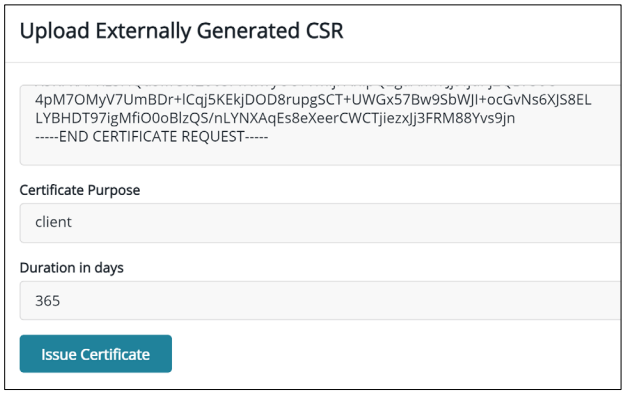



Figure 63 Issue certificate on CipherTrust Manager

**Certificate Purpose: client**

Note—After you issue the certificate, it will become available to download and save to your system. It will be the most recent certificate listed under “Subject”.

4. To upload the file you just got signed by CipherTrust Manager, on the iDRAC GUI, on the **SEKM Certificate** page, click **Upload Signed CSR**.
   A message is displayed to indicate the successful upload.

### 4.5.1 Download the server CA from CipherTrust Manager and upload to iDRAC

1. On the CipherTrust Manager UI, click **CA**.

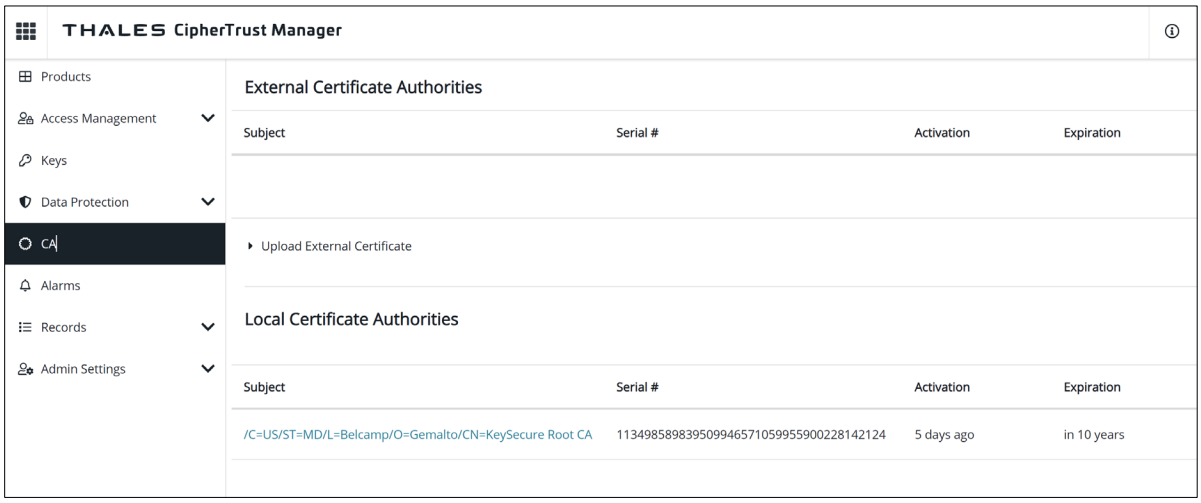



Figure 64 Download CA and upload to iDRAC

2. Click the ellipses symbol (…) in the right corner, download, and then save it to your system.
3. Upload it as the KMS CA Certificate on the iDRAC.
   A message is displayed to indicate that the upload was successful.

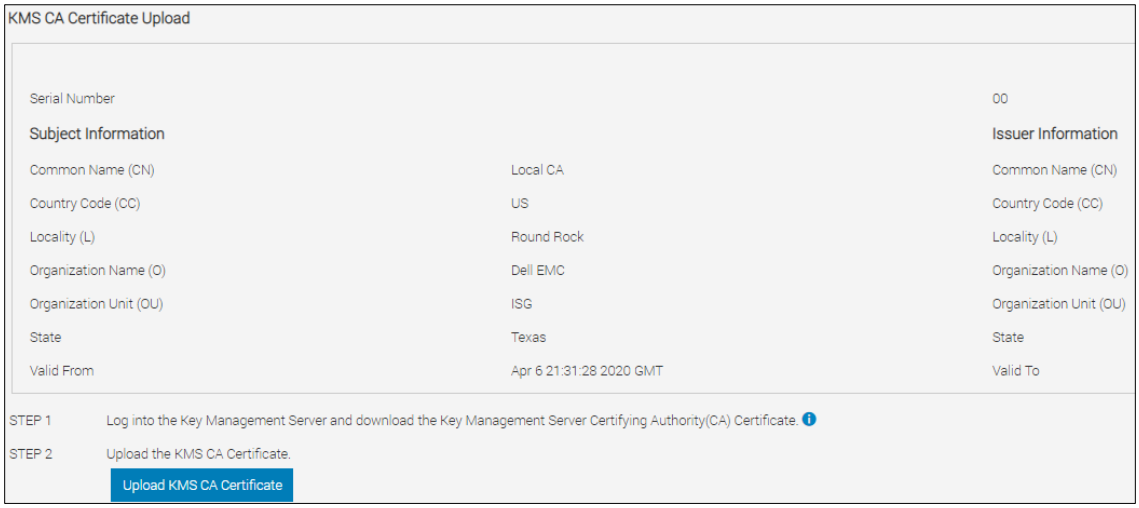



Figure 65 Upload KMS CA certificate to iDRAC

## 4.6 Configure the Key Management Server (KMS) settings on iDRAC

1. Enter or select data in the fields, and then click **Apply**.


Figure 66 Configure KMS on iDRAC

Note—The User ID and Password fields (if applicable) must match the user you've created on the Next Generation KeySecure in the steps above.

2. Go to the Job Queue page and ensure that the job ID is marked as successfully completed.
3. If you see any job status failures, view Lifecycle Logs for more information about the failure.

