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.

September 2020
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2019</td>
<td>Initial release</td>
</tr>
<tr>
<td>June 25, 2020</td>
<td>Added procedures related to KeySecure Classis, Thales Data Security Manager (DSM), and Next Generation KeySecure</td>
</tr>
<tr>
<td>September 2020</td>
<td>Added extra information about including IP information during setup and configuration</td>
</tr>
</tbody>
</table>
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

Other—N/A
Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

Contents

1 KeySecure Classic (k150v) .................................................................................................................................................. 7
   1.1 Prerequisites for KeySecure Classic .......................................................................................................................... 7
   1.2 Set up SEKM on KeySecure Classic ............................................................................................................................. 7
   1.3 Set up SEKM on iDRAC ................................................................................................................................................. 8
   1.4 Configure SEKM by using the iDRAC GUI .................................................................................................................. 9
      1.4.1 Get the CSR file signed on KeySecure Classic ..................................................................................................... 9
      1.4.2 Download the server CA file from KeySecure Classic and upload to iDRAC ................................................. 10
      1.4.3 Configure the Key Management Server (KMS) settings on iDRAC ................................................................. 14

2 Enable SEKM by using the iDRAC PERC ...................................................................................................................... 17
   2.1 Ensure that SEKM is enabled on iDRAC PERC ........................................................................................................ 19

3 Thales Data Security Manager (DSM) ............................................................................................................................ 20
   3.1 Prerequisites for Thales Data Security Manager (DSM) .......................................................................................... 20
   3.2 Set up SEKM on Thales DSM .................................................................................................................................. 20
      3.2.1 Add a new host in Thales Vormetric Data Security Manager ........................................................................ 20
      3.2.2 Set up SEKM on iDRAC ..................................................................................................................................... 21
      3.2.3 Configure SEKM by using the iDRAC GUI ......................................................................................................... 21
      3.2.4 Get for a CSR file to be signed by an external certificate authority ............................................................. 22
      3.2.5 Upload the signed CSR to Thales DSM ............................................................................................................. 24
      3.2.6 Download the Root CA that has signed the Thales DSM appliance and upload to iDRAC ......................... 25
   3.3 Configure the Key Management Server (KMS) settings on iDRAC ................................................................... 28
      3.3.1 Enable SEKM on the iDRAC PERC .................................................................................................................. 28
      3.3.2 Ensure SEKM is enabled on iDRAC PERC ......................................................................................................... 31
      3.3.3 Viewing Key ID on Thales DSM ......................................................................................................................... 31

4 Next Generation KeySecure (k170v) ........................................................................................................................... 32
   4.1 Prerequisites for Next Generation KeySecure ........................................................................................................ 32
   4.2 Set up SEKM on Next Generation KeySecure ......................................................................................................... 32
      4.2.1 Configure Auto-Client Registration .................................................................................................................. 32
      4.2.2 Configure KMIP Interface .................................................................................................................................. 36
   4.3 Configure SEKM by using the iDRAC GUI ................................................................................................................ 43

Executive summary ........................................................................................................................................................................... 6

Acknowledgements ................................................................................................................................................................................... 3

