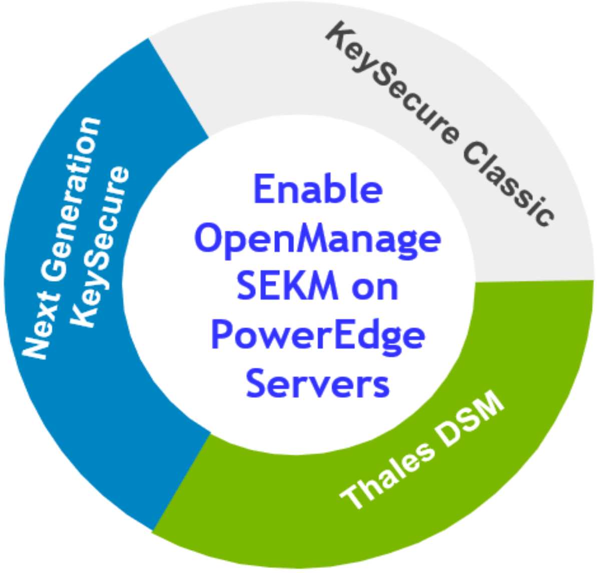
Configuration and Deployment Guide

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

This Dell 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.


KeySecure Classic
Next Generation KeySecure
Thales DSM
Enable OpenManage SEKM on PowerEdge Servers

Abstract

Keeping your business-critical operations and IT infrastructure safe and secure is key to providing seamless services. Dell provides the OpenManage Secure Enterprise Key Manager (SEKM) that assists iDRAC (the Dell 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 SEKM for supported Key Management Servers such as KeySecure Classic, Vormetric Data Security Manager, and Next Generation Key Manager (branded as CipherTrust Manager at the time of release of this guide). Also, a few important tips and troubleshooting steps are provided to help you effectively use this SEKM on your PowerEdge servers.

April 2022

Revisions

Date	Description
July 2019	Initial release
June 25, 2020	Added procedures related to KeySecure Classic, Thales Data Security Manager (DSM), and CipherTrust Manager (previously branded as Next Generation KeySecure)
September 2020	Added extra information about including IP information during setup and configuration
December 2021	Added information on how to configure SEKM solution with Redfish. Also added information on new support for SAS HBA, direct attach NVMe SEDs, and PERC LKM to SEKM transition.
April 2022	Change highlights: • Added supported storage controller table. • Removed reference to old storage config page. • Included note about “Download CSR” option introduced in UI for SRA. • Added automated deployment section (references SEKM scripting GitHub page). • Each storage device has its own section for enabling security. • Added additional Redfish calls for each storage device. • Added references to PERC / HBA user guides. • Added reference to SSD Encryption overview

Acknowledgements

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

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

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.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

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

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 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 PERC 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 and eliminates the hassle of passphrase management with PERC LKM.
- SEKM supports the industry standard OASIS KMIP protocol thus enabling use of any external third party KMIP server.

1 Supported storage devices and related properties

Storage controller	SEKM support	Minimum firmware version required
PERC H755 Front	Yes	52.16.1-4074
PERC H755N Front	Yes	52.16.1-4074
PERC H755 Adapter	Yes	52.16.1-4074
PERC H740P Mini	Yes	51.13.2-3714
PERC H740P Adapter	Yes	51.13.2-3714
HBA 355i Adapter	Yes (supported on VxRail platforms only)	17.15.08.00
HBA 355i Front	Yes (supported on VxRail platforms only)	17.15.08.00

Note: SEKM is not supported on PERC H840 Adapter

Device	Security Properties	Values	Description
PERC	Encryption Capability	“None | Local Key Management and Secure Enterprise Key Manager Capable”	Indicates if PERC supports encryption
	Encryption Mode	“None | Local Key Management | Secure Enterprise Key Manager”	Indicates current Encryption Mode for PERC
	Security Status	“Security Key Assigned”	Indicates current security status for PERC

Device	Security Properties	Values	Description
HBA	Encryption Capability	“Not Capable | Capable”	Indicates if HBA is security capable
	Encryption Mode	“Not Applicable”	HBA does not support encryption mode such as LKM or SEKM. Hence Encryption Mode is not applicable.
	Security Status	“Not Capable | Disabled | Enabled”	Indicates current security status for HBA

Device	Security Properties	Values	Description
NVMe/SAS SED	Encryption Capability	“Not Capable | Capable”	Indicates if the drive is security capable
	Security Status	“Not Capable | Encryption Capable | Secured | Locked | Foreign”	Indicates current security status of the drive
	Encryption Protocol	“None | TCG Enterprise SSC | TCG Opal SSC”	Indicates encryption protocol supported by the drive

Note: SEKM is only supported on direct attach NVMe SEDs that support TCG Opal 2.0 protocol.

Note: SEKM is only supported on SAS drives behind HBA that support TCG protocol.

For more information about TCG SEDs, see SSD Encryption Overview (delltechnologies.com)

2 CipherTrust Manager (k170v)

2.1 Prerequisites for CipherTrust Manager

Before you start setting up iDRAC SEKM support, you must first ensure that the following prerequisites are fulfilled.

PowerEdge Server Prerequisites

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

Note: To avoid an additional iDRAC firmware update, it is highly 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.

CipherTrust Manager Prerequisites

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

2.2 Automated Deployment

After configuring Auto-Client registration and KMIP interface on CipherTrust (below), you will be able to use automated python script to set up complete SEKM solution on iDRAC. For more details, see SEKM scripting GitHub page.

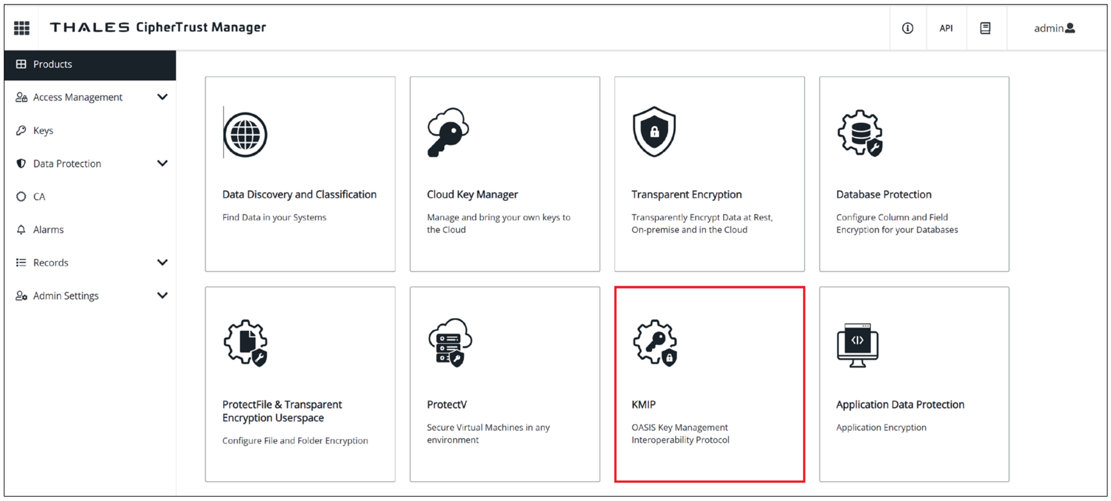
GitHub - dell/iDRAC-SEKM-Scripting: Dell Secure Enterprise Key Manager (SEKM) python scripts for configuring complete iDRAC SEKM solution.

2.3 Set up SEKM on CipherTrust Manager

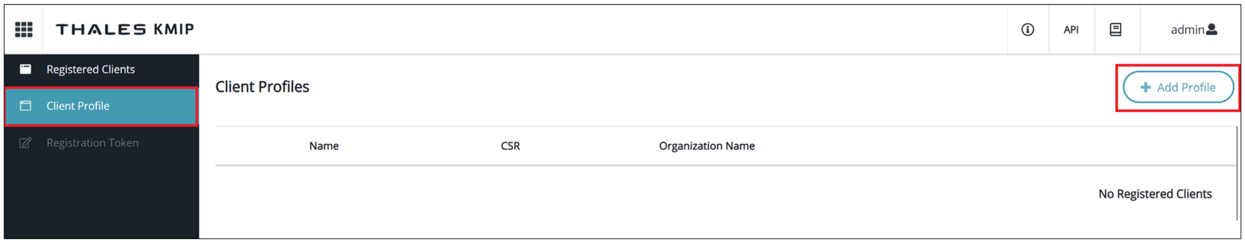
This section describes the CipherTrust Manager features that are supported by iDRAC. For information about all other CipherTrust features, see the CipherTrust Appliance Administration Guide.

2.3.1 Configure Auto-Client Registration

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


THALES CipherTrust Manager
API
admin
Products
Access Management
Keys
Data Protection
CA
Alarms
Records
Admin Settings
Data Discovery and Classification
Find Data in your Systems
Cloud Key Manager
Manage and bring your own keys to the Cloud
Transparent Encryption
Transparently Encrypt Data at Rest, On-premise and in the Cloud
Database Protection
Configure Column and Field Encryption for your Databases
ProtectFile & Transparent Encryption Userspace
Configure File and Folder Encryption
ProtectV
Secure Virtual Machines in any environment
KMIP
OASIS Key Management Interoperability Protocol
Application Data Protection
Application Encryption

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

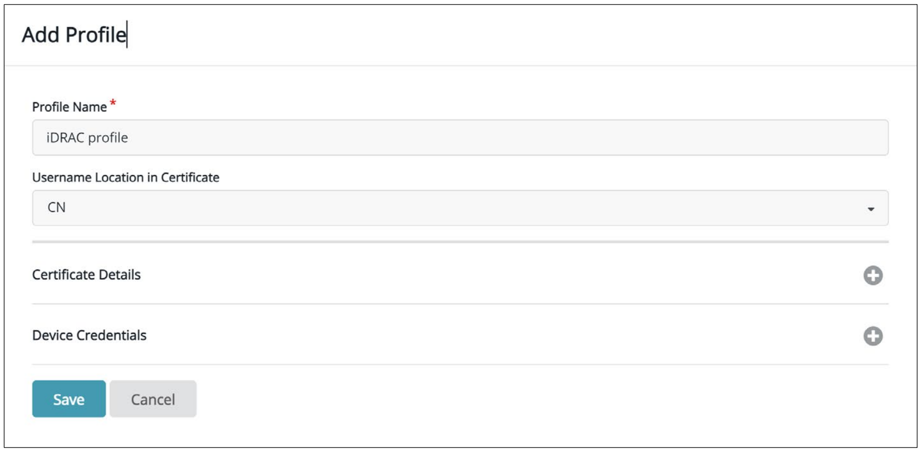


Client Profiles

Name	CSR	Organization Name

No Registered Clients

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


Add Profile

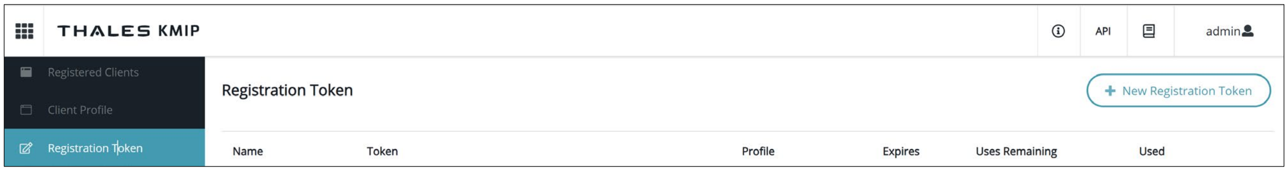
Profile Name *
iDRAC profile

Username Location in Certificate
CN

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

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

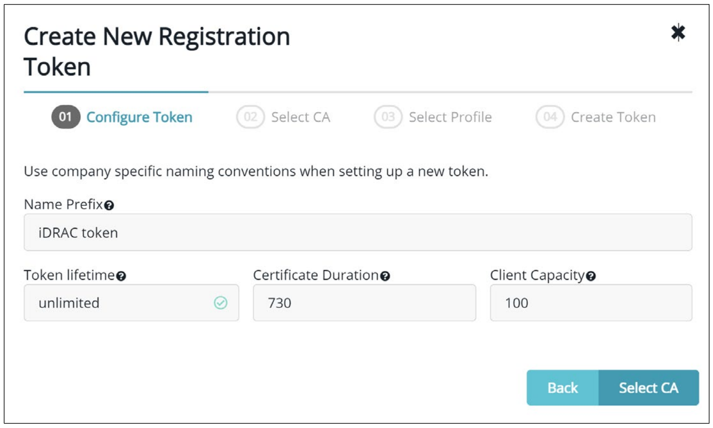
4. Click Registration Token → New Registration Token.



Registration Token

Name	Token	Profile	Expires	Uses Remaining	Used

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



Create New Registration Token

Use company specific naming conventions when setting up a new token.

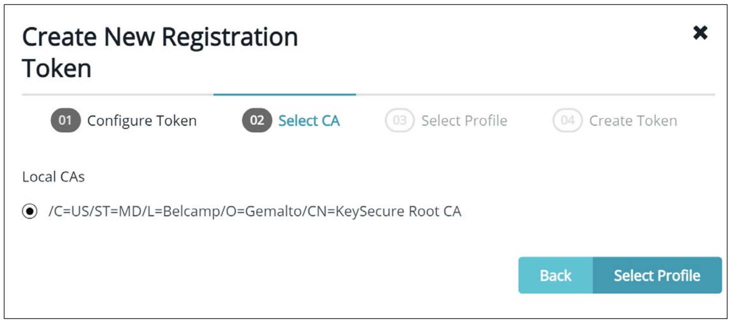
Name Prefix: iDRAC token

Token lifetime: unlimited

Certificate Duration: 730

Client Capacity: 100

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

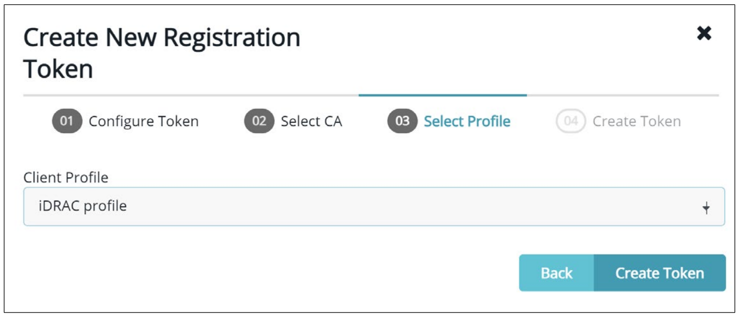


Create New Registration Token

Local CAs

● /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA

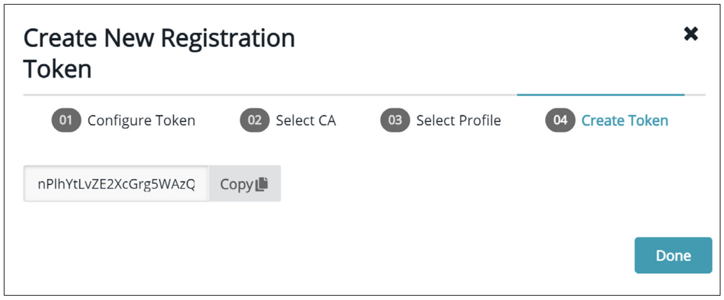
7. Select the profile you created, and then click **Create Token**.



Create New Registration Token

Client Profile: iDRAC profile

8. Copy the registration token.

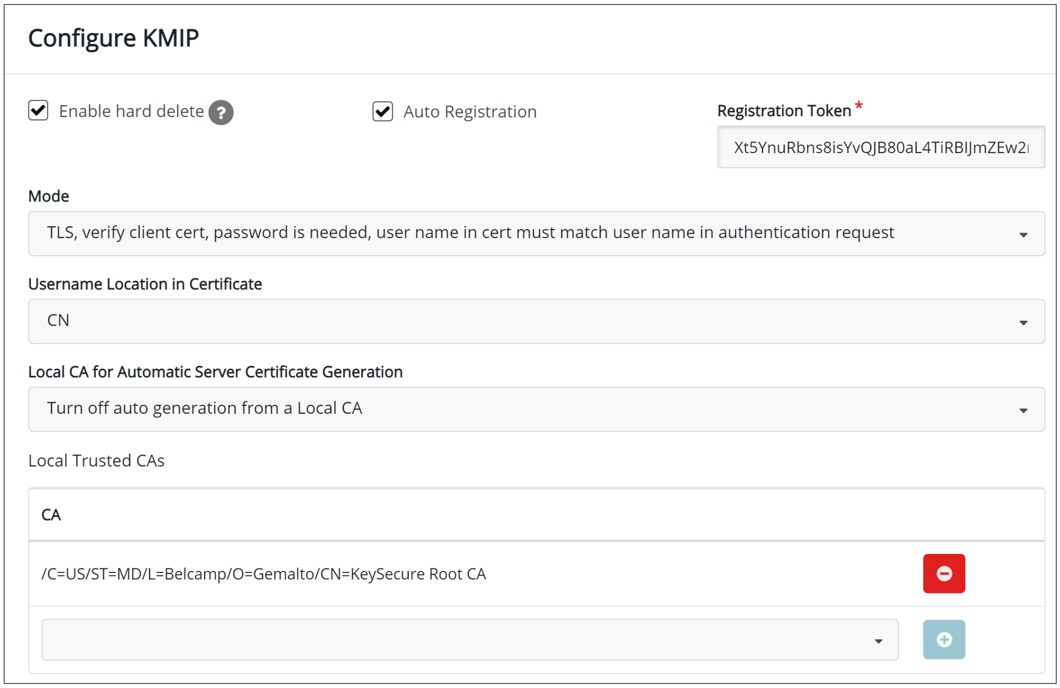


Create New Registration Token

nPlhYtLvZE2XcGrg5WAzQ

9. Navigate back to CipherTrust home page, click Admin settings
10. Click Interfaces -> Click Ellipses next to KMIP interface -> click Edit.
11. Select the **Auto Registration** check box.

12. Paste the token that you copied into the **Registration Token** box
13. Select Enable hard delete



Configure KMIP

☑ Enable hard delete ?

☑ Auto Registration

Registration Token *: Xt5YnuRbns8isYvQJB80aL4TiRBIJmZEw2

Mode: TLS, verify client cert, password is needed, user name in cert must match user name in authentication request

Username Location in Certificate: CN

Local CA for Automatic Server Certificate Generation: Turn off auto generation from a Local CA

Local Trusted CAs

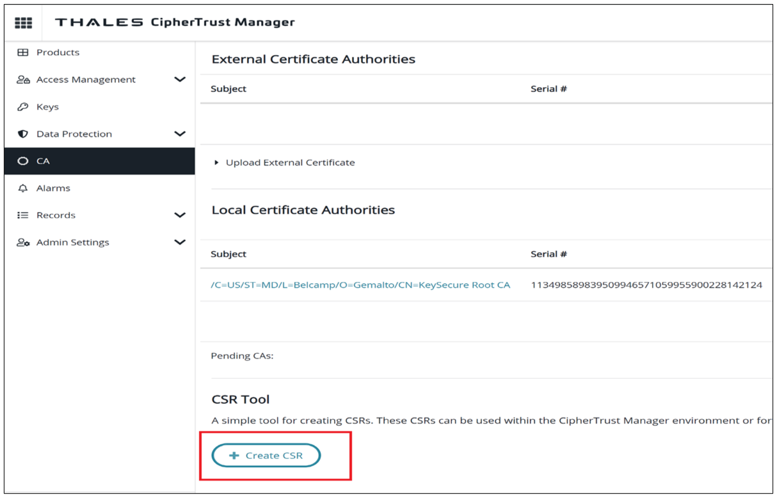
CA
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA

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

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

2.3.2 Configure KMIP Interface

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



External Certificate Authorities

Subject	Serial #

Local Certificate Authorities

Subject	Serial #
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA	113498589839509946571059955900228142124

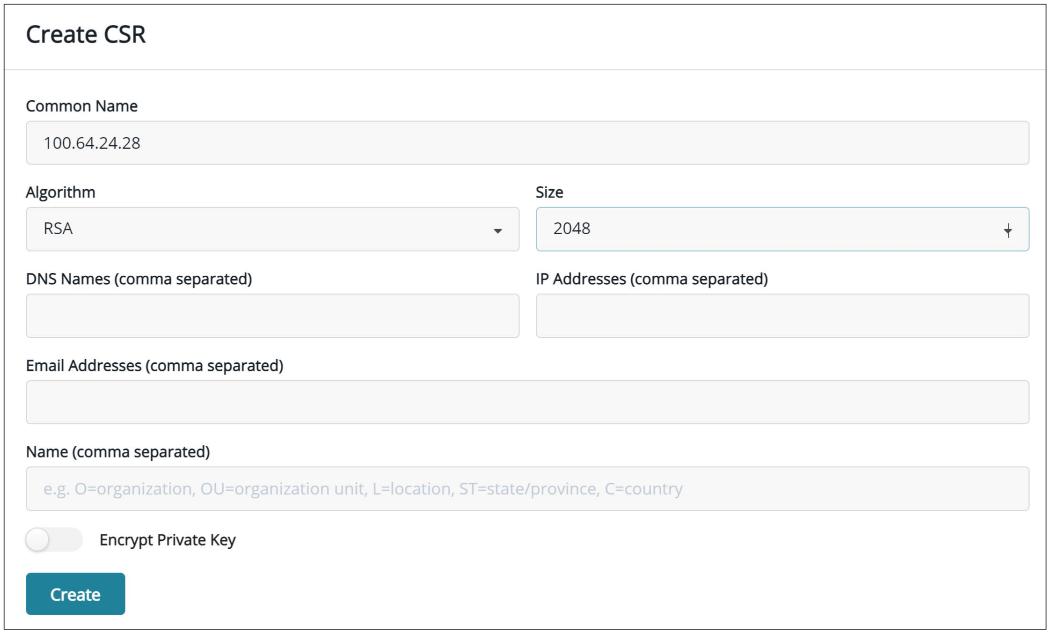
Pending CAs:

CSR Tool

A simple tool for creating CSRs. These CSRs can be used within the CipherTrust Manager environment or for

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

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



Common Name: 100.64.24.28

Algorithm: RSA

Size: 2048

DNS Names (comma separated):

IP Addresses (comma separated):

Email Addresses (comma separated):

Name (comma separated): e.g. O=organization, OU=organization unit, L=location, ST=state/province, C=country

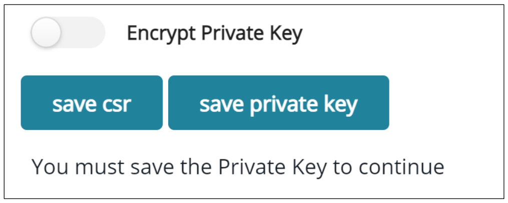
○ Encrypt Private Key

Note: If you have used an older version of Gemalto (k150v), “Subject Alternative Name” field has been split into two separate fields – DNS Names and IP addresses.