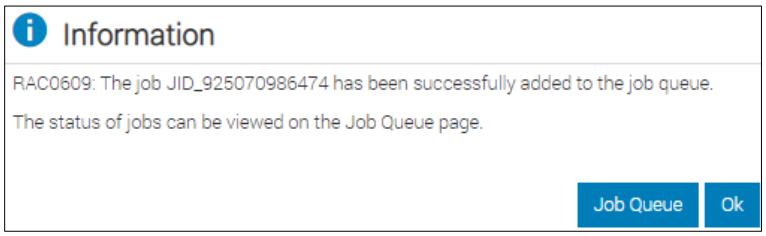



Figure 67 Create job to Configure KMS on iDRAC

4. Go to the **Job Queue** to check the job status.

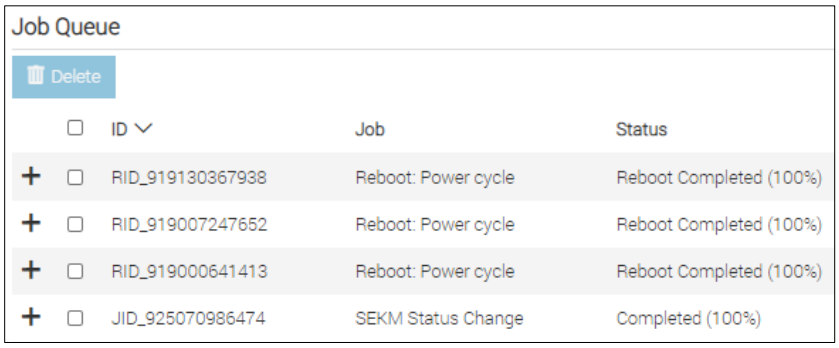



Figure 68 Check the status of job for creating a job to Configure KMS on iDRAC

The iDRAC SEKM configuration is completed.

## 4.7 Enable SEKM on the iDRAC PERC

1. On the iDRAC GUI, click **Configuration** → **Storage Configuration**.
2. Select your storage controller.
3. Expand **Controller Configuration**.
4. From the **Security (Encryption)** down-down menu, select **Secure Enterprise Key Manager**.
5. Click **Add to Pending Operations**.

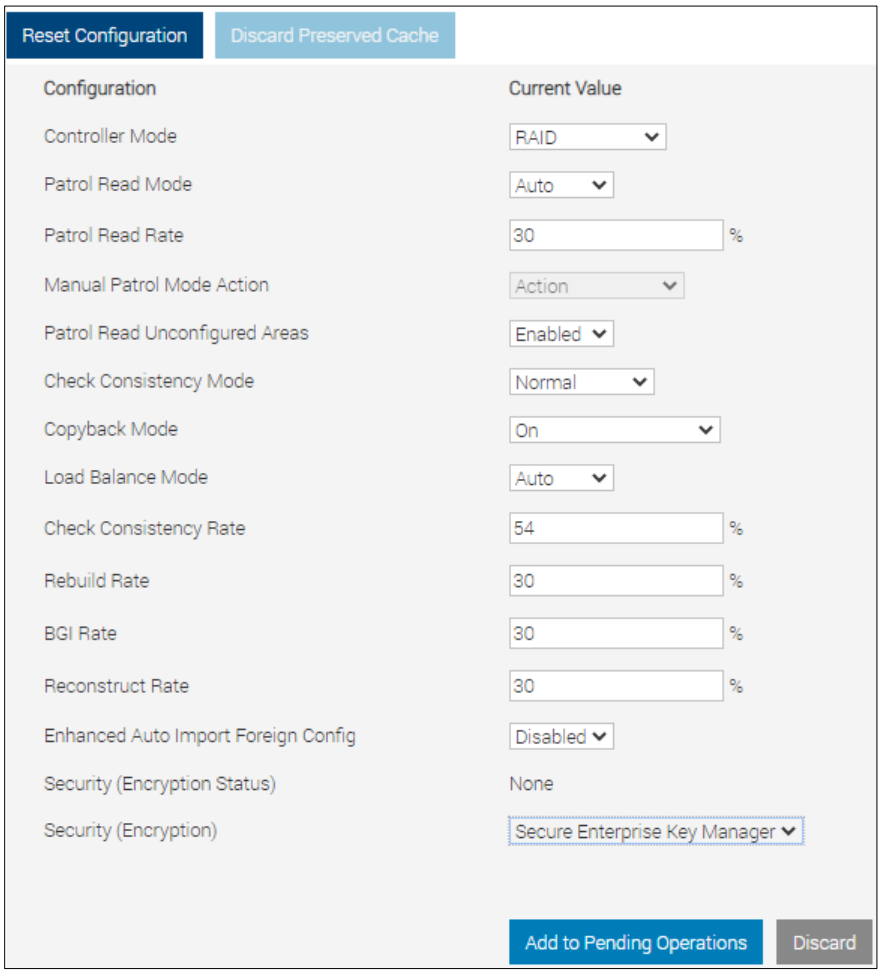



Figure 69 Enable SEKM on iDRAC PERC

6. Select **At Next Reboot**.
   A message is displayed indicating that the job ID is created
7. Go to the **Job Queue** page and ensure that this job ID is marked as **Scheduled**.

8. Restart the server to run the configuration job.

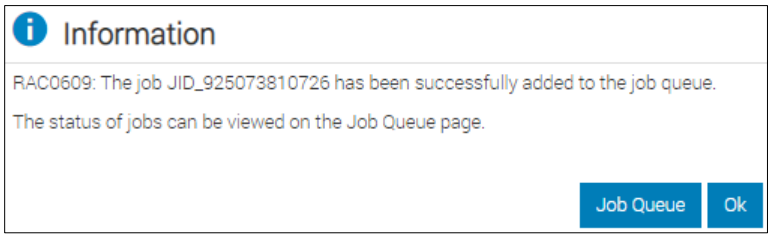



Figure 70 Start a job to Enable SEKM on iDRAC PERC

9. Go to the Job Queue to view the scheduled job
10. After restarting the server, the configuration job is run in the Automated Task Application to enable SEKM on the PERC. The server is automatically restarted.
11. After the POST or Collecting Inventory operation is completed, ensure that the job ID has been marked as **Completed** on the **Job Queue** page.