Revisions............................................................................................................................................................................................................. 2
4.5 Get the CSR file signed by Next Generation KeySecure .................................................................45
4.5.1 Download the server CA from Next Generation KeySecure and upload to iDRAC ..................47
4.6 Configure the Key Management Server (KMS) settings on iDRAC ..................................................48
4.7 Enable SEKM on the iDRAC PERC ..................................................................................................49
4.8 Ensure SEKM is enabled on iDRAC PERC ......................................................................................51
4.9 Viewing the iDRAC key ID on Next Generation KeySecure .............................................................51
5 Troubleshoot issues while setting up SEKM on iDRAC .................................................................52
5.1 I installed the SEKM license, but I cannot enable the SEKM on iDRAC? ........................................52
5.2 I set up the KMS information and uploaded SEKM SSL certificates, but I am still unable to enable SEKM on iDRAC? .................................................................52
5.3 I am unable to switch PERC to SEKM mode? ..................................................................................52
5.4 I set up SEKM on iDRAC and PERC and rebooted the host, but PERC shows the Encryption Mode as SEKM Failed? ..................................................................................52
5.5 I checked the SEKM status on iDRAC and it shows “Unverified Changes Pending”. What does that mean? 53
5.6 I changed the KMIP authentication settings on the KMS and now iDRAC SEKM status has changed to “Failed”? .................................................................53
5.7 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? ..........53
5.8 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? ............................................................54
5.9 What key size and algorithm is used to generate the key at the KMS? .............................................54
5.10 I had to replace my motherboard. How do I now enable SEKM on the new motherboard? ..........54
5.11 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? ........................................54
5.12 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? ..................................................................................54
5.13 I am unable to rollback iDRAC firmware – what could be the reason for rollback to be blocked? ....55
5.14 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? ..................................................................................55
5.15 I would like to change the keys on a PERC—is that possible? ..........................................................55
5.16 I did a system erase, but the PERC encryption mode continues to show as SEKM .........................55
5.17 I cannot switch PERC to SEKM mode when it is in LKM mode .....................................................55
5.18 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? ........................................................................55
5.19 I cannot switch PERC to SEKM mode when it is in eHBA personality mode .................................56
5.20 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? ........................................56

A Technical support and resources .............................................................................................................57
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
- PERC 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:

![Authentication Settings](image)

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
It is recommended that you enable this option only if the iDRAC IP address does not change frequently. If this option is enabled and the iDRAC IP address changes then the SEKM will stop functioning until the SSL certificates are set up again. If this option is enabled then ensure the same option is enabled on iDRAC also, as explained later in 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

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.

4. In the Generate Certificate Signing Request (CSR) dialog box, select or enter data.
5. Click Generate.
   The CSR file is generated.
KeySecure Classic (k150v)

6. Save it to your system.

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/jCAKeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GAIUECGwIRGYvbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAYBgNVBAMMEGlkcmFjdjXcXKcHAcBjAcBkqkhiGwU8BCQFED3Rl
c3RlckBkZXVsLmNbTCCASiwwDQYJKoZIhlczNAQEBBQADgEPADCCAQoCggEBBKnj
7m5g3h2z5rW9g95p5Nh5nSR7jgI+SMUqgI54UtnXXGku6a81kXXKX/cRIX9TOL
JcB4tq5kIF2dtXmAX6Eg+M18aVuz0EbfReD170mgwjgMgmRhidnIN1EyA+1WV
i/OlyeJ715knu4UpUGF1jcPvYUbD8pT11Z5bw3LotBk1rbLq1Hpi19K0g0jae
LPSXSGwv/k+cEoKuA4kuNAVFXmr3xB5ptGugkKneF92Y0boX4LLCHMFAcgp02
76vqTYAvn73oyiNMWep5hchyOTHqMBxzocYPeX01k7c4zmb3/aNjXSTSG1/KR4Zg
5VwDVJz+2ILLNyKC+5NCwEAAaApMCCG5qGSL3DQEJDJEmBwCCQGyBDV0UTBAlw
ADALBgNVQEBAMCBEaWDQYJKoZIhvcNAQEELBQADg0EBAD0K6LED0+uNioiBL7Na
V3t5lGma/I3sPy4bOoDQgNQ87NvOw/vqemZFlWn020c4/2Lklxv+bYYldH3+3
ewe4Znba5fkvXkPCrKw0/EuadtM928+pKlmF7840aVajyAXFhcaB335dtc4
Kt3m2jQQuv+eKDxG+xuvgSiwueEftZ2FJzsHUEUc16aH1cTuBhp5XiP/IUnmgF1A
Epl1GY9uwL57b160meRrvt1G2LkxSfaHVDwGmsQY/AB216U1CzpXx0a3y
kjw+SxEGos6JnYpT9yJXSCj2RmddB56ZUUUGD02DL7iALabQtfoVpjo9pFBD2lp
36A=
-----END CERTIFICATE REQUEST-----
1. Log in to Gemalto.
2. Click **Security Tab → Local CAs**.
3. Click **Sign Request**.

