

Enable SEKM on Dell PowerEdge Servers

Configuration and Deployment Guide

Abstract

This Dell Deployment Guide explains how to enable the Secure Enterprise Key Management (SEKM) feature on PowerEdge servers. It also provides key tips and troubleshooting methods for SEKM.

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Introduction.....	8
Document Changes.....	8
Contributors.....	10
About this document.....	10
Chapter 2: Executive Summary.....	11
Chapter 3: Supported Storage Devices and Key Management Servers.....	12
Chapter 4: CipherTrust Manager (k170v).....	15
CipherTrust Manager prerequisites.....	15
Migration from KeySecure Classic (k150v) or Thales Data Security Manager (DSM) to CipherTrust	15
Automated Deployment.....	16
Set up SEKM on CipherTrust Manager.....	16
Configure Auto-Client Registration.....	16
Configure KMIP Interface.....	18
Create a user that represents iDRAC on CipherTrust Manager.....	22
Set up SEKM on iDRAC.....	23
Configure SEKM using the iDRAC GUI.....	23
Get the CSR file signed by CipherTrust Manager.....	27
Download the server CA from CipherTrust Manager and upload to iDRAC.....	28
Viewing iDRAC key ID on CipherTrust Manager.....	29
Chapter 5: IBM Secure Guardium Key Lifecycle Manager.....	31
IBM Secure Guardium Key Lifecycle Manager (SGKLM) prerequisites.....	31
Set up SEKM on IBM SGKLM.....	31
Generate CSR for Server Certificate.....	31
Sign CSR with external CA	33
Upload signed CSR to IBM SGKLM.....	33
Set up SEKM on iDRAC.....	35
Configure SEKM using the iDRAC GUI.....	35
Get the CSR file signed by an external CA.....	35
Register Client on IBM SGKLM.....	36
Upload the signed CSR for iDRAC to IBM SGKLM.....	36
Import external CA into IBM SGKLM.....	36
Download the external CA and upload to iDRAC.....	37
Viewing iDRAC key ID on IBM SGKLM.....	38
Audit and debug on IBM SGKLM.....	38
Chapter 6: Utimaco.....	40
Utimaco prerequisites.....	40
Set up SEKM on Utimaco.....	40
Set up SEKM on iDRAC.....	43
Configure SEKM using the iDRAC GUI.....	43

Get the CSR file signed on Utimaco.....	46
Download the server CA file from Utimaco and upload to iDRAC.....	49
View iDRAC key ID on Utimaco.....	51
Chapter 7: Fortanix Data Security Manager.....	52
Fortanix prerequisites.....	52
Set up SEKM on Fortanix.....	52
Set up SEKM on iDRAC.....	52
Configure SEKM using the iDRAC UI.....	53
Get the CSR file signed.....	54
Download the CA and upload it to iDRAC.....	54
Chapter 8: Entrust KeyControl.....	56
Entrust KeyControl prerequisites.....	56
Set up SEKM on Entrust.....	56
Set up SEKM on iDRAC.....	56
Configure SEKM using the iDRAC GUI.....	56
Get the CSR file signed.....	58
Download the CA and upload to iDRAC.....	59
Chapter 9: Configure SEKM on iDRAC.....	61
Configure SEKM using Redfish.....	61
Configure SEKM using RACADM.....	63
Configure SEKM using Server Configuration Profile.....	66
Chapter 10: Auto Secure.....	69
Configure Auto Secure using the iDRAC UI.....	69
Configure Auto Secure using Redfish.....	69
Configure Auto Secure using RACADM.....	70
Configure Auto Secure using Server Configuration Profile.....	71
Chapter 11: PowerEdge RAID Controller.....	72
Overview.....	72
Configure PERC using the iDRAC UI.....	72
Configure PERC using Redfish.....	74
Configure PERC using RACADM.....	75
Configure PERC using Server Configuration Profile.....	77
Chapter 12: Host Bus Adapter.....	78
Overview.....	78
Configure HBA using the iDRAC UI.....	78
Configure HBA using Redfish.....	79
Configure HBA using RACADM.....	81
Configure HBA using Server Configuration Profile.....	83
Chapter 13: CPU Attached NVMe SEDs.....	85
Configure CPU attached NVMe SED using iDRAC UI.....	85
Configure CPU attached NVMe SED using Redfish.....	86
Configure CPU attached NVMe SED using RACADM.....	86

