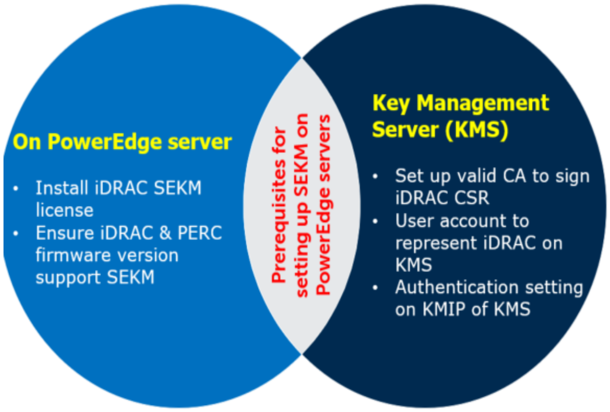
Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

This Dell EMC technical white paper describes the process of enabling SEKM on iDRAC, PERC of PowerEdge servers. Key tips and troubleshooting techniques for using SEKM are also discussed.


On PowerEdge server
• Install iDRAC SEKM license
• Ensure iDRAC & PERC firmware version support SEKM
Prerequisites for setting up SEKM on PowerEdge servers
Key Management Server (KMS)
• Set up valid CA to sign iDRAC CSR
• User account to represent iDRAC on KMS
• Authentication setting on KMIP of KMS

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 technical white paper provides step-by-step procedure to set up SKEM on iDRAC by using GUI, RACADM and SCP. Also, a few important tips and troubleshooting steps are provided to help you effectively use this SEKM on your PowerEdge servers.

July 2019

Dell EMC Technical White Paper

Revisions

Date	Description
July 2019	Initial release

Acknowledgements

This technical white paper was produced by the following members of the Dell EMC Enterprise Server Solutions team:

Author—Sanjeev Dambal and Texas Romer

Support—Sheshadri PR Rao (InfoDev)

Other—N/A

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary

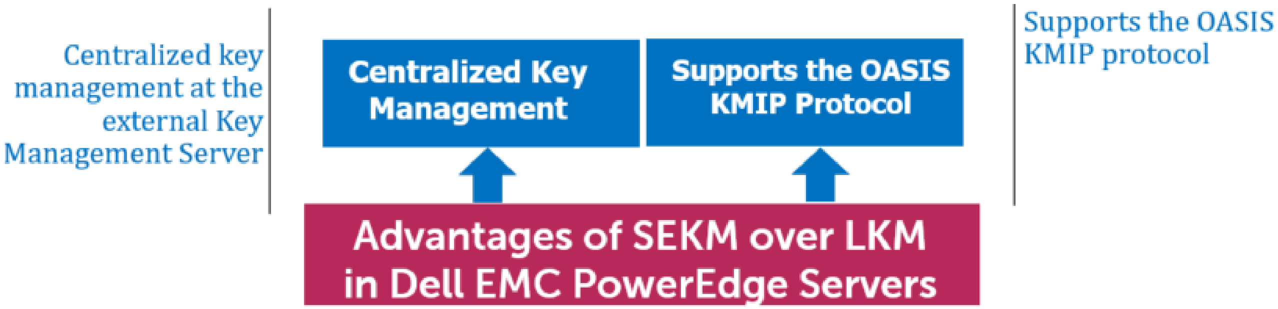

Centralized key management at the external Key Management Server
Centralized Key Management
Supports the OASIS KMIP Protocol
Supports the OASIS KMIP protocol
Advantages of SEKM over LKM in Dell EMC PowerEdge Servers

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

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

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

- In addition to the LKM–supported “Theft of a SED drive” use case, SEKM protects from a “Theft of a server” use case. Because the keys used to lock and unlock the SED drives 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.

This white paper uses the Gemalto KeySecure as an example of a Key Management Interoperability Protocol (KMIP) Key Management Server, but the workflows described in this technical white paper are applicable for any KMIP compatible KMS, which has been validated for use with PowerEdge SEKM.

Prerequisites

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

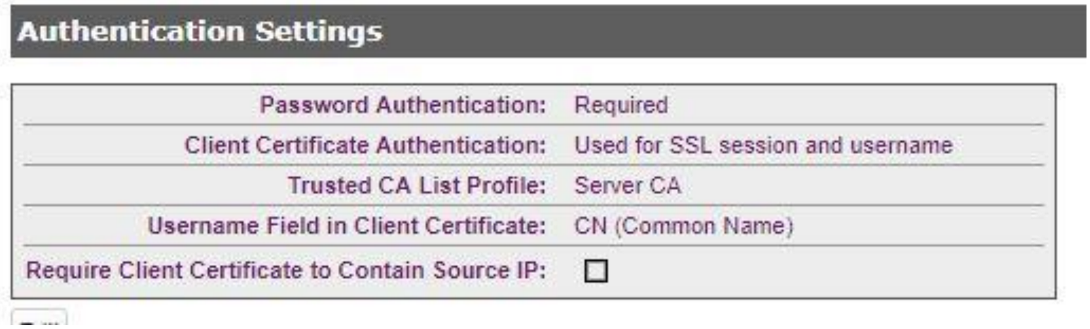
- Set up SEKM on external KMS
- Set up SEKM on iDRAC
- Enable SEKM on the PERC of iDRAC
- Enable SEKM on Storage Controllers
- Configure SEKM by using a Server Configuration Profile (SCP)

1.1 Set up SEKM on external KMS

This section describes the Gemalto KeySecure features that are supported by iDRAC. For information about all other KeySecure features, see the *KeySecure Appliace Administration Guide* available on the Gemalto support site: https://safenet.gemalto.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 user names 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

Password Authentication:	Required
Client Certificate Authentication:	Used for SSL session and username
Trusted CA List Profile:	Server CA
Username Field in Client Certificate:	CN (Common Name)
Require Client Certificate to Contain Source IP:	□

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.

1.2 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.

1.3 Configure SEKM on the iDRAC GUI

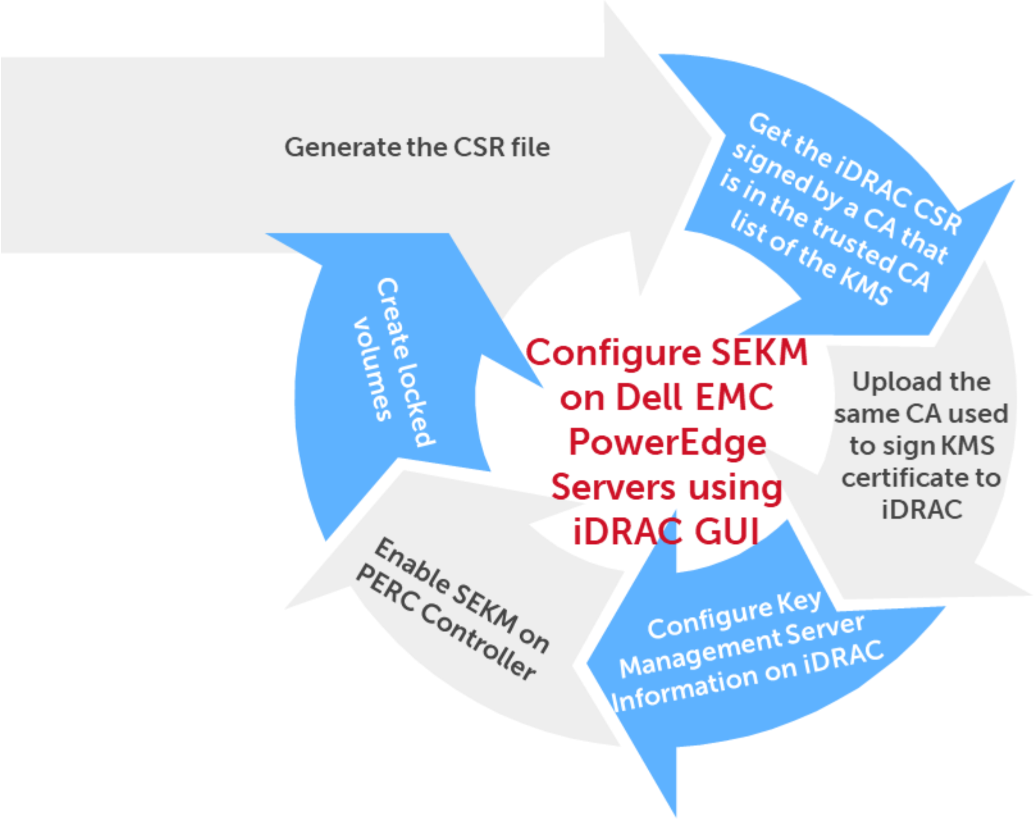
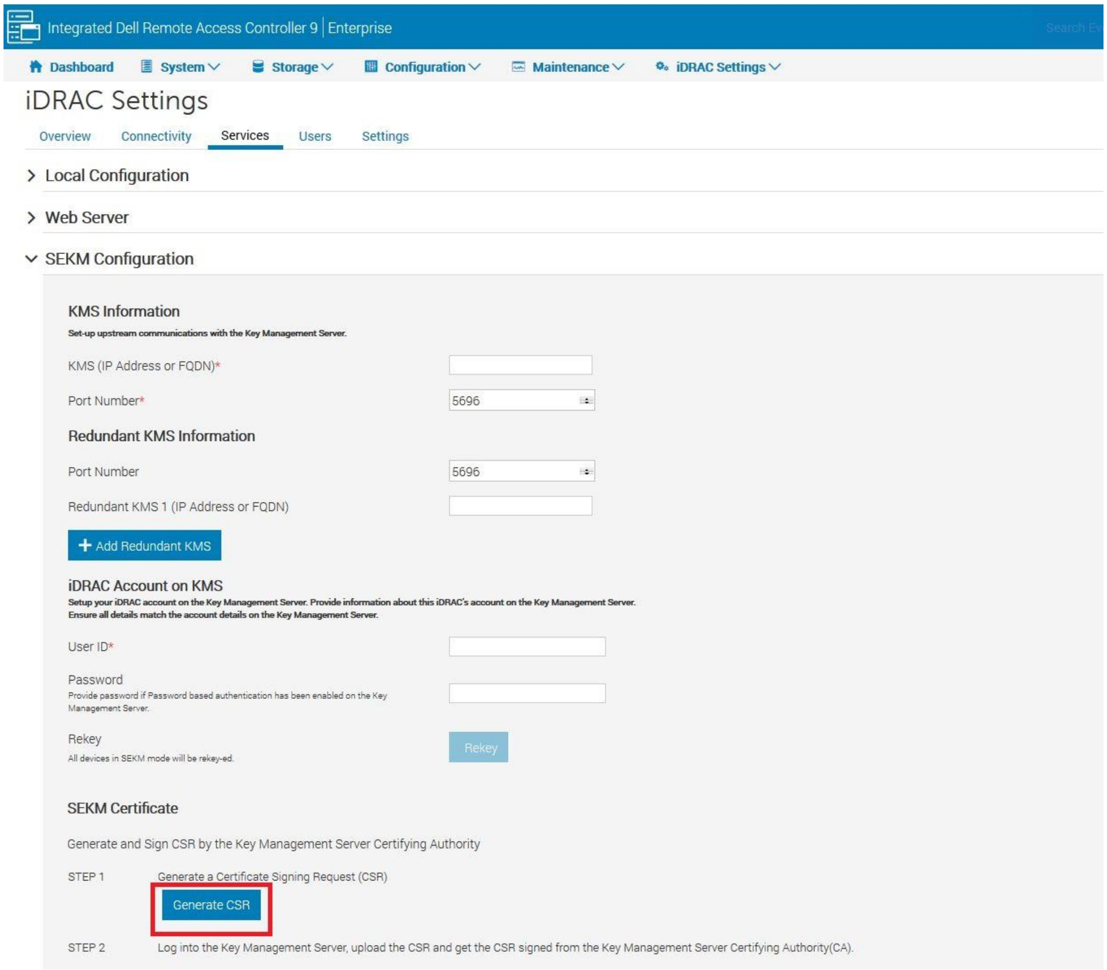

Generate the CSR file
Get the iDRAC CSR signed by a CA that is in the trusted CA list of the KMS
Upload the same CA used to sign KMS certificate to iDRAC
Configure Key Management Server Information on iDRAC
Enable SEKM on PERC Controller
Create locked volumes
Configure SEKM on Dell EMC PowerEdge Servers using iDRAC GUI

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

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

1. Start iDRAC by using any supported browser.
2. Click **iDRAC Settings → Services**.
3. Expand the **SEKM Configuration** menu and click **Generate CSR**.



Integrated Dell Remote Access Controller 9 | Enterprise

iDRAC Settings

> Local Configuration

> Web Server

SEKM Configuration

KMS Information

Set-up upstream communications with the Key Management Server.

KMS (IP Address or FQDN)*

Port Number* 5696

Redundant KMS Information

Port Number 5696

Redundant KMS 1 (IP Address or FQDN)

iDRAC Account on KMS

Setup your iDRAC account on the Key Management Server. Provide information about this iDRAC's account on the Key Management Server. Ensure all details match the account details on the Key Management Server.

User ID*

Password

Provide password if Password based authentication has been enabled on the Key Management Server.

Rekey

All devices in SEKM mode will be rekey-ed.

SEKM Certificate

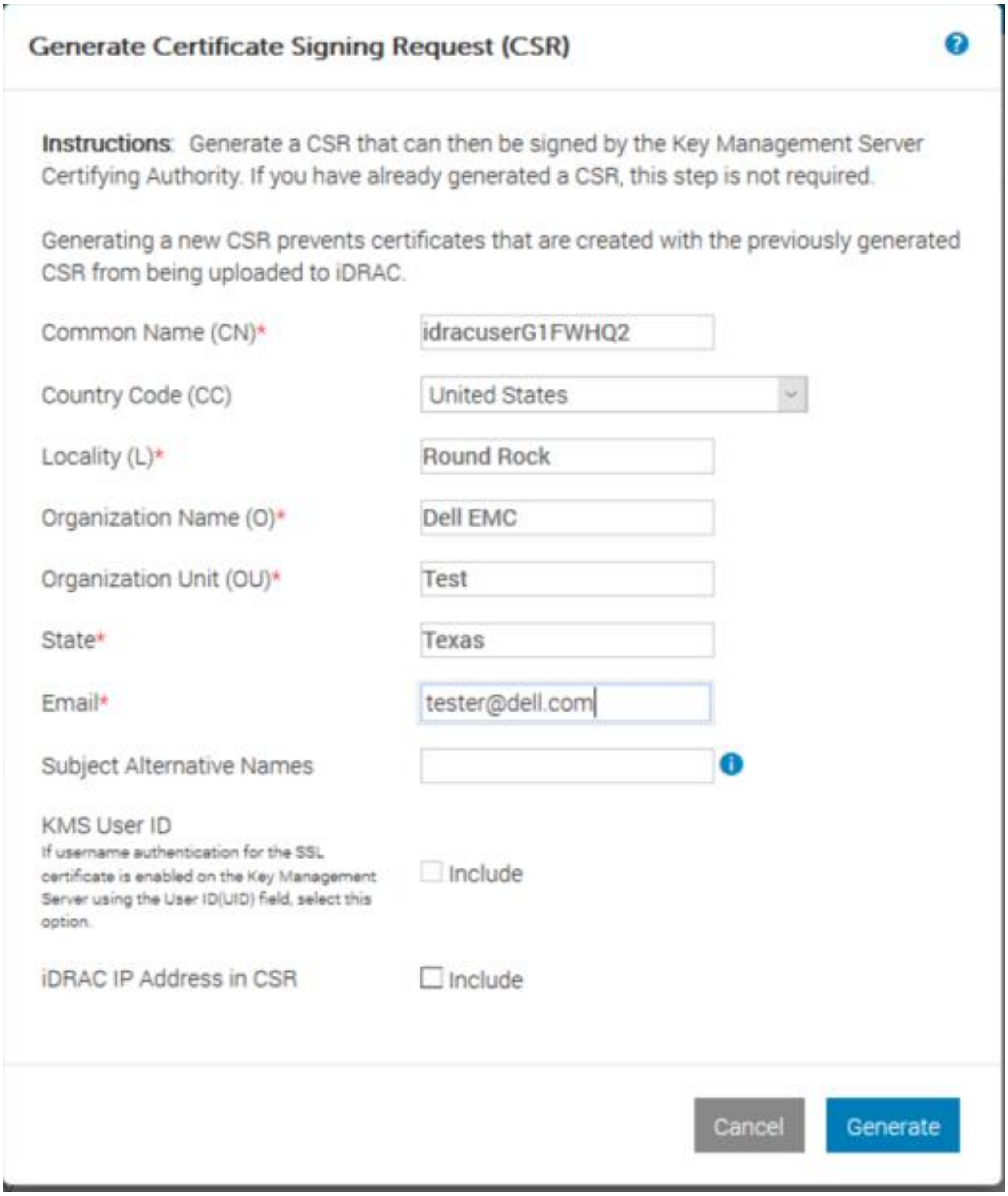
Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1 Generate a Certificate Signing Request (CSR)

STEP 2 Log into the Key Management Server, upload the CSR and get the CSR signed from the Key Management Server Certifying Authority(CA).