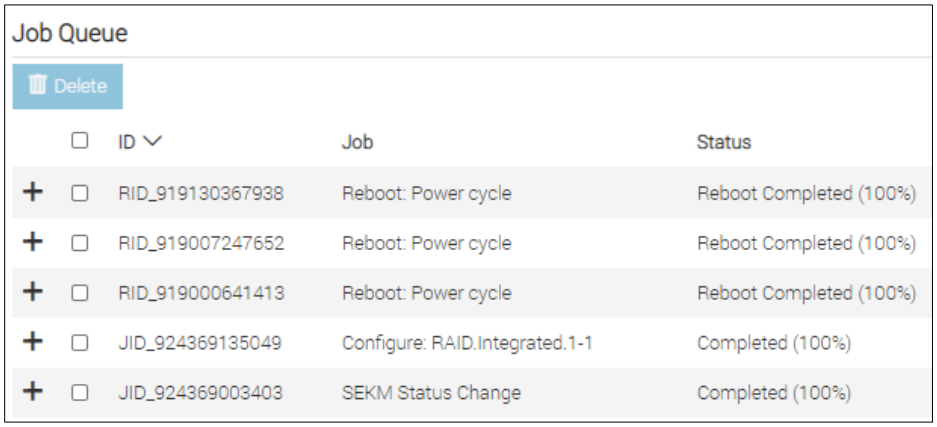



Figure 71 Check the status of job to Enable SEKM on iDRAC PERC

## 4.8 Ensure SEKM is enabled on iDRAC PERC

1. On the iDRAC GUI, click **Storage → Overview**.
2. Expand your storage controller and ensure the following statuses:

   - **Security Status** = Security Key Assigned
   - **Encryption Mode** = Secure Enterprise Key Manager

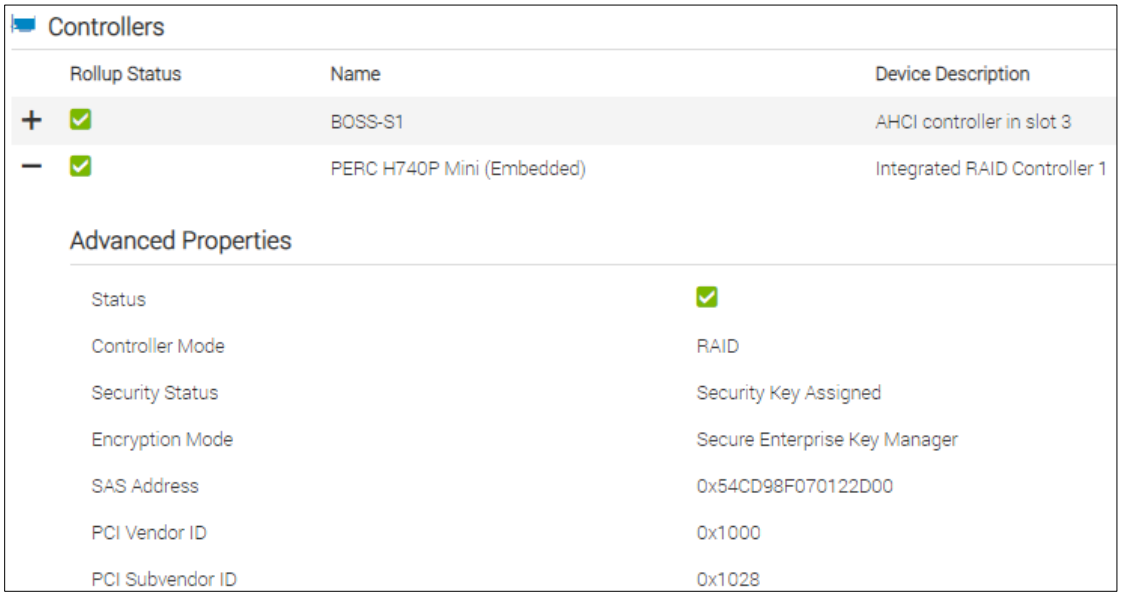



Figure 72 Ensure SEKM is enabled on iDRAC PERC

## 4.9 Viewing the iDRAC key ID on CipherTrust Manager

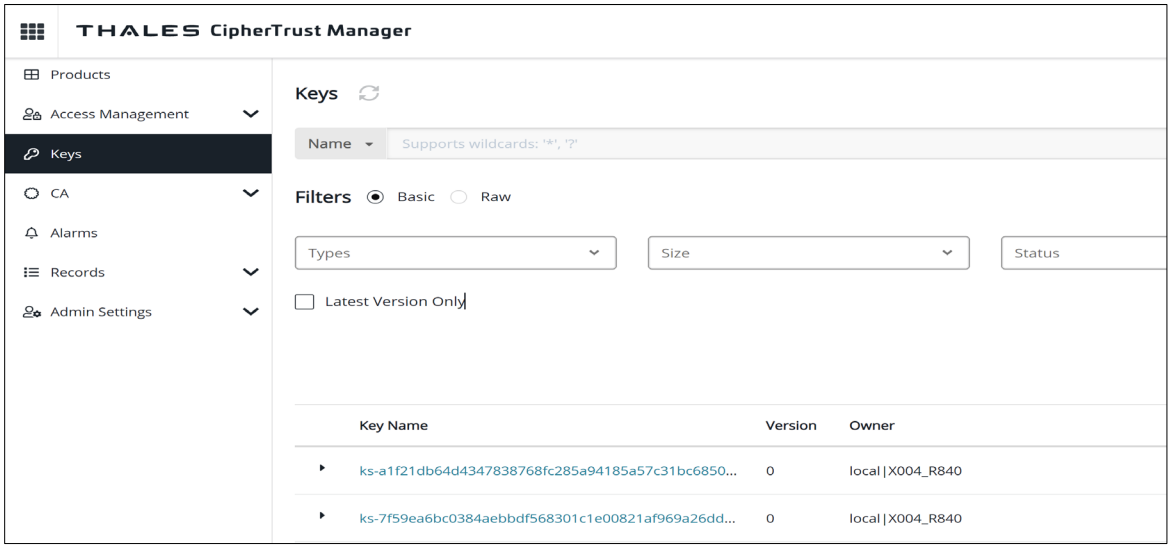



Figure 73 View iDRAC key ID on CipherTrust Manager

The SEKM setup operation is completed. You can now start creating locked RAID volumes and perform key exchanges.

# 5 Configure SEKM solution by using iDRAC RACADM CLI

In this workflow example, iDRAC RACADM is used to set up the complete SEKM solution for iDRAC.