Configure CPU attached NVMe SED using Server Configuration Profile.....	87
Chapter 14: Boot Optimized Storage Solution	88
Configure BOSS-N1 using the iDRAC UI.....	88
Configure BOSS-N1 using Redfish.....	90
Configure BOSS-N1 using RACADM.....	91
Configure BOSS-N1 using Server Configuration Profile.....	94
Chapter 15: RAID on RISER.....	95
Configure ROR-N1 using the iDRAC UI.....	95
Configure ROR-N1 using Redfish.....	97
Configure ROR-N1 using RACADM.....	98
Configure ROR-N1 using Server Configuration Profile.....	100
Chapter 16: Software Defined Persistent Memory.....	102
Configure SDPM using the iDRAC UI.....	102
Configure SDPM using Redfish.....	104
Configure SDPM using RACADM.....	106
Configure SDPM using Server Configuration Profile.....	108
Chapter 17: Cryptographic Erase.....	109
Overview.....	109
Cryptographic Erase using the iDRAC UI.....	109
Cryptographic Erase using Redfish.....	110
Cryptographic Erase using RACADM.....	110
Cryptographic Erase using Server Configuration Profile.....	111
Chapter 18: PSID Revert.....	113
Overview.....	113
PSID revert using the iDRAC UI.....	113
PSID revert using Redfish.....	114
PSID revert using RACADM.....	114
PSID revert using Server Configuration Profile.....	114
Chapter 19: PERC LKM to SEKM Transition.....	116
Overview.....	116
PERC LKM to SEKM transition using the iDRAC UI.....	116
PERC LKM to SEKM transition using Redfish.....	119
PERC LKM to SEKM transition using RACADM.....	119
PERC LKM to SEKM transition using Server Configuration Profile.....	120
Chapter 20: iDRAC Initiated KMS Key Purge.....	121
Overview.....	121
Configure Key Purge Policy using Redfish.....	122
Configure Key Purge Policy using RACADM.....	122
Configure Key Purge Policy using Server Configuration Profile.....	122
Disable Key Purge on SEKM.....	123
Chapter 21: iDRAC Volatile Key Caching.....	124

Overview.....	124
Configure VKC using Redfish.....	126
Configure VKC using RACADM.....	127
VKC guidelines and limitations.....	127
Chapter 22: Import Pre-Generated Host Certificate and Private Key into iDRAC using Redfish..	129
Overview.....	129
Custom Certificate.....	130
Custom PEM certificate.....	131
Chapter 23: Periodic Sync with Key Management Server.....	134
Chapter 24: Scheduled Rekey.....	136
Chapter 25: Easy Restore.....	139
Chapter 26: Crypto-Erase All Drives in a Single Operation.....	140
Chapter 27: Troubleshooting.....	141
SEKM license installed but cannot enable on iDRAC.....	141
SEKM SSL certificates uploaded but cannot enable SEKM.....	141
Cannot switch PERC to SEKM mode.....	142
SEKM failed for PERC encryption mode.....	142
SEKM status shows "Unverified Changes Pending".....	142
SEKM status shows "Failed" after changing KMIP authentication settings.....	142
SED shows as Locked and Foreign after moving to another SEKM-enabled PERC.....	143
SEKM failed after moving SEKM-enabled PERC to another server.....	143
Key size and algorithm used by KMS.....	143
New PERC encryption mode is "None" after replacement.....	143
New key generated after replacing SEKM-enabled PERC.....	144
New BOSS-N1 security status after replacement.....	144
Rollback of iDRAC firmware blocked.....	144
Restoring SEKM mode on PERC after network outage.....	144
Changing keys on a PERC.....	144
PERC encryption mode still shows SEKM after system erase.....	144
Cannot switch PERC to SEKM mode from LKM mode.....	144
SED shows as Locked and Foreign after migrating from LKM to SEKM mode.....	145
Cannot switch PERC to SEKM from eHBA personality mode.....	145
Information on SEKM setup failures, key exchange issues, successful exchanges, or rekey operations..	145
SEKM key exchange after deleting SEKM license.....	145
SEKM key exchange after an iDRAC reset.....	145
SEKM key exchange failed after a warm reboot, but secured volume drives are still online and secured.....	145
Auto Secure not enabling security on HBA or PERC.....	146
Hot-plugged SED not showing up in the OS.....	146
Cannot disable SEKM on iDRAC.....	146
Cannot disable security on HBA or BOSS controller.....	146
Confirming IP address in the KMS certificate SAN field.....	146
Recovering from a key exchange failure after changing the iDRAC IP.....	147

Updating PERC or HBA 12 firmware to version 12.2 or later.....	148
Chapter 28: Technical support and resources.....	149

Introduction

Topics:

- [Document Changes](#)
- [Contributors](#)
- [About this document](#)

Document Changes

Table 1. Document changes

Date	Description
July 2019	Initial release
June 2020	Added procedures that are 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 about how to configure the SEKM solution with Redfish and new support for SAS HBA, direct attach NVMe SEDs, and PERC LKM to SEKM transition.
April 2022	Change highlights: <ul style="list-style-type: none"> • Added supported storage controller table. • Removed reference to the old storage configuration page. • Included notes about the "Download CSR" option introduced in the UI. • Added automated deployment section (reference 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.
August 2022	Added Utimaco KMS and IBM KMS sections.
October 2022	Added steps on how to confirm if an IP address is in the KMS certificate Subject Alternative Name (SAN) field.
May 2023	Change highlights: <ul style="list-style-type: none"> • Updated supported storage controller table. • Added GUI instructions for enabling SEKM on BOSS-N1 and SDPM/VOSS solutions. • Added RACADM commands for BOSS-N1 and SDPM/VOSS solutions. • Added Redfish calls for BOSS-N1 and SDPM/VOSS solutions. • Added reference to Redfish API guide. • Added reference to the BOSS-N1 User Guide.
July 2023	Change highlights:

Table 1. Document changes (continued)