In the example above, we have included the IP address of CipherTrust in the Common Name field.

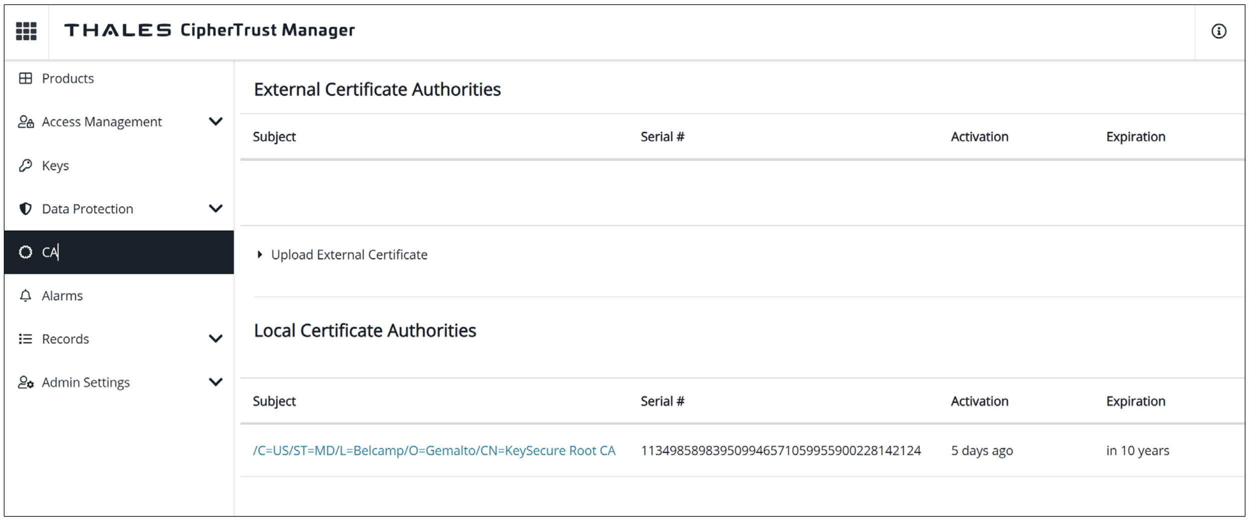
- Algorithm—RSA
- Size—2048

3. Click both the buttons.



You must save the Private Key to continue

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



External Certificate Authorities

Subject	Serial #	Activation	Expiration

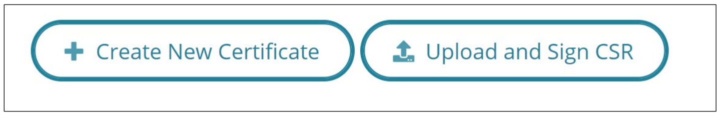
Local Certificate Authorities

Subject	Serial #	Activation	Expiration
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA	113498589839509946571059955900228142124	5 days ago	in 10 years

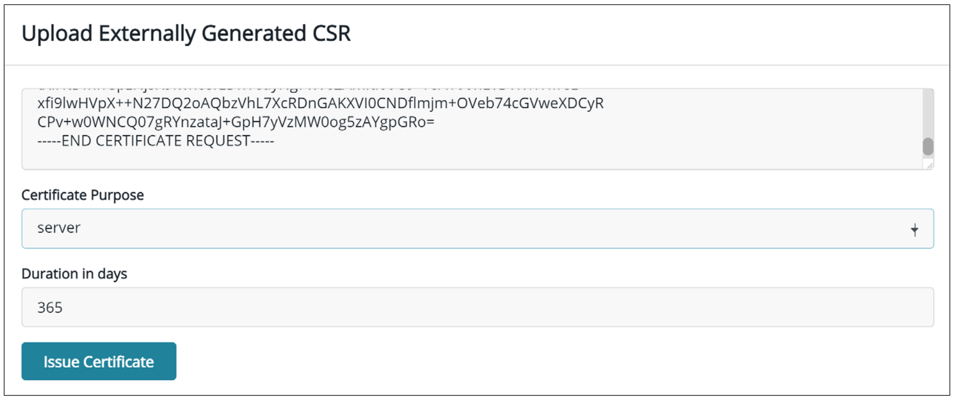
5. Select the Certificate Authority (CA).

6. After you select the CA, the Create New Certificate and Upload and Sign CSR buttons are displayed.

7. Select Upload and Sign CSR, and then upload the contents from the CSR you generated in the above steps.



8. Upload the externally generated CSR.



Upload Externally Generated CSR

```
xfi9lwHVpX++N27DQ2oAQbzVhL7XcRDnGAKXVI0CNDflmjm+OVeb74cGVweXDCyR
CPv+w0WNCQ07gRYnzataJ+GpH7yVzMW0og5zAYgpGRo=
-----END CERTIFICATE REQUEST-----
```

Certificate Purpose: server

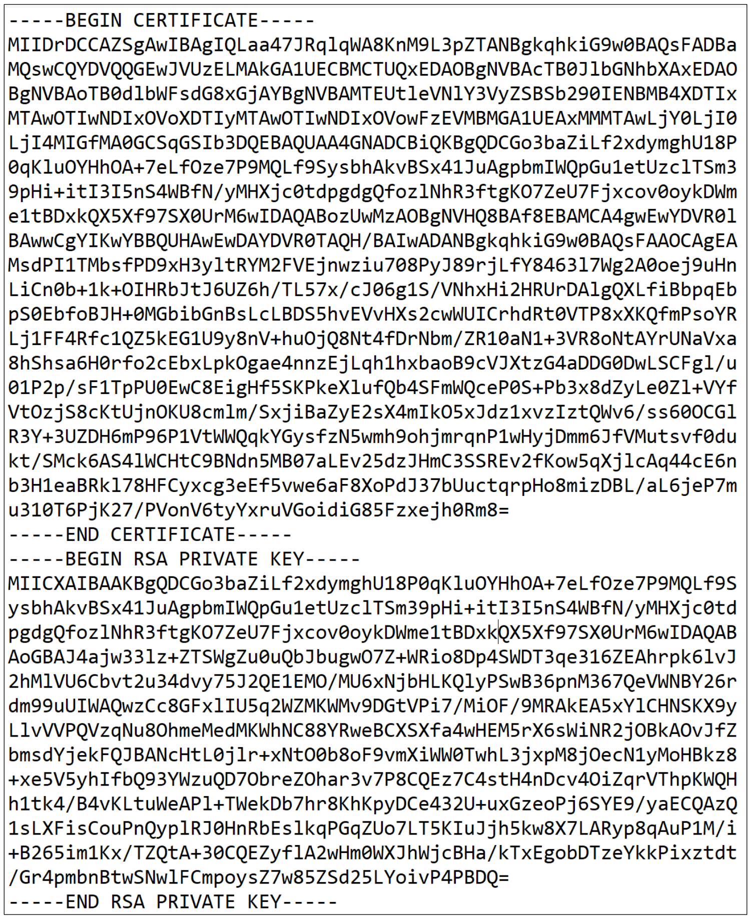
Duration in days: 365

Note: Make sure you select **server** for Certificate Purpose

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

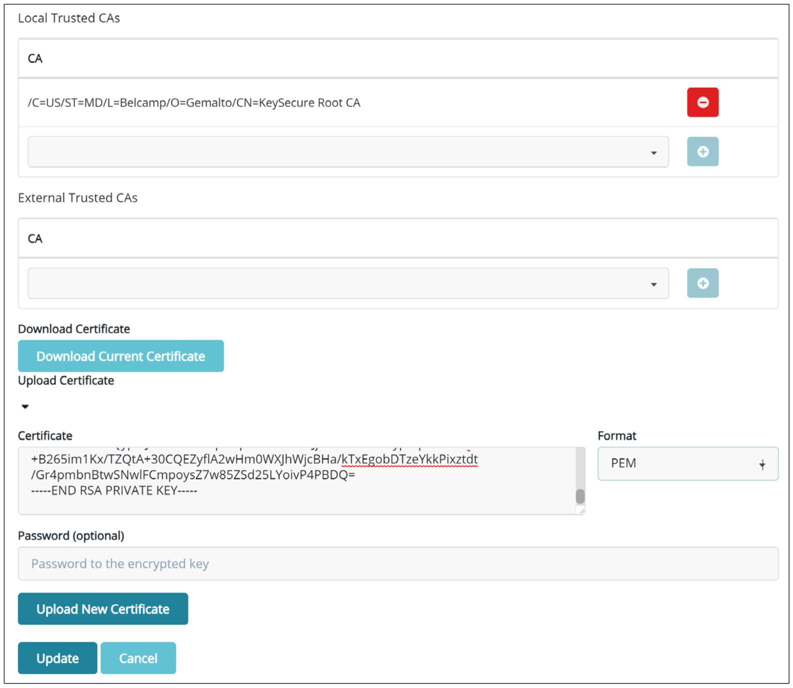
9. Click the ellipses (…) symbol, download the signed certificate, and then save it to your system.

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



```
-----BEGIN CERTIFICATE-----
MIIDrDCCAZSgAwIBAgIQLaa47JRqlqWA8KnM9L3pZTANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO
BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx
MTAwOTIwNDIxOVoXDTIyMTAwOTIwNDIxOVowFzEVMBMGA1UEAxMMMTAwLjY0LjI0
LjI4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCGo3baZiLf2xdymghU18P
0qKluOYHhOA+7eLfOze7P9MQLf9SysbhAkvBSx41JuAgpbmIWQpGu1etUzclTSm3
9pHi+itI3I5nS4WBfN/yMHXjc0tdpgdgQfozlNhR3ftgKO7ZeU7Fjxcov0oykDWm
e1tBDxkQX5Xf97SX0UrM6wIDAQABozUwMzAOBgNVHQ8BAf8EBAMCA4gwEwYDVR0l
BAwwCgYIKwYBBQUHAwEwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAgEA
MsdPI1TMbsfPD9xH3yltRYM2FVEjnwziu708PyJ89rjLfY84631 7Wg2A0oej9uHn
LiCn0b+1k+OIHRbJtJ6UZ6h/TL57x/cJ06g1S/VNhxHi2HRUrDAlgQXLfiBbpqEb
pS0EbfoBJH+0MGbibGnBsLcLBDS5hvEVvHXs2cwWUICrhdRt0VTP8xXKQfmPsoYR
Lj1FF4Rfc1QZ5kEG1U9y8nV+huOjQ8Nt4fDrNbm/ZR10aN1+3VR8oNtAYrUNaVxa
8hShsa6H0rfo2cEbxLpkOgae4nnzEjLqh1hxbaoB9cVJXtzG4aDDG0DwLSCFgl/u
01P2p/sF1TpPU0EwC8EigHf5SKPkeXlufQb4SFmWQceP0S+Pb3x8dZyLe0Zl+VYf
VtOzjS8cKtUjnOKU8cmlm/SxjiBaZyE2sX4mIkO5xJdz1xvzIztQWv6/ss60OCGl
R3Y+3UZDH6mP96P1VtWWQqkYGysfzN5wmh9ohjmrqnP1wHyjDmm6JfVMutsvf0du
kt/SMck6AS4lWCHtC9BNdn5MB07aLEv25dzJHmC3SSREv2fKow5qXjlcAq44cE6n
b3H1eaBRkl78HFCyxcg3eEf5vwe6aF8XoPdJ37bUuctqrpHo8mizDBL/aL6jeP7m
u310T6PjK27/PVonV6tyYxruVGoidiG85Fzxejh0Rm8=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDCGo3baZiLf2xdymghU18P0qKluOYHhOA+7eLfOze7P9MQLf9S
ysbhAkvBSx41JuAgpbmIWQpGu1etUzclTSm39pHi+itI3I5nS4WBfN/yMHXjc0td
pgdgQfozlNhR3ftgKO7ZeU7Fjxcov0oykDWme1tBDxkQX5Xf97SX0UrM6wIDAQAB
AoGBAJ4ajw33lz+ZTSWgZu0uQbJbugwO7Z+WRio8Dp4SWDT3qe316ZEAhrpk6lvJ
2hMlVU6Cbvt2u34dvy75J2QE1EMO/MU6xNjbHLKQlyPSwB36pnM367QeVWNBY26r
dm99uUIWAQwzCc8GFxlIU5q2WZMKWMv9DGtVPi7/MiOF/9MRAkEA5xYlCHNSKX9y
LlvVVPQVzqNu8OhmeMedMKWhNC88YRweBCXSXfa4wHEM5rX6sWiNR2jOBkAOvJfZ
bmsdYjekFQJBANcHtL0jlr+xNtO0b8oF9vmXiWW0TwhL3jxpM8jOecN1yMoHBkz8
+xe5V5yhIfbQ93YWzuQD7ObreZOhar3v7P8CQEz7C4stH4nDcv4OiZqrVThpKWQH
h1tk4/B4vKLtuWeAPl+TWekDb7hr8KhKpyDCe432U+uxGzeoPj6SYE9/yaECQAzQ
1sLXFisCouPnQyplRJ0HnRbEslkqPGqZUo7LT5KIuJjh5kw8X7LARyp8qAuP1M/i
+B265im1Kx/TZQtA+30CQEZyflA2wHm0WXJhWjcBHa/kTxEgobDTzeYkkPixztdt
/Gr4pmbnBtwSNwlFCmpoysZ7w85ZSd25LYoivP4PBDQ=
-----END RSA PRIVATE KEY-----
```

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



Local Trusted CAs

CA

/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA

External Trusted CAs

CA

Download Certificate

Upload Certificate

Certificate

```
+B265im1Kx/TZQtA+30CQEZyflA2wHm0WXJhWjcBHa/kTxEgobDTzeYkkPixztdt
/Gr4pmbnBtwSNwlFCmpoysZ7w85ZSd25LYoivP4PBDQ=
-----END RSA PRIVATE KEY-----
```

Format: PEM

Password (optional): Password to the encrypted key

Certificate: Contains the signed
Format: PEM

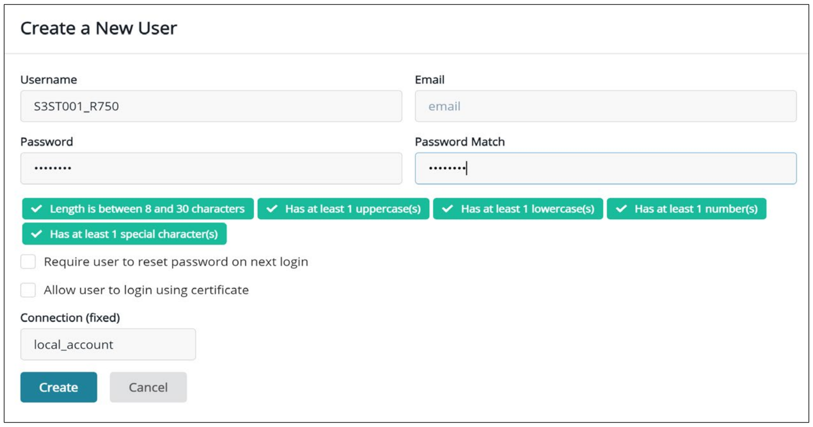
13. Click Upload New Certificate
14. Click Update

Note: A green check mark is displayed after uploading the new certificate. If you are using an older version of CipherTrust (versions 1.10 and below), you will need to restart the KMIP services.

Go to System -> Services -> Restart KMIP

2.3.3 Create a user that represents iDRAC on CipherTrust Manager

1. Click Users → Create New User.



Create a New User

Username: S3ST001_R750

Email: email

Password: ••••••••

Password Match: ••••••••

✓ Length is between 8 and 30 characters ✓ Has at least 1 uppercase(s) ✓ Has at least 1 lowercase(s) ✓ Has at least 1 number(s) ✓ Has at least 1 special character(s)

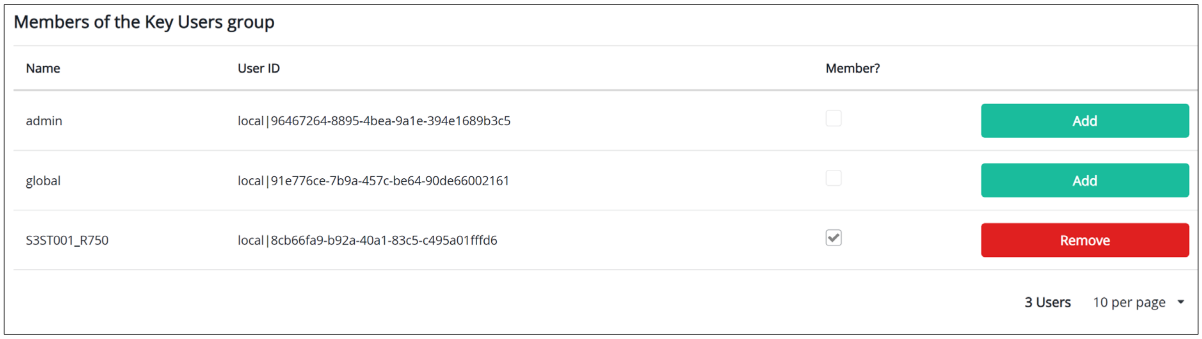
□ Require user to reset password on next login

□ Allow user to login using certificate

Connection (fixed): local_account

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

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



Members of the Key Users group

Name	User ID	Member?	
admin	local|96467264-8895-4bea-9a1e-394e1689b3c5	□	Add
global	local|91e776ce-7b9a-457c-be64-90de66002161	□	Add
S3ST001_R750	local|8cb66fa9-b92a-40a1-83c5-c495a01fffd6	☑	Remove

3 Users 10 per page

2.4 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.

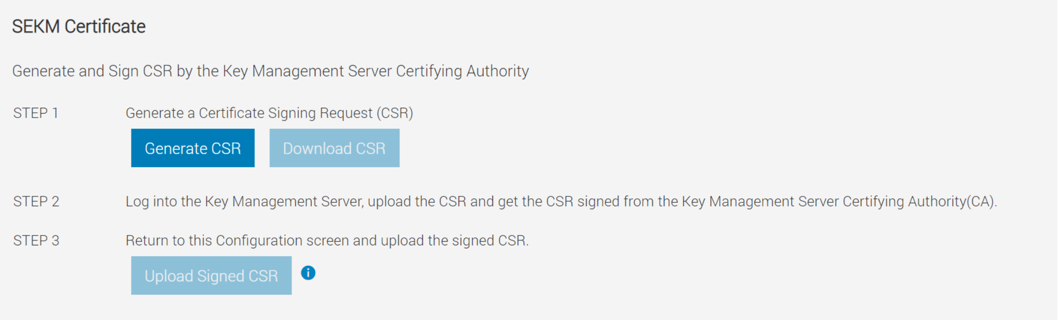
Set up SSL certificate

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.