1. Configure iDRAC SEKM certificate attributes. These must be configured first before you generate a CSR file.

2. To set each attribute, run the SET command. The examples here use the default iDRAC username and password (root/calvin)

3. Replace it with an appropriate iDRAC username and password set up on the PowerEdge server

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.sekmcert
[Key=idrac.Embedded.1#SEKMCert.1]
#CertificateStatus=NOT_PENDING
CommonName=
CountryCode=
EmailAddress=
LocalityName=
OrganizationName=
OrganizationUnit=
StateName=
SubjectAltName=
UserId=

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.CommonName idrac-PTC8502
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.CountryCode US
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120-u root -p calvin --nocertwarn set idrac.sekmcert.EmailAddress tester@dell.com
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.LocalityName "Round Rock"
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationName "Dell EMC"
[Key=idrac.Embedded.1#SEKMCert.1]
```

```
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationUnit "ISG"
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.sekmcert.StateName Texas
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
```

4. Generate a CSR by getting the CSR contents signed on the Key Management Server

5. Download the signed file, and then upload it back to iDRAC. Run the following at the RACADM CLI:

   ```
   C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sslcsrgen -g -t 3 -f sekm_csr
   CSR generated and downloaded from RAC successfully
   ```

6. Upload the CSR certificate to the iDRAC. Run the following command at the RACADM CLI:

   ```
   C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sslcertupload -t 6 -f
   signed_sekm_ssl_cert.pem
   Certificate successfully uploaded to the RAC.
   ```

7. Upload the Server CA file to the iDRAC

   ```
   C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sslcertupload -t 7 -f server_ca_new.pem
   Certificate successfully uploaded to the RAC.
   ```

8. Configure Key Management Server settings on iDRAC

   **Note** – Ensure you have a user created on the Key Management Server (KMS) you will be using for key exchange with the iDRAC. For the username, make sure it matches the same value in the CSR certificate property you selected for the KMIP **Username field in client certificate** Authentication Settings.

9. Run the following command at RACADM CLI:

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.kms
[Key=idrac.Embedded.1#KMS.1]
!!iDRACPassword=******** (Write-Only)
iDRACUserName=
KMIPPortNumber=5696
PrimaryServerAddress=
RedundantKMIPPortNumber=5696
RedundantServerAddress1=
RedundantServerAddress2=
RedundantServerAddress3=
RedundantServerAddress4=
RedundantServerAddress5=
RedundantServerAddress6=
RedundantServerAddress7=
RedundantServerAddress8=
Timeout=10

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.kms.iDRACUserName idrac-
PTC8502
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120-u root -p calvin --nocertwarn set idrac.kms.iDRACPassword Dell123!
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sekm enable
SEKM0212: The operation is successfully started.
        To view the status of a job, run the "racadm jobqueue view -i JID_348909866879" command at the
Command Line Interface (CLI).

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_348909866879
---------------------------- JOB ------------------------
[Job ID=JID_348909866879]
Job Name=SEKM Status Change
Status=Completed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Not Applicable]
Actual Completion Time=[Not Applicable]
Message=[SEKM020: The SEKM feature on the iDRAC is enabled.]
Percent Complete=[100]
-------------------------------------------------------------
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sekm getstatus
SEKM Status = Enabled
```

# 6 Configure SEKM using Server Configuration Profile (SCP)

In this workflow example, the Server Configuration Profile feature is used to set up complete SEKM solution for iDRAC.

1. Using SCP, import the signed SSL certificate, Server CA, iDRAC KMS attributes

2. Enable SEKM on iDRAC

For the signed SSL certificate, a CSR is already generated, signed on the Key Management Server, and then downloaded. The Server CA is also downloaded from the Key Management Server.

3. In the SCP, copy the contents of the signed SSL certificate and Server CA as shown in the example SCP file below.

4. SCP example for configuring iDRAC SEKM configuration

This SCP file has been edited to show you only the SEKM configuration changes required to enable SEKM on iDRAC:

<SystemConfiguration Model="PowerEdge R750" ServiceTag="JHK6TYG" TimeStamp="Fri Oct 22 03:55:37 2021">