Date	Description
	<ul style="list-style-type: none"> • Added notes regarding real-time operation support for PERC 12 and newer generations.. • Added notes regarding the Identity Module required for SEKM HBA support. • Added FIPS Compliance descriptor in Redfish section.
January 2024	<p>Change highlights:</p> <ul style="list-style-type: none"> • Updated supported storage controller table. • Added commands for all supported interfaces on ROR-N1. • Added reference to instructions on how to migrate data from KeySecure Classic or Data Security Manager to CipherTrust Manager. • Added Volatile Key Caching (VKC) section. • Added reference to SCP guide. • Added reference to drive erase process (ISE). • Added additional information to the troubleshooting section. • Added reference on where to find supported KMS versions (iDRAC release notes).
March 2024	<p>Added support for importing a pregenerated host certificate and private key into iDRAC.</p>
August 2024	<p>Change highlights:</p> <ul style="list-style-type: none"> • Added SEKM support for HBA 465i. • Updated supported storage controller table. • Added support for SEKM custom PEM certificates. • Added support for Periodic Sync with Key Management Server. • Added support for Scheduled Rekey on iDRAC. • Added support for Redfish <code>OperationApplyTime</code> on BOSS-N1 security enable operation. • Added support for reduced reboots on SDPM systems with security enabled. • Added support for real-time erase operation SDPM SEDs. • Added section for Easy Restore. • Added additional information to the troubleshooting section.
October 2024	<p>Change highlights:</p> <ul style="list-style-type: none"> • Updated format for supported storage controller table. • Added support for <code>ControllerDrivesDecommission</code> action URI to crypto-erase all drives behind BOSS-N1 in a single action. • Added support for Redfish API <code>GET</code> request on Periodic Sync schedule. • Added support for Fortanix Data Security Manager.
December 2024	<p>Added HBA 465i support for <code>ControllerDrivesDecommission</code>.</p>
March 2025	<p>Change highlights:</p> <ul style="list-style-type: none"> • Updated supported storage devices table. • Added support for Entrust KeyControl key management server. • Added supported key management server table. • Modified Redfish URIs to be compatible with both iDRAC9 and iDRAC10. • Added additional information to Periodic Sync section.

Table 1. Document changes (continued)

Date	Description
April 2025	Change highlights: <ul style="list-style-type: none">• Added additional information related to BOSS-N1/ROR-N1 security disablement.• Removed references to a suppressed attribute.• Updated BIOS SdpmCurrentSize and SEKM.1.RekeyMode Redfish URIs.
June 2025	Change highlights: <ul style="list-style-type: none">• Added support for PERC H975i Front.

Contributors

The Dell Enterprise Server Solutions team created this guide.

Authors: Sanjeev Dambal, Texas Roemer, Xavier Conley, Ajay Shenoy, Srikanth Krishnamurthy, Anila Sri y

Content Engineering & Translation: Krista Chen

About this document

NOTE: Many PDF viewers add a line break to the end of each line of text in a PDF. Adobe Acrobat (Reader, Standard, and Pro) and other common PDF viewers, including Google Chrome and Microsoft Edge, insert these line breaks. As a result, when you copy commands that wrap across multiple lines in a PDF, the copied commands contain erroneous line breaks. If you copy and paste commands, the line breaks cause issues.

To address this known limitation and ensure that copied commands do not contain unintentional line breaks, do one of the following:

- Paste the copied commands into a text editor and remove the line breaks.
- Use the HTML version of this document when you are copying commands.

Executive Summary

This guide provides an overview of how to secure storage devices on Dell PowerEdge servers using the OpenManage Secure Enterprise Key Manager (SEKM). By integrating SEKM with supported Key Management Servers (KMS) such as CipherTrust, Utimaco, IBM, Fortanix, and Entrust, you can ensure robust key management and enhanced security for your IT infrastructure. The guide includes setup instructions, key tips, and troubleshooting methods to help you deploy and manage SEKM.

Supported Storage Devices and Key Management Servers

NOTE: See iDRAC release notes for supported Key Management Server versions.

NOTE: iDRAC Key Management does not support PERC H840 Adapter or HBA 465e Adapter.

Table 2. Supported storage devices

Storage controller	Auto Secure	LKM support	SEKM support	Minimum firmware
Direct-attach NVMe	Yes	No	Yes	N/A
SDPM	Yes	No	16G only	N/A
PERC H975i Front	No	No	17G only	8.11.0.0.28-86
PERC H365i Front	No	15G/16G only	16G/17G only	8.11.0.0.15-22
PERC H365i Adapter	No	15G/16G only	16G/17G only	8.11.0.0.15-22
PERC H965i Front	No	15G/16G only	16G/17G only	8.0.0.0.18-81
PERC H965i Adapter	No	15G/16G only	16G/17G only	8.0.0.0.18-81
PERC H965e Adapter	No	15G/16G only	16G/17G only	8.4.10.0.18-4
PERC H965i MX	No	15G/16G only	16G/17G only	8.8.0.0.18-26
PERC H755 Front	No	15G/16G only	15G/16G only	52.16.1-4074
PERC H755N Front	No	15G/16G only	15G/16G only	52.16.1-4074
PERC H755 Adapter	No	15G/16G only	15G/16G only	52.16.1-4074
PERC H750 Adapter	No	15G/16G only	15G/16G only	52.16.1-4074
PERC H740P Mini	No	15G/16G only	15G/16G only	51.13.2-3714
PERC H740P Adapter	No	15G/16G only	15G/16G only	51.13.2-3714
HBA 465i Front	No	No	16G only	8.8.0.0.15-26
HBA 465i Adapter	No	No	16G only	8.8.0.0.15-26
HBA 355i Adapter	Yes*	No	VxRail/16G only	17.15.08.00
HBA 355i Front	Yes*	No	VxRail/16G only	17.15.08.00
BOSS-N1 DC-MHS	No	No	17G only	2.2.13.2033
BOSS-N1 Monolithic	No	No	16G only	2.1.13.2017
BOSS-N1 Modular	No	No	16G only	2.1.13.2017
ROR-N1	No	No	16G only	2.1.13.2025