Figure 4 Generate CSR on the iDRAC GUI

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



Generate Certificate Signing Request (CSR)

Instructions: Generate a CSR that can then be signed by the Key Management Server Certifying Authority. If you have already generated a CSR, this step is not required.

Generating a new CSR prevents certificates that are created with the previously generated CSR from being uploaded to iDRAC.

Common Name (CN)*	idracuserG1FWHQ2
Country Code (CC)	United States
Locality (L)*	Round Rock
Organization Name (O)*	Dell EMC
Organization Unit (OU)*	Test
State*	Texas
Email*	tester@dell.com
Subject Alternative Names	
KMS User ID If username authentication for the SSL certificate is enabled on the Key Management Server using the User ID(UID) field, select this option.	□ Include
iDRAC IP Address in CSR	□ Include

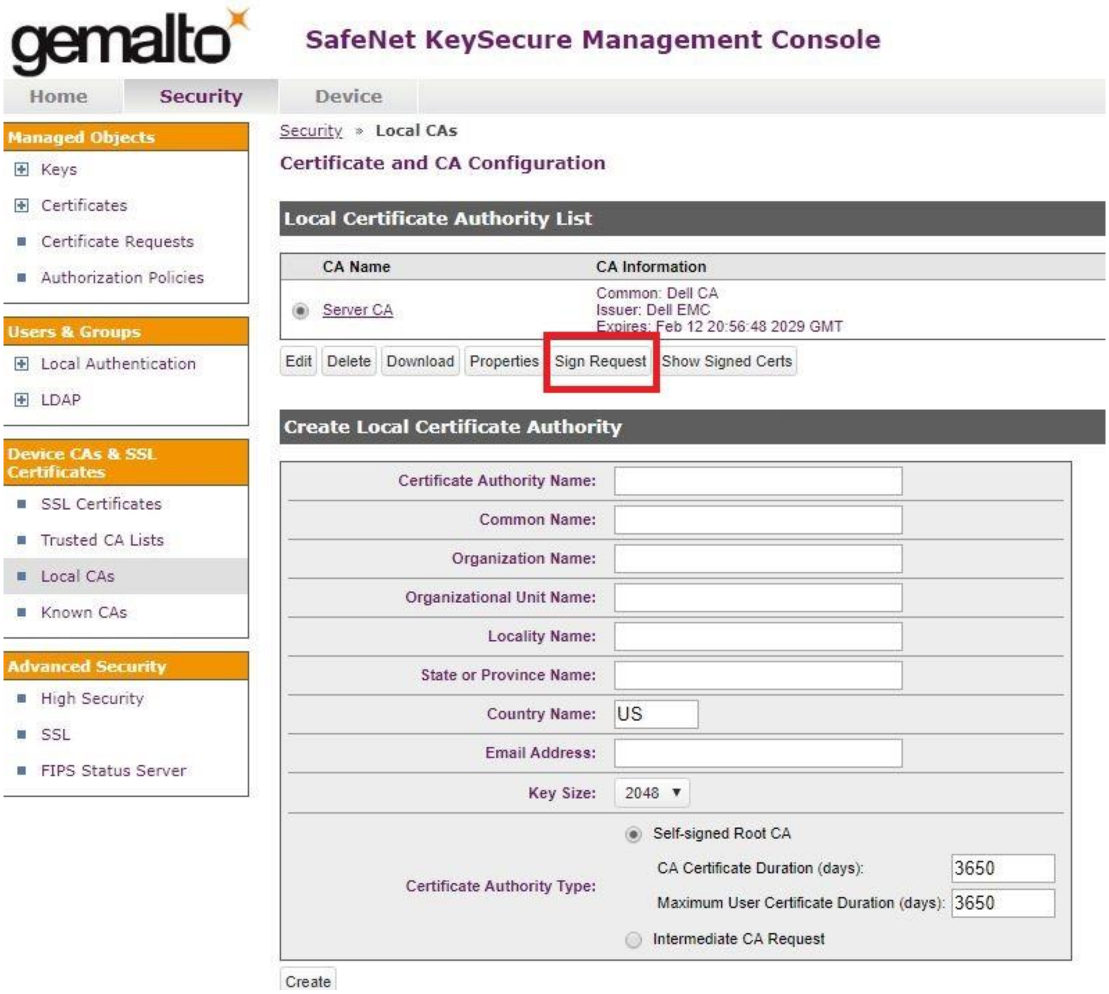
Figure 5 Enter or select data in the CSR dialog box of iDRAC

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

1.3.1 Get the CSR file signed on Gemalto

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

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG

A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl

c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl

c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj

7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL

JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV

i/OyLyeJ7l1SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae

LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z

76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg

5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw

ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na

V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+

ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4

Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A

EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB2l6UP1CzpXxF02yA3y

kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp

36A=

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

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



Certificate and CA Configuration

Local Certificate Authority List

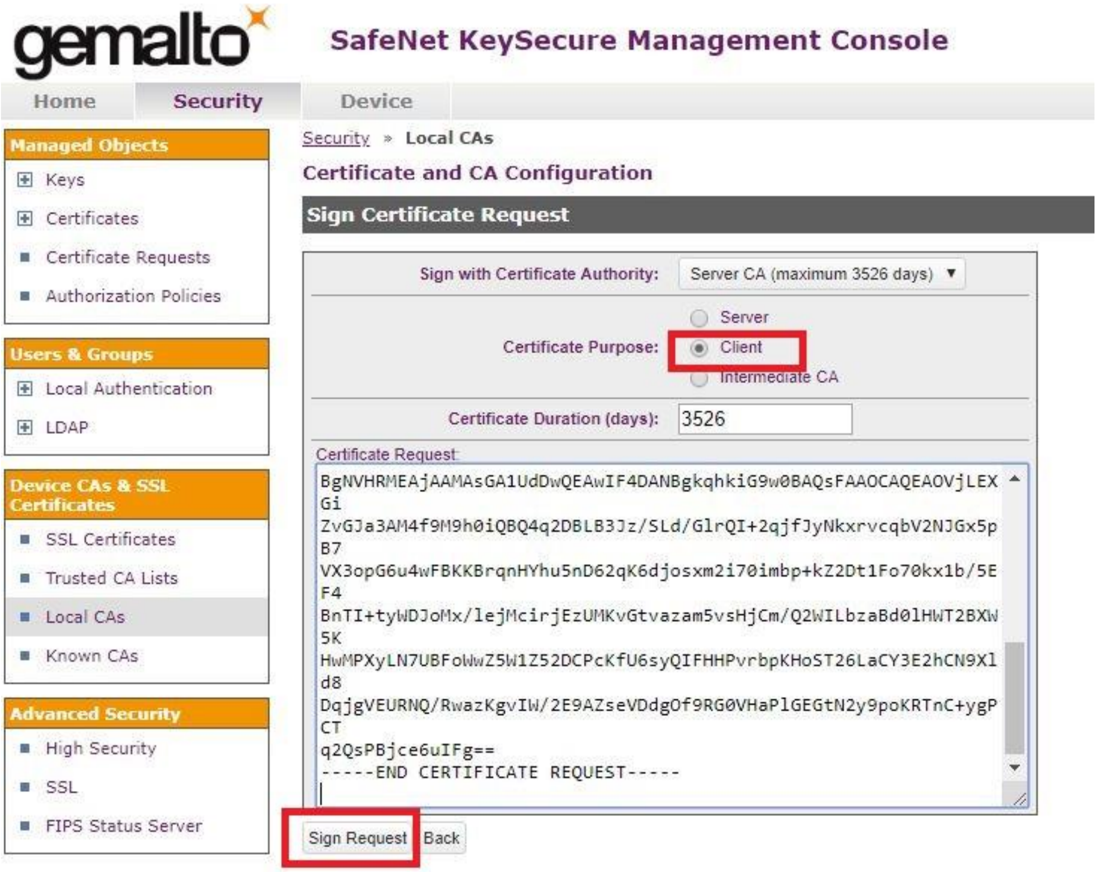
	CA Name	CA Information
●	Server CA	Common: Dell CA Issuer: Dell EMC Expires: Feb 12 20:56:48 2029 GMT

Create Local Certificate Authority

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048 ▼
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

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

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



Sign with Certificate Authority: Server CA (maximum 3526 days) ▼

Certificate Purpose: ○ Server ● Client ○ Intermediate CA

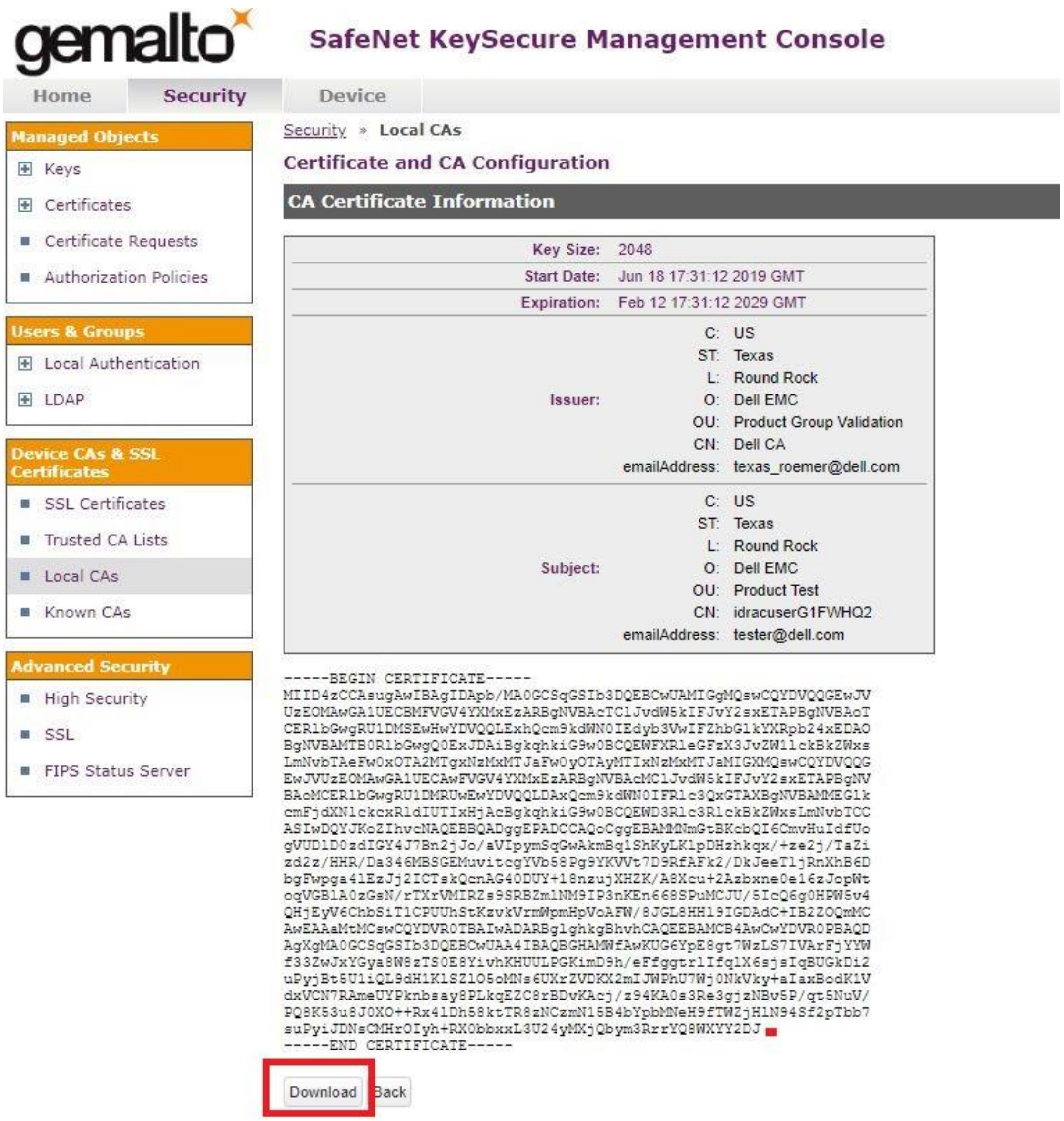
Certificate Duration (days): 3526

Certificate Request:

```
BgNVHRMEAjAAMAsGA1UdDwQEAwIF4DANBgkqhkiG9w0BAQsFAAOCAQEAOVjLEX
Gi
ZvGJa3AM4f9M9h0iQBQ4q2DBLB3Jz/SLd/GlrQI+2qjfJyNkxrvcqbV2NJGx5p
B7
VX3opG6u4wFBKKBrqnHYhu5nD62qK6djosxm2i70imbp+kZ2Dt1Fo70kx1b/5E
F4
BnTI+tyWDJoMx/lejMcirjEzUMKvGtvazam5vsHjCm/Q2WILbzaBd0lHWT2BXW
5K
HwMPXyLN7UBFoWwZ5W1Z52DCPcKfU6syQIFHHPvrbpKHoST26LaCY3E2hCN9Xl
d8
DqjgVEURNQ/RwazKgvIW/2E9AZseVDdgOf9RG0VHaPlGEGtN2y9poKRTnC+ygP
CT
q2QsPBjce6uIFg==
-----END CERTIFICATE REQUEST-----
```