<Component FQDD="iDRAC.Embedded.1">

<Attribute Name="SEKM.1#IPAddressInCertificate">Disabled</Attribute>

<Attribute Name="SEKM.1#SEKMStatus">Enabled</Attribute>

<Attribute Name="SEKM.1#KeyAlgorithm">AES-256</Attribute>

<Attribute Name="SEKM.1#Rekey">False</Attribute>

<Attribute Name="SEKM.1#KMSKeyPurgePolicy">Keep All Keys</Attribute>

<Attribute Name="SEKM.1#AutoSecure">Disabled</Attribute>

<Attribute Name="KMS.1#PrimaryServerAddress">100.64.40.167</Attribute>

<Attribute Name="KMS.1#KMIPPortNumber">5696</Attribute>

<Attribute Name="KMS.1#RedundantServerAddress1"/>

<Attribute Name="KMS.1#RedundantServerAddress2"/>

<Attribute Name="KMS.1#RedundantServerAddress3"/>

<Attribute Name="KMS.1#RedundantServerAddress4"/>

<Attribute Name="KMS.1#RedundantServerAddress5"/>

<Attribute Name="KMS.1#RedundantServerAddress6"/>

<Attribute Name="KMS.1#RedundantServerAddress7"/>

<Attribute Name="KMS.1#RedundantServerAddress8"/>

<Attribute Name="KMS.1#Timeout">10</Attribute>

<Attribute Name="KMS.1#iDRACUserName">idrac-PTC8502</Attribute>

<Attribute Name="KMS.1#iDRACPassword">Dell123!</Attribute>

<Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute>

<Attribute Name="SEKMCert.1#CommonName">idrac-PTC8502</Attribute>

<Attribute Name="SEKMCert.1#OrganizationName">Dell EMC</Attribute>

<Attribute Name="SEKMCert.1#OrganizationUnit">ISG</Attribute>

<Attribute Name="SEKMCert.1#LocalityName">Round Rock</Attribute>

<Attribute Name="SEKMCert.1#StateName">Texas</Attribute>

<Attribute Name="SEKMCert.1#CountryCode">US</Attribute>

<Attribute Name="SEKMCert.1#EmailAddress">tester@dell.com</Attribute>

<Attribute Name="SEKMCert.1#SubjectAltName"/>

<Attribute Name="SEKMCert.1#UserId"/>

<Attribute Name="SecurityCertificate.1#CertData">-----BEGIN CERTIFICATE-----

MIIFgTCCA2mgAwIBAgIQbL1BjtEwBL3fNQCMjT47TDANBgkqhkiG9w0BAQsFADBa

MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO

BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx

MDYyMzE0MDU0N1oXDTMxMDYyMTE0MDU0N1owWjELMAkGA1UEBhMCVVMxCzAJBgNV

BAgTAk1EMRAwDgYDVQQHEwdCZWxjYW1wMRAwDgYDVQQKEwdHZW1hbHRvMRowGAYD

VQQDExFLZXlTZWN1cmUgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC

AgoCggIBANbjXWXrloVYosJiwxpSz2fCXGLWQQfUlFCEwUPFw+R8fAO29lSo6tHa

sQ3Tx+QMZlFEa9DaZbhcuOyQsoIUoG1V+oBpZSvx1+QTVcO6PRM8Tv3RD75xl36Y

KDQXxJoABB414laHM9pyAmkI1dnHs7wQhHBrb7PBW8Ol2+Qzk3CDAyaa4t/s332/

KlDQs18JTBHceMnNEdXkG9rVcYmpjZXvrhjYHSvvVoGZWCtzuKvszL6NOKj7ruUT

uq2WSSBRjiwPSysJNtubcGNravOm4FCgSNZi0v1bqKFTBq0lXgamhScjyIHGkrFm

aO71v1OmDtjih7c69gtOQG+yyCKPkNrxh5CVEU7yoJDWa1ak7TJaiYczH2cvMDY2

3r9uFWdfeM0E4EQ5kM5KvLXzygM8FxzZE3XkrekFw+6kOZuZmf0FoptQYATOaQpK

xGrTWGjlcAlnoQDgINGjZFD70y/mf01JkS/UWtdX0yZysw/iNDzqmh7ELy9dsR2s

PkXyMlAOVW/ydlFRcY+s32kMqRXIFKgy8vuyPMLhIi/tMGNpvJ4N6vnjzHfDpsWK
d5n/T7tDMAf/zlmUSvwhtsHkMnXyCPpAR/uVW5DMwbf9d6TCJs7ofIFpsSptkw53
UDL7ThX9klqO0WV5FbGBlY1OfNMeX6LIwJ+v3A1VVNFNiYxCUTA/AgMBAAGjQzBB
MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB4GA1UdEQQXMBWBE3N1
cHBvcnRAZ2VtYWx0by5jb20wDQYJKoZIhvcNAQELBQADggIBANFZGyBqQ6u26G/C
P2vhIr5i3UrlOyLFC+erX2IGU68GFloHF26ZKBej3kAkFi6naThR3vjOlj2crM6+
PZlyW/JTpmBa0aVfyfVlKytOmkXXM27bPheeBInDPOFfgJROG7xiMfMKRdDwMJ+B
iyYX+rHO8xc72e7FUnF72dUN1AK+2sLvaFSdWYWQ/Aj2Dm5qXxRqw3YPtToax3m1
c+O3Wb5jCW01s+7w+E74CPRCiFISRsP23qDJV3xGbMF7pTwJEDzIQTtrXT5DXOXa
o7yJm9Uyw5QF589agesVybH8KsJJZLN+wW75NHUp+OnTuC/gy8viccaYzCCXuqGH
R3aX/k9UBkaOcAI9M6bGHn7XwsJWKsyWHtsCqJKyGvo9+48kgg0dximWDwUBMBjx
tP0lmOMOLcgE3xB72L2OtpNZHlU/4w87sLVxPJyrDRT+Zn1zjFdBDGUdNEW2di+2
qW1xwoy8TQK/cOKC5/cMQVqQr4PriRTBhnU5WDSfQ/fuiyGmU+L9/LOrjL/S2/8C
RTsQzOmQC+1ADOXHedMFPhsRZcMTZgSWXThERrn46ZiuO+yvBvh5rfvNf6JH+LLL
uwpUDmwzRF3rmXqGzeuk0ou620kQuylK4nnyii3GsCgq/ZOn6Gqz+afcUoCPN39n
6CTqqYiFHUXl4pZJrrXhQ+Vkxh6t
-----END CERTIFICATE-----</Attribute>
<Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
<Attribute Name="SecurityCertificate.2#CertData">-----BEGIN CERTIFICATE-----
MIIEpTCCAo2gAwIBAgIQUO1US/yDXsY8uGv+lxAuQDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO
BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx
MTAyMDE4MDUwMloXDTIyMTAyMDE4MDUwMlowgYsxCzAJBgNVBAYTAlVTMQ4wDAYD
VQQIEwVUZXhhczETMBEGA1UEBxMKUm91bmQgUm9jazERMA8GA1UEChMIRGVsbCBF
TUMxDDAKBgNVBAsTA0lTRzEWMBQGA1UEAxMNaWRyYWMtUFRDODUwMjEeMBwGCSqG
SIb3DQEJAQwPdGVzdGVyQGRlbGwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA1HX6hIV1ggy0R5aU03MjoS2CkanRClFOtWPIW+r87hkrRN9FodCA
Uud1WoU1gFoAb6U+wNDmGHZuF1CkKMl62gLdCcoKB3A5Wz5FyDYmDn8ql7TKvp3g
THDYCNKCsr4z3eVdQcJwvILzV3Pnv0bNdBNwi0GjC24P70/VhPSjZMFvg6x/3mcn