![SafeNet KeySecure Management Console](image)

**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**.

![Request for certificate signing on Gemalto](image)

**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.

![Download and save the CSR file on Gemalto](image)

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.

![Upload the signed CSR certificate by using iDRAC GUI](image)

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.

![Download from Gemalto GUI](image)

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.

![Upload to iDRAC GUI](image)

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.

   ![iDRAC Settings](image)

   **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
Enable SEKM by using the iDRAC PERC

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**.

![Enable SEKM on iDRAC PERC](image)

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**.
Enable SEKM by using the iDRAC PERC

8. Restart the server to run the configuration job.

![Information](image1)

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

![Maintenance](image2)

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.

![Maintenance](image3)

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

![StorageController](image)

**Figure 19** Ensure that SEKM is enabled on your controller
3. **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
- PERC 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*.

When you install and configure the appliance, include the IP address of the DSM as the hostname. Also include the IP address as the host name when generating a certificate authority on the DSM.

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

![Figure 21 Adding a new host in Thales Vormetric Data Security Manager](image)

*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 Get for a CSR file to be signed by an external certificate authority

---BEGIN CERTIFICATE REQUEST-----

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

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**.

![Download certificate](image)

**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.

![Upload signed CSR](image)

**Figure 25** Upload the signed CSR certificate on iDRAC GUI
3.2.5 Upload the signed CSR to Thales DSM

1. Select your host.

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 26 Select your host on Thales Vormetric Data Security Manager

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).

![Certificate (Invalid) Not Secure](image)

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**.

![View Certificate](image)

**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**.

![Certificate Export Wizard](image)

**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.

![KMS CA Certificate Upload](image)

**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**.

   ![SEKM Configuration](image)

   **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.

   ![Information](image)

   **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**.
4. From the **Security (Encryption)** down-down menu, select **Secure Enterprise Key Manager**.
5. Click **Add to Pending Operations**.

![Job Queue](image)

Figure 34 A job to enable SEKM is successfully completed

![Enable SEKM on iDRAC PERC](image)

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.

   ![Image of Job Queue page]

   **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.

   ![Image of 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

![iDRAC GUI Screenshot](image)

**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**.

![Thales DSM Screenshot](image)

**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 Next Generation KeySecure (k170v)

4.1 Prerequisites for Next Generation KeySecure
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
- PERC updated to the firmware version which supports SEKM

**Thales KeySecure k170v (KMS) Prerequisites**
- Configure KMIP interface
- Create a user that represents the iDRAC on the KMS

4.2 Set up SEKM on Next Generation KeySecure
This section describes the Thales KeySecure k170v features that are supported by iDRAC. For information about all other Thales features, see the Thales Appliance Administration Guide.

4.2.1 Configure Auto-Client Registration
1. Log in to the KeySecure appliance and click **KMIP (OASIS Key Management Interoperability)**.

![Figure 40 Start the OSASIS Key Management Interoperability (KMIP) application](image)

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

![Figure 41 Add Client Profiles in KMIP](image)
3. Enter or select data in the Add Profile dialog box.

![Add Profile](image1)

**Figure 42** Add profile information on KMIP

Note—For the Common Name (CN) field, a user with this name must already exist on the KeySecure appliance. In the example above, “iDRAC” has been created as a user prior to the creation of the profile. This user need not be added to a group.

4. Click Registration Token → New Registration Token.

![Registration Tokens](image2)

**Figure 43** Create a new registration token

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

![Create New Registration Token](image3)

**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**.

![Create New Registration Token](image1)

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**.

![Create New Registration Token](image2)

Figure 46  Select a profile for creating a new registration token

8. Copy the registration token.

![Copy registration token](image3)

Figure 47  Copy registration token

9. Click **Admin Settings**.
10. Click **System → Interfaces → Ellipses**.
11. Select the **Auto Registration** check box.
12. Paste the token that you copied into the **Registration Token** box.
13. Click Update.