Figure 7 Request for certificate signing on Gemalto

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



Certificate and CA Configuration

CA Certificate Information

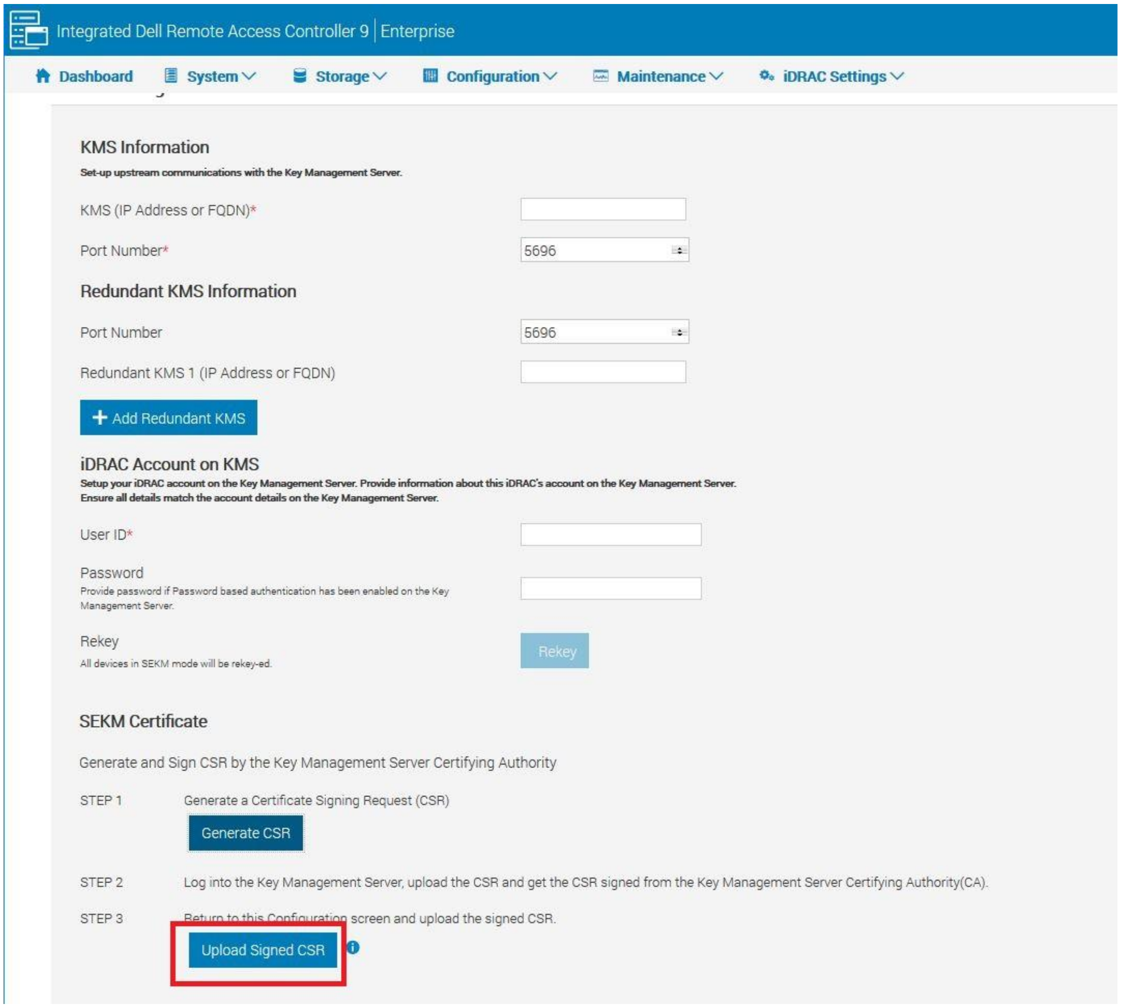
Key Size:	2048	
Start Date:	Jun 18 17:31:12 2019 GMT	
Expiration:	Feb 12 17:31:12 2029 GMT	
Issuer:	C:	US
	ST:	Texas
	L:	Round Rock
	O:	Dell EMC
	OU:	Product Group Validation
	CN:	Dell CA
	emailAddress:	texas_roemer@dell.com
Subject:	C:	US
	ST:	Texas
	L:	Round Rock
	O:	Dell EMC
	OU:	Product Test
	CN:	idracuserG1FWHQ2
	emailAddress:	tester@dell.com

```
-----BEGIN CERTIFICATE-----
MIID4zCCAsugAwIBAgIDApb/MA0GCSqGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV
UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJvdW5kIFJvY2sxETAPBgNVBAoT
CERlbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbGlkYXRpb24xEDAO
BgNVBAMTB0RlbGwgQ0ExJDAiBgkqhkiG9w0BCQEWFXRleGFzX3JvZW1lckBkZWxs
LmNvbTAeFw0xOTA2MTgxNzMxMTJaFw0yOTAyMTIxNzMxMTJaMIGXMQswCQYDVQQG
EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV
BAoMCERlbGwgRU1DMRUwEwYDVQQLDAxQcm9kdWN0IFRlc3QxGTAXBgNVBAMMEGlk
cmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rlc3RlckBkZWxsLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMMNmGtBKcbQI6CmvHuIdfUo
gVUDlD0zdIGY4J7Bn2jJo/aVIpymSqGwAkmBq1ShKyLKlpDHzhkqx/+ze2j/TaZi
zd2z/HHR/Da346MBSGEMuvitcgYVb58Pg9YKVVt7D9RfAFk2/DkJeeTljRnXhB6D
bgFwpga4lEzJj2ICTskQcnAG40DUY+18nzujXHZK/A8Xcu+2Azbxne0e16zJopWt
oqVGBlA0zGsN/rTXrVMIRZs9SRBZmlNM9IP3nKEn668SPuMCJU/5IcQ6g0HPW5v4
QHjEyV6ChbSiT1CPUUhStKzvkVrmWpmHpVoAFW/8JGL8HH19IGDAdC+IB2ZOQmMC
AwEAAaMtMCswCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCB4AwCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBCwUAA4IBAQBGHAMWfAwKUG6YpE8gt7WzLS7IVArFjYYW
f33ZwJxYGya8W8zTS0E8YivhKHUULPGKimD9h/eFfggtrlIfqlX6sjsIqBUGkDi2
uPyjBt5U1iQL9dH1KlSZlO5oMNs6UXrZVDKX2mIJWPhU7Wj0NkVky+aIaxBodK1V
dxVCN7RAmeUYPknbsay8PLkqEZC8rBDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/
PQ8K53u8J0XO++Rx4lDh58ktTR8zNCzmN15B4bYpbMNeH9fTWZjH1N94Sf2pTbb7
suPyiJDNsCMHrOIyh+RX0bbxxL3U24yMXjQbym3RrrYQ8WXYY2DJ
-----END CERTIFICATE-----
```

Figure 8	Download and save the CSR file on Gemalto

8. On the iDRAC GUI, in the **SEKM Certificate** page, click **Upload Signed CSR** to upload the file you just got signed on Gemalto.

   A message is displayed to indicate the successful upload.



KMS Information

Set-up upstream communications with the Key Management Server.

KMS (IP Address or FQDN)*

Port Number* 5696

Redundant KMS Information

Port Number 5696

Redundant KMS 1 (IP Address or FQDN)

iDRAC Account on KMS

Setup your iDRAC account on the Key Management Server. Provide information about this iDRAC's account on the Key Management Server. Ensure all details match the account details on the Key Management Server.

User ID*

Password
Provide password if Password based authentication has been enabled on the Key Management Server.

Rekey
All devices in SEKM mode will be rekey-ed.

SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1 Generate a Certificate Signing Request (CSR)

STEP 2 Log into the Key Management Server, upload the CSR and get the CSR signed from the Key Management Server Certifying Authority(CA).

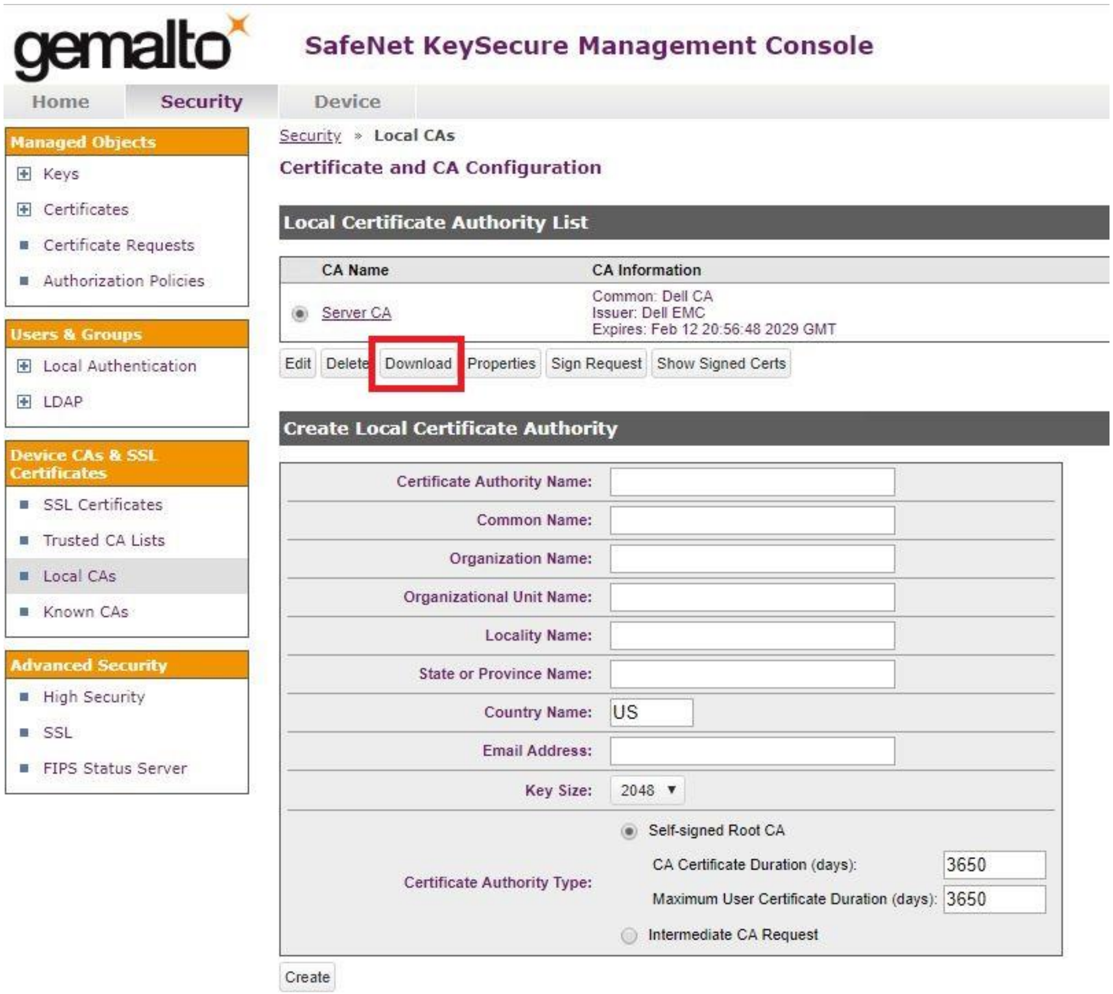
STEP 3 Return to this Configuration screen and upload the signed CSR.

Figure 9 Upload the signed CSR certificate on iDRAC GUI

1.3.2 Download the server CA file from Gemalto 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.



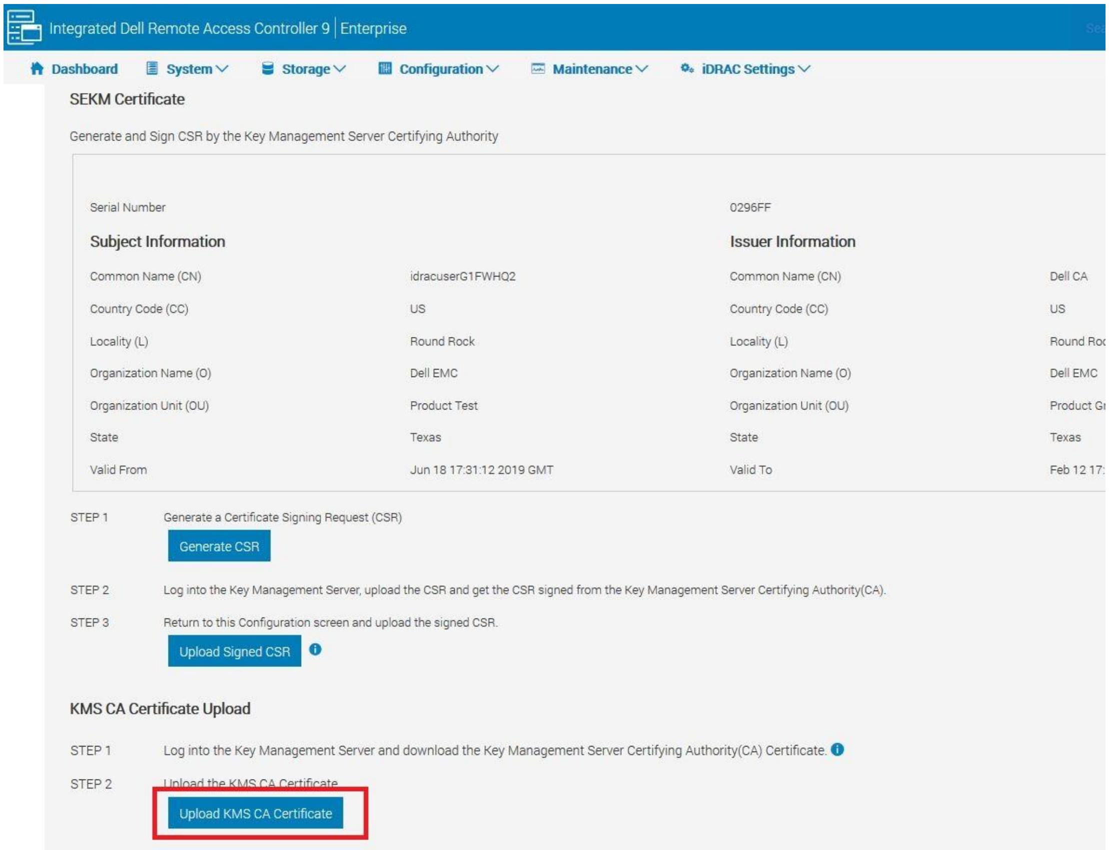
	CA Name	CA Information
●	Server CA	Common: Dell CA Issuer: Dell EMC Expires: Feb 12 20:56:48 2029 GMT

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048 ▼
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

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.



SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

Serial Number		0296FF	
Subject Information		**Issuer Information**	
Common Name (CN)	idracuserG1FWHQ2	Common Name (CN)	Dell CA
Country Code (CC)	US	Country Code (CC)	US
Locality (L)	Round Rock	Locality (L)	Round Roc
Organization Name (O)	Dell EMC	Organization Name (O)	Dell EMC
Organization Unit (OU)	Product Test	Organization Unit (OU)	Product Gr
State	Texas	State	Texas
Valid From	Jun 18 17:31:12 2019 GMT	Valid To	Feb 12 17:

STEP 1 Generate a Certificate Signing Request (CSR)

STEP 2 Log into the Key Management Server, upload the CSR and get the CSR signed from the Key Management Server Certifying Authority(CA).

STEP 3 Return to this Configuration screen and upload the signed CSR.

KMS CA Certificate Upload

STEP 1 Log into the Key Management Server and download the Key Management Server Certifying Authority(CA) Certificate.