NOTE: *Encryption capable drives behind HBA 355i support Auto Secure, but security on the controller needs to be manually enabled first. For more information, see the [HBA section](#).

Table 3. Supported key managers

Key management servers
CipherTrust Manager
IBM Secure Guardium Key Lifecycle Manager
Utimaco Enterprise Secure Key Manager
Fortanix Data Security Manager
Entrust KeyControl Vault Manager

Table 4. Security properties

Device	Security Properties	Values	Description
PERC with iDRAC10	Encryption capability	Not Capable Capable	Indicates if the controller supports encryption.
	Encryption mode	Disabled Enabled	Indicates current Encryption Mode for the controller.
	Security status	Encryption Capable Security Key Assigned	Indicates current security status for the controller.

 **NOTE:** PERC 11 and earlier generations are not supported on 17G platforms.


 **NOTE:** iDRAC Key Management does not support the PERC H840 Adapter or the HBA 465e Adapter.

Table 5. Security properties, continued

Device	Security Properties	Values	Description
PERC with iDRAC9	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 Secure Enterprise Key Manager Failed"	Indicates current encryption mode for PERC.
	Security Status	"Security Key Assigned"	Indicates current security status for PERC.
HBA 465i	Encryption capability	"Not Capable Capable"	Indicates if HBA 465i supports encryption.
	Encryption mode	"Disabled Enabled Secure Enterprise Key Manager Failed"	Indicates current encryption mode for HBA 465i.
	Security status	"Encryption Capable Security Key Assigned"	Indicates current security status for HBA 465i.
HBA 355i, BOSS-N1, ROR-N1	Encryption capability	"Not Capable Capable"	Indicates if the controller is security-capable.
	Encryption mode	"Not Applicable"	HBA, BOSS-N1, and ROR-N1 do not support encryption mode property such as LKM or SEKM. Therefore, encryption mode is not applicable.

Table 5. Security properties, continued (continued)

Device	Security Properties	Values	Description
	Security status	"Not Capable Disabled Enabled"	Indicates current security status for the controller.
SED	Encryption capability	"Not Capable Capable"	Indicates if the drive is security-capable.
	Encryption mode	"Not Capable Encryption Capable Secured Locked Foreign"	Indicates current security status of the drive.
	Security status	"None TCG Enterprise SSC TCG Opal SSC"	Indicates encryption protocol that is supported by the drive.

NOTE: SEKM supports CPU-attached NVMe SEDs only if they use the TCG Opal 2.0 protocol.

NOTE: SEKM supports the HBA 355i only on VxRail platforms. (E660F, P670F, and V670F models).

NOTE: SEKM supports HBA solutions only on SEDs that use the TCG Enterprise Protocol. For more details, see the HBA section.

NOTE: SEKM supports BOSS-N1, ROR-N1, and SDPM solutions only on M.2 NVMe SEDs that use the TCG Opal 2.0 protocol.

CipherTrust Manager (k170v)

Topics:

- CipherTrust Manager prerequisites
- Migration from KeySecure Classic (k150v) or Thales Data Security Manager (DSM) to CipherTrust
- Automated Deployment
- Set up SEKM on CipherTrust Manager
- Configure Auto-Client Registration
- Configure KMIP Interface
- Create a user that represents iDRAC on CipherTrust Manager
- Set up SEKM on iDRAC
- Configure SEKM using the iDRAC GUI
- Get the CSR file signed by CipherTrust Manager
- Download the server CA from CipherTrust Manager and upload to iDRAC
- Viewing iDRAC key ID on CipherTrust Manager

CipherTrust Manager prerequisites

Before you set up iDRAC SEKM support, you must fulfill the following prerequisites.

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 that are updated to the firmware version which supports SEKM

CipherTrust Manager prerequisites

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

Migration from KeySecure Classic (k150v) or Thales Data Security Manager (DSM) to CipherTrust

You can migrate data from KeySecure Classic or Thales DSM to the latest supported version of CipherTrust Manager. The migration takes place by creating a backup file on KeySecure Classic or DSM, then importing that file to CipherTrust. For more information about supported data and steps that are required to perform the migration from KeySecure Classic, see [Migrate from KeySecure Classic](#) on the Thales support site. For Thales DSM steps, see [Migrate from Data Security Manager](#).

 **NOTE:** To use CipherTrust, reconfigure iDRAC SEKM certificates and KMS settings. For more information, see [Set up SEKM on CipherTrust Manager](#) and [Configure iDRAC with CipherTrust](#).