2.5 Configure SEKM by using the iDRAC GUI

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

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **Storage** -> **SEKM**
3. Click **Generate CSR**



SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

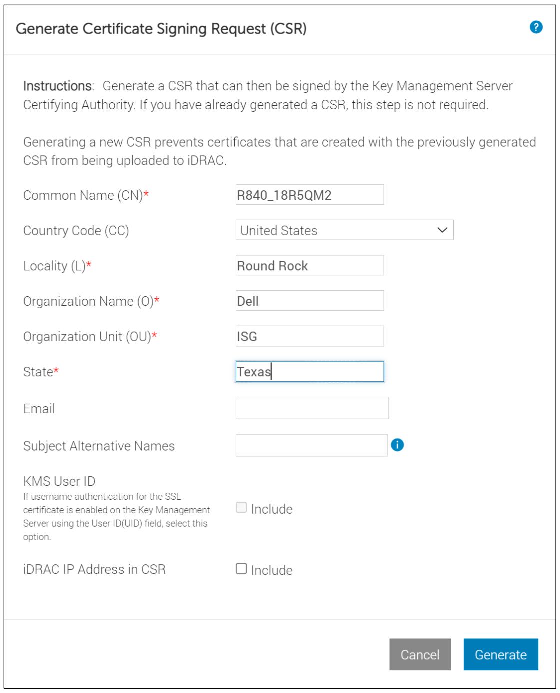
STEP 1 Generate a Certificate Signing Request (CSR)

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.

Note: Download CSR option will become available after generating a CSR.

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



Generate Certificate Signing Request (CSR)

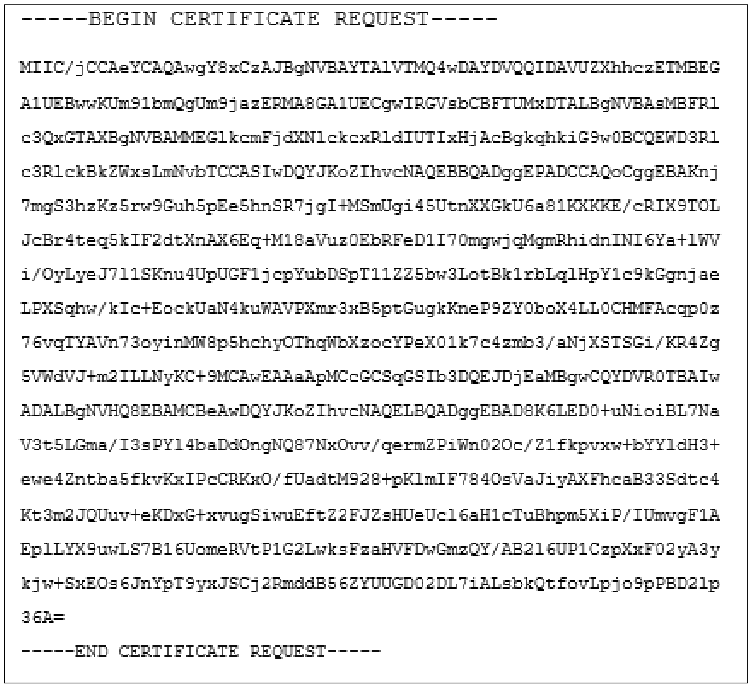
Instructions: Generate a CSR that can then be signed by the Key Management Server Certifying Authority. If you have already generated a CSR, this step is not required.

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

Common Name (CN)*	R840_18R5QM2
Country Code (CC)	United States
Locality (L)*	Round Rock
Organization Name (O)*	Dell
Organization Unit (OU)*	ISG
State*	Texas
Email	
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

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

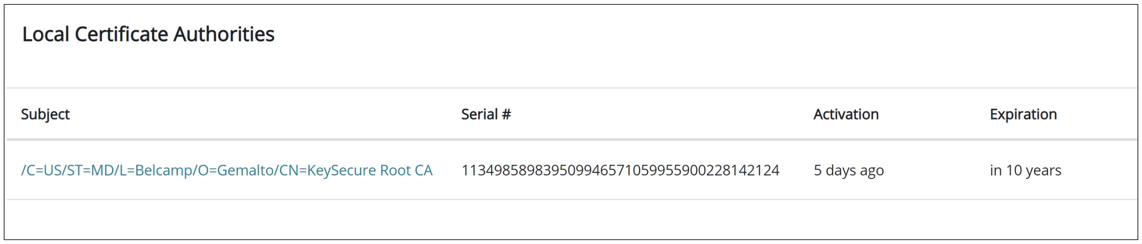
2.6 Get the CSR file signed by CipherTrust Manager



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

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV
i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYY1dH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=
-----END CERTIFICATE REQUEST-----
```

1. Log in to CipherTrust Manager.

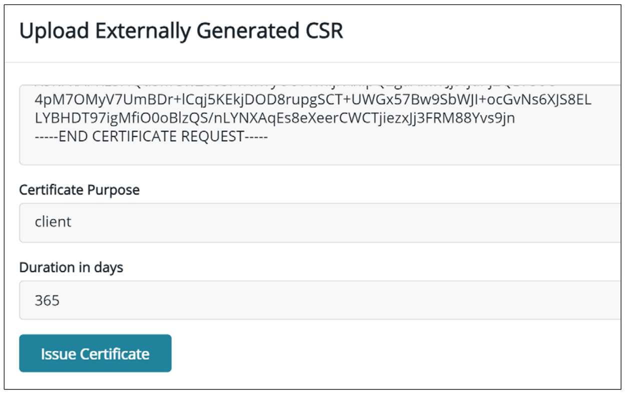
2. Click **CA → Local Certificate Authority**.



Local Certificate Authorities

Subject	Serial #	Activation	Expiration
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA	113498589839509946571059955900228142124	5 days ago	in 10 years

3. Click Upload and Sign CSR.



Upload Externally Generated CSR

```
4pM7OMyV7UmBDr+lCqj5KEkjDOD8rupgSCT+UWGx57Bw9SbWJl+ocGvNs6XJS8EL
LYBHDT97igMfiO0oBlzQS/nLYNXAqEs8eXeerCWCTjiezxJj3FRM88Yvs9jn
-----END CERTIFICATE REQUEST-----
```

Certificate Purpose: client

Duration in days: 365

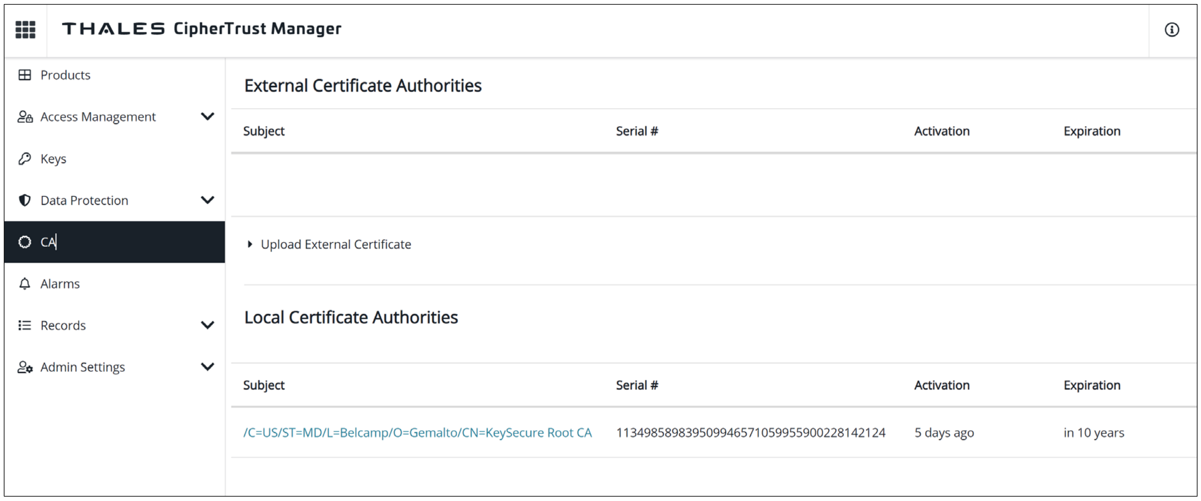
Certificate Purpose: client

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

4. To upload the file you just got signed, navigate to iDRAC Dashboard -> Storage -> SEKM then click **Upload Signed CSR**.
   A message is displayed to indicate the successful upload.

2.6.1 Download the server CA from CipherTrust Manager and upload to iDRAC

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



External Certificate Authorities

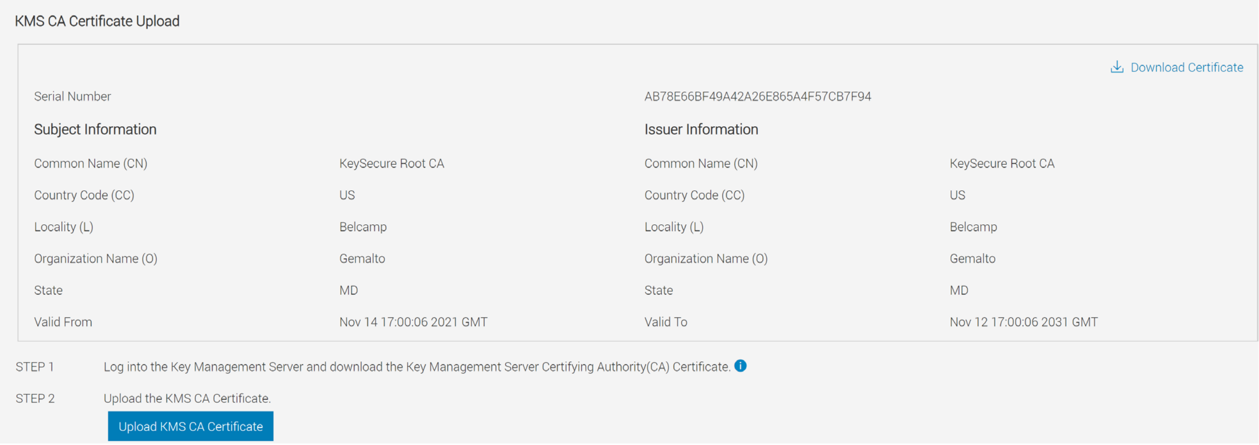
Subject	Serial #	Activation	Expiration

Local Certificate Authorities

Subject	Serial #	Activation	Expiration
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA	113498589839509946571059955900228142124	5 days ago	in 10 years

2. Click the ellipses symbol (…) in the right corner, download, and then save it to your system.

3. Upload it as the KMS CA Certificate on the iDRAC.
   A message is displayed to indicate that the upload was successful.



KMS CA Certificate Upload

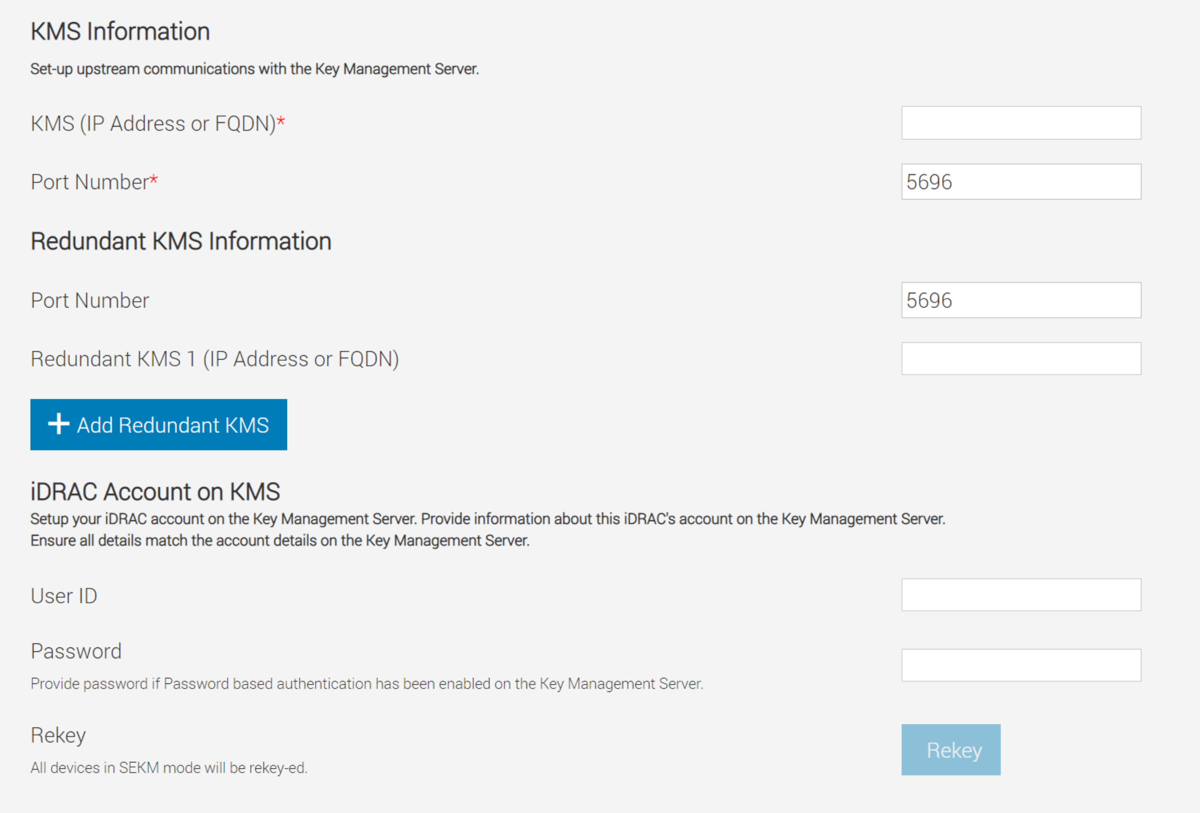
Serial Number		AB78E66BF49A42A26E865A4F57CB7F94	
Subject Information		**Issuer Information**	
Common Name (CN)	KeySecure Root CA	Common Name (CN)	KeySecure Root CA
Country Code (CC)	US	Country Code (CC)	US
Locality (L)	Belcamp	Locality (L)	Belcamp
Organization Name (O)	Gemalto	Organization Name (O)	Gemalto
State	MD	State	MD
Valid From	Nov 14 17:00:06 2021 GMT	Valid To	Nov 12 17:00:06 2031 GMT

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.

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

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



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

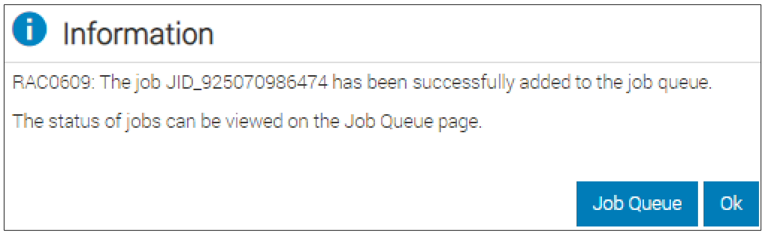
Provide password if Password based authentication has been enabled on the Key Management Server.

Rekey

All devices in SEKM mode will be rekey-ed.

Note: User ID and Password fields must match the user you created on CipherTrust in the above steps.

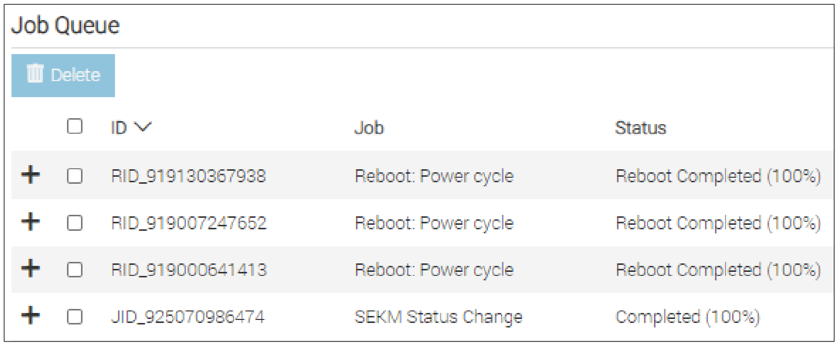
2. Go to the Job Queue page and ensure that the job ID is marked as successfully completed.
3. If you see any job status failures, view Lifecycle Logs for more information about the failure.



RAC0609: The job JID_925070986474 has been successfully added to the job queue.

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

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

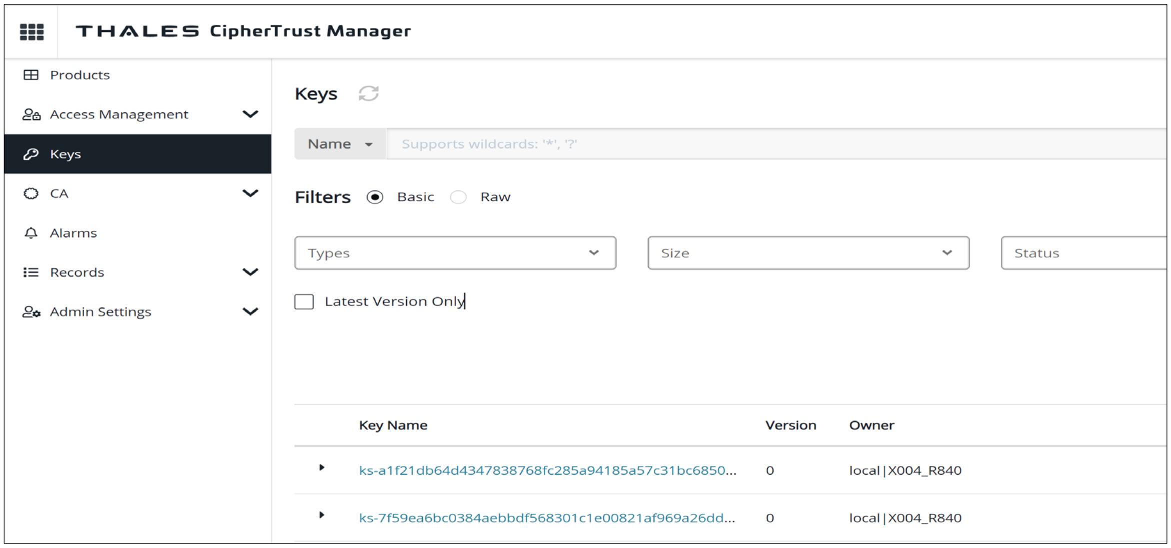


	□	ID	Job	Status
+	□	RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
+	□	RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
+	□	RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
+	□	JID_925070986474	SEKM Status Change	Completed (100%)

iDRAC SEKM configuration with CipherTrust Manager is now complete.

2.8 Viewing iDRAC key ID on CipherTrust Manager

Note: You will not see a key generated for your iDRAC until you enable SEKM on a supported storage device. For details on how to enable SEKM on supported storage devices, see related section for your storage device.



● Basic ○ Raw

□ Latest Version Only

	Key Name	Version	Owner
▸	ks-a1f21db64d4347838768fc285a94185a57c31bc6850...	0	local|X004_R840
▸	ks-7f59ea6bc0384aebbdf568301c1e00821af969a26dd...	0	local|X004_R840

3 KeySecure Classic (k150v)

3.1 Prerequisites for KeySecure Classic

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

PowerEdge Server Prerequisites

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

Key Management Server (KMS) Prerequisites

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

3.2 Set up SEKM on KeySecure Classic

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

SSL Certificate

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

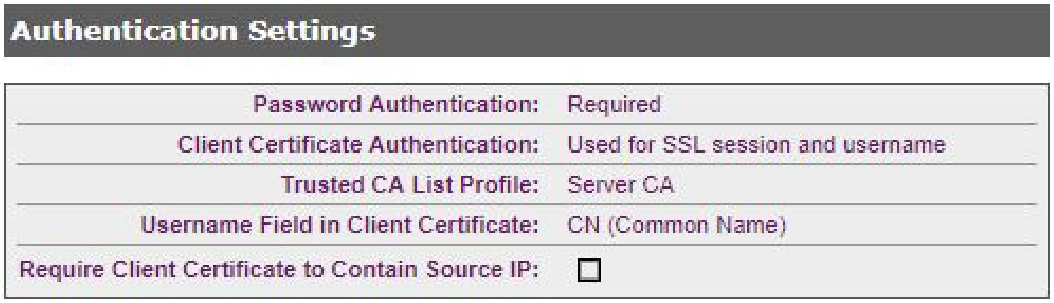
The IP address must be given in the format listed below:

IP:xxx.xxx.xxx.xxx

Users and groups

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

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



Authentication Settings

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:	□

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.

3.3 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.

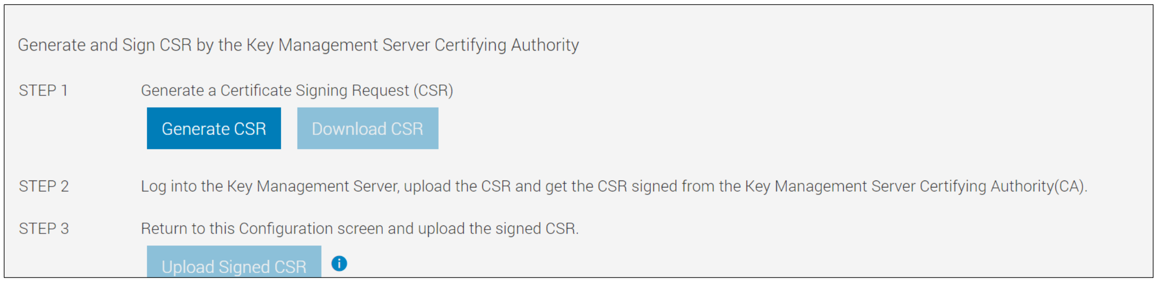
Generate iDRAC CSR
Though most of the CSR properties are standard and self-explanatory, here are a few important guidelines:

- 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.

3.4 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. From iDRAC **Dashboard** -> **Storage** -> **SEKM**
3. Click **Generate CSR**.



Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1 Generate a Certificate Signing Request (CSR)

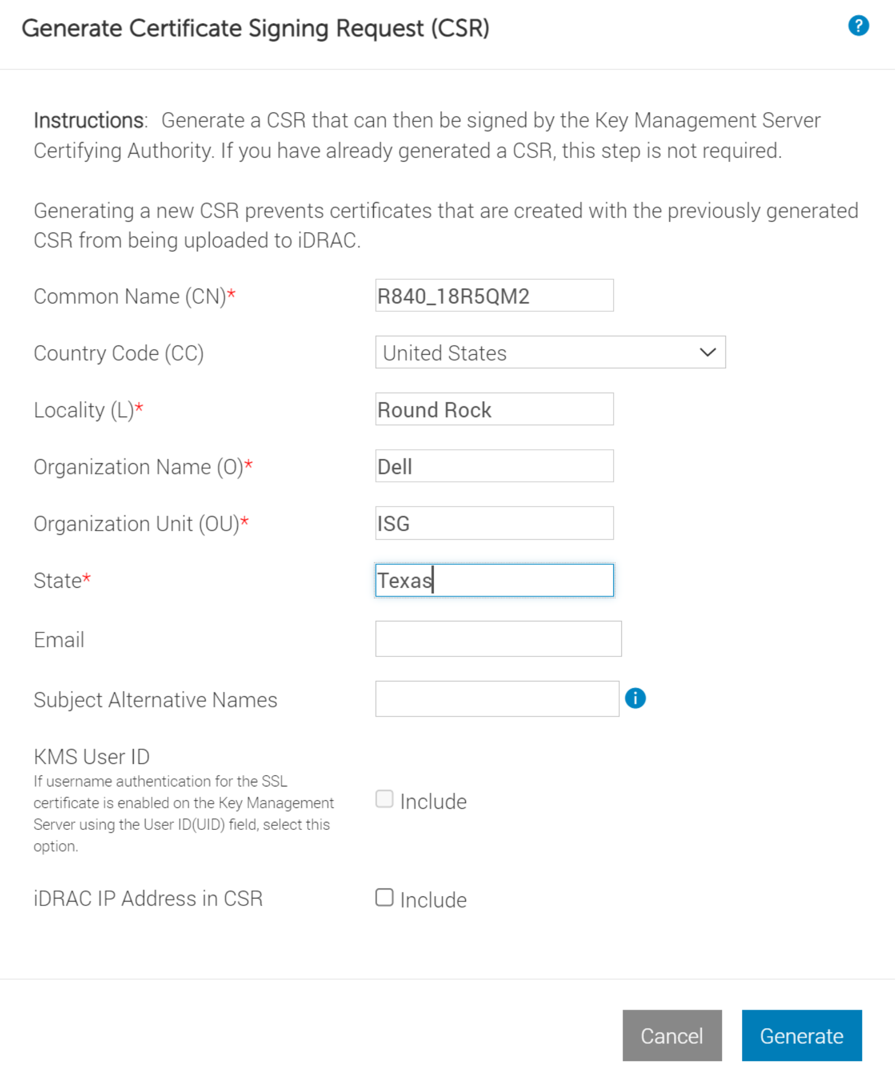
STEP 2 Log into the Key Management Server, upload the CSR and get the CSR signed from the Key Management Server Certifying Authority(CA).

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

Note: Download CSR option will become available after generating a 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.



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)*	R840_18R5QM2
Country Code (CC)	United States
Locality (L)*	Round Rock
Organization Name (O)*	Dell
Organization Unit (OU)*	ISG
State*	Texas
Email	
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

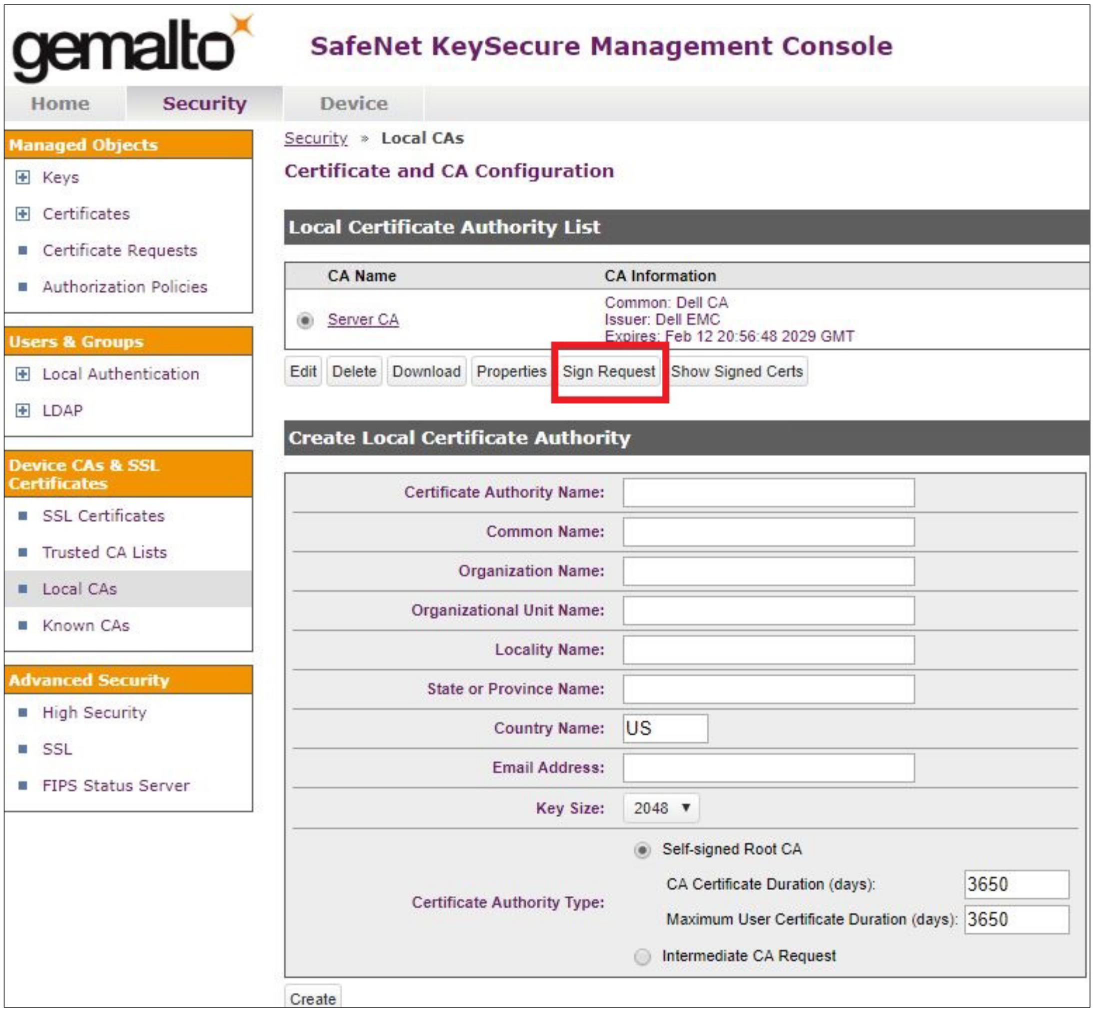
7. Get the full CSR file contents signed on Gemalto. See Get the CSR file signed on Gemalto.
8. Download the signed image file, and then upload it to iDRAC.

3.4.1 Get the CSR file signed on KeySecure Classic

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

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG

A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl

c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl

c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj

7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL

JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+lWV

i/OyLyeJ7l1SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae

LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z

76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
```

```
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB2l6UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=
-----END CERTIFICATE REQUEST-----
```