STEP 2 Upload the KMS CA Certificate

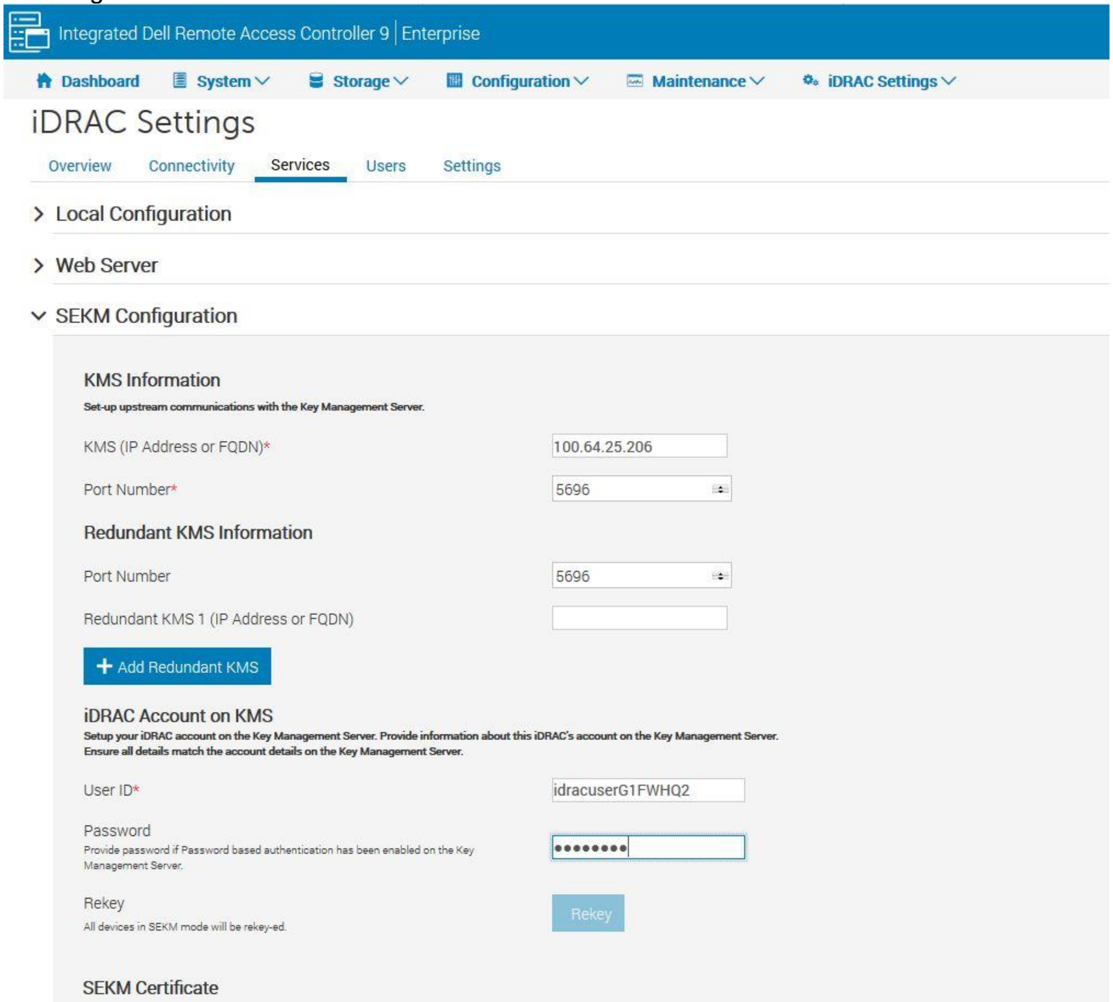
Figure 11 Upload the CA certificate to iDRAC

1.3.3 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 user name on Gemalto, you must create a user with the name “idracuserG1FWHQ2”. This is the user which iDRAC will be using for key exchange.



KMS Information

Set-up upstream communications with the Key Management Server.

KMS (IP Address or FQDN)* 100.64.25.206

Port Number* 5696

Redundant KMS Information

Port Number 5696

Redundant KMS 1 (IP Address or FQDN)

iDRAC Account on KMS

Setup your iDRAC account on the Key Management Server. Provide information about this iDRAC's account on the Key Management Server. Ensure all details match the account details on the Key Management Server.

User ID* idracuserG1FWHQ2

Password ••••••••

Provide password if Password based authentication has been enabled on the Key Management Server.

Rekey

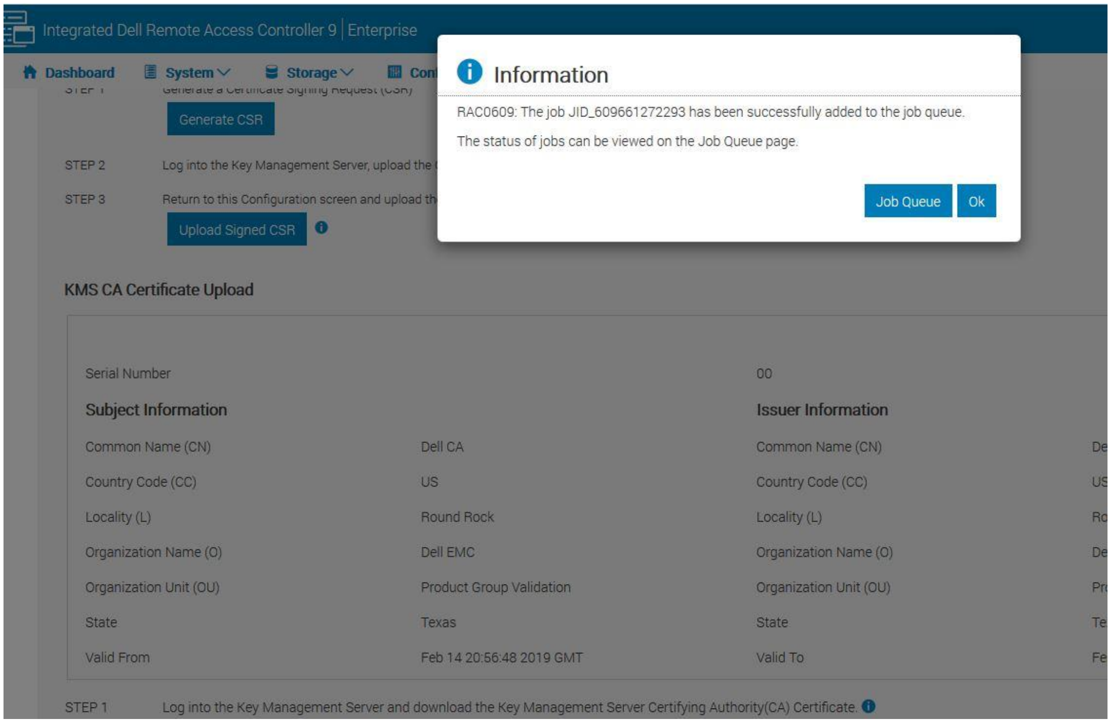
All devices in SEKM mode will be rekey-ed.

SEKM Certificate

Figure 12 Configure the KMS properties on iDRAC GUI

A message is displayed stating 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.



Information

RAC0609: The job JID_609661272293 has been successfully added to the job queue.

The status of jobs can be viewed on the Job Queue page.

STEP 1 Generate a Certificate Signing Request (CSR)

STEP 2 Log into the Key Management Server, upload the

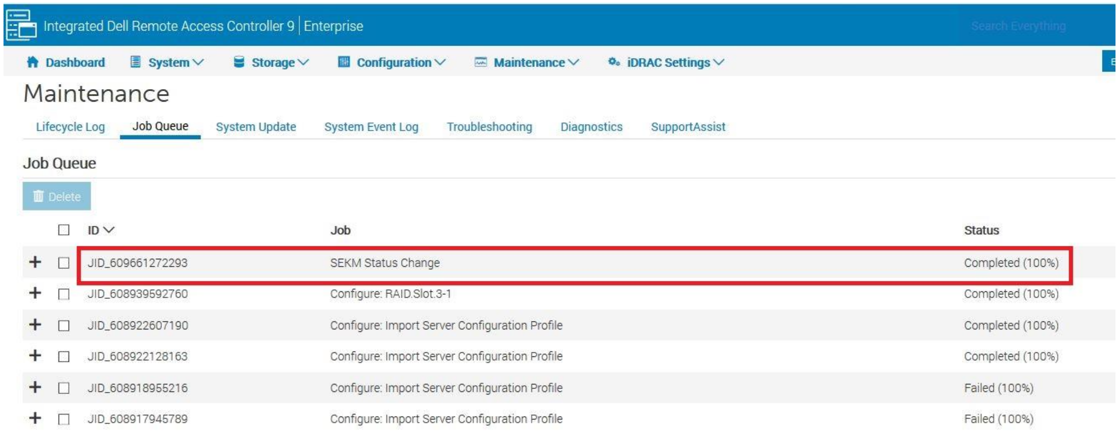
STEP 3 Return to this Configuration screen and upload th

KMS CA Certificate Upload

Serial Number		00	
Subject Information		**Issuer Information**	
Common Name (CN)	Dell CA	Common Name (CN)	De
Country Code (CC)	US	Country Code (CC)	US
Locality (L)	Round Rock	Locality (L)	Ro
Organization Name (O)	Dell EMC	Organization Name (O)	De
Organization Unit (OU)	Product Group Validation	Organization Unit (OU)	Pr
State	Texas	State	Te
Valid From	Feb 14 20:56:48 2019 GMT	Valid To	Fe

STEP 1 Log into the Key Management Server and download the Key Management Server Certifying Authority(CA) Certificate.

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



Maintenance

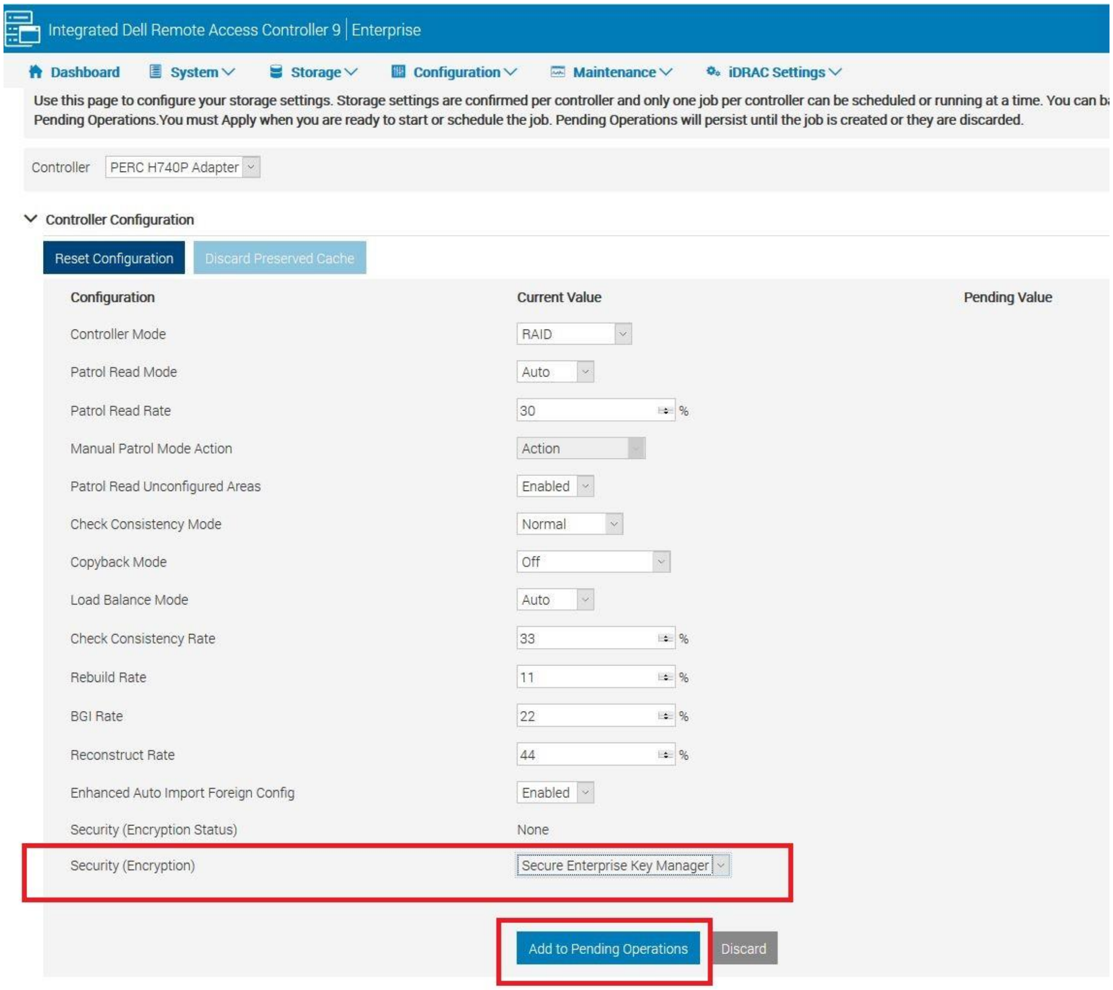
Job Queue

ID	Job	Status
JID_609661272293	SEKM Status Change	Completed (100%)
JID_608939692760	Configure: RAID.Slot.3-1	Completed (100%)
JID_608922607190	Configure: Import Server Configuration Profile	Completed (100%)
JID_608922128163	Configure: Import Server Configuration Profile	Completed (100%)
JID_608918955216	Configure: Import Server Configuration Profile	Failed (100%)
JID_608917945789	Configure: Import Server Configuration Profile	Failed (100%)

iDRAC SEKM configuration is now complete.

2 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**.



Use this page to configure your storage settings. Storage settings are confirmed per controller and only one job per controller can be scheduled or running at a time. You can b
Pending Operations.You must Apply when you are ready to start or schedule the job. Pending Operations will persist until the job is created or they are discarded.

