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.

June 2020
Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

<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>
</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
Support—Sheshadri PR Rao (InfoDev)
Other—N/A
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Executive summary</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>KeySecure Classic (k150v)</td>
<td>7</td>
</tr>
<tr>
<td>1.1</td>
<td>Prerequisites for KeySecure Classic</td>
<td>7</td>
</tr>
<tr>
<td>1.2</td>
<td>Set up SEKM on KeySecure Classic</td>
<td>7</td>
</tr>
<tr>
<td>1.3</td>
<td>Set up SEKM on iDRAC</td>
<td>8</td>
</tr>
<tr>
<td>1.4</td>
<td>Configure SEKM by using the iDRAC GUI</td>
<td>9</td>
</tr>
<tr>
<td>1.4.1</td>
<td>Get the CSR file signed on KeySecure Classic</td>
<td>10</td>
</tr>
<tr>
<td>1.4.2</td>
<td>Download the server CA file from KeySecure Classic and upload to iDRAC</td>
<td>14</td>
</tr>
<tr>
<td>1.4.3</td>
<td>Configure the Key Management Server (KMS) settings on iDRAC</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>Enable SEKM by using the iDRAC PERC</td>
<td>17</td>
</tr>
<tr>
<td>2.1</td>
<td>Ensure that SEKM is enabled on iDRAC PERC</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>Thales Data Security Manager (DSM)</td>
<td>20</td>
</tr>
<tr>
<td>3.1</td>
<td>Prerequisites for Thales Data Security Manager (DSM)</td>
<td>20</td>
</tr>
<tr>
<td>3.2</td>
<td>Set up SEKM on Thales DSM</td>
<td>20</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Add a new host in Thales Vormetric Data Security Manager</td>
<td>20</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Set up SEKM on iDRAC</td>
<td>21</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Configure SEKM by using the iDRAC GUI</td>
<td>21</td>
</tr>
<tr>
<td>3.2.4</td>
<td>Get for a CSR file to be signed by an external certificate authority</td>
<td>22</td>
</tr>
<tr>
<td>3.2.5</td>
<td>Upload the signed CSR to Thales DSM</td>
<td>24</td>
</tr>
<tr>
<td>3.2.6</td>
<td>Download the Root CA that has signed the Thales DSM appliance and upload to iDRAC</td>
<td>25</td>
</tr>
<tr>
<td>3.3</td>
<td>Configure the Key Management Server (KMS) settings on iDRAC</td>
<td>28</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Enable SEKM on the iDRAC PERC</td>
<td>28</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Ensure SEKM is enabled on iDRAC PERC</td>
<td>31</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Viewing Key ID on Thales DSM</td>
<td>31</td>
</tr>
<tr>
<td>4</td>
<td>Next Generation KeySecure (k170v)</td>
<td>32</td>
</tr>
<tr>
<td>4.1</td>
<td>Prerequisites for Next Generation KeySecure</td>
<td>32</td>
</tr>
<tr>
<td>4.2</td>
<td>Set up SEKM on Next Generation KeySecure</td>
<td>32</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Configure Auto-Client Registration</td>
<td>32</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Configure KMIP Interface</td>
<td>36</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Create a user that represents the iDRAC on the Next Generation KeySecure</td>
<td>41</td>
</tr>
<tr>
<td>4.3</td>
<td>Set up SEKM on iDRAC</td>
<td>43</td>
</tr>
<tr>
<td>4.4</td>
<td>Configure SEKM by using the iDRAC GUI</td>
<td>43</td>
</tr>
</tbody>
</table>

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

4.5 Get the CSR file signed by Next Generation KeySecure

4.5.1 Download the server CA from Next Generation KeySecure and upload to iDRAC

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

4.7 Enable SEKM on the iDRAC PERC

4.8 Ensure SEKM is enabled on iDRAC PERC

4.9 Viewing the iDRAC key ID on Next Generation KeySecure

4.10 Troubleshoot issues while setting up SEKM on iDRAC

A Technical support and resources
Executive summary

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.