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



Certificate and CA Configuration

Local Certificate Authority List

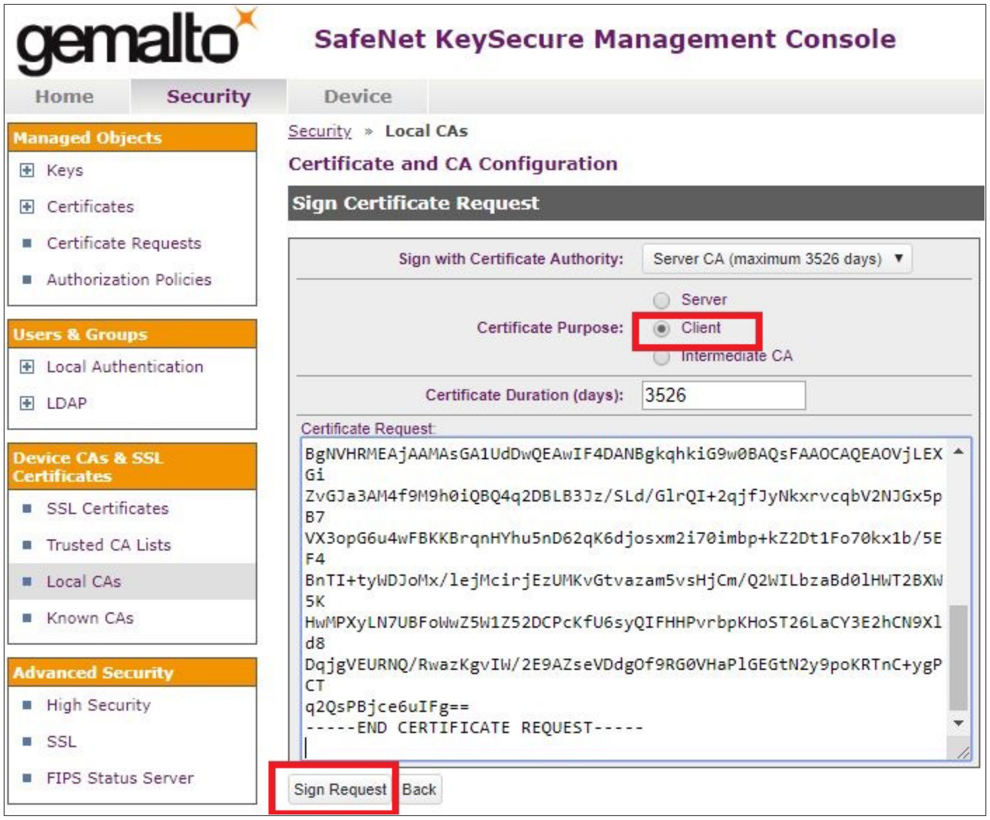
	CA Name	CA Information
●	Server CA	Common: Dell CA Issuer: Dell EMC Expires: Feb 12 20:56:48 2029 GMT

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

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**.



Certificate and CA Configuration

Sign Certificate Request

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

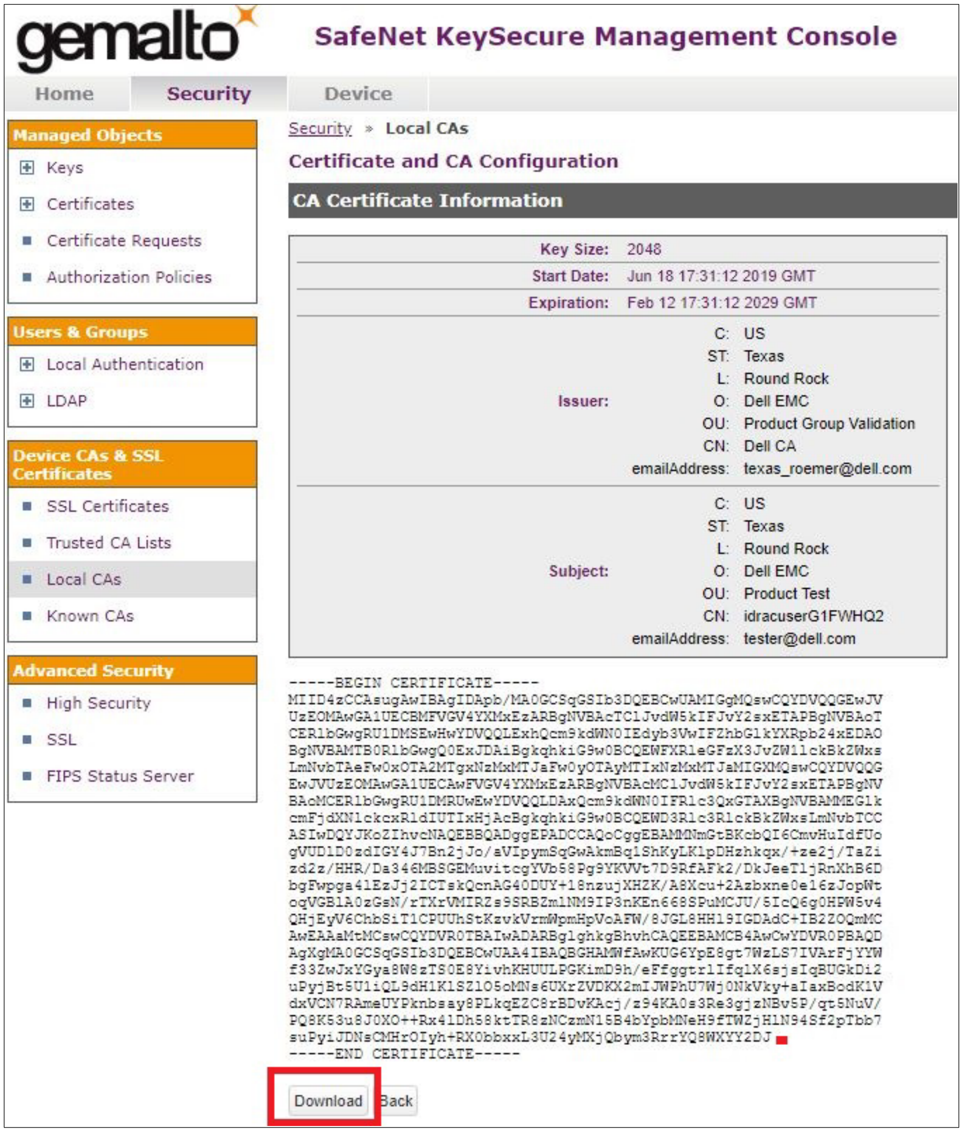
Certificate Purpose: ○ Server ● Client ○ Intermediate CA

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-----
```

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

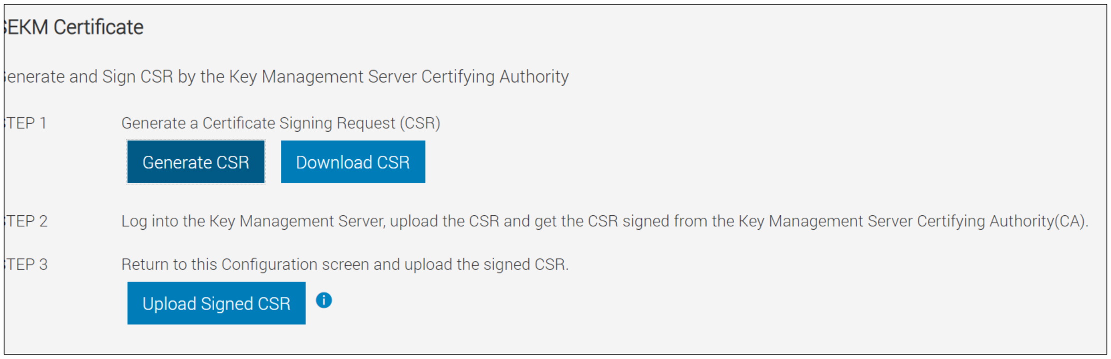
Issuer:
C: US
ST: Texas
L: Round Rock
O: Dell EMC
OU: Product Group Validation
CN: Dell CA
emailAddress: texas_roemer@dell.com

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
gVUD1D0zdIGY4J7Bn2jJo/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-----
```

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.



;EKM Certificate

;enerate and Sign CSR by the Key Management Server Certifying Authority

;TEP 1 Generate a Certificate Signing Request (CSR)

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

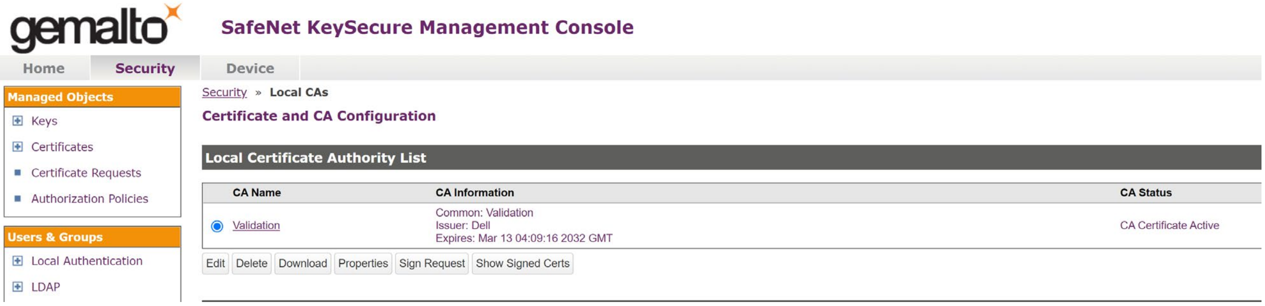
;TEP 3 Return to this Configuration screen and upload the signed CSR.

3.4.2 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.



Security » Local CAs

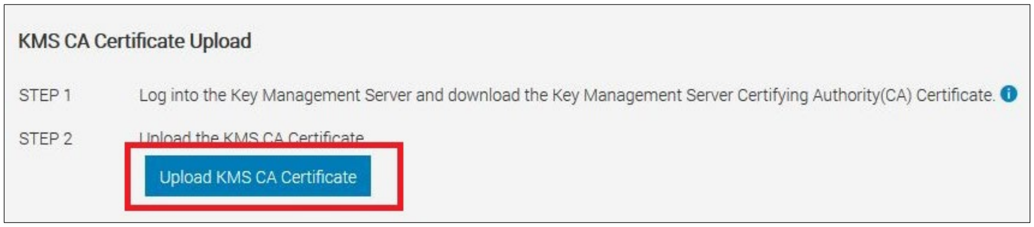
Certificate and CA Configuration

Local Certificate Authority List

CA Name	CA Information	CA Status
● Validation	Common: Validation Issuer: Dell Expires: Mar 13 04:09:16 2032 GMT	CA Certificate Active

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.