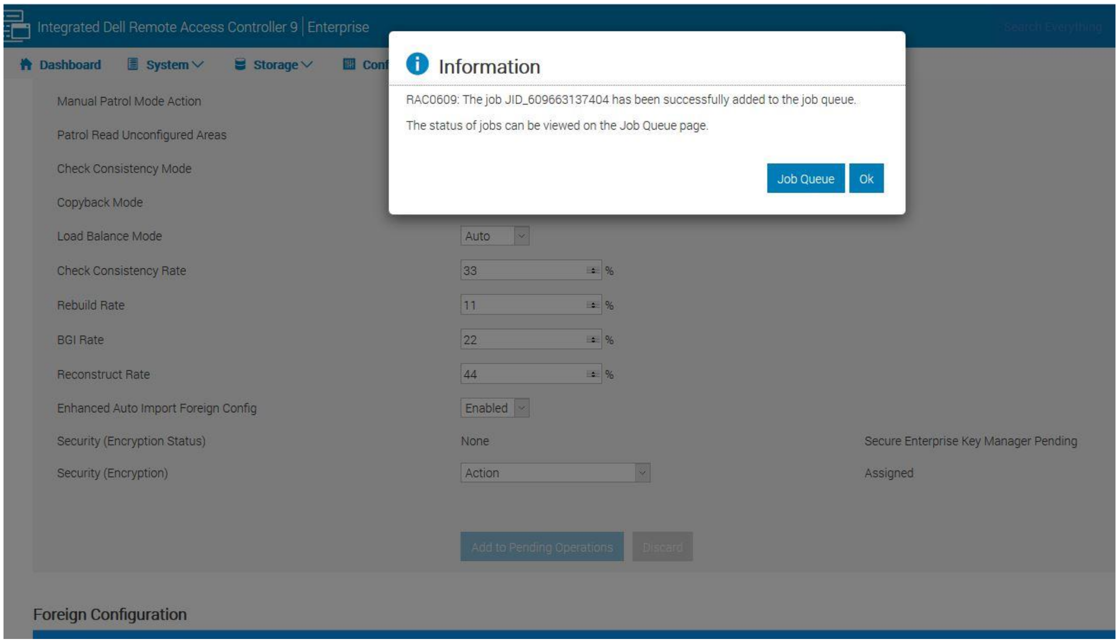
Controller: PERC H740P Adapter

Configuration	Current Value	Pending Value
Controller Mode	RAID	
Patrol Read Mode	Auto	
Patrol Read Rate	30 %	
Manual Patrol Mode Action	Action	
Patrol Read Unconfigured Areas	Enabled	
Check Consistency Mode	Normal	
Copyback Mode	Off	
Load Balance Mode	Auto	
Check Consistency Rate	33 %	
Rebuild Rate	11 %	
BGI Rate	22 %	
Reconstruct Rate	44 %	
Enhanced Auto Import Foreign Config	Enabled	
Security (Encryption Status)	None	
Security (Encryption)	Secure Enterprise Key Manager	

Figure 14 Enable SEKM on iDRAC PERC

6. Select **At Next Reboot**.

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



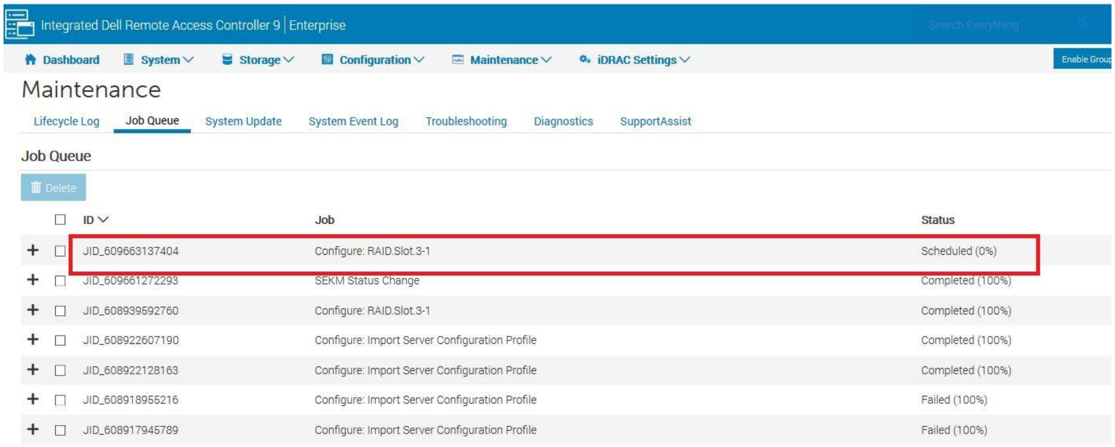
Information

RAC0609: The job JID_609663137404 has been successfully added to the job queue.

The status of jobs can be viewed on the Job Queue page.

Manual Patrol Mode Action		
Patrol Read Unconfigured Areas		
Check Consistency Mode		
Copyback Mode		
Load Balance Mode	Auto	
Check Consistency Rate	33 %	
Rebuild Rate	11 %	
BGI Rate	22 %	
Reconstruct Rate	44 %	
Enhanced Auto Import Foreign Config	Enabled	
Security (Encryption Status)	None	Secure Enterprise Key Manager Pending
Security (Encryption)	Action	Assigned

Figure 15 A job is created to enable SEKM on IDRAC PERC



Job Queue

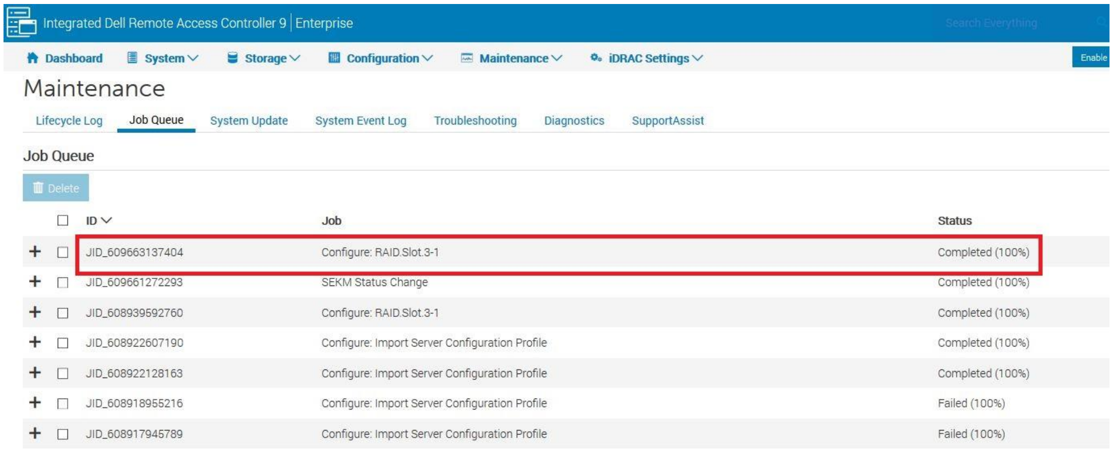
	□	ID	Job	Status
+	□	JID_609663137404	Configure: RAID.Slot.3-1	Scheduled (0%)
+	□	JID_609661272293	SEKM Status Change	Completed (100%)
+	□	JID_608939592760	Configure: RAID.Slot.3-1	Completed (100%)
+	□	JID_608922607190	Configure: Import Server Configuration Profile	Completed (100%)
+	□	JID_608922128163	Configure: Import Server Configuration Profile	Completed (100%)
+	□	JID_608918955216	Configure: Import Server Configuration Profile	Failed (100%)
+	□	JID_608917945789	Configure: Import Server Configuration Profile	Failed (100%)

Figure 16 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.

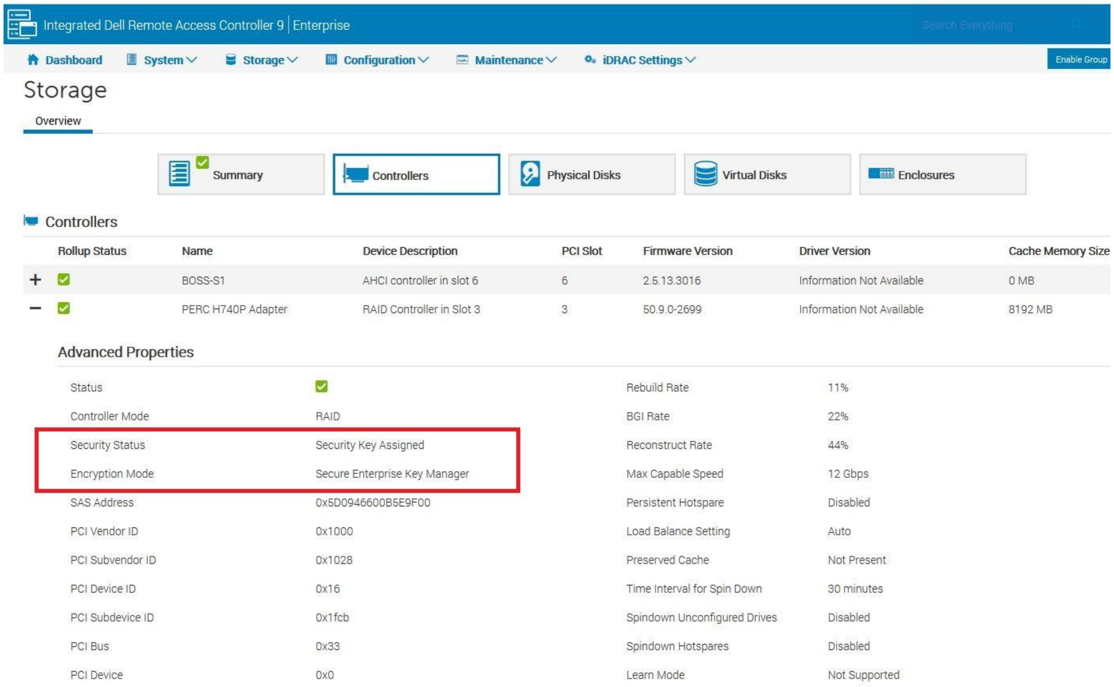


	□	ID	Job	Status
+	□	JID_609663137404	Configure: RAID.Slot.3-1	Completed (100%)
+	□	JID_609661272293	SEKM Status Change	Completed (100%)
+	□	JID_608939592760	Configure: RAID.Slot.3-1	Completed (100%)
+	□	JID_608922607190	Configure: Import Server Configuration Profile	Completed (100%)
+	□	JID_608922128163	Configure: Import Server Configuration Profile	Completed (100%)
+	□	JID_608918955216	Configure: Import Server Configuration Profile	Failed (100%)
+	□	JID_608917945789	Configure: Import Server Configuration Profile	Failed (100%)

Figure 17 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



Controllers

	Rollup Status	Name	Device Description	PCI Slot	Firmware Version	Driver Version	Cache Memory Size
+	✓	BOSS-S1	AHCI controller in slot 6	6	2.5.13.3016	Information Not Available	0 MB
−	✓	PERC H740P Adapter	RAID Controller in Slot 3	3	50.9.0-2699	Information Not Available	8192 MB

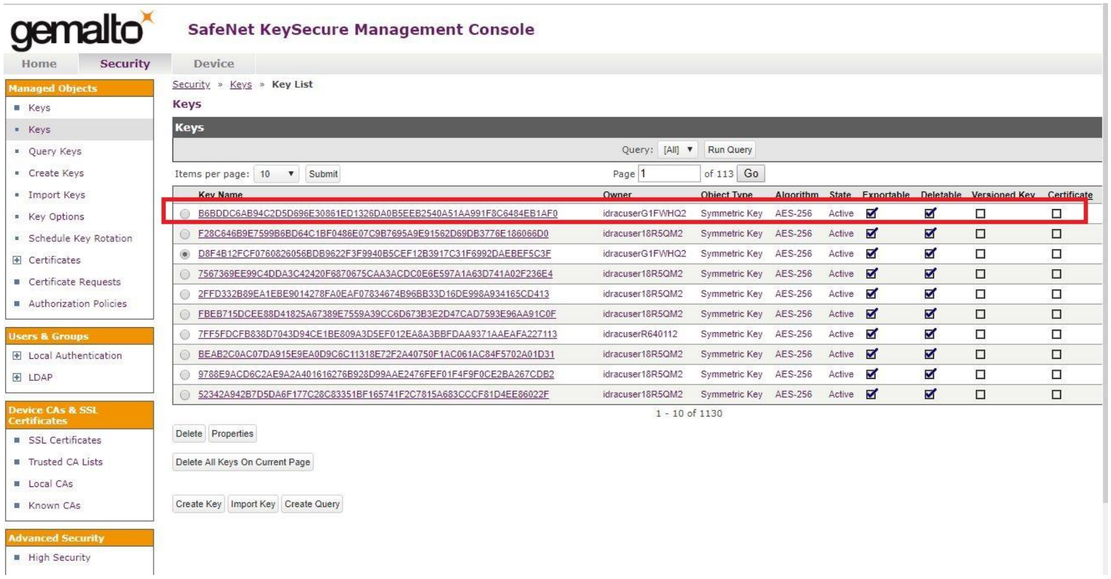
Advanced Properties

Status	✓	Rebuild Rate	11%
Controller Mode	RAID	BGI Rate	22%
Security Status	Security Key Assigned	Reconstruct Rate	44%
Encryption Mode	Secure Enterprise Key Manager	Max Capable Speed	12 Gbps
SAS Address	0x5D0946600B5E9F00	Persistent Hotspare	Disabled
PCI Vendor ID	0x1000	Load Balance Setting	Auto
PCI Subvendor ID	0x1028	Preserved Cache	Not Present
PCI Device ID	0x16	Time Interval for Spin Down	30 minutes
PCI Subdevice ID	0x1fcb	Spindown Unconfigured Drives	Disabled
PCI Bus	0x33	Spindown Hotspares	Disabled
PCI Device	0x0	Learn Mode	Not Supported

Figure 18 Ensure that SEKM is enabled on your controller

3. On the Gemalto GUI, click the **Security** tab.

A Key ID is generated and displayed for the user you assigned to the iDRAC. This is the key ID that iDRAC uses for key exchange.



	Key Name	Owner	Object Type	Algorithm	State	Exportable	Deletable	Versioned Key	Certificate
○	B6BDDC6AB94C2D5D696E30861ED1326DA0B5EEB2540A51AA991F8C6484EB1AF0	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	F28C646B9E7599B6BD64C1BF0486E07C9B7695A9E91562D69DB3776E186066D0	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
●	D8F4B12FCF0760826056BDB9622F3F9940B5CEF12B3917C31F6992DAEBEF5C3F	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	7567369EE99C4DDA3C42420F6870675CAA3ACDC0E6E597A1A63D741A02F236E4	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	2FFD332B89EA1EBE9014278FA0EAF07834674B96BB33D16DE998A934165CD413	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	FBEB715DCEE88D41825A67389E7559A39CC6D673B3E2D47CAD7593E96AA91C0F	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	7FF5FDCFB838D7043D94CE1BE809A3D5EF012EA8A3BBFDAA9371AAEAFA227113	idracuserR640112	Symmetric Key	AES-256	Active	☑	☑	□	□
○	BEAB2C0AC07DA915E9EA0D9C6C11318E72F2A40750F1AC061AC84F5702A01D31	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	9788E9ACD6C2AE9A2A401616276B928D99AAE2476FEF01F4F9F0CE2BA267CDB2	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	52342A942B7D5DA6F177C28C83351BF165741F2C7815A683CCCF81D4EE86022F	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□

1 - 10 of 1130

Figure 19 The iDRAC key ID is generated on Gemalto

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

3 Configure the SEKM Solution by using iDRAC RACADM CLI

In this workflow example, an iDRAC RACDM (remote) is used to set up the complete SEKM solution for the iDRAC. For the Key Management Server (KMS), Gemalto KeySecure is used as the Key Management Server.