Automated Deployment

After configuring Auto-Client registration and the KMIP interface on CipherTrust, you can use an automated Python script to set up the complete SEKM solution iDRAC. For more details, see the [SEKM scripting GitHub page](#).

Set up SEKM on CipherTrust Manager

iDRAC supports the following CipherTrust Manager features. For information about other CipherTrust features, see the [CipherTrust Appliance Administration Guide](#).

Configure Auto-Client Registration

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

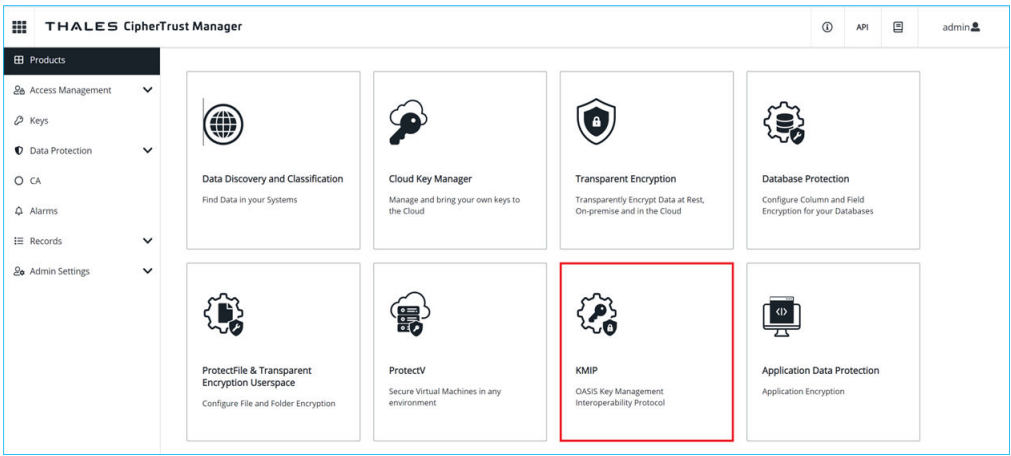


Figure 1. CipherTrust Manager dashboard

2. Click **Client Profile > Add Profile**.



Figure 2. Add client profile

3. Enter or select data in the **Add Profile** dialogue box.

Add Profile

Profile Name *

Username Location in Certificate

IDRAC Profile

CN

Subject DN field to modify ?

Do not modify subject DN

NONE

☒

Certificate Details

+

Device Credentials

+

Cancel

Save

Figure 3. Add profile

NOTE: Certificate Details and Device Credentials are not necessary for this step. If you are using CipherTrust version 1.10 or below, specify the Common Name field in the certificate to add a profile. Ensure that a user with this name exists on the CipherTrust appliance. This user does not need to be added to the group.

4. Click **Registration Token > New Registration Token**.

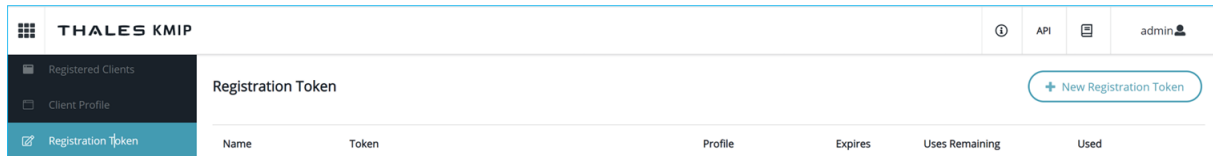


Figure 4. New registration token

5. Enter the prefix name of the Registration Token. For example, "iDRAC token."

This is the 'Create New Registration Token' form, step 01: Configure Token. It includes a progress bar with steps: 01 Configure Token, 02 Select CA, 03 Select Profile, and 04 Create Token. A note says 'Use company specific naming conventions when setting up a new token.' There are three input fields: 'Name Prefix' (containing 'iDRAC token'), 'Token lifetime' (set to 'unlimited' with a checkmark), 'Certificate Duration' (set to '730'), and 'Client Capacity' (set to '100'). At the bottom right are 'Back' and 'Select CA' buttons.

Figure 5. Configure new registration token

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

This is the 'Create New Registration Token' form, step 02: Select CA. The progress bar shows steps: 01 Configure Token, 02 Select CA, 03 Select Profile, and 04 Create Token. Under 'Local CAs', there is a radio button selected for '/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA'. At the bottom right are 'Back' and 'Select Profile' buttons.

Figure 6. Select CAs

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

This is the 'Create New Registration Token' form, step 03: Select Profile. The progress bar shows steps: 01 Configure Token, 02 Select CA, 03 Select Profile, and 04 Create Token. Under 'Client Profile', there is a dropdown menu showing 'iDRAC profile'. At the bottom right are 'Back' and 'Create Token' buttons.