KMS CA Certificate Upload

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

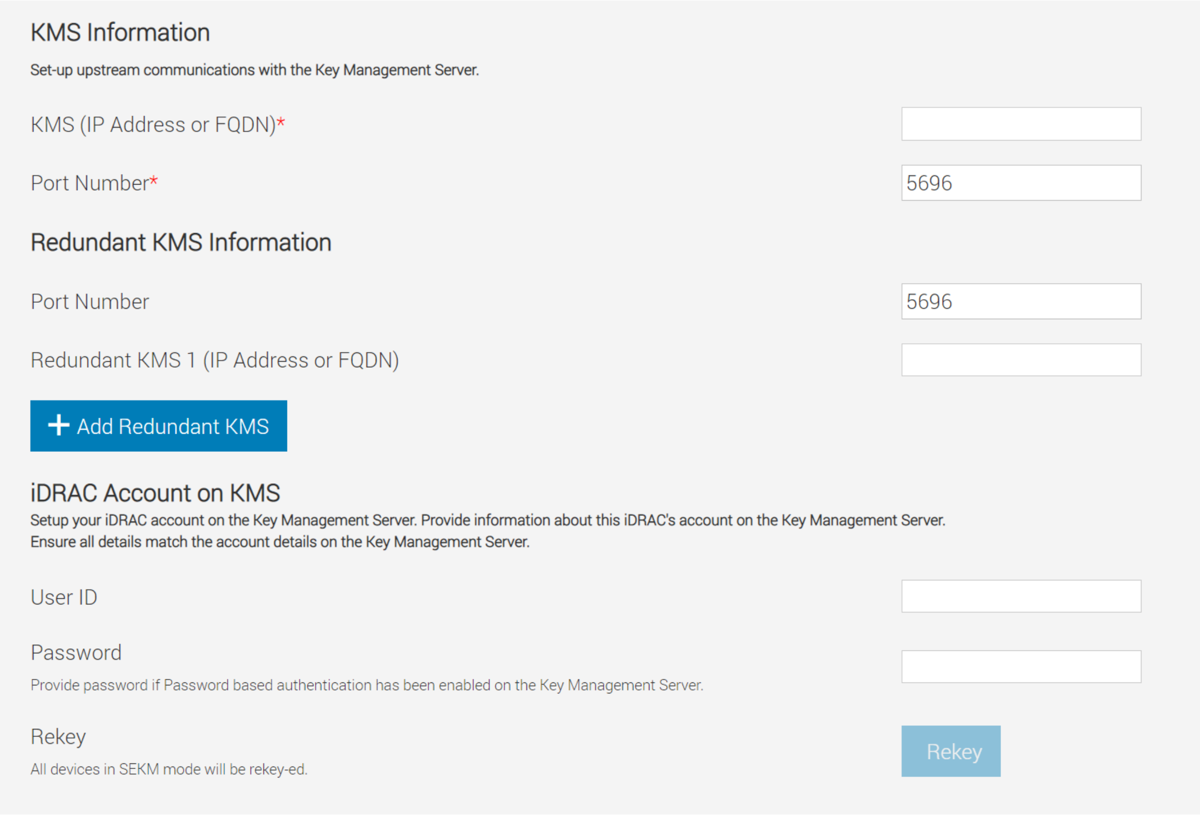
STEP 2 Upload the KMS CA Certificate

3.4.3 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. Now pass in the same username and password in the User ID and Password fields below.



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.

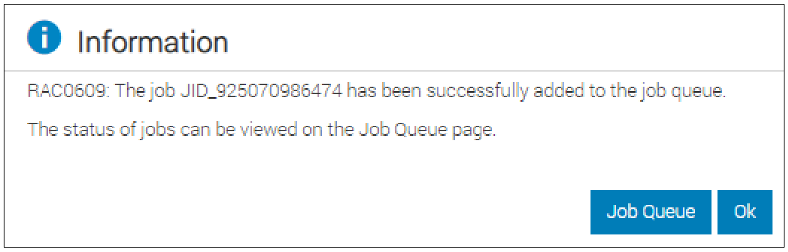
Rekey

All devices in SEKM mode will be rekey-ed.

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.

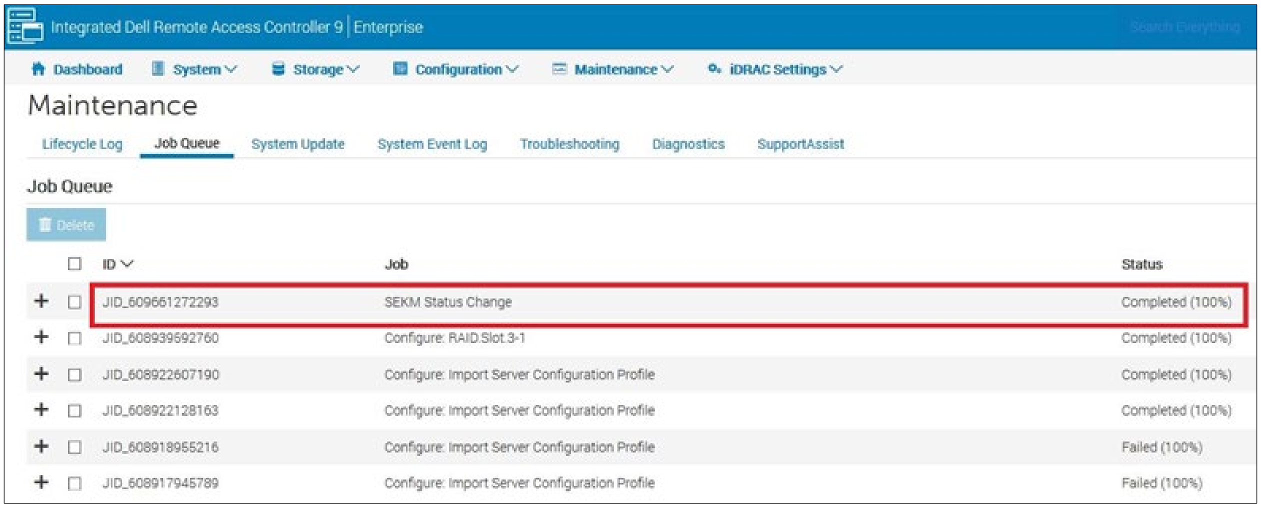
iDRAC SEKM configuration is now complete.



Information

RAC0609: The job JID_925070986474 has been successfully added to the job queue.

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



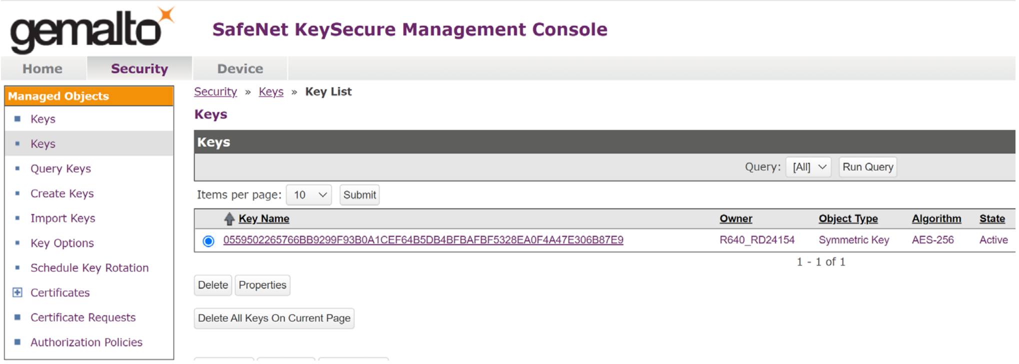
ID	Job	Status
JID_609661272293	SEKM Status Change	Completed (100%)
JID_608939592760	Configure: RAID.Slot.3-1	Completed (100%)
JID_608922607190	Configure: Import Server Configuration Profile	Completed (100%)
JID_608922128163	Configure: Import Server Configuration Profile	Completed (100%)
JID_608918955216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

iDRAC SEKM configuration with KeySecure Classic is now complete.

3.5 Viewing iDRAC key ID on KeySecure Classic

Note: You will not see a key generated for your iDRAC until you enable SEKM on a supported storage device. For details on how to enable SEKM on supported storage devices, see related section for your storage device.

1. Log into KeySecure UI
2. Security -> Keys



Key Name	Owner	Object Type	Algorithm	State
● 0559502265766BB9299F93B0A1CEF64B5DB4BFBAFBF5328EA0F4A47E306B87E9	R640_RD24154	Symmetric Key	AES-256	Active

1 - 1 of 1

4 Thales Data Security Manager (DSM)

4.1 Prerequisites for Thales Data Security Manager (DSM)

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

PowerEdge Server Prerequisites

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

Thales Vormetric DSM Prerequisites

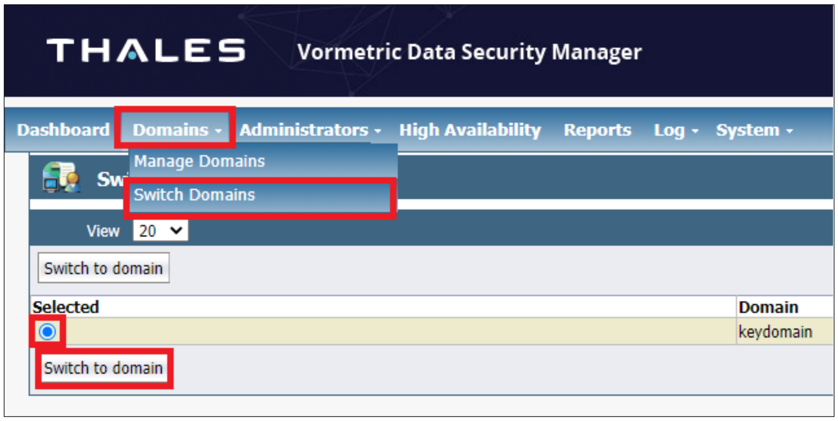
- Set up a valid external certificate authority to sign the iDRAC CSR.
- Create a host that represents the iDRAC on the KMS.
- Ensure a KMIP—enabled license is applied to the DSM. If applying a new KMIP enabled license to an existing DSM for the first time, restart the DSM after applying the license.

4.2 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*.

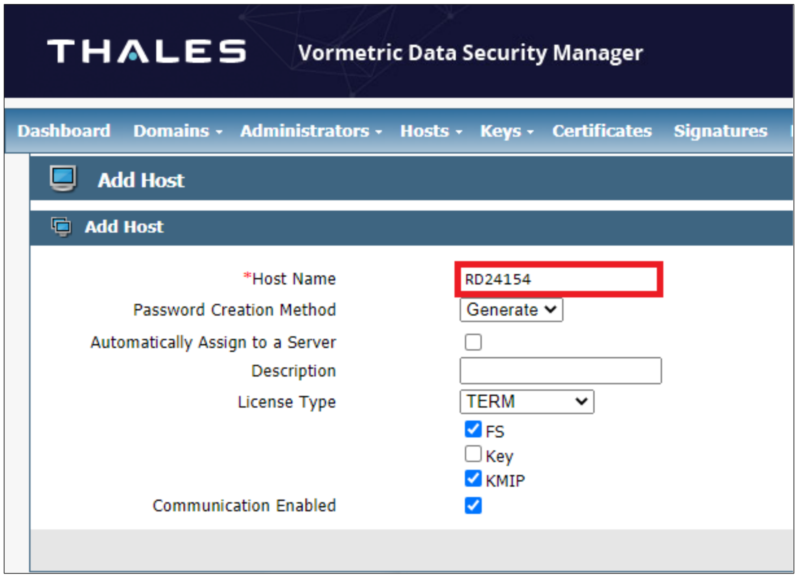
4.2.1 Add a new host in Thales Vormetric Data Security Manager

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**.



Selected	Domain
●	keydomain

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



*Host Name: RD24154

Password Creation Method: Generate

Automatically Assign to a Server: □

Description:

License Type: TERM

☑ FS

□ Key

☑ KMIP

Communication Enabled: ☑

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

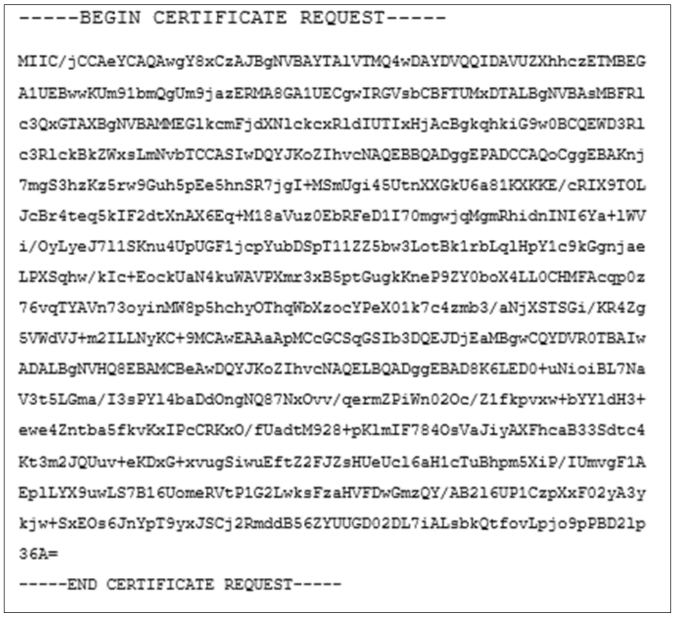
4.2.2 Set up SEKM on iDRAC

See Set up SEKM on iDRAC

4.2.3 Configure SEKM by using the iDRAC GUI

See Configure SEKM by using the iDRAC GUI

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



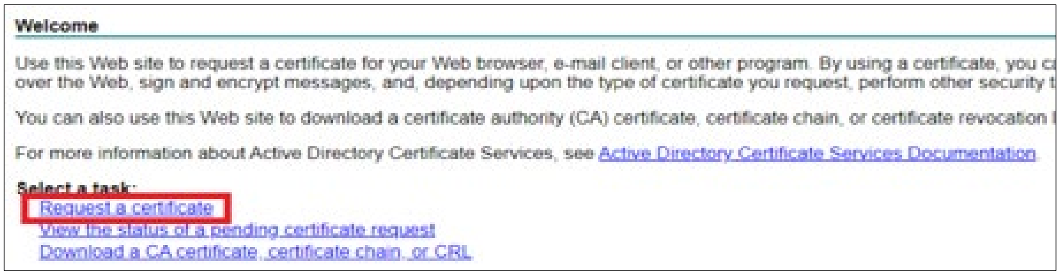
```
-----BEGIN CERTIFICATE REQUEST-----

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFRl
c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl
c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+1WV
i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y
kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=
-----END CERTIFICATE REQUEST-----
```

Note: The Microsoft CA below was specifically configured for iDRAC Validation. 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**.



Welcome

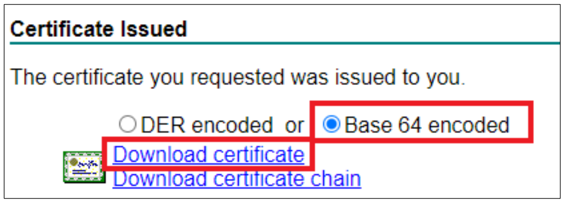
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you c over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security t

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

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**.

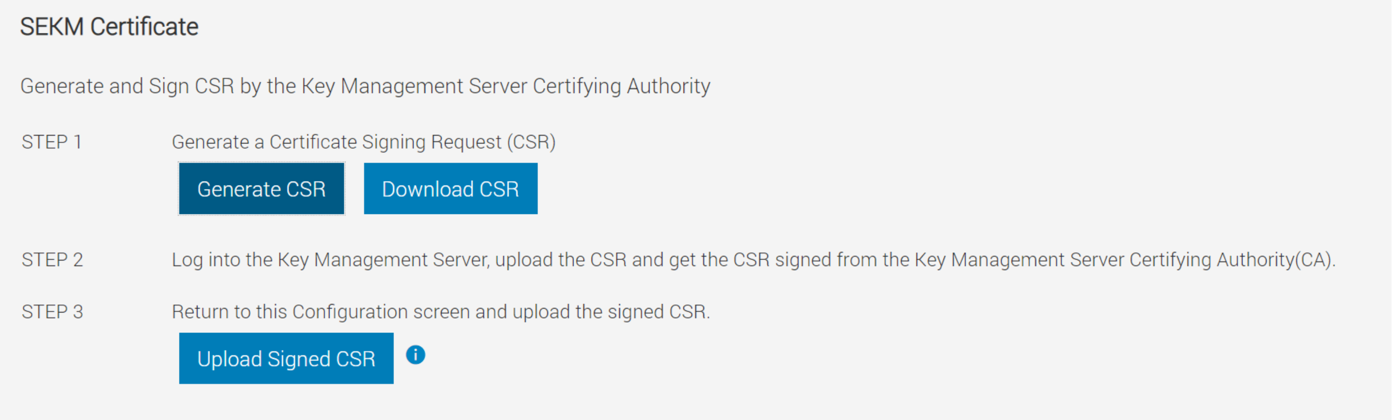


Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded
Download certificate
Download certificate chain

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.



SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

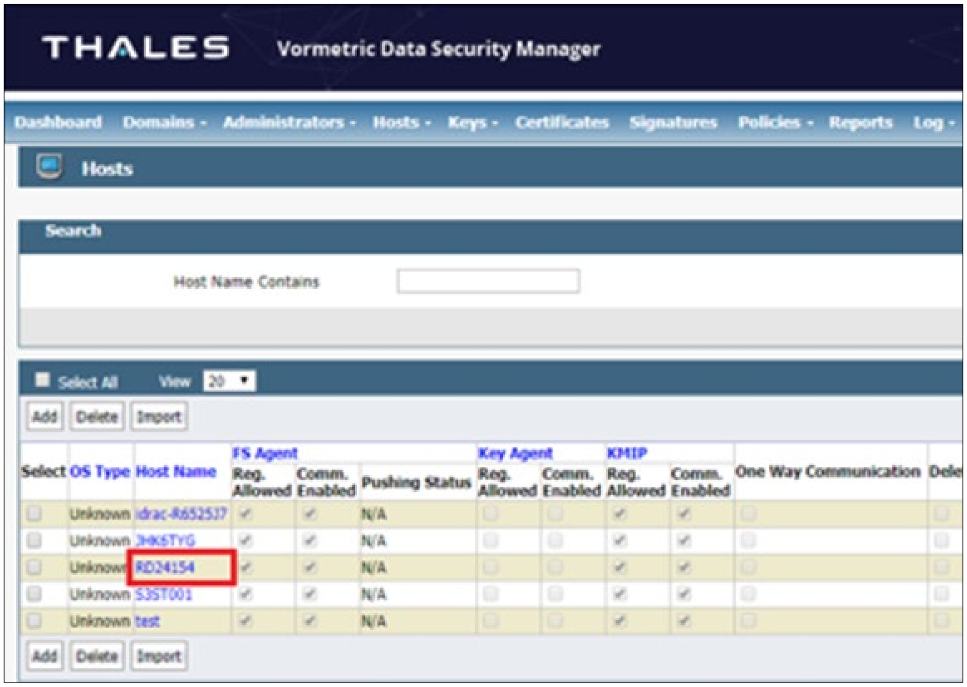
STEP 1 Generate a Certificate Signing Request (CSR)

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.

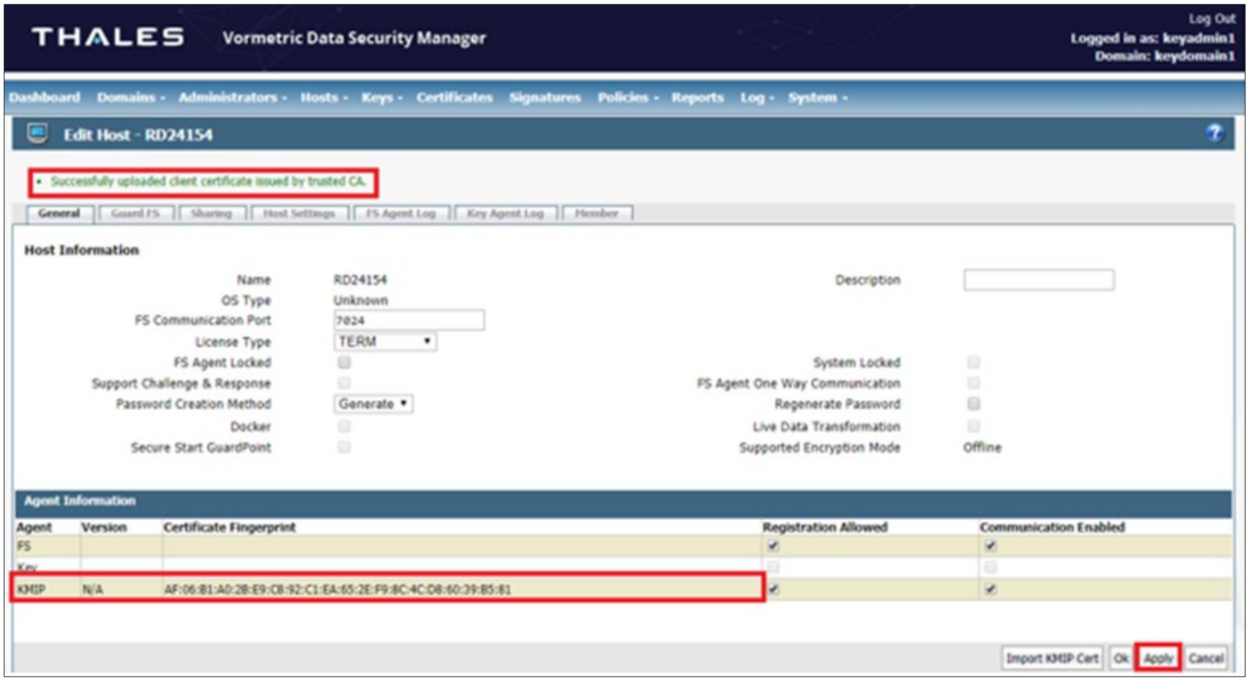
4.2.5 Upload the signed CSR to Thales DSM

1. Select your host.



Select	OS Type	Host Name	FS Agent			Key Agent		KMIP		One Way Communication	Dele
			Reg. Allowed	Comm. Enabled	Pushing Status	Reg. Allowed	Comm. Enabled	Reg. Allowed	Comm. Enabled		
□	Unknown	idrac-R652537	✓	✓	N/A	□	□	✓	✓	□	□
□	Unknown	JHK6TYG	✓	✓	N/A	□	□	✓	✓	□	□
□	Unknown	RD24154	✓	✓	N/A	□	□	✓	✓	□	□
□	Unknown	S3ST001	✓	✓	N/A	□	□	✓	✓	□	□
□	Unknown	test	✓	✓	N/A	□	□	✓	✓	□	□

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**.