1. Configure the iDRAC SEKM certificate attributes. These must be configured first before you generate a CSR file.
2. To set each attribute, run the `SET` command. The examples here use the default iDRAC user name and password (`root`/`calvin`).
3. Replace it with an appropriate iDRAC user name and password set up on the PowerEdge server.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn get idrac.sekmcert
[Key=idrac.Embedded.1#SEKMCert.1]
#CertificateStatus=NOT_PENDING
CommonName=
CountryCode=US
EmailAddress=
LocalityName=
OrganizationName=
OrganizationUnit=
StateName=
SubjectAltName=
UserId=

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.CommonName
idracuserG1FWHQ2
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.CountryCode US
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.EmailAddress
tester@dell.com
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.LocalityName "Dell
EMC"
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationName
"DELL EMC"
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationUnit
Test

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

Object value modified successfully


C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.StateName Texas

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

Object value modified successfully
```

3.1 Generate a CSR

1. Get the CSR contents signed on the Gemalto server. See Get the CSR file signed on Gemalto.
2. Download the signed file, and then upload it back to iDRAC. Run the following command at the RACADM CLI:

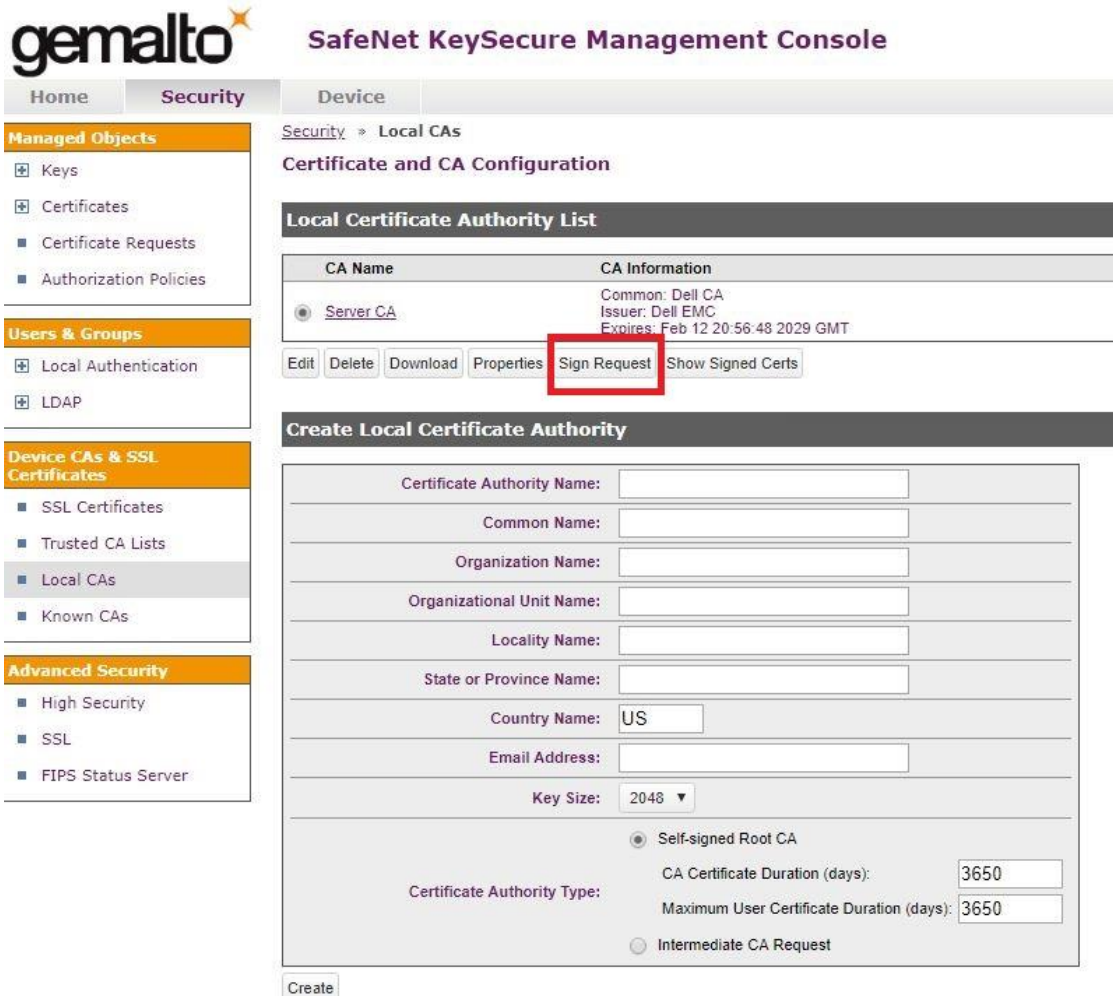
   ```
   C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcsrgen -g -t 3 -f sekm_csr
   ```

   A CSR is successfully generated and downloaded.

3.2 Get the CSR file signed on the Gemalto GUI

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

1. On the Gemalto GUI, click **Security Tab → Local CAs**.
2. Click **Sign Request**.



Certificate and CA Configuration

Local Certificate Authority List

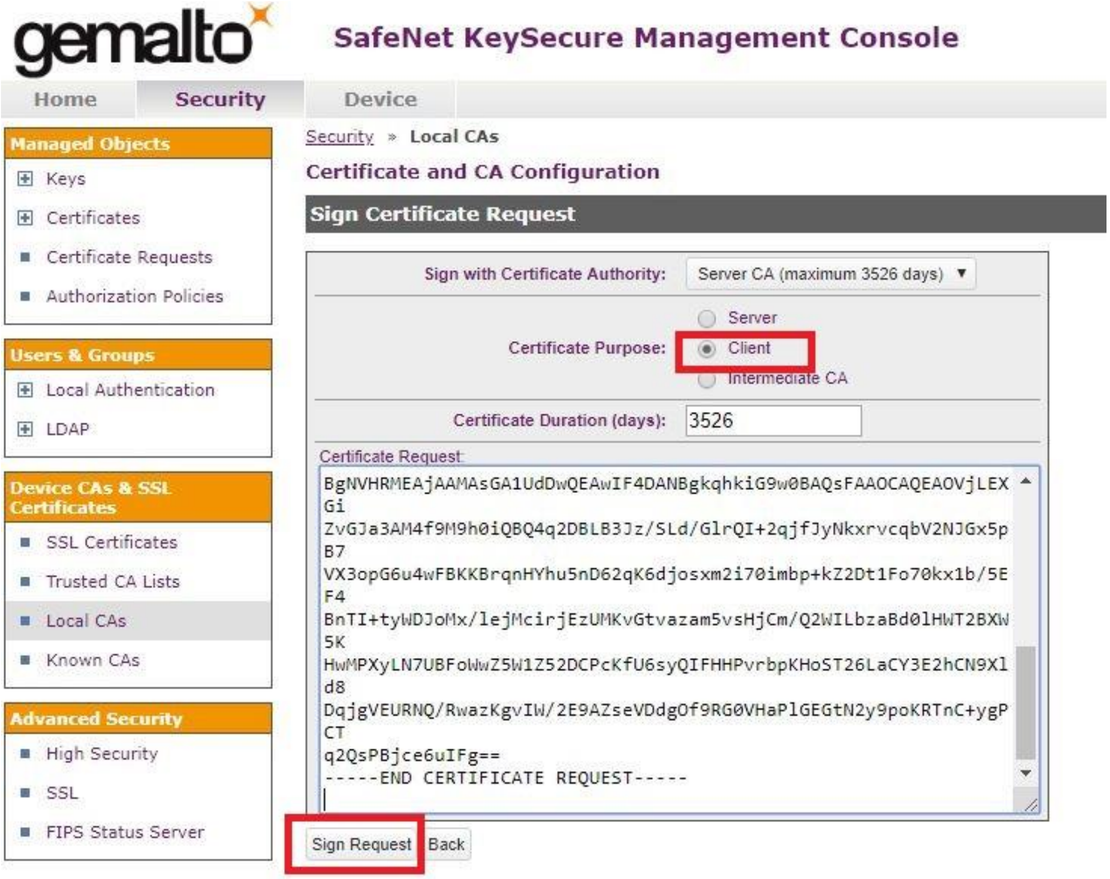
	CA Name	CA Information
●	Server CA	Common: Dell CA Issuer: Dell EMC Expires: Feb 12 20:56:48 2029 GMT

Create Local Certificate Authority

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

Figure 20 Get the CSR request signed on Gemalto GUI

3. Select **Client** as the purpose of generating a certificate.
4. Paste the complete CSR contents and click **Sign Request**.



Sign with Certificate Authority: Server CA (maximum 3526 days) ▼

Certificate Purpose: ○ Server ● Client ○ Intermediate CA

Certificate Duration (days): 3526

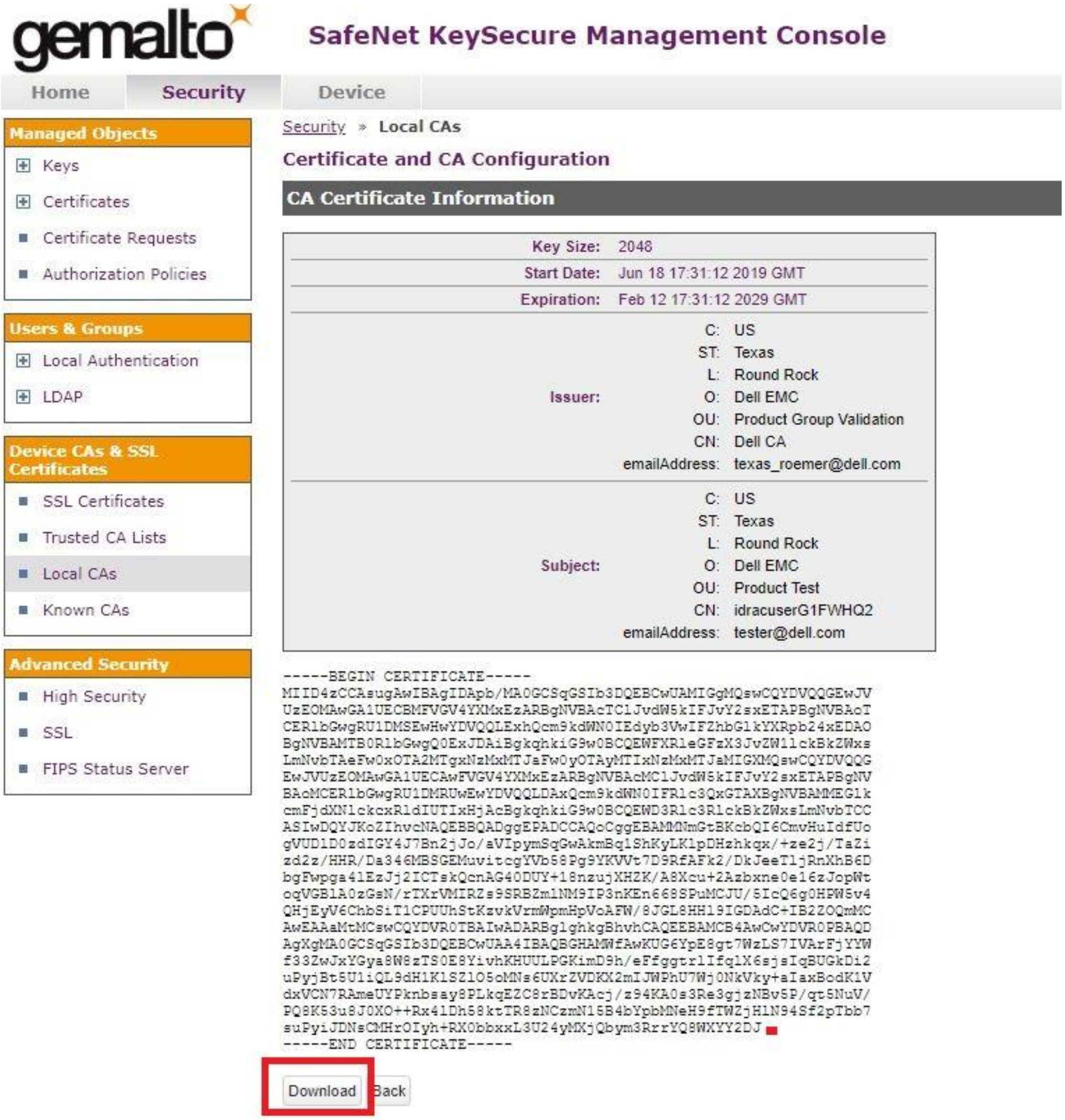
Certificate Request:

```
BgNVHRMEAjAAMAsGA1UdDwQEAwIF4DANBgkqhkiG9w0BAQsFAAOCAQEAOVjLEX
Gi
ZvGJa3AM4f9M9h0iQBQ4q2DBLB3Jz/SLd/GlrQI+2qjfJyNkxrvcqbV2NJGx5p
B7
VX3opG6u4wFBKKBrqnHYhu5nD62qK6djosxm2i70imbp+kZ2Dt1Fo70kx1b/5E
F4
BnTI+tyWDJoMx/lejMcirjEzUMKvGtvazam5vsHjCm/Q2WILbzaBd0lHWT2BXW
5K
HwMPXyLN7UBFoWwZ5W1Z52DCPcKfU6syQIFHHPvrbpKHoST26LaCY3E2hCN9Xl
d8
DqjgVEURNQ/RwazKgvIW/2E9AZseVDdgOf9RG0VHaPlGEGtN2y9poKRTnC+ygP
CT
q2QsPBjce6uIFg==
-----END CERTIFICATE REQUEST-----
```

Figure 21 Submit a Sign Request job

5. After the CSR is successfully signed, click **Download**.

   The signed CSR file is saved to your system.



Certificate and CA Configuration

CA Certificate Information

Key Size: 2048

Start Date: Jun 18 17:31:12 2019 GMT

Expiration: Feb 12 17:31:12 2029 GMT

Issuer:
C: US
ST: Texas
L: Round Rock
O: Dell EMC
OU: Product Group Validation
CN: Dell CA
emailAddress: texas_roemer@dell.com

Subject:
C: US
ST: Texas
L: Round Rock
O: Dell EMC
OU: Product Test
CN: idracuserG1FWHQ2
emailAddress: tester@dell.com

```
-----BEGIN CERTIFICATE-----
MIID4zCCAsugAwIBAgIDApb/MA0GCSqGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV
UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJvdW5kIFJvY2sxETAPBgNVBAoT
CERlbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbGlkYXRpb24xEDAO
BgNVBAMTB0RlbGwgQ0ExJDAiBgkqhkiG9w0BCQEWFXRleGFzX3JvZW1lckBkZWxs
LmNvbTAeFw0xOTA2MTgxNzMxMTJaFw0yOTAyMTIxNzMxMTJaMIGXMQswCQYDVQQG
EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV
BAoMCERlbGwgRU1DMRUwEwYDVQQLDAxQcm9kdWN0IFRlc3QxGTAXBgNVBAMMEGlk
cmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rlc3RlckBkZWxsLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMMNmGtBKcbQI6CmvHuIdfUo
gVUDlD0zdIGY4J7Bn2jJo/aVIpymSqGwAkmBq1ShKyLKlpDHzhkqx/+ze2j/TaZi
zd2z/HHR/Da346MBSGEMuvitcgYVb58Pg9YKVVt7D9RfAFk2/DkJeeTljRnXhB6D
bgFwpga4lEzJj2ICTskQcnAG40DUY+18nzujXHZK/A8Xcu+2Azbxne0e16zJopWt
oqVGBlA0zGsN/rTXrVMIRZs9SRBZmlNM9IP3nKEn668SPuMCJU/5IcQ6g0HPW5v4
QHjEyV6ChbSiT1CPUUhStKzvkVrmWpmHpVoAFW/8JGL8HH19IGDAdC+IB2ZOQmMC
AwEAAaMtMCswCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCB4AwCwYDVR0PBAQD
AgXgMA0GCSqGSIb3DQEBCwUAA4IBAQBGHAMWfAwKUG6YpE8gt7WzLS7IVArFjYYW
f33ZwJxYGya8W8zTS0E8YivhKHUULPGKimD9h/eFfggtrlIfqlX6sjsIqBUGkDi2
uPyjBt5U1iQL9dH1K1SZ1O5oMNs6UXrZVDKX2mIJWPhU7Wj0NkVky+aIaxBodK1V
dxVCN7RAmeUYPknbsay8PLkqEZC8rBDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/
PQ8K53u8J0XO++Rx41Dh58ktTR8zNCzmN15B4bYpbMNeH9fTWZjH1N94Sf2pTbb7
suPyiJDNsCMHrOIyh+RX0bbxxL3U24yMXjQbym3RrrYQ8WXYY2DJ
-----END CERTIFICATE-----
```

Figure 22 Download the signed CSR file from Gemalto to your local system

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

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertupload -t 6 -f
C:\Users\tester\Downloads\signed_cert.crt
```