wj/bec3BrxbxGT24koxpyip24wgJ82qA064R1Z6fWPGiZhBMY8h0r3BXG6uVzHG1
2Ue2FoqYBocs9EkUm7RB5la3m0g7B2nVRggc5UCqXeIYBmdzVhdU4XoJ5z1lGtpb
dpLQQZIKrapKBGC2nfrL3RVPAzDOe6hWnQIDAQABozUwMzAOBgNVHQ8BAf8EBAMC
A4gwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0B
AQsFAAOCAgEAmDs2mfdD1N2POKvD0cbfhUX8/edAyBDEEe+ylXAplgPiJ/Hl5WU4
LGUdDNVg6NKGBoXyQKePxP8fcR35xN6MSzThM8tRRR32TFfRelNxmfGB2YeyngY8
aZ8eFg4O5+sbYyV/josXfbr27mryuWy4KuDUgtzUrZnP5waKpS6ZpkqgXvA+lhS7
7Etj7HZfWF6PWMy6rdbw0KSVzZUg0BFTh6bSO62qYSFx+jxclaZHE6YCmT+q1mPN
K+AjbXi41YeMVa5iXrFIsQt8jNlU+XVt5yyO4AH+50ZQPJ6YlveTOr9Ieo0Bdn43
Ac4PlazRyTQ7iCAtdYOFKltDQZwvaodSzUe8/NxzanGnCjhNdR/SfZ7+Fe7f0NFd
gc3KrrD8n2+iuwAXWGdEeFres1JVjLEDGM2UwmcUK3wOUUaaJHmGCyg2WylgWZ0l
DV7LlyQEaBpHIBxldQFHdPs44S/LtnGUxXTZHPuELVIGcLvQm/+GPt49m0tnVX4O
HmXJnEYdTaKYYvrJCLcec+jTfDp7wJlCNspqT1Wfaw+pthGr6uHyAdXcBzH3Cg1V
33ozhpRDxvolSYexvgLbH0dHlVl8P+sr0RZm7v8bB54qIrb//1UJBtlyJ5sl7/IR
rSEXSX3hC04a+BVoYAhzLf1ZVPp0sX+agKJQv8osHIMqze9If2nl8qE=
-----END CERTIFICATE-----</Attribute>
 <Attribute Name="SecurityCertificate.2#CertType">SEKM_SSL_CERT</Attribute>
</Component>
</SystemConfiguration>

5. Run the RACADM set command to import this SCP file which is located on a HTTP share
6. Ensure the SCP import job is marked as completed.

7. Check to validate iDRAC SEKM is enabled, SEKM SSL and KMS server certificates are installed.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sslcertview -t 7

Serial Number           : 6CBD418ED13004BDDF35008C8D3E3B4C

Subject Information:
Country Code (CC)       : US
State (S)               : MD
Locality (L)            : Belcamp
Organization (O)        : Gemalto
Organizational Unit (OU) : Not Available
Common Name (CN)        : KeySecure Root CA

Issuer Information:
Country Code (CC)       : US
State (S)               : MD
Locality (L)            : Belcamp
Organization (O)        : Gemalto
Organizational Unit (OU) : Not Available
Common Name (CN)        : KeySecure Root CA


Valid From              : Jun 23 14:05:47 2021 GMT
Valid To                : Jun 21 14:05:47 2031 GMT



C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sslcertview -t 6

Serial Number           : D3A4EE0676049B17ED51F94F89A5C185

Subject Information:
Country Code (CC)       : US
State (S)               : Texas
Locality (L)            : Round Rock
Organization (O)        : Dell EMC
Organizational Unit (OU) : ISG
Common Name (CN)        : RD24154_R640

Issuer Information:
Country Code (CC)       : US
State (S)               : MD
Locality (L)            : Belcamp
Organization (O)        : Gemalto
Organizational Unit (OU) : Not Available
Common Name (CN)        : KeySecure Root CA
```