- Successfully uploaded client certificate issued by trusted CA.

Host Information

Name RD24154
OS Type Unknown
FS Communication Port 7024
License Type TERM
FS Agent Locked □
Support Challenge & Response □
Password Creation Method Generate
Docker □
Secure Start GuardPoint □

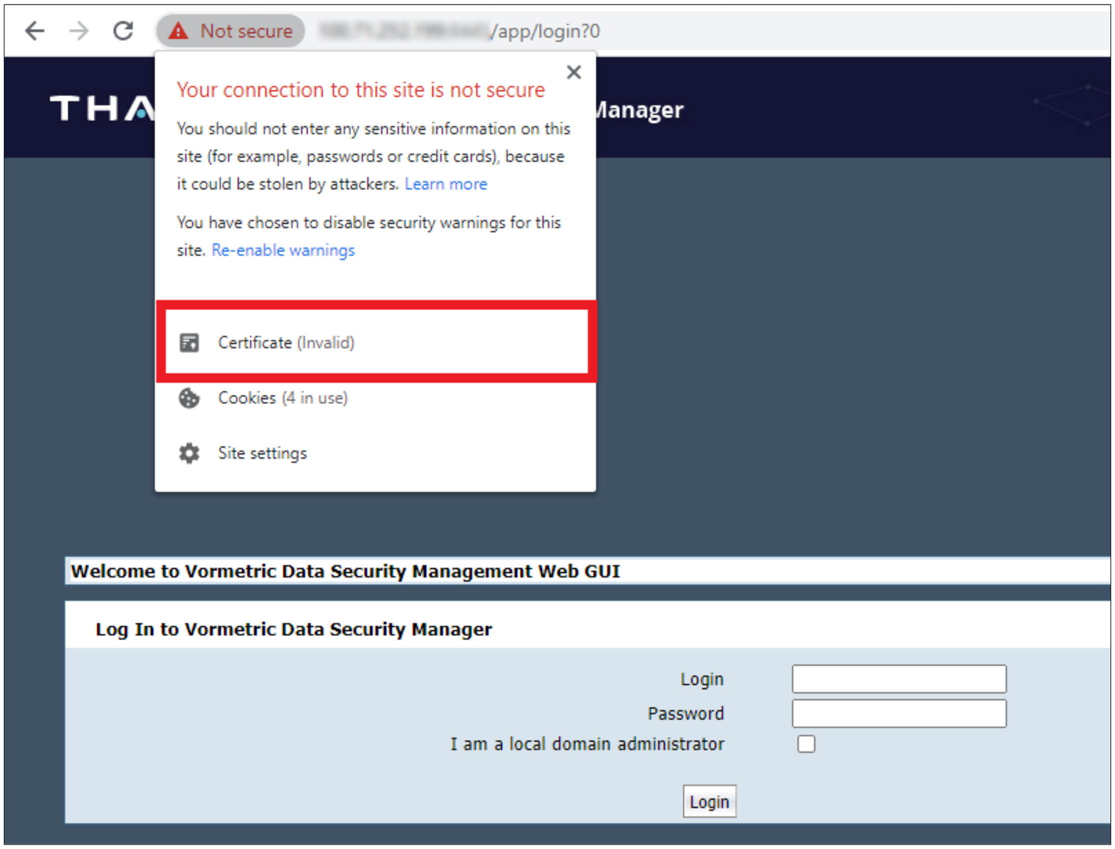
Description
System Locked □
FS Agent One Way Communication □
Regenerate Password □
Live Data Transformation □
Supported Encryption Mode Offline

Agent Information

Agent	Version	Certificate Fingerprint	Registration Allowed	Communication Enabled
FS			✓	✓
Key			□	□
KMIP	N/A	AF:06:B1:A0:2B:E9:C8:92:C1:EA:65:2E:F9:8C:4C:D8:60:39:B5:81	✓	✓

4.2.6 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)**.



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

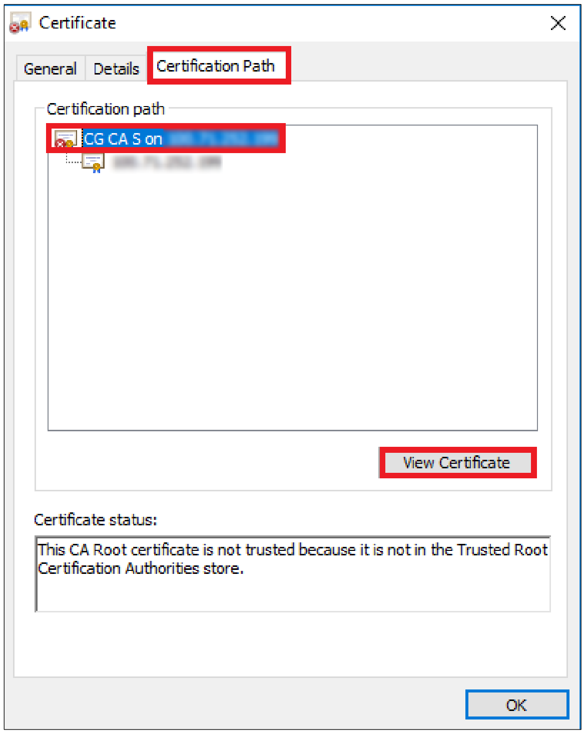
You have chosen to disable security warnings for this site. Re-enable warnings

Welcome to Vormetric Data Security Management Web GUI

Log In to Vormetric Data Security Manager

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

4. Click **View Certificate**.



Certification path

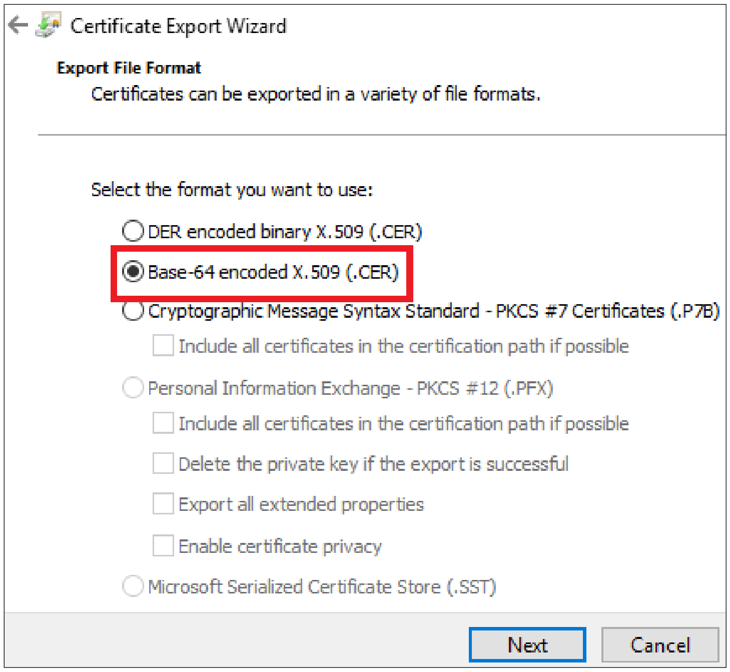
CG CA S on [redacted]

[redacted]

Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

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**.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

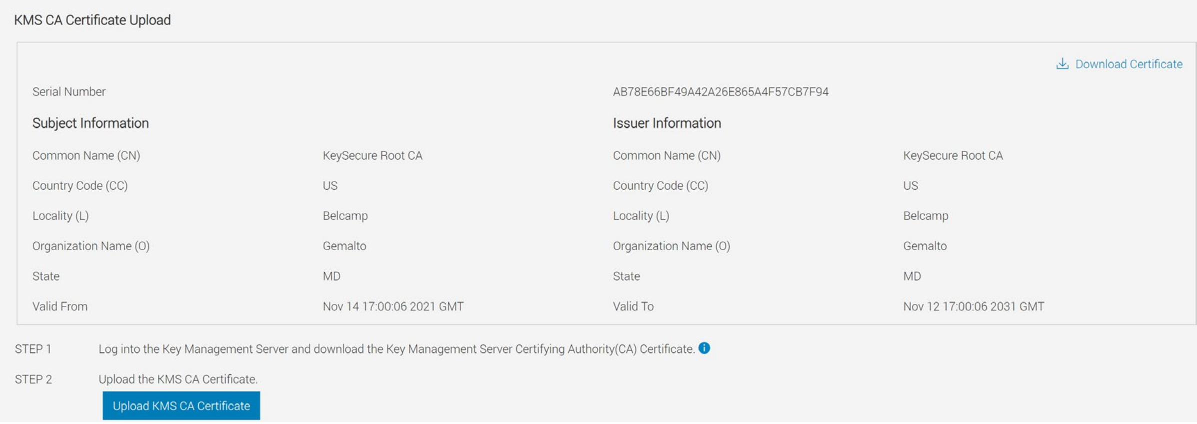
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

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



KMS CA Certificate Upload

Serial Number AB78E66BF49A42A26E865A4F57CB7F94

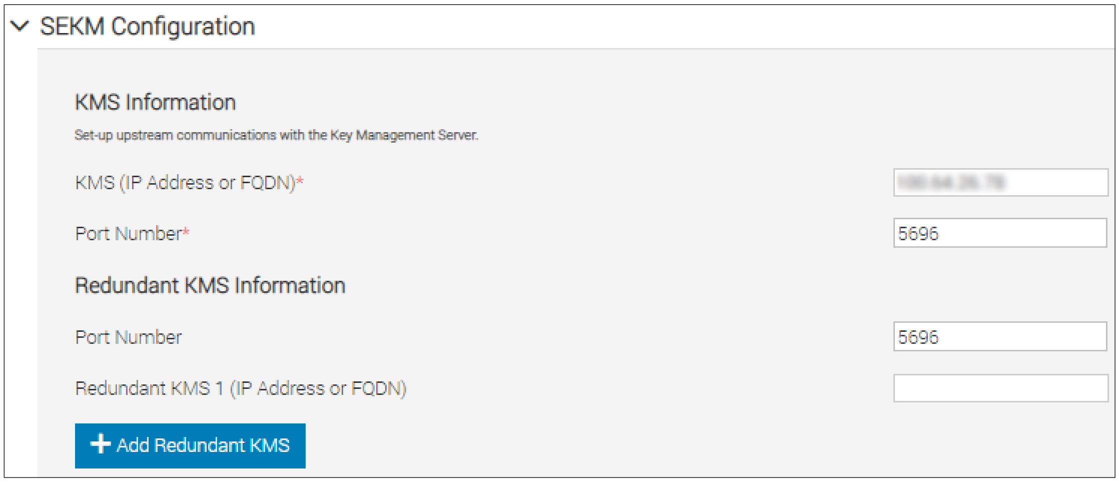
Subject Information		Issuer Information	
Common Name (CN)	KeySecure Root CA	Common Name (CN)	KeySecure Root CA
Country Code (CC)	US	Country Code (CC)	US
Locality (L)	Belcamp	Locality (L)	Belcamp
Organization Name (O)	Gemalto	Organization Name (O)	Gemalto
State	MD	State	MD
Valid From	Nov 14 17:00:06 2021 GMT	Valid To	Nov 12 17:00:06 2031 GMT

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.

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

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



KMS Information

Set-up upstream communications with the Key Management Server.

KMS (IP Address or FQDN)* [redacted]

Port Number* 5696

Redundant KMS Information

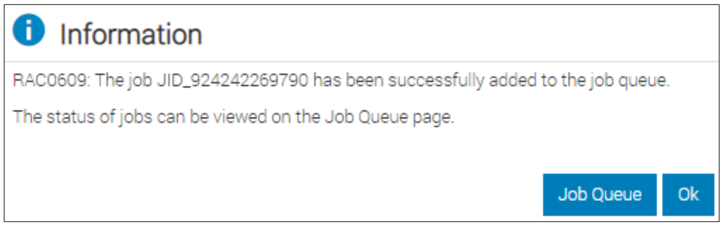
Port Number 5696

Redundant KMS 1 (IP Address or FQDN)

Note: User Authentication is not supported on Thales Vormetric 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.

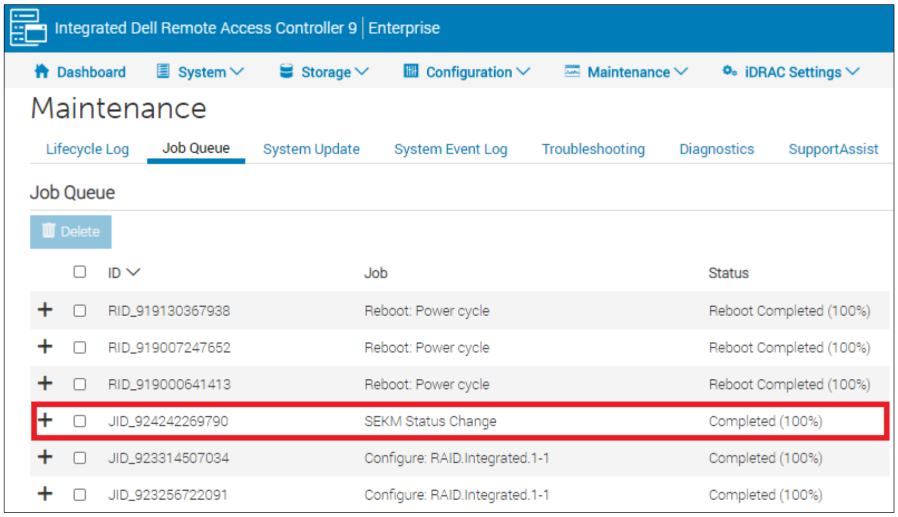
3. If you see any job status failures, view Lifecycle Logs for more information about the failure.



Information

RAC0609: The job JID_924242269790 has been successfully added to the job queue.

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



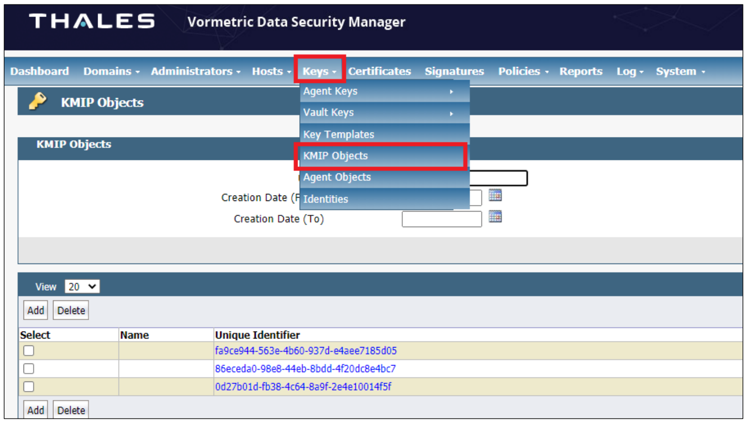
ID	Job	Status
RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
JID_924242269790	SEKM Status Change	Completed (100%)
JID_923314507034	Configure: RAID.Integrated.1-1	Completed (100%)
JID_923256722091	Configure: RAID.Integrated.1-1	Completed (100%)

iDRAC SEKM configuration with Thales DSM is now complete.

4.4 Viewing iDRAC key ID on Thales DSM

Note: You will not see a key generated for your iDRAC until you enable SEKM on a supported storage device. For details on how to enable SEKM on supported storage devices, see related section for your storage device.

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

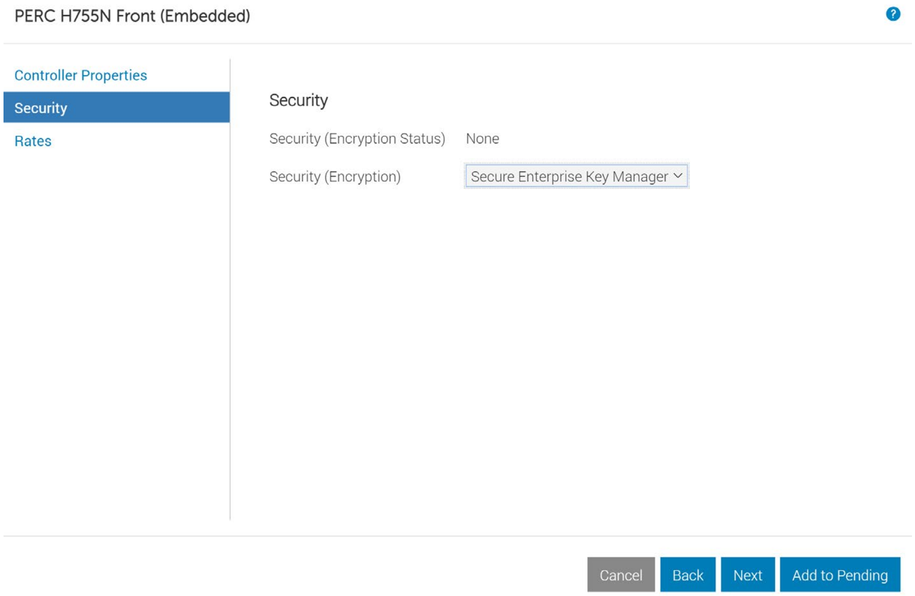


Select	Name	Unique Identifier
□		fa9ce944-563e-4b60-937d-e4aee7185d05
□		86eceda0-98e8-44eb-8bdd-4f20dc8e4bc7
□		0d27b01d-fb38-4c64-8a9f-2e4e10014f5f

5 PERC

5.1.1 Enable SEKM on PERC from iDRAC UI

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **Storage** -> **Overview** -> **Controllers**
3. Select the Actions dropdown for your PERC controller
4. Select **Edit** -> **Security** -> **Secure Enterprise Key Manage**r from the Actions dropdown



PERC H755N Front (Embedded)

Security

Security (Encryption Status) None

Security (Encryption) Secure Enterprise Key Manager

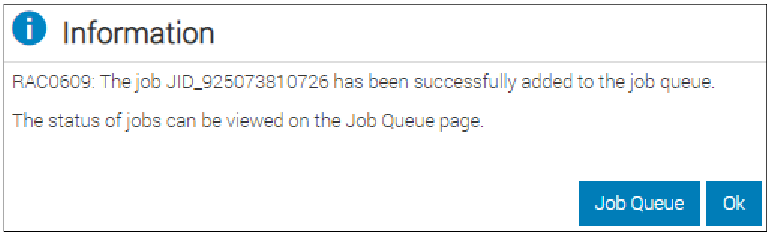
5. Click **Add to Pending.**

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

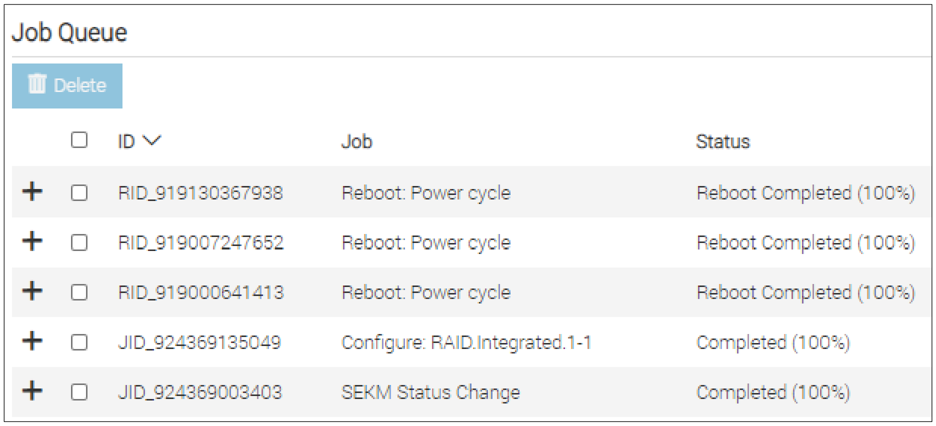
RAC0609: The job JID_925073810726 has been successfully added to the job queue.