**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.
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/jCCAeYCAQAwY8vCzAJBgNVBAYTAlVTM4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwBwKm91biBhQWU9jazEMRA8GA1UECgwIRGVYsbCBFTUMxDTALBgNVBAsMBFRl
c3QtGTAkBgNVBAMMEG1kcmFjXcnlzdXMwIzA0MQYDVQQDDAVTbyAEMwIwYDVQQFBKkg
S3JhZ2luMjw0MDEwNTA5Njc2MDAwMDBd
-----END CERTIFICATE REQUEST-----
```

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

-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwY8vCzAJBgNVBAYTAlVTM4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwBwKm91biBhQWU9jazEMRA8GA1UECgwIRGVYsbCBFTUMxDTALBgNVBAsMBFRl
c3QtGTAkBgNVBAMMEG1kcmFjXcnlzdXMwIzA0MQYDVQQDDAVTbyAEMwIwYDVQQFBKkg
S3JhZ2luMjw0MDEwNTA5Njc2MDAwMDBd
-----END CERTIFICATE REQUEST-----

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

---

Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers
1. Log in to Gemalto.
2. Click Security Tab → Local CAs.
3. Click Sign Request.

![SafeNet KeySecure Management Console]

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**.

![Image of SafeNet KeySecure Management Console](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.

**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.

![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.

![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 GUI Screenshot](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.

![Image of Lifecycle Logs](image1.png)

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

![Image of iDRAC SEKM configuration](image2.png)

**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.

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.

![Image of Job Queue with successful job entry](image1)

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

![Image of Job Queue with scheduled job entry](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.

![Image of Job Queue with completed job entry](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

![Integrated Dell Remote Access Controller 9](image)

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
- 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.

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**.

![Add Host](image)

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 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 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 the signed CSR certificate on iDRAC GUI](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.

![Select host](image1.png)

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.

![Select host](image2.png)

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 dialog](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**.

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 29** View Root CA

**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**.

![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.

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](image)

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](image)

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)**.

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

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

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

![Add Profile Dialog Box]

**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 Dialog Box]

**Figure 43** Create a new registration token

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

![Create New Registration Token Dialog Box]

**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.png)

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.png)

Figure 46 Select a profile for creating a new registration token

8. Copy the registration token.

![Create New Registration Token](image3.png)

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.

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

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

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

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.

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.

Copy CSR content on Gemalto

Figure 53: Copy CSR content on Gemalto

4. Click both the buttons.

5. 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.

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.

Copy CSR content on Gemalto

Figure 54: Upload and Sign CSR on Gemalto

Figure 52: Saving CSR and Private Key

You must save the Private Key to continue.

Save Private Key

Save CSR

Encrypt Private Key

Size—2048

Algorithm—RSA

Name box:
8. Upload the externally generated CSR.

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

![Image of CSR upload](image1)

**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 CSR download](image2)

**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 screen shot here:

```
---- BEGIN CERTIFICATE -----
MIIEczCCAhugAwIBAgIRAKubYrTdTINhmT+9cxtLR8xGQKxQKoZUhvcnANTELBAwQg
WjEzELM0GA1UEBhMCVVMxICA3BjBwVBAgTAkkEMRAoVGYDVQFHBwCzAChjYwVQMARe
Dy9YVQQKExdH2J1bHRiMaRwOQAYVQQDEXFLXZITmZ1cmMgUm5vdBGQFAAeFwIDAQAB
MDAxNTY2MIEiNNTyFwYnAToTbMDIzNNTN8BkFxIAVBgNBAMDdjJwEME43MS4y
NTIuZwxEZI0IjNABkbghakj1G6gwBwAQFEAAACQ8AM1BIGkCIDEA9hUG6Q33rbrw
J3Hzx1hJKXMarkJGDX16Hb22q1zlUbrkkrFujCBnUQkTV4oA2V6yVMXkotBuwh
IckZwKvVgylxUSC7LGDD1YyID5Q6uswPwEprWvfuqUprXIR1FvQvLxQ5nXbHrS2d1xw0s9o9ahVXB
+nFqEO9m5Tj52Phz7shhGud1vDokBGMLQJ9z1c1ebf/
6AcdkezPAEGO18h8k0pe08Jfr2f2q9yMLX4LsM5hMnulAovy61t7bAQBVql7Yf1d40RikIhpbw9VRqY5il5sIDgk/d+HMeZg1D9g9crj
+0vOz2v/DkNODXcL8p45ylFp1hrRZP2seY5wIDAQbc0zUmuoZBGsNQVQAE8BEBCAAgAvCyYDVR01BAwMGiYKvYb
BQJUHauEmDVYDRYR5Qj49/BA1wDANBqgkqkHg0vBA0sFAA3CAeg342d4a9m9h/9wUh0khnFCq5SRNTRJ
+3McnaFhL3i2VQ3qz0CMFhjsd/FDFDtbW0KRo0
2TFrR4AY50kaluPigPl5WyH352b/5J5M3eqvmmxtzAnnRKG/1XPbgkVCR3s4/fL0
Oc4nLKbgksG46ggv8AYX6V5ONmfaOd3BnmCNuyCrcBr+B4wummmLau5pNrJwECYcH18pcsu3g1InIHpccfr
+yU3JSTX99enNhPh7JD7Ljtsr+rd0eU61oJFccu1upPciscXRzlq1tq5FyYNQ4wnbH8Z10dCVGCcH157hOhS8h3f79y12twXwYMYxjBb
s1a5a5EB1eyv/3u3vKXQX72nq2opD7GNNvcs115j8e7b225s30OGKX1akOmncf1y4QT61c25Fscftg9mktfQ8r18/9w2kIA9a
+hXK93h/bq801TqDy14DA4w+3nh7c7wG7o1/djGx7YSsF7z23Fk49a4687/2pgmbsntavJLzLctYYY7rGF2KyyR
7+i6FiosMmLhoCoL8s6VX73DUARfcrBc7hUjCk3gapRbt8Jx5EjlLmg53s17
Rw3N3jhtZG6szgMvFD88nmd2Z0EELr1JC9AmCv6qTpe4E3me5zrF7o1tbvNAO6hG8y7ntc7H7HuBy80yTr9g6EED0nSp88k----END
CERTIFICATE-----
---- BEGIN RSA PRIVATE KEY -----
MIIEpAIBAAKQgAE0n69g8xBRbrweJHtuxJUXMarkJGDX16Hb22q1zlUbrkkr
fujCBnUQkTV4oA2V6yVMXkotBuwh
+0vOz2v/DkNODXcL8p45ylFp1hrRZP2seY5wIDAQbc0zUmuoZBGsNQVQAE8BEBCAAgAvCyYDVR01BAwMGiYKvYb
BQJUHauEmDVYDRYR5Qj49/BA1wDANBqgkqkHg0vBA0sFAA3CAeg342d4a9m9h/9wUh0khnFCq5SRNTRJ
VY7mAk2s3mHbC4pCAM0OAxK5qjL7s277uJ112m/80mQ7q
VmyyoeKk84cCAHAYLXlXK60lbbasxcJ0xbqdpqVwp06fA6g9eK97Xw0tuw+X4mcXh1m3013ON3m+Zv46mgtJG6sUP3Q7
+yDikv43d74x7y6QxLqrdX3E5US0301AyMXEQG3AE131E8Xt8ku0C7MN820kx51+v5YDyKvj89lN92Chs3HufAr13m
P2SFLXkx0bWwNz565ZmKvep5y/cem64AQLbiWf3J3kE6670J9lq9BuPy7YQ10c69r3F
685cB9ag2jX53so5tF27zjK681BRCXN00vaWV0k7UQo7hLuSjtZJzk3EYAGhS
RJxtrlvAn03aj32Bi40b48wPy76G91h6edzjris2b6DG0G7Xe00OtmovA977755Av
HX4N4OY2IkdfkTctk10hnLumrnhMrk6/p3MkY6GTI135w5e/Khalha
MtwkE4URQMA53pEJ6c3Q030PTY6E5FCcoxxsGrEaEa+8BLyLs+Y5B1t17jZ7/nR5SB+5t7KT+3K57VAXvZLoVvNC/x
+yomgCMWkKc/cdG5xU11nto9+d905U35C17U1R9r37987G6NDBn1C9656b04QDc10L669g9j6twXMAA
9y3c63b8PvK8RcP+ossx2EgYAnbkbavAi358Hh4gzz+9NBhJlyhHsf8r+37Ttd0
821LJJgjompE7NieeQnK1Zm61nF0v19G05Ll/nv0QJyfyFCcO02VKnkJt5fF36eGdS
x2101T1hXckMuQdt0Q106S151Ta7a46s+803+3Fg+9PS5P6bx5Qg3yUp
SWogScGybaGAcAcS9m9vM7ta+Y97y39C0KXs6sFMxpp+m+yJY3s4AhMhUtZ71.0L
EUNmShsTw308b7j7UpfH88b0K candidatesDl32m992USF9eStegQ0cyrcXhYrLDkR01kInSKEB3EEZ0mevq
+yXHNgGw1vHhc2ZXeMSuVABdAtt3sG4uXa----END RSA PRIVATE KEY-----