```
Valid From              : Oct 20 19:29:08 2021 GMT
Valid To                : Oct 20 19:29:08 2022 GMT
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sekm getstatus
SEKM Status = Enabled
```

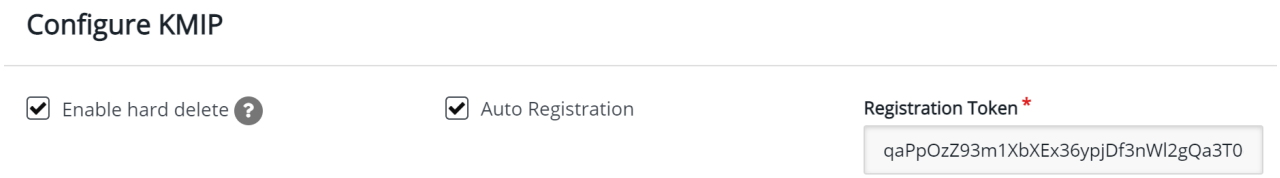
# 7 iDRAC initiated KMS key purge

This section describes the ability for iDRAC to purge unused keys at the Key Management Server (KMS).

As part of the SEKM solution, iDRAC allows users to rekey the secured storage devices on the server. Every time a rekey operation is request, iDRAC generates a new key at the KMS to rekey all the storage devices on the server to this newly generated key. The old key continues to remain at the KMS. Over time the number of unused keys at the KMS continues to grow – the problem gets compounded when users have multiple iDRACs with SEKM enabled.

1. Configure KMIP to delete keys

The following setting must be enabled on the CipherTrust Manager KMS so that when iDRAC requests a key to be deleted at the KMS the metadata associated with the key is also deleted. If this setting is not enabled, then the key is deleted but the key ID associated with the key is still retained and displayed at the KMS.




Note: This setting is not required on other supported Key Management servers.

2. Key Purge Policy

iDRAC will provide a policy setting that will allow users to choose if they wish iDRAC to purge old unused keys at the KMS when they perform a Rekey operation. iDRAC attribute KMSKeyPurgePolicy can be set by the user to one of the following values:

- **Keep All Keys** – this is the default setting and is the existing behavior where iDRAC will leave all the keys on the KMS untouched.
- **Keep N and N-1 keys** – iDRAC will delete all keys at the KMS except the current (N) and previous key (N-1).

Below is an example of setting this attribute using the RACADM interface.

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.SEKM.KMSKeyPurgePolicy

[Key=idrac.Embedded.1#SEKM.1]

KMSKeyPurgePolicy=Keep All Keys

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.SEKM.KMSKeyPurgePolicy "Keep N and N-1 Keys"

Object value modified successfully

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.SEKM.KMSKeyPurgePolicy

[Key=idrac.Embedded.1#SEKM.1]

KMSKeyPurgePolicy=Keep N and N-1 keys

On a Rekey operation, iDRAC will check the policy and purge keys as per the policy and log a message to LCL to indicate success or failure.

Below is an example of a LC log entry after a Rekey operation with the Purge policy set to “Keep N and N -1 keys”:

| | |
|---|---|
| SEKM036 | The Key Purge operation is successfully completed at the KMS. 5 keys are purged. |

3. Purge Old keys

Once iDRAC key purge policy is set, iDRAC will tag keys it generates using the server service tag. This allows iDRAC to identify keys that it has generated and purge them. But users may have keys generated by an older firmware version of iDRAC that do not have a server service tag associated with them. To purge such keys iDRAC attribute KMSPurgeOldKeys has been added with a default value of Disabled. Users can set the value of this attribute to Enabled and when they perform a Rekey operation, iDRAC will delete all old keys it has access to that do not have a server service tag associated with them. Once iDRAC is done with the delete process, it will reset the value of this attribute back to Disabled.

**Warning**: If users have shared keys between different iDRACs or if the keys from other iDRACs are in the same KMS Domain all such keys will be deleted.

Below is an example of setting this attribute using the RACADM interface.

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.SEKM.KMSPurgeOldKeys

[Key=idrac.Embedded.1#SEKM.1]

KMSPurgeOldKeys=Disabled

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn set idrac.SEKM.KMSPurgeOldKeys "Enabled"

[Key=idrac.Embedded.1#SEKM.1]

Object value modified successfully

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.SEKM.KMSPurgeOldKeys

[Key=idrac.Embedded.1#SEKM.1]

KMSPurgeOldKeys=Enabled

**NOTE**: Make sure the user that represents your iDRAC on the KMS is not configured as a Key Admin during KMSPurgeOldKeys operation.

4. KMS Key Purge on SEKM disable

This section describes ability for iDRAC to purge unused keys at the Key Management Server (KMS) when SEKM is disabled.

As part of the SEKM solution, iDRAC allows users to disable SEKM on iDRAC. Once SEKM is disabled on iDRAC, the keys generated by iDRAC at the KMS are unused and remain at the KMS. This feature is for allowing iDRAC to delete those keys when SEKM is disabled.

iDRAC will provide a new option “-purgeKMSKeys” to existing legacy command “racadm sekm disable” which will let users purge keys at the KMS when SEKM is disabled on iDRAC.

**NOTE**: If SEKM is already disabled and you want to purge old keys, you must re-enable SEKM, then disable passing in option -purgeKMSKeys

Below is an example of running this command using the RACADM interface.

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn sekm disable -purgeKMSKeys

On a SEKM disabled operation, iDRAC will check the additional option and purge keys which are tagged with server service tag, log a message to LCL indicating success or failure. Old keys that were generated with no server service tag can be deleted by iDRAC as part of SEKM disabled if user sets the KMSPurgeOldKeys attribute to Enabled.”

# 8 Troubleshoot issues while setting up SEKM on iDRAC

This section addresses some of the common issues encountered when using SEKM.

## 8.1 I installed the SEKM license, but I cannot enable the SEKM on iDRAC?

Make sure you update the iDRAC firmware after you install the SEKM license. This is required even if you had a SEKM supported iDRAC firmware version prior to installing the SEKM license.

## 8.2 I set up the KMS information and uploaded SEKM SSL certificates, but I am still unable to enable SEKM on iDRAC?

There are many possible reasons why iDRAC is unable to enable SEKM. Check the SEKM enable job Config Results for information about the job failure. Also, check the Lifecycle Controller logs for possible reasons for failure to enable SEKM. Also, check the following SEKM settings:

- Ensure that the:
  - Primary and Redundant KMS IP addresses are correct
  - Primary and Secondary KMIP port numbers are correct.
  - KMS CA certificate is the same as the one used to sign the KMS Server certificate.
  - CA used to sign the iDRAC CSR is in the Trusted CA list on the KMS server.
  - SSL Timeout value is large enough to allow iDRAC to be able to establish the SSL connection to the KMS.
  - User name of the iDRAC account on the KMS is entered in the correct field—It should match the value chosen in the “Username field in the Client Certificate” authentication property on the KMS.
- If the “Require Client Certificate to contain Source IP” option is enabled on the KMS then ensure that the iDRAC CSR contains the IP address in the **Common Name** field.

## 8.3 I am unable to switch PERC to SEKM mode?

- Make sure the PERC firmware has been upgraded to a version that supports SEKM.
- Make sure the SEKM status on iDRAC is Enabled. You can use the “***racadm sekm getstatus***” command to see the current SEKM status.

## 8.4 I set up SEKM on iDRAC and PERC and rebooted the host, but PERC shows the Encryption Mode as SEKM Failed?

The primary reason for this is that the PERC could not get the key from the iDRAC. In this case the iDRAC SEKM status will change to Failed. Therefore, refer to the troubleshooting tips mentioned earlier and make sure iDRAC can communicate to the KMS.

## 8.5 I checked the SEKM status on iDRAC and it shows “Unverified Changes Pending”. What does that mean?

This means that changes were made to the SEKM settings on iDRAC, but these changes were never validated. Use the racadm command “***racadm sekm enable***” to enable SEKM to ensure that iDRAC can validate the changes made and set the SEKM status back to either Enabled or Failed.

## 8.6 I changed the KMIP authentication settings on the KMS and now iDRAC SEKM status has changed to “Failed”?

- If you changed the user name or password of the iDRAC account on the KMS then make sure you change the corresponding properties on the iDRAC as well and enable SEKM.
- If you changed the value of the “Username field in the Client Certificate” option on the KMS, then you need to generate a new CSR from iDRAC by setting the appropriate CSR property to the username, get the CSR signed by the KMS CA and then upload it to iDRAC. For example, if you change the value of the “Username field in the Client Certificate” option on the KMS from “Common Name” to “Organizational Unit” then generate a new CSR by setting the OU property to the iDRAC KMS username, sign it using the KMS CA and then upload it to iDRAC.