![Configure KMIP](image)

**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.

14. Restart the KMIP services.

![Restart KMIP services](image)

**Figure 49** Restart KMIP services after configuring KMIP
4.2.2 Configure KMIP Interface

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

Figure 50 Create CSR on Thales

Note—By default, the Local Certificate Authority shown in the image is available.

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

Figure 51 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.

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)*

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.
8. Upload the externally generated CSR.

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

![Image of certificate upload process]

**Figure 55** Issue certificate on Gemalto

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

9. Click the ellipses (…) symbol, download the signed certificate, and then save it to your system.

![Image of certificate download process]

**Figure 56** Download CSR on Gemalto
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 screenshot here:

![Private Key](image)

Figure 57  Appending the private key on Gemalto
11. Save this file and upload it to the KMIP interface.
12. Upload signed certificate and private key to KMIP interface.
   a. Click **Settings → Interfaces → Interface Configurations**.

   ![Image of Interface Configurations](image)

   **Figure 58** Upload CSR and Private Key to KMIP by using Gemalto

   b. Click the ellipses symbol, and then click **Edit**.

   After you click **Edit**, the **Configure KMIP** screen is displayed.

   ![Image of Configure KMIP](image)

   **Figure 59** 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**.

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

   a. Click **Update**.
   b. Restart the KMIP service to apply the configuration changes.
   c. Click **Services → Restart KMIP**.

![System Services](image)

**Figure 60** Restart the KMIP service on Gemalto

### 4.2.3 Create a user that represents the iDRAC on the Next Generation KeySecure

1. Click Users → Create New User.

![Create a New User](image)

**Figure 61** Create iDRAC user on the next generation KeySecure

**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 Groups → Key Users.
   b. Add your newly created user to the group.

![Add new user to the group on Gemalto](image)

   c. After you select this group, a green color Add button is displayed.
   d. Click this button to add your user to the group.
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 Next Generation KeySecure 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**.

![Generate CSR on iDRAC](image)

**Figure 63** 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.

![Specify CSR properties on iDRAC GUI](image)

**Figure 64** Specify CSR properties on iDRAC GUI

7. Get the full CSR file contents signed on the Next Generation KeySecure.

8. Download the signed image file, and then upload it to iDRAC.
4.5 Get the CSR file signed by Next Generation KeySecure

1. Log in to Next Generation KeySecure.
2. Click CA → Local Certificate Authority.

![Certificate properties](image1.png)

3. Click Upload and Sign CSR.

![Issue certificate on Gemalto](image2.png)

Certificate Purpose: client
Next Generation KeySecure (k170v)

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”.

![Gemalto Certificate Management](image)

Figure 68  Edit and upload the CSR certificate on Gemalto

4. To upload the file you just got signed by Gemalto, 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 Next Generation KeySecure and upload to iDRAC

1. On the KeySecure UI, click **CA**.

   ![KeySecure UI](image)

   **Figure 69** 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.

   ![KMS CA Certificate Upload](image)

   **Figure 70** 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**.

![SEKM Configuration](image)

**Figure 71** 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.

![Information](image)

**Figure 72** Create job to Configure KMS on iDRAC

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

![Job Queue](image)

**Figure 73** 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**.

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**.

![Enable SEKM on iDRAC PERC](image-url)
8. Restart the server to run the configuration job.

![Information]

Figure 75  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.

![Job Queue]

Figure 76  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 77 Ensure SEKM is enabled on iDRAC PERC](image)

4.9 **Viewing the iDRAC key ID on Next Generation KeySecure**

![Figure 78 View iDRAC key ID on next generation KeySecure](image)

The SEKM setup operation is completed. You can now start creating locked RAID volumes and perform key exchanges.
5 Troubleshoot issues while setting up SEKM on iDRAC

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

5.1 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.

5.2 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.

5.3 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.

5.4 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.
5.5 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.

5.6 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.

5.7 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.
5.8 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.

5.9 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.

5.10 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.

5.11 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.

5.12 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.
5.13 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.

5.14 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.

5.15 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).

5.16 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.

5.17 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.

5.18 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.
5.19 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.

5.20 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.
A Technical support and resources

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