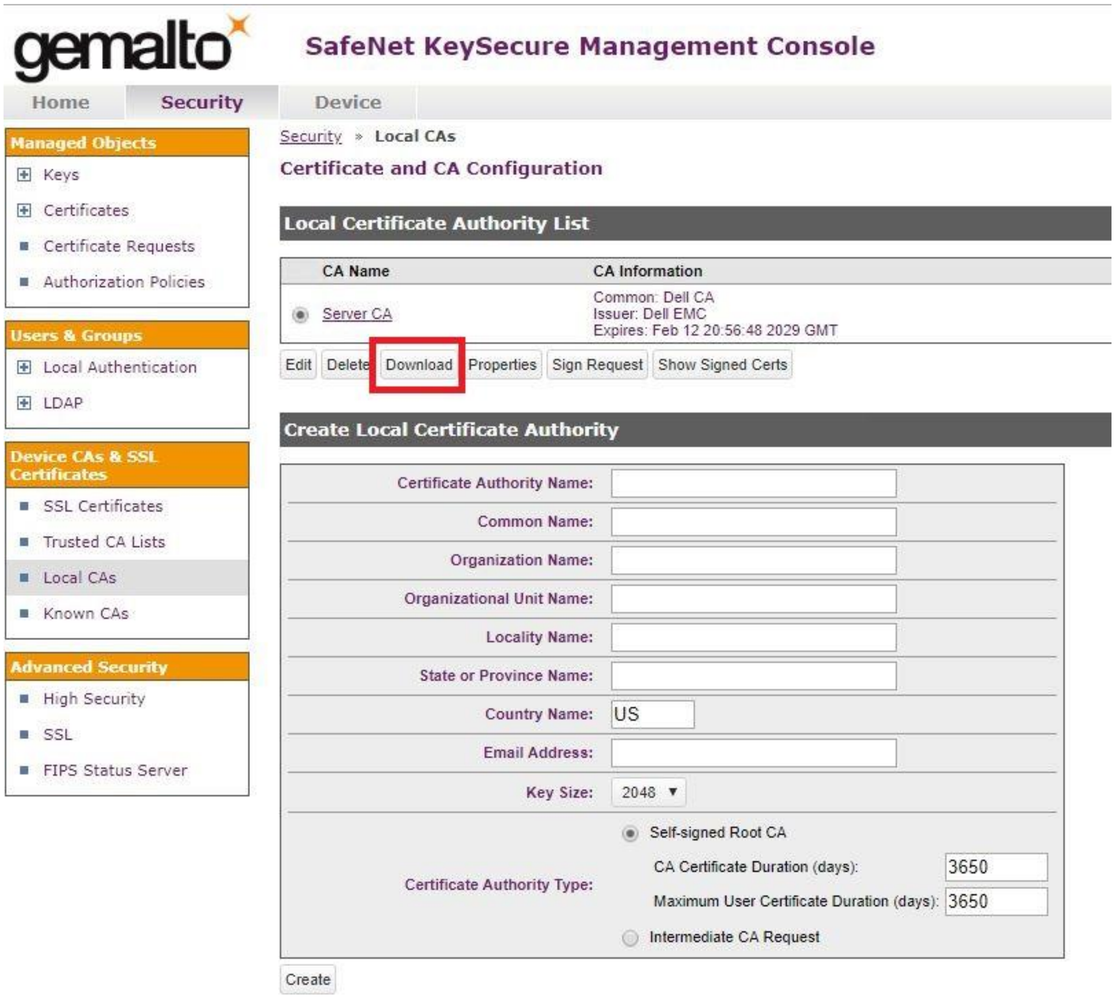
Certificate is successfully uploaded to the RAC.

3.3 Download the server CA file from Gemalto 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 locally saved to your system.



Security » Local CAs

Certificate and CA Configuration

Local Certificate Authority List

	CA Name	CA Information
●	Server CA	Common: Dell CA Issuer: Dell EMC Expires: Feb 12 20:56:48 2029 GMT

Create Local Certificate Authority

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048 ▼
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

Figure 23 Download the server CA file from Gemalto

3.4 Upload the Server CA file to the iDRAC

Run the following command at the RACADM CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertupload -t 7 -f
C:\Users\texas_roemer\Downloads\Server_CA.crt
```

The certificate is successfully uploaded to the RAC.

3.5 Configure the Key Management Server settings on the iDRAC

Note—Ensure you already have a user created on the Key Management Server (KMS) you will be using for key exchange with the iDRAC. For the user name, make sure it matches the same 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 user name on Gemalto, you must create a user with the name “idracuserG1FWHQ2”. This is the user name which iDRAC will be using for key exchange.

1. Run the following command at the RACADM CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn get idrac.kms

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

!!iDRACPassword=******** (Write-Only)

iDRACUserName=

KMIPPortNumber=5696

PrimaryServerAddress=

RedundantKMIPPortNumber=5696

RedundantServerAddress1=

RedundantServerAddress2=

RedundantServerAddress3=

RedundantServerAddress4=

RedundantServerAddress5=

RedundantServerAddress6=

RedundantServerAddress7=

RedundantServerAddress8=

Timeout=10
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.PrimaryServerAddress
100.64.25.206

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

Object value modified successfully
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.iDRACUserName
idracuserG1FWHQ2

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

Object value modified successfully
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.iDRACPassword P@ssw0rd

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

Object value modified successfully
```

3. After configuring all the KMS attributes, enable the SEKM on the iDRAC. When you execute the command, job ID is returned.
4. Query the job ID to ensure that the job status is displayed as “Completed”.
5. If you see a job failure, check Lifecycle logs for more information about the failure:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm enable
```

SEKM0212—The SEKM Enable operation is successfully started. To view the status of a job, run the "racadm jobqueue view -i JID_580315196579" command at the Command Line Interface (CLI).

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID_580315196579

---------------------------- JOB -------------------------

[Job ID=JID_580315196579]

Job Name=SEKM Status Change

Status=Completed

Start Time=[Not Applicable]

Expiration Time=[Not Applicable]

Message=[SEKM020: The SEKM feature on the iDRAC is enabled.]

Percent Complete=[100]

----------------------------------------------------------
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm getstatus

SEKM Status = Enabled
```

The iDRAC SEKM setup operation is complete.

4 Enable SEKM on Storage Controllers

1. Get the FQDD of the controller you are going to enable SEKM. In this workflow, the controller FQDD is “RAID.Slot.3-1”. Run the following RACADM command at the CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get controllers -o -p name

RAID.Slot.3-1

Name = PERC H740P Adapter  (PCI Slot 3)
```

2. Use this controller FQDD and run the command to enable SEKM pending value:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage setencryptionmode:RAID.Slot.3-1 -
mode SEKM
```

RAC1040—Successfully accepted the storage configuration operation. To apply the configuration operation, create a configuration job, and then restart the server. To create the required commit and reboot jobs, run the `jobqueue` command. For more information about the jobqueue command, enter the RACADM command "racadm help jobqueue".

3. Create a job ID to apply the pending changes.
4. Use the same controller FQDD to create a config job.
5. Also, for the job to run, a server reboot is required. Use the `–r` option which will automatically create a reboot job ID and reboot the server:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue create RAID.Slot.3-1 -s
TIME_NOW -r pwrcycle
```

RAC1024—Successfully scheduled a job. Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

```
Commit JID = JID_580317754984

Reboot JID = RID_580317755572
```

The server is automatically restarted.

6. Run the config job in Automated Task Application.

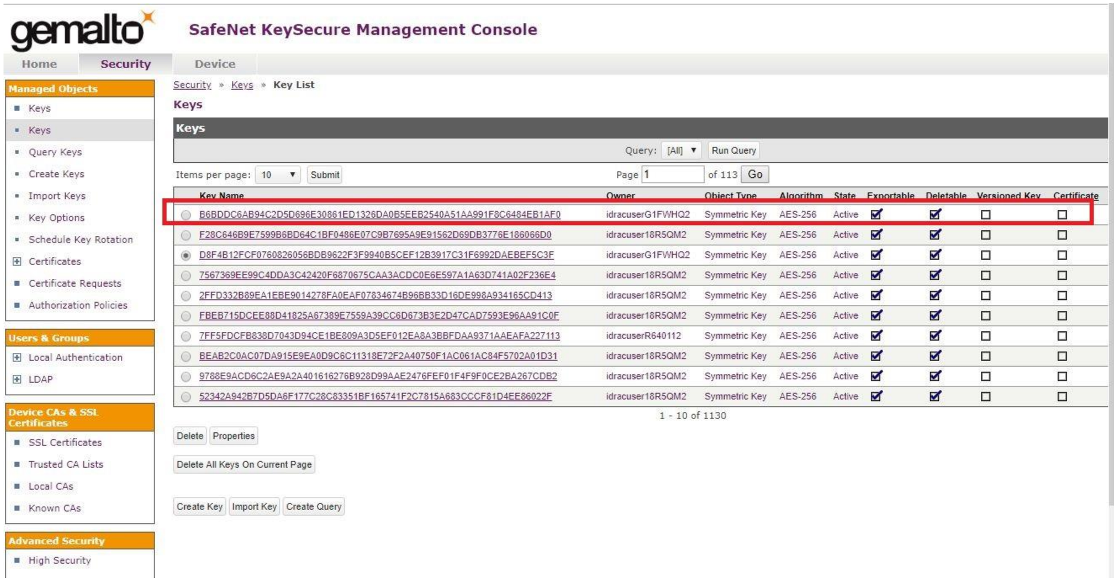
   Server is restarted again. After the POST or Collecting Inventory operation is completed, the job status is indicated as **Completed**.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID_580317754984

---------------------------- JOB -------------------------

[Job ID=JID_580317754984]

Job Name=Configure: RAID.Slot.3-1

Status=Completed

Start Time=[Now]

Expiration Time=[Not Applicable]

Message=[PR19: Job completed successfully.]

Percent Complete=[100]

----------------------------------------------------------
```

7. Check the storage controller.

   It is now in the SEKM encryption mode. It will also report the Key ID assigned to controller which iDRAC uses for key exchanges:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get controllers:RAID.Slot.3-1
-p encryptionmode,keyid

RAID.Slot.3-1

EncryptionMode                  = Secure Enterprise Key Manager

KeyID                           =
4163A493F1B50C8E727E9474627DC9D19193B0FEB0F40CAA03FD42DC81447BED
```



	Key Name	Owner	Object Type	Algorithm	State	Exportable	Deletable	Versioned Key	Certificate
○	B6BDDC6AB94C2D5D696E30861ED1326DA0B5EEB2540A51AA991F8C6484EB1AF0	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	F28C646B9E7599B6BD64C1BF0486E07C9B7695A9E91562D69DB3776E186066D0	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
●	D8F4B12FCF0760826056BDB9622F3F9940B5CEF12B3917C31F6992DAEBEF5C3F	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	7567369EE99C4DDA3C42420F6870675CAA3ACDC0E6E597A1A63D741A02F236E4	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	2FFD332B89EA1EBE9014278FA0EAF07834674B96BB33D16DE998A934165CD413	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	FBEB715DCEE88D41825A67389E7559A39CC6D673B3E2D47CAD7593E96AA91C0F	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	7FF5FDCFB838D7043D94CE1BE809A3D5EF012EA8A3BBFDAA9371AAEAFA227113	idracuserR640112	Symmetric Key	AES-256	Active	☑	☑	□	□
○	BEAB2C0AC07DA915E9EA0D9C6C11318E72F2A40750F1AC061AC84F5702A01D31	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	9788E9ACD6C2AE9A2A401616276B928D99AAE2476FEF01F4F9F0CE2BA267CDB2	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□
○	52342A942B7D5DA6F177C28C83351BF165741F2C7815A683CCCF81D4EE86022F	idracuser18R5QM2	Symmetric Key	AES-256	Active	☑	☑	□	□

1 - 10 of 1130

The SEKM solution is now completely set up. You can now create locked RAID volumes and perform key exchanges.

5 Configure SEKM by using a Server Configuration Profile (SCP)

In this workflow example, the Server Configuration Profile (SCP) feature is used to set up the complete SEKM solution for the iDRAC. For the Key Management Server, Gemalto KeySecure is used as the Key Management Server.

1. Using SCP, import the signed SSL certificate, Server CA, iDRAC KMS attributes.
2. Enable SEKM on the iDRAC.

   For the signed SSL certificate, a CSR is already generated, signed on Gemalto, and then downloaded. The Server CA is also downloaded from Gemalto.
3. In the SCP, copy the complete contents of the signed SSL certificate and Server CA as shown in the example SCP file below.

5.1 An SCP file example for configuring iDRAC SEKM configuration

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