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

9. Go to the Job Queue to view the scheduled job

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

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

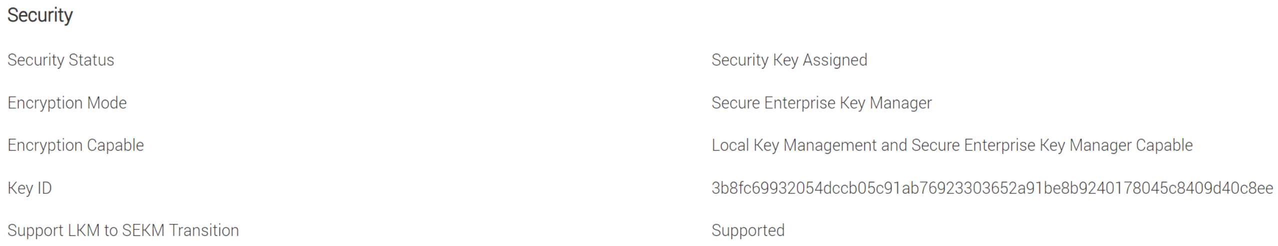


Job Queue

	□	ID	Job	Status
+	□	RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
+	□	RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
+	□	RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
+	□	JID_924369135049	Configure: RAID.Integrated.1-1	Completed (100%)
+	□	JID_924369003403	SEKM Status Change	Completed (100%)

5.1.2 Verify SEKM status on PERC from iDRAC UI

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **Storage** -> **Overview** -> **Controllers**
3. Expand your storage controller and ensure the following:



Security

Security Status	Security Key Assigned
Encryption Mode	Secure Enterprise Key Manager
Encryption Capable	Local Key Management and Secure Enterprise Key Manager Capable
Key ID	3b8fc69932054dccb05c91ab76923303652a91be8b9240178045c8409d40c8ee
Support LKM to SEKM Transition	Supported

For more information about PERC features, see PERC user guide.

PERC 11: Dell Technologies PowerEdge RAID Controller 11 User’s Guide PERC H755 adapter, H755 front SAS, H755N front NVMe, H755 MX adapter, H750 adapter SAS, H355 adapter SAS, H355 front SAS, and H350 adapter SAS

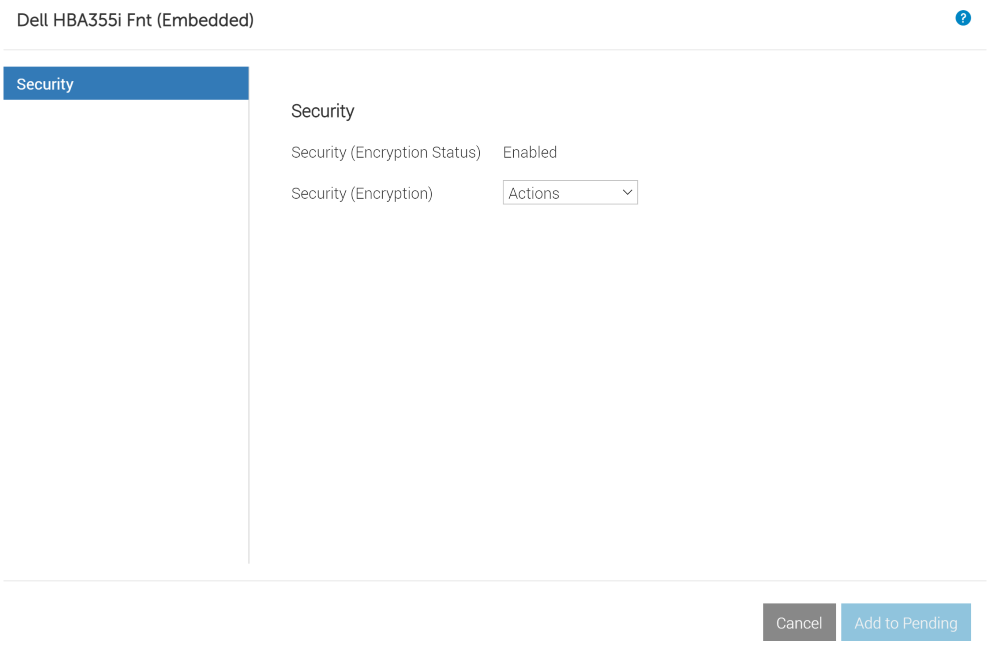
PERC 10: Dell EMC PowerEdge RAID Controller 10 User’s Guide PERC H345, H740P, H745, H745P MX, and H840

6 HBA / SAS SEDs

6.1.1 Enable SEKM on HBA from iDRAC UI

Note: SEKM capable HBA is currently only supported on Veral platforms (E660F, P670F, and V670F).

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **Storage** -> **Overview** -> **Controllers**
3. Select the Actions dropdown for your HBA controller
4. Select **Edit** -> **Security** -> **Enable Security** from the Actions dropdown



Dell HBA355i Fnt (Embedded)

Security

Security (Encryption Status) Enabled

Security (Encryption) Actions

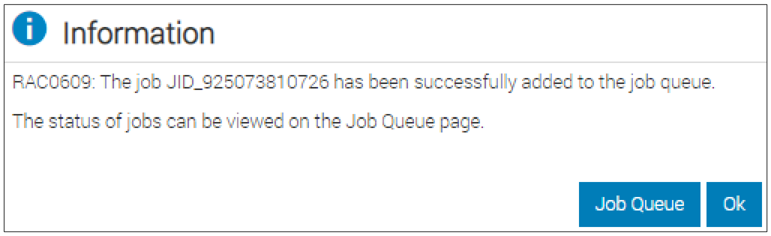
5. Click **Add to Pending.**

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

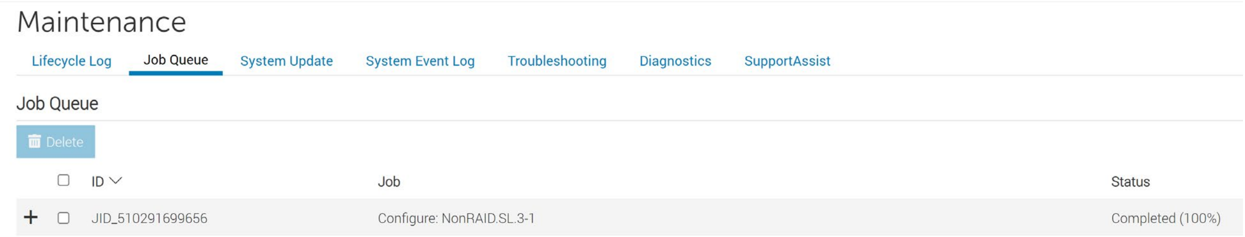
RAC0609: The job JID_925073810726 has been successfully added to the job queue.

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

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 HBA. The server is automatically restarted.

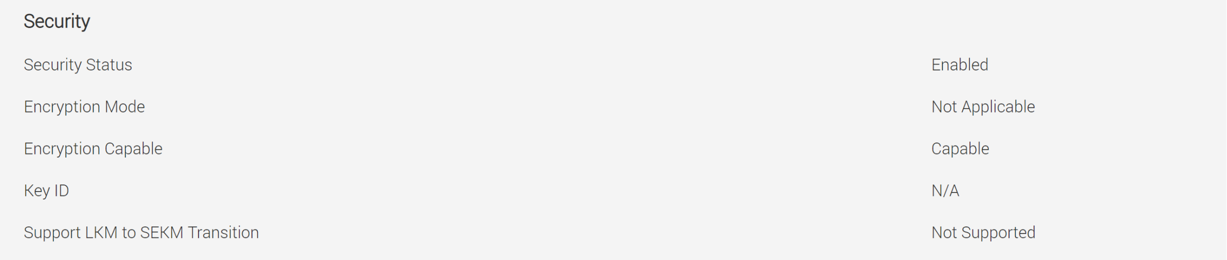
11. After the POST or Collecting Inventory operation is completed, ensure that the job ID has been marked as **Completed** on the **Job Queue** page.



	☐	ID	Job	Status
+	☐	JID_510291699656	Configure: NonRAID.SL.3-1	Completed (100%)

6.1.2 Verify SEKM status on HBA from iDRAC UI

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **Storage** -> **Overview** -> **Controllers**
3. Expand your storage controller and ensure the following:



Security

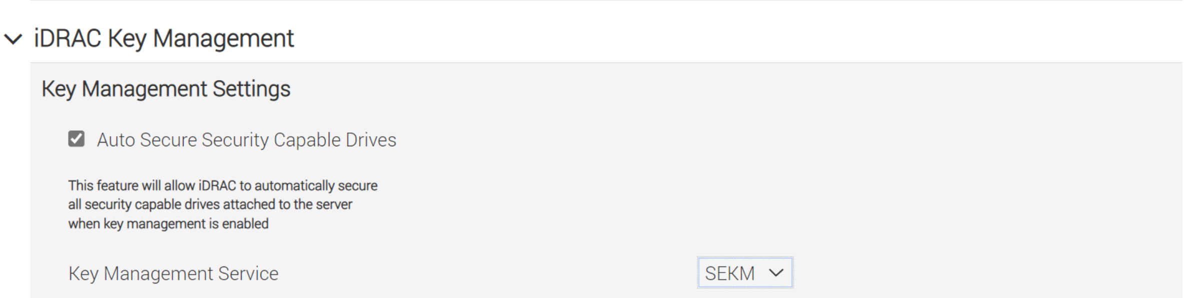
Security Status	Enabled
Encryption Mode	Not Applicable
Encryption Capable	Capable
Key ID	N/A
Support LKM to SEKM Transition	Not Supported

For more information about HBA features, see HBA user guide.

[Dell Host Bus Adapter User's Guide HBA355e Adapter, HBA355i Front, HBA355i Adapter, HBA350i MX, and HBA350i Adapter]

6.1.3 Enable SEKM on SAS SEDs behind HBA from iDRAC UI

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **iDRAC Settings** -> **Services** -> **iDRAC Key Management ->** select **Auto Secure** option



☑ Auto Secure Security Capable Drives

This feature will allow iDRAC to automatically secure all security capable drives attached to the server when key management is enabled

Key Management Service: SEKM

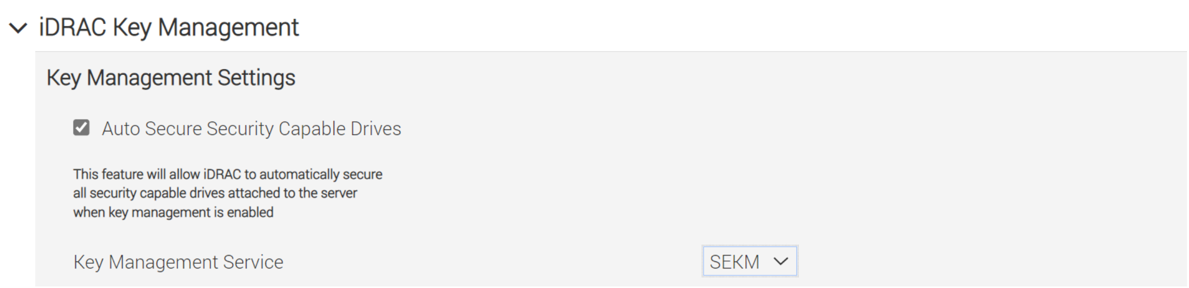
Note: This option will allow iDRAC to automatically secure all security capable drives attached to server when SEKM is enabled. If security is manually enabled on HBA then SAS SEDs behind HBA will be auto secured by iDRAC if Auto Secure option is enabled. For more information about Auto Secure feature, see Auto Secure section.

7 Direct attach NVMe SEDs

SEKM is only supported on direct attach NVMe SEDs that support TCG Opal 2.0 protocol.

7.1.1 Enable SEKM on direct attach NVMe SEDs from iDRAC UI

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **iDRAC Settings** -> **Services** -> **iDRAC Key Management ->** select **Auto Secure** option



iDRAC Key Management

Key Management Settings

☑ Auto Secure Security Capable Drives

This feature will allow iDRAC to automatically secure all security capable drives attached to the server when key management is enabled

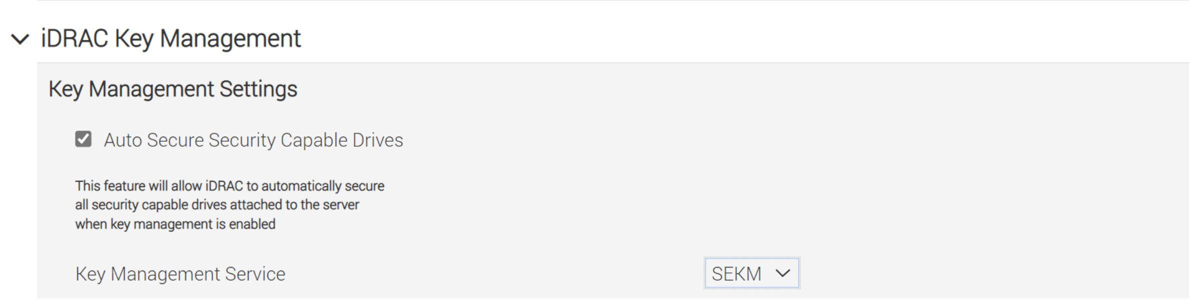
Key Management Service: SEKM

Note: If Auto Secure is enabled while enabling SEKM on iDRAC, then iDRAC will attempt to secure NVMe SEDs in a single job. This job will complete with errors when non-SEDs are present in the system. This is to ensure users are warned and aware there are non-secured drives in the system. For more information about Auto Secure feature, see Auto Secure section below.

8 Auto Secure

In order to make it easy to secure all SEDs, Auto Secure has been added as part of SEKM enablement. This option will be enabled by default.

1. Start iDRAC by using any supported browser.
2. From iDRAC **Dashboard** -> **iDRAC Settings** -> **Services** -> **iDRAC Key Management ->** select **Auto Secure** option:



iDRAC Key Management

Key Management Settings

☑ Auto Secure Security Capable Drives

This feature will allow iDRAC to automatically secure all security capable drives attached to the server when key management is enabled

Key Management Service: SEKM

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

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

AutoSecure=Enabled

Controllers such as PERC/HBA will not be auto secured and will need to be manually secured.

9 Cryptographic Erase SEDs

Cryptographic erase is a process to erase all data permanently on an encryption-capable and reset the security attributes. This is supported for SEDs behind PERC, HBA, and direct attach NVMe SEDs.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage cryptographicerase:{SED FQDD}
```

Note: Drives will become secured again on next system boot if Auto Secure is enabled. To prevent this disable Autosecure option first before erasing a SED.

PSID revert

This feature is only supported on SAS SED connected to SAS HBA and NVMe SED. For PERC attached NVMe SEDs, PSID revert is not supported. The legacy cryptographic erase operation command above is sufficient.

PSID revert is required when a drive is secured by an authentication key that iDRAC has no access to and cannot be unlocked. All user data will be permanently erased using this feature. If access to data on the drive is required, then the user can take the drive back to the original system to unlock it.

Users can select an individual SED and perform a PSID revert operation by using the command below. The PSID is printed on the physical label of the drive and is not displayed in iDRAC drive inventory.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage cryptographicerase:{SED FQDD} -psid
{PSID}
```

10 PERC LKM to SEKM transition

This section will give an overview of PERC LKM to SEKM migration. This feature has been added to give PERC LKM users the ability to transition to SEKM once SEKM has been enabled on iDRAC.

A new property ***SupportsLKMtoSEKMTransition*** has been added. A value of **Yes** indicates PERC supports the transition from LKM to SEKM.

SEKM must be enabled on iDRAC before a PERC LKM to SEKM transition can be requested. Users can use any of the iDRAC interfaces to request a PERC LKM to SEKM transition. For security reasons, PERC LKM passphrase is required when requesting the transition.

The command below will demonstrate how to transition PERC from LKM to SEKM mode.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage setencryptionmode:RAID.Integrated.1-1 -mode SEKM -passphrase Dell123!
```

Note: Make sure to use the same passphrase that was used to enable LKM on PERC

A staged job must be scheduled for this operation. A host reboot is required for PERC LKM to SEKM transition. Once PERC is in SEKM mode, a transition to LKM mode is not allowed. PERC LKM to SEKM transition is also not allowed while the system is in lockdown mode.

The workflow below will demonstrate how to transition PERC from LKM to SEKM mode.

```
 C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage get controllers -o -p encryptionmode,keyid,supportslkmtosekmtransition

RAID.Integrated.1-1

   EncryptionMode = Local Key Management

   KeyID = testID

   SupportsLKMtoSEKMTransition  = Yes

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage setencryptionmode:RAID.Integrated.1-1 -mode SEKM -passphrase Test123

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue create RAID.Integrated.1-1 -r pwrcycle -s TIME_NOW

RAC1024: Successfully scheduled a job.

Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

Commit JID = JID_385106379901

Reboot JID = RID_385106380800
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_385106379901

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

[Job ID=JID_385106379901]

Job Name=Configure: RAID.Integrated.1-1

Status=Scheduled

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Not Applicable]

Actual Completion Time=[Not Applicable]

Message=[JCP001: Task successfully scheduled.]

Percent Complete=[0]

---------------------------------------------------------


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_385106379901

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

[Job ID=JID_385106379901]

Job Name=Configure: RAID.Integrated.1-1

Status=Running

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 23:57:05]

Actual Completion Time=[Not Applicable]

Message=[PR20: Job in progress.]

Percent Complete=[1]

---------------------------------------------------------

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_385106379901

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

[Job ID=JID_385106379901]

Job Name=Configure: RAID.Integrated.1-1
```

```
Status=Completed

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 23:57:05]

Actual Completion Time=[Fri, 03 Dec 2021 00:01:11]

Message=[PR19: Job completed successfully.]

Percent Complete=[100]

-------------------------------------------------------

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage get controllers -o -p encryptionmode,keyid

RAID.Integrated.1-1

  EncryptionMode        =        Secure Enterprise Key Manager

  KeyID        =     9DC2F2F0D42DDE89AD9FFD5F3B68239195FE32DF2F75BFB73B44BD61B7A01E39
```

11 Configure SEKM solution using iDRAC RACADM CLI

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

For more information about RACADM commands, see RACADM guide.

Integrated Dell Remote Access Controller 9 RACADM CLI Guide

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

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

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

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

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


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


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


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

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

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

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

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

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

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

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

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

5. Upload the Server CA file to the iDRAC

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

6. Configure Key Management Server settings on iDRAC

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

7. Run the following command at RACADM CLI:

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

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


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


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

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

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

11.1.1 Enable SEKM on HBA and SAS SEDs using RACADM

The commands below will show how to enable and disable security on SAS HBA.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage security:NonRAID.SL.8-1 -enable
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage security:NonRAID.SL.8-1 -disable
```

Note: A staged job must be scheduled for both operations. A host reboot is required for security mode change to occur.

“One or more Storage device(s) are not in a state where the operation can be completed.”

Note: If disable operation fails with above message, make sure all drives have been erased behind HBA first.

The workflow below will demonstrate how to enable security on SAS HBA and SAS drives behind HBA. Auto Secure will be disabled in this example.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.sekm.AutoSecure

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

AutoSecure=Disabled

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage security:NonRAID.SL.8-1 -enable

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".


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue create NonRAID.SL.8-1 -r pwrcycle -s
TIME_NOW

RAC1024: Successfully scheduled a job.

Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

Commit JID = JID_384818826920

Reboot JID = RID_384818827401
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_384818826920

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

[Job ID=JID_384818826920]

Job Name=Configure: NonRAID.SL.8-1

Status=Running

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 15:57:50]

Actual Completion Time=[Not Applicable]

Message=[PR20: Job in progress.]

Percent Complete=[1]

----------------------------------------------------------

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_384818826920

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

[Job ID=JID_384818826920]

Job Name=Configure: NonRAID.SL.8-1

Status=Completed

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 15:57:50]

Actual Completion Time=[Thu, 02 Dec 2021 16:02:17]

Message=[PR19: Job completed successfully.]

Percent Complete=[100]

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

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage get controllers -o -p securitystatus

NonRAID.SL.8-1

  SecurityStatus                  = Enabled


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage
encryptpd:Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1

STOR094 : The storage configuration operation is successfully completed

and the change is in pending state.

To apply the configuration operation immediately, create a configuration job

using the --realtime option.

To apply the configuration after restarting

the server, create a configuration job using the -r option.

To create the necessary real-time and restart jobs, run the jobqueue command.

For more information about jobqueue command, run the

'racadm help jobqueue' command.

C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage
encryptpd:Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1

STOR094 : The storage configuration operation is successfully completed

and the change is in pending state.

To apply the configuration operation immediately, create a configuration job

using the --realtime option.