```

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.

   ![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.

   ![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**.

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

1. Click **Users → Create New User**.

**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.
   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](image1)

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](image2)

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

-----BEGIN CERTIFICATE REQUEST-----
MTIC/3CCAeTCAeAwY860gY6aM2p7Ca9BqyVWbTA1Y1THQcWBt974yQ7WTQG3AIVM3VEhDWEKcGAgMBAAECAY enforceSv2eQZ8oQaNG/5jnnSEUR/62G1QUPgqY5yG715VY3eCBFVvQa92ZIALQgNVhAmEfR1
526G9Xk2gYb9VWbMG/1vc0fbG0G81cR10c0BCVzQ5cjAc8Cq6G95CGWJ80BCG5MvUL1
z05LeuBkxVXaLeNh9b2CCLS1nQOQJYk2l4vDHQ6N8BQAeZgZDADECCQIzC7yEBEHk-j
7ue5HsU5jv39uhEpEn5hbSS77j1QfH4eUQ5Q5GUSa8S1fQkx/cBKSTqCL
J3m64049g1kFZyX9A65qH+M16Av4u0KhRAxM177/mqorqg6g0r4d1d156J6441YW
1i/QyEyJ711JhKu4OqUt1jycyYubhSdp1fI1f5boCJ5cBk1ibLqHypY1c9k3kqjse
LXG6Agv/1k0+nHkEiAokrjWA/DKmx3z8ptCnq6kRna92fI9Box4ILcOHItFACmgs
7v9e9ZIvNhV79Oykn5u6ehyo9Tnzg6xKaoofPGlC15k7e3xmb9/oaMjZ7TGG1/9542g
SWX1U4mmZ1HN/cRHCsZ0CveA4ApNOC6ScQsPS61S0OMJhEahB4goCQYV7R0T8Ew
ADMLBqYKVQ4EBXhCEoeoQ4jVcZKhvQAXELBQD9gEBADJ6kLED0+uhMoi8IL7Na
Y3z5L0ma/15yX4k5oaD0uqNQ87Yo60Vv/qercZEmH0020/cZLFnxv4+bYfGC3H+
Cwv4z02EnaS4FctXc1DxCHk0/EIAmTeH928+pXKm1F7840aAlJlyAVFhca83SHc4t
cX3mEJQ5VU7+eKDiW+x8ruq5lCw6FZ12FJz0rHm0c1e6aR1cTbmn5X1P/IDa1qFIA
kplL6X9uwL71616LmmwEvP1il2L6eFzaHVF16mrsST/AN21KIDC8zXzFQ2gaSy
k'action='57YeO65JHYpt5Yno3Cj2RnndBD62YV0D05Z7iALsUbKzfcovLpjo3pB621p
6ea-----END CERTIFICATE REQUEST-----

Figure 65 CSR certificate signed by next generation KeySecure

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

Figure 66 Copy Local Certificate properties

3. Click Upload and Sign CSR.

Figure 67 Issue certificate on Gemalto

Certificate Purpose: client

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

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”.

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.

![Download CA and upload to iDRAC](image)

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.

![Upload KMS CA certificate to iDRAC](image)
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.
8. Restart the server to run the configuration job.

![Image of information message](image1)

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.

![Image of job queue](image2)

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

![Controller Information](image)

Figure 77  Ensure SEKM is enabled on iDRAC PERC

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

![Key Information](image)

Figure 78  View iDRAC key ID on next generation KeySecure

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