```
<SystemConfiguration>
<Component FQDD="iDRAC.Embedded.1">
 <Attribute Name="SEKM.1#IPAddressInCertificate">Disabled</Attribute>
 <Attribute Name="SEKM.1#SEKMStatus">Enabled</Attribute>
 <Attribute Name="SEKM.1#KeyAlgorithm">AES-256</Attribute>
 <Attribute Name="SEKM.1#Rekey">False</Attribute>
 <Attribute Name="KMS.1#PrimaryServerAddress">100.64.25.206</Attribute>
 <Attribute Name="KMS.1#KMIPPortNumber">5696</Attribute>
 <Attribute Name="KMS.1#RedundantServerAddress1"/>
 <Attribute Name="KMS.1#RedundantServerAddress2"/>
 <Attribute Name="KMS.1#RedundantServerAddress3"/>
 <Attribute Name="KMS.1#RedundantServerAddress4"/>
 <Attribute Name="KMS.1#RedundantServerAddress5"/>
 <Attribute Name="KMS.1#RedundantServerAddress6"/>
 <Attribute Name="KMS.1#RedundantServerAddress7"/>
 <Attribute Name="KMS.1#RedundantServerAddress8"/>
 <Attribute Name="KMS.1#Timeout">10</Attribute>
 <Attribute Name="KMS.1#iDRACUserName">idracuserG1FWHQ2</Attribute>
 <Attribute Name="KMS.1#iDRACPassword">P@ssw0rd</Attribute>
 <Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute>
 <Attribute Name="SEKMCert.1#CommonName">idracuserG1FWHQ2</Attribute>
 <Attribute Name="SEKMCert.1#OrganizationName">Dell EMC</Attribute>
 <Attribute Name="SEKMCert.1#OrganizationUnit">Test</Attribute>
 <Attribute Name="SEKMCert.1#LocalityName">Round Rock</Attribute>
 <Attribute Name="SEKMCert.1#StateName">Texas</Attribute>
 <Attribute Name="SEKMCert.1#CountryCode">US</Attribute>
 <Attribute Name="SEKMCert.1#EmailAddress">tester@dell.com</Attribute>
 <Attribute Name="SEKMCert.1#SubjectAltName"/>
 <Attribute Name="SEKMCert.1#UserId"/>
 <Attribute Name="SecurityCertificate.1#CertData">-----BEGIN CERTIFICATE-----
MIIEvzCCA6egAwIBAgIBADANBgkqhkiG9w0BAQsFADCBoDELMAkGA1UEBhMCVVMx
DjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQKEwhE
ZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAwDgYD
VQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVsbC5j
b20wHhcNMTkwMjE0MjA1NjQ4WhcNMjkwMjEyMjA1NjQ4WjCBoDELMAkGA1UEBhMC
VVMxDjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQK
EwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAw
DgYDVQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVs
bC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQChyihz1suLIIzl
K+XxI9nh59J+yCNXsMpKzneX0CSr1Aiay1Yyd1Uy2lcifJbmuocP2wLQUEWTnR19
K0zbRKTMNty0fr9NhnwiRFVfUzUPiEGPwTyqR7w2WmHqu5jCnOodC9n+6w8lGnV9
3LzKLaJYdJ9TPGn63ffVrDeprhQ376EK6QjR1xlrTG7kUH2Hu9D1thwxQCykS2eQ
50icshUAsy5sCo5quisNLZZmJefREPxlx7ih/NtMGe5lEiZGyHIf91Ucf5L2vP6J
lYKLZL7AqvJioHSSxD8nvP7naxKmIL3d1zohV8V+8DMc1UabDLhgUek/UX+jqSQ3
cuCY6LhLAgMBAAGjggEAMIH9MB0GA1UdDgQWBBQEk+OPdA03pnzCGUBnUK5a2Z/v
hzCBzQYDVR0jBIHFMIHCgBQEk+OPdA03pnzCGUBnUK5a2Z/vh6GBpqSBozCBoDEL
MAkGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2Nr
MREwDwYDVQQKEwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxp
ZGF0aW9uMRAwDgYDVQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19y
b2VtZXJAZGVsbC5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOC
AQEAgumRcKE3+dbYgNRNeYbvKH29B1NI0l/PIP2V6he4/rDLYgyBLqNmtvRCUvu9
DnZczchZoGIdWm0j/1gW21O8nptDM+R3olMEwNGdl+ZQNLUdMKdzKJbji8IaSxun
B4Y21uLvykGm0Ts+X2/R84RAFHgDrRrentaM2WyJ7GCT470CDdUIg7NApxm8WoSA
EQrt6RGJYQlRZTFTW12f9+2K7CifHvNnth0zLjaK+vK4bTwhaPhkbM/OO/qE1vaH
zgwN+ZaVbl+amGabZdMvQbtDRgNoS+hQ7T91kbJjPJfza4frrxDzZyhxEN2H99pt
zIto472w7hLB56tRjHfA6Vnh4w==
-----END CERTIFICATE-----
</Attribute>
 <Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
 <Attribute Name="SecurityCertificate.2#CertData">-----BEGIN CERTIFICATE-----
MIID2zCCAsOgAwIBAgIDAmNQMA0GCSqGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV
UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJvdW5kIFJvY2sxETAPBgNVBAoT
CERlbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbGlkYXRpb24xEDAO
BgNVBAMTB0RlbGwgQ0ExJDAiBgkqhkiG9w0BCQEWFXRleGFzX3JvZW1lckBkZWxs
LmNvbTAeFw0xOTA1MTYxODMyMzlaFw0yOTAyMTIxODMyMzlaMIGPMQswCQYDVQQG
EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV
BAoMCERlbGwgRU1DMQ0wCwYDVQQLDARUZXN0MRkwFwYDVQQDDBBpZHJhY3VzZXJH
MUZXSFEyMR4wHAYJKoZIhvcNAQkBFg90ZXN0ZXJAZGVsbC5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCl2WXSI3N9OEXmbCxwylhkk2g/OYyvupwg
nL5uEF4TF8+BKjc3hw1PryzK+vPMPSv7J9fX4Ropy5bjsLXL7ZUdKTYMrhSlZ/13
v7qdZkBInHJfpHTiXbKQwvaMryPedToLNTWdG0Mr+ni05Ebzx/eG+x3LJQsbkxwX
```

```
f5NQGVZNtZnYzdTCkQnwmfseBRfJSzbxTm8HpoT9KGchVsYZDpPSz54ZIRlbqRmz
wJBlcyEPq63CjFp4RxfmZW0IPOGbmmcnGy3Rd4YFBmiC75pR3Wx+J1Xzr3inyRJ2
/XWpgm4XYfGSbyQ2in6Kzwf8CA3hTdsdx20FGJ0j3EUnj1PpOOq1AgMBAAGjLTAr
MAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMAsGA1UdDwQEAwIF4DANBgkq
hkiG9w0BAQsFAAOCAQEAVJdEgKMfmhjrRulC/f7SZjy6pDhLSGM5KwJjQm/8fSjm
lfEyVTbD/eedWo6U6cah2uZrY0jD6SN17CAGMU/J6r4jkhZMrmB/cr3HXiCDQd/x
ReqmjVWOCJDb/tStOkWAS3VFuRZzXfkO83Kp6Zzak4Ue3mwJywThklOsoyXx1XEs
esNFxcsAGL9ABcuGUShpdKtYYwWo98og6P1w1aiWRnaZQ6HP4To3tfmnQ9QKUeZ1
i3QsZ5Q6l86dBZjaaoKSWp5y1fph2ciV//SoOtPhNHXYP5H/3AUQoEqNw7lSX2H/
w9TJtElsc2htmbp6bHudrVIlB80lehk6IE4UxAEO/w==
-----END CERTIFICATE-----</Attribute>
 <Attribute Name="SecurityCertificate.2#CertType">SEKM_SSL_CERT</Attribute>
</Component>
</SystemConfiguration>
```

1. Run the RACADM `set` command to import this SCP file which is located on a HTTP share.
2. Ensure the SCP import job is marked as completed.
3. Check config results to see what changes got applied to the iDRAC.

   The examples here use the default iDRAC user name and password (`root`/`calvin`).
4. Replace it with the appropriate iDRAC user name and password set up on the PowerEdge server.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set -f 2019-5-17_132647_export.xml -t xml
-l http://100.65.84.72/http_share_vm
```

RAC977—Import configuration XML file operation initiated. Use the "racadm jobqueue view -i JID_581182121065" command to view the status of the operation.

```
C:>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID_581182121065
---------------------------- JOB -------------------------
[Job ID=JID_581182121065]
Job Name=Configure: Import Server Configuration Profile
Status=Completed
Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Message=[SYS053: Successfully imported and applied Server Configuration Profile.]
Percent Complete=[100]
----------------------------------------------------------


C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn lclog viewconfigresult -j JID_581182121065
SeqNumber       = 5966
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
DisplayValue    = SEKM.1#SEKMStatus
Name            = SEKM.1#SEKMStatus
OldValue        = Disabled
```

```
NewValue        = Enabled
Status          = Success
ErrCode         = 0
SeqNumber       = 5963
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
DisplayValue    = Certificate Data
Name            = SecurityCertificate.1#CertData
OldValue        = ******
NewValue        = ******
Status          = Success
ErrCode         = 0
DisplayValue    = Certificate Type
Name            = SecurityCertificate.1#CertType
OldValue        = ""
NewValue        = KMS_SERVER_CA
Status          = Success
ErrCode         = 0
DisplayValue    = Certificate Data
Name            = SecurityCertificate.2#CertData
OldValue        = ******
NewValue        = ******
Status          = Success
ErrCode         = 0
DisplayValue    = Certificate Type
Name            = SecurityCertificate.2#CertType
OldValue        = ""
NewValue        = SEKM_SSL_CERT
Status          = Success
ErrCode         = 0
SeqNumber       = 5961
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
DisplayValue    = Primary Server Address
Name            = KMS.1#PrimaryServerAddress
OldValue        = ""
NewValue        = 100.64.25.206
Status          = Success
ErrCode         = 0
DisplayValue    = iDRAC User Name
Name            = KMS.1#iDRACUserName
OldValue        = ""
NewValue        = idracuserG1FWHQ2
Status          = Success
```

```
ErrCode         = 0
DisplayValue    = iDRAC Password
Name            = KMS.1#iDRACPassword
OldValue        = ******
NewValue        = ******
Status          = Success
ErrCode         = 0
```

5. Check to validate iDRAC SEKM is enabled, and the SSL certificate and Server CA are installed.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm getstatus
SEKM Status = Enabled

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertview -t 6
Serial Number            : 026350

Subject Information:
Country Code (CC)        : US
State (S)                : Texas
Locality (L)             : Round Rock
Organization (O)         : Dell EMC
Organizational Unit (OU) : Test
Common Name (CN)         : idracuserG1FWHQ2

Issuer Information:
Country Code (CC)        : US
State (S)                : Texas
Locality (L)             : Round Rock
Organization (O)         : Dell EMC
Organizational Unit (OU) : Product Group Validation
Common Name (CN)         : Dell CA

Valid From               : May 16 18:32:39 2019 GMT
Valid To                 : Feb 12 18:32:39 2029 GMT

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertview -t 7
Serial Number            : 00

Subject Information:
Country Code (CC)        : US
State (S)                : Texas
Locality (L)             : Round Rock
Organization (O)         : Dell EMC
Organizational Unit (OU) : Product Group Validation
Common Name (CN)         : Dell CA
```

```
Issuer Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell EMC
Organizational Unit (OU) : Product Group Validation
Common Name (CN)          : Dell CA

Valid From                : Feb 14 20:56:48 2019 GMT
Valid To                  : Feb 12 20:56:48 2029 GMT
```

6. After setting up iDRAC SEKM, use SCP to enable SEKM on the PERC along with creating a locked RAID volume. SCP enable you to stack multiple RAID operations without the need of running multiple jobs or commands.
7. Run one import command to stack these RAID operations and apply them.

5.2 Example of SCP file that has been modified to only show RAID changes which will enable SEKM on the PERC and create a RAID locked volume

```
<SystemConfiguration>
<Component FQDD="RAID.Slot.3-1">
    <Attribute Name="RAIDresetConfig">True</Attribute>
    <Attribute Name="EncryptionMode">Secure Enterprise Key Manager</Attribute>
    <Component FQDD="Disk.Virtual.0:RAID.Slot.3-1">
        <Attribute Name="RAIDaction">Create</Attribute>
        <Attribute Name="LockStatus">Locked</Attribute>
        <Attribute Name="BootVD">True</Attribute>
        <Attribute Name="RAIDinitOperation">None</Attribute>
        <Attribute Name="DiskCachePolicy">Disabled</Attribute>
        <Attribute Name="RAIDdefaultWritePolicy">WriteBack</Attribute>
        <Attribute Name="RAIDdefaultReadPolicy">ReadAhead</Attribute>
        <Attribute Name="Name">SCP VD</Attribute>
        <Attribute Name="Size">0</Attribute>
        <Attribute Name="StripeSize">512</Attribute>
        <Attribute Name="SpanDepth">1</Attribute>
        <Attribute Name="SpanLength">2</Attribute>
        <Attribute Name="RAIDTypes">RAID 1</Attribute>
        <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.0:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
        <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.1:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
    </Component>
</Component>
```

```
</SystemConfiguration>
```

The SCP file is located on HTTP share and imported by using the RACADM `set` command to import it.

8. After the SCP import job is marked as completed, verify configuration results to see what changes are applied.
9. Check storage configuration now to ensure that the PERC is in SEKM mode along with locked volume created.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set -f 2019-5-17_135217_export.xml -t xml
-l http://100.65.84.72/http_share_vm
```

RAC977—Import configuration XML file operation initiated. Use the "racadm jobqueue view -i JID_581203847849" command to view the status of the operation.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID_581203847849
---------------------------- JOB -------------------------
[Job ID=JID_581203847849]
Job Name=Configure: Import Server Configuration Profile
Status=Completed
Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Message=[SYS053: Successfully imported and applied Server Configuration Profile.]
Percent Complete=[100]
----------------------------------------------------------


C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn lcllog viewconfigresult -j JID_581203847849
SeqNumber       = 6094
FQDD            = RAID.Slot.3-1
DisplayValue    = PERC H740P Adapter
Name            = PERC H740P Adapter
Status          = Success
DisplayValue    = PERC H740P Adapter
Name            = PERC H740P Adapter
Status          = Success
DisplayValue    = SCP VD
Name            = SCP VD
NewValue        = RAID 1
NewValue        = Physical Disk 0:1:0
NewValue        = Physical Disk 0:1:1
NewValue        = Virtual Disk Size in Bytes : 899527213056
NewValue        = Virtual Disk Stripe Size : 256 Kb
NewValue        = Physical Disks per Span : 2
NewValue        = VirtualDisk Lock status: Locked
Status          = Success
DisplayValue    = RAIDbootVD
Name            = RAIDbootVD
OldValue        = None
```

```
NewValue        = Disk.Virtual.0:RAID.Slot.3-1
Status          = Success
SeqNumber       = 6091
FQDD            = RAID.Slot.3-1
DisplayValue    = PERC H740P Adapter
Name            = PERC H740P Adapter
Status          = Success
DisplayValue    = PERC H740P Adapter
Name            = PERC H740P Adapter
Status          = Success


C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get controllers -o -p
encryptionmode,keyid
RAID.Slot.3-1
   EncryptionMode                   = Secure Enterprise Key Manager
   KeyID                            =
B13FCCB4D926F0AEA37A718856F366E78F7D4AB6D76B793FAACB01D05993D22E
AHCI.Embedded.2-1
   EncryptionMode                   = None
   KeyID                            = null
AHCI.Slot.6-1
   EncryptionMode                   = None
   KeyID                            = null
AHCI.Embedded.1-1
   EncryptionMode                   = None
   KeyID                            = null



C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get vdisks -o
Disk.Virtual.0:RAID.Slot.3-1
   Status                           = Ok
   DeviceDescription                = Virtual Disk 0 on RAID Controller in Slot 3
   Name                             = SCP VD
   RollupStatus                     = Ok
   State                            = Online
   OperationalState                 = Not applicable
   Layout                           = Raid-1
   Size                             = 837.750 GB
   SpanDepth                        = 1
   AvailableProtocols               = SAS
   MediaType                        = HDD
   ReadPolicy                       = Read Ahead
   WritePolicy                      = Write Back
   StripeSize                       = 256K
   DiskCachePolicy                  = Disabled
```

```
BadBlocksFound                   = NO
Secured                          = YES
RemainingRedundancy              = 1
EnhancedCache                    = Not Applicable
T10PIStatus                      = Disabled
                                    BlockSizeInBytes                 = 512
```

6 Troubleshoot issues while setting up SEKM on iDRAC

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

6.1 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.

6.2 I set up the KMS information and uploaded the 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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.

6.8 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.

6.9 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.

6.10 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.

6.11 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.

6.12 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.

6.13 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.

6.14 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.

6.15 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).

6.16 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**.

6.17 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.

6.18 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.

6.19 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.

6.20 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.

Conclusion

Security has always been the highest challenge in data management and server solutions applications. Dell EMC PowerEdge servers, along with iDRAC, have been ensuring that your business-critical data is secure. The Secure Key Enterprise Management (SEKM)—in partnership with Gemalto—is now strengthening such security features for the PowerEdge customers. In this technical white paper, the procedure to enable the SEKM on iDRAC, PERC, and Storage Controller—by using both iDRAC and RACAM interfaces—is discussed. At the end of this technical white paper, tips and resolutions to some commonly faced issues are also discussed.

A Technical support and resources

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