- If you enabled the “Require Client Certificate to contain Source IP” property on the KMS then generate a new CSR by selecting the “Include iDRAC IP Address in CSR”, sign it using the KMS CA and then upload it to iDRAC.

## 8.7 I moved a SED from one SEKM enabled PERC to another SEKM enabled PERC on another server and now my drive shows up as Locked and Foreign. How do I unlock the drive?

Because each iDRAC is represented on the KMS by a separate user account, the keys created by one iDRAC are by default not accessible to another iDRAC. To enable the other iDRAC to get the key generated by the first iDRAC and provide it to PERC to unlock the migrated SED, create a Group to include the two iDRAC usernames and then give the key group permissions so that the iDRACs in the group can share the key. The steps to do this for the Gemalto KeySecure are described below.

1. Log in to the KeySecure Management Console and click **Users and Groups** → **Local Users and Groups**.
2. To create a new group, click **Add** in the **Local groups** section.
3. Select the newly created group and click **Properties**.
4. In the **User List** section, click **Add**, and then add both the iDRAC user names to this group.
5. After the group is created, click **Security** → **Keys**.
6. Identify the key created by the first iDRAC using the iDRAC unique user name.
7. Select the key and click **Properties**.
8. Click the **Permissions** tab, and then click **Add** under **Group Permissions**.
9. Enter the name of the newly created Group in step 2 above.
10. Remove and insert the drive to initiate a key exchange.
    Now the second iDRAC should be able to get the key and provide it to PERC to successfully unlock the drive. The SED should appear as Foreign and Unlocked, and now you can import or clear the foreign configuration on the drive.

The steps to do this for the CipherTrust Manager k170v are also described below.

1. Log in to the CipherTrust Manager and click **Keys and Access Management** -> **Groups.**
2. To create a new group, insert the name of your new group in the **Create New Group** section, then click **Add.**
3. Select your newly created group and add the desired users to the group.
4. After the group is created and the users are added, click **Keys** to identify the key you want to be shared between iDRACs.
5. Select the desired key, click **Edit** then find your newly created group and add the key to the group, then click **Update.**

## 8.8 I moved a SEKM enabled PERC to another server and now my PERC encryption mode shows as SEKM Failed. How do I enable SEKM on the PERC?

Follow the steps outlined in I moved a SED from one SEKM enabled PERC to another SEKM enabled PERC on another server and now my drive shows up as Locked and Foreign. How do I unlock the drive? and restart the host.

## 8.9 What key size and algorithm is used to generate the key at the KMS?

In this release, iDRAC uses the AES-256 to generate keys at the KMS.

## 8.10 I had to replace my motherboard. How do I now enable SEKM on the new motherboard?

After a mother board replacement, the Easy Restore feature will restore the SEKM license and all SEKM attributes to the newly replaced iDRAC. But it will not restore the SEKM certificates as these are iDRAC specific.

1. Update the iDRAC firmware to a version that supports SEKM. This is irrespective of the version that came with the new iDRAC.
2. Generate a CSR on the new iDRAC, get it signed by the KMS CA, and then upload it to the new iDRAC.
3. Upload the KMS CA certificate to iDRAC.
4. Enable SEKM on the new iDRAC.
5. Ensure that the job is successfully completed.

## 8.11 I replaced a SEKM enabled PERC with another PERC and now I see that the new PERC encryption mode is None. Why is the new PERC encryption mode not SEKM?

On a Part Replacement, iDRAC will set the encryption mode of the new PERC to SEKM only if the firmware version on the new PERC is SEKM capable. Make sure that the replacement PERC has a firmware version

that supports SEKM. If not, then perform a firmware update of the PERC to a version that supports SEKM and then check the PERC encryption mode.

## 8.12 I replaced a SEKM enabled PERC and now I see that iDRAC has generated a new key. Why was the key from the original PERC not used?

Each PERC needs its own key for SEKM – so when a PERC is replaced the new PERC will request iDRAC to create a new key and it will use the old key to unlock the drives and then rekey them with its own new key. Hence you will see iDRAC creating a new key after PERC part replacement.

## 8.13 I am unable to rollback iDRAC firmware – what could be the reason for rollback to be blocked?

Make sure that there are no storage devices that are in SEKM mode. iDRAC will block a rollback to a version that does not support SEKM if there are any storage devices that are in the SEKM mode. This is to prevent data lockout since after rollback iDRAC will not be able to provide keys to the storage devices to be unlocked.

## 8.14 I rebooted the host and key exchange failed because of a network outage and the PERC is in SEKM failed state. The network outage has been resolved – what do I need to do to put PERC back in SEKM mode?

Ideally, you do not have do anything because iDRAC will periodically try to connect to the KMS. After the network is started, iDRAC should be able to connect to the KMS, get the keys and provide them to PERC, and put it back in the SEKM mode. After five minutes, if the PERC is still in SEKM Failed state then reboot the host and check if key exchange is successful.

## 8.15 I would like to change the keys on a PERC—is that possible?

Yes, iDRAC allows a rekey operation, with which, you can rekey all storage devices supported for SEKM or a specific storage device. These rekey operations are supported by using either iDRAC GUI, RACADM, or Server Configuration Profile (SCP).

## 8.16 I did a system erase, but the PERC encryption mode continues to show as SEKM

This is an expected behavior—system erase does not change the encryption mode of the storage controller. To delete security on the PERC, use any of the supported iDRAC interfaces and switch the PERC encryption mode to **None**.

## 8.17 I cannot switch PERC to SEKM mode when it is in LKM mode

This is an expected behavior—switching from LKM to SEKM mode is currently not supported.

## 8.18 I migrated an SED, locked by a PERC in LKM mode, to a PERC in SEKM mode. The drive is indicated as Locked and Foreign. Why was it not unlocked?

This is an expected behavior. Because the SED was locked by a PERC in LKM mode, it must be unlocked manually by providing the LKM passphrase by using any of the IDRAC interfaces. After unlocking, the foreign configuration on the drive can be imported, and then the drive will be locked by the SEKM key.

## 8.19 I cannot switch PERC to SEKM mode when it is in eHBA personality mode

This is an expected behavior. In eHBA personality mode, the SEKM encryption mode is not supported.

## 8.20 Where can I get more information about any type of failures when setting up SEKM or for key exchange failures, successful key exchanges or rekey operations?

In all these cases, refer to the iDRAC Lifecycle logs for detailed log entries. Alongside checking iDRAC Lifecycle logs for detailed log entries, check logs on the key management server for any key exchange activity.

## 8.21 Will SEKM key exchange functionality continue to work after I delete the SEKM license?

Yes, SEKM key exchange will continue to work even if the SEKM license is deleted.

**NOTE**: Updating the iDRAC firmware without a SEKM license will cause iDRAC to lose SEKM functionality. To recover from this, re-install the SEKM license and update the iDRAC firmware again to restore SEKM functionality.

## 8.22 Will SEKM key exchange functionality continue to work after an iDRAC reset?

SEKM key exchange will continue to work after a racreset, as long as the SEKM attributes and certs on iDRAC are still valid.

**NOTE**: racresetcfg will be blocked while SEKM is enabled. To perform a racresetcfg operation, you will need to disable SEKM on iDRAC first.

## 8.23 SEKM key exchange failed after a warm reboot but the drives part of my secured volumes are still online and secured?

Drives will not lose power on a warm reboot and will stay Online and Unlocked. Only during a cold reboot will the drives lose power and become Foreign and Locked.

# A Technical support and resources

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