Figure 7. Select client profile

8. Copy the registration token.

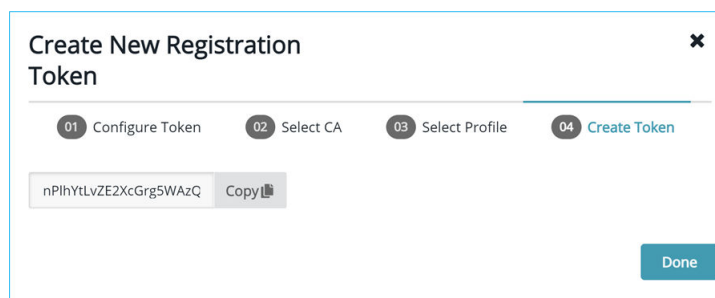


Figure 8. Copy registration token

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

Figure 9. Edit KMIP interface

NOTE: Disable automatic generation from a Local CA on the configured KMIP page. If you do not disable this option, CipherTrust will replace the KMIP server certificate with a new certificate after rebooting. You can find this option under Local CA for Automatic Server Certificate Generation in the Edit section.

15. If you are using an older version of CipherTrust (versions 1.10 and below), restart the KMIP services by clicking **System > Services > Restart KMIP**.

Configure KMIP Interface

The Local Certificate Authority that is shown in the image is available by default.

<div>Products</div> <div>Access Management</div> <div>Keys</div> <div>CA</div> <div>Local</div> <div>External</div> <div>CSR Tool</div>	<h2>Local Certificate Authorities</h2> <p>1 Result 1 Local CA</p> <table> <tr> <th>Name</th><th>Subject</th></tr> <tr> <td>localca-5681a012-408c-44cf-bb0d-e086fa4e26e9</td><td>/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA</td></tr> </table>	Name	Subject	localca-5681a012-408c-44cf-bb0d-e086fa4e26e9	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Name	Subject				
localca-5681a012-408c-44cf-bb0d-e086fa4e26e9	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA				

Figure 10. Local Certificate Authorities

If you are using a newer version of CipherTrust (version 2.3 and above), click **Local CA > Issue Certificate** and do the following:

Issue Certificate

Display Name

Common Name

Algorithm

Size

RSA

2048

Subject Alternative Names

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

Issue Certificate

Figure 11. Issue Certificate

- **Algorithm:** RSA
- **Size:** 2048

NOTE: The older version of Gemalto had a single field for Subject Alternative Name (SAN). This field has been split into two separate fields on CipherTrust: DNS Names and IP Addresses. It is mandatory to enter both fields to prevent iDRAC SEKM setup issues or key exchange failures.

1. Click both "save csr" and "save private key."

☐ Encrypt Private Key

save csr

save private key

You must save the Private Key to continue

Figure 12. Save csr and private key buttons

- Copy the contents of your CSR and get it signed by your Certificate Authority. In this example, we use the Certificate Authority that is available by default.
- Click **CA > Local Certificate Authority**.

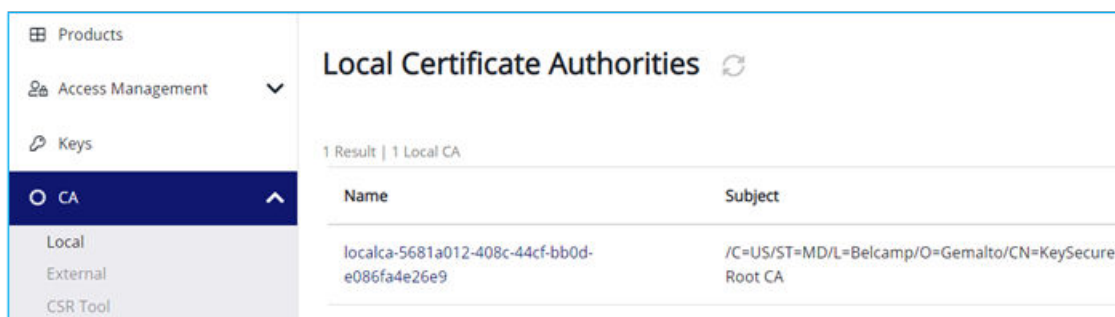


Figure 13. Local Certificate Authorities

- Select **CA** (Certificate Authority). After you select the CA, the **Issue Certificate** and **Upload CSR** buttons are displayed.



Figure 14. Issue Certificate and Upload CSR buttons

- Select **Upload CSR**, then upload the contents from the CSR you generated in the steps above.
- Upload the externally generated CSR.

Figure 15. Upload Externally Generated CSR

NOTE: Select **server** for Certificate Purpose.