To apply the configuration after restarting

the server, create a configuration job using the -r option.

To create the necessary real-time and restart jobs, run the jobqueue command.

For more information about jobqueue command, run the

'racadm help jobqueue' command.


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue create NonRAID.SL.8-1 --realtime -s
TIME_NOW
```

```
RAC1024: Successfully scheduled a job.

Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

Commit JID = JID_384841257680


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_384841257680

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

[Job ID=JID_384841257680]

Job Name=Configure: NonRAID.SL.8-1

Status=Completed

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 16:28:46]

Actual Completion Time=[Thu, 02 Dec 2021 16:30:27]

Message=[PR19: Job completed successfully.]

----------------------------------------------------------


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage get pdisks -o -p securitystatus

Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1

   SecurityStatus                  = Secured
```

11.1.2 Enable SEKM on direct attach NVMe SEDs using RACADM

The command below will show how to manually enable security on NVMe SEDs.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage
encryptpd:Disk.Bay.15:Enclosure.Internal.0-1
```

Note: This operation supports real-time jobs. A host reboot is not required.

The workflow below will demonstrate how to enable security on direct attached NVMe SEDs. Auto Secure will be disabled in this example.

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn get idrac.sekm.AutoSecure

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

AutoSecure=Disabled
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage
encryptpd:Disk.Bay.15:Enclosure.Internal.0-1

STOR094 : The storage configuration operation is successfully completed

and the change is in pending state.

To apply the configuration operation immediately, create a configuration job

using the --realtime option.

To apply the configuration after restarting

the server, create a configuration job using the -r option.

To create the necessary real-time and restart jobs, run the jobqueue command.

For more information about jobqueue command, run the

'racadm help jobqueue' command.
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue create Disk.Bay.15:Enclosure.Internal.0-
1 --realtime -s TIME_NOW

RAC1024: Successfully scheduled a job.

Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

Commit JID = JID_384841257680
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_384818826920

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

[Job ID=JID_384818826920]

Job Name=Configure: Disk.Bay.15:Enclosure.Internal.0-1

Status=Running

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 15:57:50]

Actual Completion Time=[Not Applicable]

Message=[PR20: Job in progress.]

Percent Complete=[1]
```

```
C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn jobqueue view -i JID_384818826920

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

[Job ID=JID_384818826920]

Job Name=Configure: Disk.Bay.15:Enclosure.Internal.0-1

Status=Completed

Scheduled Start Time=[Now]

Expiration Time=[Not Applicable]

Actual Start Time=[Thu, 02 Dec 2021 15:57:50]

Actual Completion Time=[Thu, 02 Dec 2021 16:02:17]

Message=[PR19: Job completed successfully.]

Percent Complete=[100]

----------------------------------------------------------


C:\>racadm -r 192.168.0.120 -u root -p calvin --nocertwarn storage get pdisks -o -p securitystatus

Disk.Bay.15:Enclosure.Internal.0-1

   SecurityStatus                  = Secured
```

12 Configure SEKM using Server Configuration Profile (SCP)

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

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

2. Enable SEKM on iDRAC

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

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

4. SCP example for configuring iDRAC SEKM configuration

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

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

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

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

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

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

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

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

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

 <Attribute Name="KMS.1#PrimaryServerAddress">192.168.0.130</Attribute>

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

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

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

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

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

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

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

 <Attribute Name="KMS.1#RedundantServerAddress7"/>
 <Attribute Name="KMS.1#RedundantServerAddress8"/>
 <Attribute Name="KMS.1#Timeout">10</Attribute>
 <Attribute Name="KMS.1#iDRACUserName">idrac-PTC1234</Attribute>
 <Attribute Name="KMS.1#iDRACPassword">Password</Attribute>
 <Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute>
 <Attribute Name="SEKMCert.1#CommonName">idrac-PTC1234</Attribute>
 <Attribute Name="SEKMCert.1#OrganizationName">Dell</Attribute>
 <Attribute Name="SEKMCert.1#OrganizationUnit">ISG</Attribute>
 <Attribute Name="SEKMCert.1#LocalityName">Round Rock</Attribute>
 <Attribute Name="SEKMCert.1#StateName">Texas</Attribute>
 <Attribute Name="SEKMCert.1#CountryCode">US</Attribute>
 <Attribute Name="SEKMCert.1#EmailAddress">tester@dell.com</Attribute>
 <Attribute Name="SEKMCert.1#SubjectAltName"/>
 <Attribute Name="SEKMCert.1#UserId"/>
 <Attribute Name="SecurityCertificate.1#CertData">-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIQbL1BjtEwBL3fNQCMjT47TDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO
BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx
MDYyMzE0MDU0N1oXDTMxMDYyMTE0MDU0N1owWjELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1EMRAwDgYDVQQHEwdCZWxjYW1wMRAwDgYDVQQKEwdHZW1hbHRvMRowGAYD
VQQDExFLZXlTZWN1cmUgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBANbjXWXrloVYosJiwxpSz2fCXGLWQQfUlFCEwUPFw+R8fAO29lSo6tHa
sQ3Tx+QMZlFEa9DaZbhcuOyQsoIUoG1V+oBpZSvx1+QTVcO6PRM8Tv3RD75xI36Y
KDQXxJoABB414laHM9pyAmkI1dnHs7wQhHBrb7PBW8Ol2+Qzk3CDAyaa4t/s332/
KlDQs18JTBHceMnNEdXkG9rVcYmpjZXvrhjYHSvvVoGZWCtzuKvszL6NOKj7ruUT
uq2WSSBRjiwPSysJNtubcGNravOm4FCgSNZi0v1bqKFTBq0lXgamhScjyIHGkrFm
aO71v1OmDtjih7c69gtOQG+yyCKPkNrxh5CVEU7yoJDWa1ak7TJaiYczH2cvMDY2
3r9uFWdfeM0E4EQ5kM5KvLXzygM8FxzZE3XkrekFw+6kOZuZmf0FoptQYATOaQpK
xGrTWGjlcAlnoQDgINGjZFD70y/mf01JkS/UWtdX0yZysw/iNDzqmh7ELy9dsR2s
```

```
PkXyMlAOVW/ydlFRcY+s32kMqRXIFKgy8vuyPMLhIi/tMGNpvJ4N6vnjzHfDpsWK
d5n/T7tDMAf/zlmUSvwhtsHkMnXyCPpAR/uVW5DMwbf9d6TCJs7ofIFpsSptkw53
UDL7ThX9klqO0WV5FbGBlY1OfNMeX6LIwJ+v3A1VVNFNiYxCUTA/AgMBAAGjQzBB
MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB4GA1UdEQQXMBWBE3N1
cHBvcnRAZ2VtYWx0by5jb20wDQYJKoZIhvcNAQELBQADggIBANFZGyBqQ6u26G/C
P2vhIr5i3UrlOyLFC+erX2lGU68GFloHF26ZKBej3kAkFi6naThR3vjOIj2crM6+
PZlyW/JTpmBa0aVfyfVlKytOmkXXM27bPheeBInDPOFfgJROG7xiMfMKRdDwMJ+B
iyYX+rHO8xc72e7FUnF72dUN1AK+2sLvaFSdWYWQ/Aj2Dm5qXxRqw3YPtToax3m1
c+O3Wb5jCW01s+7w+E74CPRCiFISRsP23qDJV3xGbMF7pTwJEDzIQTtrXT5DXOXa
o7yJm9Uyw5QF589agesVybH8KsJJZLN+wW75NHUp+OnTuC/gy8viccaYzCCXuqGH
R3aX/k9UBkaOcAI9M6bGHn7XwsJWKsyWHtsCqJKyGvo9+48kgg0dximWDwUBMBjx
tP0lmOMOLcgE3xB72L2OtpNZHlU/4w87sLVxPJyrDRT+Zn1zjFdBDGUdNEW2di+2
qW1xwoy8TQK/cOKC5/cMQVqQr4PriRTBhnU5WDSfQ/fuiyGmU+L9/LOrjL/S2/8C
RTsQzOmQC+1ADOXHedMFPhsRZcMTZgSWXThERrn46ZiuO+yvBvh5rfvNf6JH+LLL
uwpUDmwzRF3rmXqGzeuk0ou620kQuylK4nnyii3GsCgq/ZOn6Gqz+afcUoCPN39n
6CTqqYiFHUXl4pZJrrXhQ+16gdtrd
-----END CERTIFICATE-----</Attribute>
 <Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
 <Attribute Name="SecurityCertificate.2#CertData">-----BEGIN CERTIFICATE-----
MIIEpTCCAo2gAwIBAgIQUO1US/yDXsY8uGv+lxAuQDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxEDAO
BgNVBAoTB0dlbWFsdG8xGjAYBgNVBAMTEUtleVNlY3VyZSBSb290IENBMB4XDTIx
MTAyMDE4MDUwMloXDTIyMTAyMDE4MDUwMlowgYsxCzAJBgNVBAYTAlVTMQ4wDAYD
VQQIEwVUZXhhczETMBEGA1UEBxMKUm91bmQgUm9jazERMA8GA1UEChMIRGVsbCBF
TUMxDDAKBgNVBAsTA0lTRzEWMBQGA1UEAxMNaWRyYWMtUFRDODUwMjEeMBwGCSqG
SIb3DQEJAQwPdGVzdGVyQGRlbGwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA1HX6hIV1ggy0R5aU03MjoS2CkanRClFOtWPlW+r87hkrRN9FodCA
Uud1WoU1gFoAb6U+wNDmGHZuF1CkKMl62gLdCcoKB3A5Wz5FyDYmDn8ql7TKvp3g
THDYCNKCsr4z3eVdQcJwvILzV3Pnv0bNdBNwi0GjC24P70/VhPSjZMFvg6x/3mcn
```

```
wj/bec3BrxbxGT24koxpyip24wgJ82qA064R1Z6fWPGiZhBMY8h0r3BXG6uVzHG1
2Ue2FoqYBocs9EkUm7RB5la3m0g7B2nVRggc5UCqXeIYBmdzVhdU4XoJ5z1lGtpb
dpLQQZIKrapKBGC2nfrL3RVPAzDOe6hWnQIDAQABozUwMzAOBgNVHQ8BAf8EBAMC
A4gwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0B
AQsFAAOCAgEAmDs2mfdD1N2POKvD0cbfhUX8/edAyBDEEe+ylXAplgPiJ/HI5WU4
LGUdDNVg6NKGBoXyQKePxP8fcR35xN6MSzThM8tRRR32TFfRelNxmfGB2YeyngY8
aZ8eFg4O5+sbYyV/josXfbr27mryuWy4KuDUgtzUrZnP5waKpS6ZpkqgXvA+IhS7
7Etj7HZfWF6PWMy6rdbw0KSVzZUg0BFTh6bSO62qYSFx+jxclaZHE6YCmT+q1mPN
K+AjbXi41YeMVa5iXrFIsQt8jNlU+XVt5yyO4AH+50ZQPJ6YlveTOr9Ieo0Bdn43
Ac4PlazRyTQ7iCAtdYOFKltDQZwvaodSzUe8/NxzanGnCjhNdR/SfZ7+Fe7f0NFd
gc3KrrD8n2+iuwAXWGdEeFres1JVjLEDGM2UwmcUK3wOUUaaJHmGCyg2WylgWZ0l
DV7LlyQEaBpHIBxldQFHdPs44S/LtnGUxXTZHPuELVIGcLvQm/+GPt49m0tnVX4O
HmXJnEYdTaKYYvrJCLcec+jTfDp7wJlCNspqT1Wfaw+pthGr6uHyAdXcBzH3Cg1V
33ozhpRDxvolSYexvgLbH0dHlVl8P+sr0RZm7v8bB54qIrb//1UJBtlyJ5sl7/IR
rSEXSX3hC04a+BVoYAhzLf1ZVPp0sX+agKJQv8osHIMqze9If2n1bgF1=
-----END CERTIFICATE-----</Attribute>
 <Attribute Name="SecurityCertificate.2#CertType">SEKM_SSL_CERT</Attribute>
</Component>
</SystemConfiguration>
```

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

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

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

Serial Number          : 6CBD418ED13004BDDF35008C8D3E3B4C

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

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


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




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

Serial Number          : D3A4EE0676049B17ED51F94F89A5C185

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

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

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



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

13 Configure SEKM solution using Redfish API

This section will demonstrate how to configure SEKM on iDRAC using Redfish interface.

Set SEKMCert attributes

SEKM attributes on iDRAC are located under this URI: /redfish/v1/Managers/iDRAC.Embedded.1/Attributes

Use **PATCH** method to set SEKMCert attributes before generating a CSR.

Example request body: `{"Attributes": {"SEKMCert.1.CommonName": "PTC8502"}}`

The following fields are required before generating a CSR: `SEKMCert.1.CommonName, SEKMCert.1.CountryCode, SEKMCert.1.EmailAddress, SEKMCert.1.LocalityName, SEKMCert.1.OrganizationName, SEKMCert.1.OrganizationUnit, SEKMCert.1.StateName`

Generate a CSR

POST

/redfish/v1/Dell/Managers/iDRAC.Embedded.1/DelliDRACCardService/Actions/DelliDRACCardService.GenerateSEKMCSR

Request body is not required.

Take the CSR and get it signed by the Certificate Authority on your supported key management server.

Upload SEKM certificates to iDRAC

POST

/redfish/v1/Dell/Managers/iDRAC.Embedded.1/DelliDRACCardService/Actions/DelliDRACCardService.ImportCertificate

Example request body for KMS server certificate:

```
{"CertificateType": "KMS_SERVER_CA", "CertificateFile": "certificate_authority.pem"}
```

Example request body for signed SEKM SSL certificate:

```
{"CertificateType": "SEKM_SSL_CERT", "CertificateFile": "signed_certificate.pem"}
```

Set KMS attributes

PATCH

/redfish/v1/Managers/iDRAC.Embedded.1/Attributes

`KMS.1.PrimaryServerAddress, KMS.1.KMIPPortNumber, KMS.1.iDRACUserName, KMS.1.iDRACPassword`

Set SEKM attributes

PATCH

/redfish/v1/Managers/iDRAC.Embedded.1/Attributes

`SEKM.1.AutoSecure, SEKM.1.KMSKeyPurgePolicy`

Enable SEKM on iDRAC

PATCH

/redfish/v1/Managers/iDRAC.Embedded.1/Attributes

Example request body: `{"Attributes": {"SEKM.1.SetState": "Enabled"}}`

Verify overall SEKM status

GET

“/redfish/v1/Managers/iDRAC.Embedded.1/Attributes?$select=SEKM.1.SetState

Note: This value will report “Configured” if SEKM is set up correctly.

PERC

Enable SEKM

POST

/redfish/v1/Dell/Systems/System.Embedded.1/DellRaidService/Actions/DellRaidService.EnableControllerEncryption

Example request body: `{"Mode":"SEKM","TargetFQDD":"RAID.Integrated.1-1"}`

Verify SEKM

GET

/redfish/v1/Systems/System.Embedded.1/Storage/RAID.Integrated.1-1

Expected attributes if SEKM security is enabled: `“EncryptionMode”: “SecureEnterpriseKeyManager”`

Disable SEKM

POST

/redfish/v1/Dell/Systems/System.Embedded.1/DellRaidService/Actions/DellRaidService.RemoveControllerKey

Example request body：`{"TargetFQDD":"RAID.Integrated.1-1"}`

Note：If above operation fails with message below, make sure to reset the controller to remove any secured volumes.

“One or more Storage device(s) are not in a state where the operation can be completed.”

HBA

Enable SEKM

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.EnableSecurity

Example request body：`{"TargetFQDD":"NonRAID.SL.8-1"}`

Verify SEKM

GET

/redfish/v1/Systems/System.Embedded.1/Storage/NonRAID.SL.8-1

Expected attributes if SEKM security is enabled：`"SecurityStatus": "Enabled"`

Disable SEKM

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.DisableSecurity

Example request body：`{"TargetFQDD":"NonRAID.SL.8-1"}`

Note：If above operation fails with message below, make sure to erase all drives which is shown in steps below.

“One or more Storage device(s) are not in a state where the operation can be completed.”

SAS SED behind HBA

Enable SEKM

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.EnableSecurity

Example request body：`{"TargetFQDD":" Disk.Bay.7:Enclosure.Internal.0-1:NonRAID.SL.8-1"}`

Verify SEKM

GET

/redfish/v1/Systems/System.Embedded.1/Storage/NonRAID.SL.8-1/Drives/Disk.Bay.7:Enclosure.Internal.0-1:NonRAID.SL.8-1

Expected attributes if SEKM security is enabled: `"EncryptionStatus": "Unlocked"`

Disable SEKM

PSID revert

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.CryptographicEraseWithPSID

Example request body: `{"DriveFQDD":"Disk.Bay.7:Enclosure.Internal.0-1:NonRAID.SL.3-1", "PSID":"CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0"}`

Note: PSID information can be found on the physical label of the drive.

Cryptographic erase

POST

/redfish/v1/Systems/System.Embedded.1/Storage/NonRAID.SL.3-1/Drives/Disk.Bay.7:Enclosure.Internal.0-1:NonRAID.SL.3-1/Actions/Drive.SecureErase

Example request body: {}

NVMe SED

Enable SEKM

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.EnableSecurity

Example request body: `{"TargetFQDD":" Disk.Bay.12:Enclosure.Internal.0-1"}`

Verify SEKM

GET

/redfish/v1/Systems/System.Embedded.1/Storage/CPU.1//Drives/Disk.Bay.12:Enclosure.Internal.0-1

Expected attributes if SEKM security is enabled: `"EncryptionStatus": "Unlocked"`

Disable SEKM

PSID revert

POST

/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.CryptographicEraseWithPSID

Example request body: `{"DriveFQDD":" Disk.Bay.12:Enclosure.Internal.0-1", "PSID":"CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0"}`

Note: PSID information can be found on the physical label of the drive.

Cryptographic erase

POST

/redfish/v1/Systems/System.Embedded.1/Storage/ CPU.1/Drives/ Disk.Bay.12:Enclosure.Internal.0-1/Actions/Drive.SecureErase

Example request body: {}

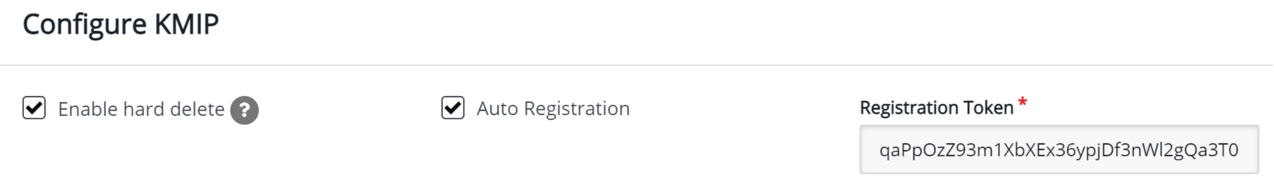
14 iDRAC initiated KMS key purge

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

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

1. Configure KMIP to delete keys

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



Configure KMIP

☑ Enable hard delete

☑ Auto Registration

Registration Token *

qaPpOzZ93m1XbXEx36ypjDf3nWl2gQa3T0

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

2. Key Purge Policy

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

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

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

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

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

KMSKeyPurgePolicy=Keep All Keys

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

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

Object value modified successfully
```

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

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

KMSKeyPurgePolicy=Keep N and N-1 keys
```

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

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

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

3. Purge Old keys

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

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

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

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

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

KMSPurgeOldKeys=Disabled


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

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

Object value modified successfully
```

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

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

KMSPurgeOldKeys=Enabled
```

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

4. KMS Key Purge on SEKM disable

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

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

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

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

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

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

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

15 Troubleshoot issues while setting up SEKM on iDRAC

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

15.1 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.

15.2 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.
    - Username 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.

15.3 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.

15.4 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.

15.5 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.

15.6 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.

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

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

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

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

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

15.8 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.

15.9 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.

15.10 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.

15.11 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.

15.12 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.

15.13 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.

15.14 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.

15.15 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).

15.16 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**.

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

Update to latest iDRAC and PERC firmware.

15.18 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.

15.19 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.

15.20 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.

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

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

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

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

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

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

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

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

15.24 Enabled Auto-Secure option but security was not enabled on SAS HBA or PERC

Controllers such as PERC/SAS HBA will not be auto secured and will need to be manually secured.

15.25 Hot plugged a SED but the drive is not showing up in the OS.

Rescan the drive in the OS after it’s reported in iDRAC storage inventory as secured.

15.26 Unable to disable SEKM on iDRAC?

Make sure security is disabled on all storage devices before attempting to disable SEKM on iDRAC.

15.27 Unable to disable security on SAS HBA?

Make sure all drives have security disabled.

A Technical support and resources

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