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

- Click the ellipses (...) symbol, download the signed certificate, and save it to your system.
- Take the private key that you downloaded in the steps above and append it to the signed certificate you downloaded. An example of a private key is shown in the screenshot here:

```

-----BEGIN CERTIFICATE-----
MIIDrDCCAZSgAwIBAgIQLa47JRqlqWA8KnM9L3pZTANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEDAOBgNVBACwBTB0J1bG9nbHhXaXEDAO
BgNVBAoTB0d1bWFnZsdG8xGjAYBgNVBAMTEUt1eVN1Y3VyZSB5b290IENBMBA4XDITx
MTAwOTIwNDIxOVVoXDTIyMTAwOTIwNDIxOVVowFzEVMBMGA1UEAxMmMTAwLjY0LjI0
LjI4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCGo3baZiLf2xdymghU18P
0qK1uOYHh0A+7eLf0ze7P9MQLf9SsysbhAkVBSx41JuAgpbmIWQpGu1etUzc1TSm3
9pHi+itI3I5nS4WBfN/yMHXjc0tdpgdgQfoz1NhR3ftgK07ZeU7Fjxcov0oykDWme1t
BDxkQX5Xf97SX0UrM6wIDAQABoZUwMzA0BgNVHQ8BAf8EBAMCA4gwEwYDVR01
BAwwCgYIKwYBBQUHAwEwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAGEA
MsdPI1TMbsfPD9xH3yltRYM2FVEjnwziU708PyJ89rjLfY846317Wg2A0oej9uHn
LiCn0b+1k+OIHRbJtJ6UZ6h/TL57x/cJ06g1S/VNhxHi2HRUrDA1gQXLfiBbpqEb
pS0EbfoBjH+0MgibGnBsLcLBD55hvEVvHXs2cwWUICrHdRt0VTP8xXKQfmPsoYR
Lj1FF4Rfc1QZ5kEG1U9y8nV+huOjQ8Nt4fDrNbm/ZR10aN1+3VR8oNtAYrUNaVxa
8hShsa6H0rfo2cEbxLpkOgae4nnzEjLqh1hxbaoB9cVJXtzG4aDDG0DwLSCFg1/u
01P2p/sF1TpU0EwC8EigHf5SKPkeX1ufQb4SFmWQceP0S+Pb3x8dZyLe0Z1+VYf
Vt0zj58cKtUjnOKU8cm1m/SxjiBaZyE2sX4mIkO5xJdz1xvzIztQWv6/ss600CG1
R3Y+3UZDH6mP96P1VtWwQqkYGysfzN5wmh9ohjmrqnP1wHyjDmm6JfVMutsvf0du
kt/SMck6AS41WCHtC9BNdn5MB07aLEv25dzJHmC3SSREv2fKow5qXjlcAq44cE6n
b3H1eaBRk178HFCyxcg3eEf5vwe6aF8XoPdJ37bUuctqrPho8mizDBL/aL6jeP7m
u310T6PjK27/PVonV6tyYxruVGoidiG85Fzxejh0Rm8=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDCGo3baZiLf2xdymghU18P0qK1uOYHh0A+7eLf0ze7P9MQLf9S
ysbhAkVBSx41JuAgpbmIWQpGu1etUzc1TSm39pHi+itI3I5nS4WBfN/yMHXjc0td
pgdgQfoz1NhR3ftgK07ZeU7Fjxcov0oykDWme1tBDxkQX5Xf97SX0UrM6wIDAQAB
AoGBAJ4ajw33lz+ZTSWgZu0uQbJbugw07Z+WRio8Dp4SWDT3qe316ZEAhrpk61vJ
2hM1VU6Cbtv2u34dvy75J2QE1EM0/MU6xNjbHLKQlyPSwB36pnM367QeVWNB26r
dm99uUIWAQwzCc8GFx1IU5q2WZMKWmV9DgtVPi7/MiOF/9MRaKEA5xY1CHNSKX9y
LlvVVPQVzqNu80hmeMedMKWhNC88YRweBCXSXfa4wHEM5rX6sWiNR2j0BKA0vJfZ
bmsdYjekFQJBANChTl0jlr+xNt00b8oF9vmXiWw0TwhL3jxpM8j0ecN1yMoHBkz8
+xe5V5yhIfbQ93YWzuQD70breZ0har3v7P8CQEz7C4stH4nDcv40iZqrVThpKWQH
h1tk4/B4vKLtuWeAP1+TWekDb7hr8KhKpyDCe432U+uxGzeoPj6SYE9/yaECQAZQ
1sLXFisCouPnQyp1RJ0HnRbEs1kqPGqZUo7LT5KIuJjh5kw8X7LARYp8qAuP1M/i
+B265im1Kx/TZQtA+30CQEZyflA2wHm0WXJhwjcbHa/kTxEgobDTzeYkkPixztdt
/Gr4pmbnBtwSNw1FCmpoysZ7w85ZSd25LYoivP4PBDQ=
-----END RSA PRIVATE KEY-----

```

Figure 16. Private key example

9. Save this file and upload it to the KMIP interface.
10. Upload the signed certificate and private key to the KMIP interface.
11. Click **Admin Settings > Interfaces**.
12. Click the ellipses symbol next to the KMIP interface, then click **Upload New Certificate**.

Upload Certificate [X]

Certificate *

☐ File Upload ☒ Text

The certificate and key data in PEM format or base64 encoded PKCS12 format

Format *

PEM

Password (optional)

Password to the encrypted key

Cancel Upload Certificate

Figure 17. Upload Certificate

- **Text:** Includes the signed certificate and appended private key.
- **Format:** PEM

13. Click **Upload Certificate**.

NOTE: If you are using an older version of CipherTrust (versions 1.10 and below), you must restart the KMIP services.

14. Go to **System > Services > Restart KMIP**.

Create a user that represents iDRAC on CipherTrust Manager

1. Click **Access Management > Users > Add User**.

Create a New User

Username: S3ST001_R750

Email: email

Password:

Password Match:

☒ Has at least 1 characters

☐ Require user to reset password on next login

☐ Allow user to login using certificate

Connection (fixed): local_account

Figure 18. Create a new user

NOTE: The username must match the Username Location 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	<input type="checkbox"/>	<button>Add</button>
global	local 91e776ce-7b9a-457c-be64-90de66002161	<input type="checkbox"/>	<button>Add</button>
S3ST001_R750	local 8cb66fa9-b92a-40a1-83c5-c495a01fffd6	<input checked="" type="checkbox"/>	<button>Remove</button>

3 Users 10 per page ▾

Figure 19. Key users

Set up SEKM on iDRAC

Licensing and firmware update

SEKM requires an iDRAC Enterprise or Data Center license. To avoid an extra firmware update, install the SEKM license first, then update the iDRAC firmware to a version that supports SEKM. An iDRAC firmware update is always needed after installing the SEKM license, even if the current firmware supports SEKM. Use existing methods to install licenses and firmware updates for SEKM.

Set up SSL certificate

The SEKM solution requires two-way authentication between iDRAC and the KMS. Generate a CSR on iDRAC, get it signed by a CA on the KMS, and upload the signed certificate to iDRAC. For KMS authentication, upload the KMS CA certificate to iDRAC.

Configure SEKM using the iDRAC GUI

1. Start iDRAC using any supported browser.

2. Click **iDRAC Settings > Services**.
3. Expand the **iDRAC Key Management** menu and select **SEKM** for Key Management Service.
4. Go to **SEKM Configuration**.
5. Enter the KMS IP address and iDRAC KMS user ID and password, if applicable.

Configuration Secure Enterprise Key Manager (SEKM)

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

KMS (IP Address or FQDN)*

Port Number*

Redundant KMS Information

Port Number

Redundant KMS 1 (IP Address or FQDN)

+ Add Redundant KMS

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.

Step 2 of 5

Cancel Back Next Finish

Figure 20. iDRAC Key Management window for SEKM

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

6. Click **Next**.
7. Click **Generate CSR**.

Configuration Secure Enterprise Key Manager (SEKM)

?

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1

Generate a Certificate Signing Request (CSR)

Generate CSR

Download 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.

Upload Signed CSR

i

Step 3 of 5

Cancel

Back

Next

Finish

Figure 21. SEKM certificate

NOTE: The Download CSR option becomes available after generating a CSR.

- Enter the certificate information in the **Generate Certificate Signing Requests (CSR)** dialog box.

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)*

idrac-HC02502

Country Code (CC)

United States ▼

Locality (L)*

Round Rock

Organization Name (O)*

Dell

Organization Unit (OU)*

ISG

State*

Texas

Email

Subject Alternative Names

i

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-HC02502

iDRAC IP Address in CSR

☒ Include

Cancel

Generate

Figure 22. Generate Certificate Signing Request box

i | NOTE: Include both the user ID and iDRAC IP address options in the CSR field.

9. Click **Generate**.
10. Save it to your system.

Get the CSR file signed by CipherTrust Manager

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

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVUZXBhczETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAzMBFRl
c3QxGTAXBgNVBAMMEG1kcmFjdXN1ckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWDRl
c3R1ckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj
7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL
JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjgMgmRhIdnINI6Ya+lWV
i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLqlHpY1c9kGgnjae
LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFACqp0z
76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg
5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAlw
ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na
V3t5LGma/I3sPY14baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+
ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4
Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvGf1A
EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y
kjwt+SxEOs6JnYpT9yxJSCj2RmddB56ZYUGD02DL7iALsbkQtfovLpjo9pPBD2lp
36A=

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

Figure 23. 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

Figure 24. Local Certificate Authorities

3. Click **Upload CSR**.

Upload Externally Generated CSR

4pM70MyV7UmBDr+ICqj5KEkjDOD8rupg5CT+UWGx57Bw95bWJl+ocGvNs6XJS8EL
LYBHDT97igMfIO0oBlzQS/nLYNXAqEs8eXeerCWCTjjezxj3FRM88Yvs9jn
-----END CERTIFICATE REQUEST-----

Certificate Purpose
client

Duration in days
365

Issue Certificate

Figure 25. Upload Externally Generated CSR

- **Certificate Purpose:** client

NOTE: After issuing the certificate, you can download and save it to your system. It will be the most recent certificate listed under certificates issued by your local CA.

- To upload the signed certificate, go to the SEKM Certificate section and click **Upload Signed CSR**.

Download the server CA from CipherTrust Manager and upload to iDRAC

- Click **CA** on the CipherTrust Manager UI.

THALES CipherTrust Manager			
Products	External Certificate Authorities		
Access Management	Subject	Serial #	Activation
Keys			Expiration
Data Protection	Upload External Certificate		
CA	Local Certificate Authorities		
Alarms	Subject	Serial #	Activation
Records	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA	113498589839509946571059955900228142124	5 days ago
Admin Settings			in 10 years

Figure 26. Certificate authorities

- Click the ellipses symbol (...) in the right corner, download it, and save it to your system.
- Go to the KMS CA Certificate section and click **Upload KMS CA Certificate**.

The screenshot shows the 'Configuration Secure Enterprise Key Manager (SEKM)' window. On the left is a sidebar with navigation options: 'SEKM Rekey', 'SEKM Configuration', 'SEKM Certificate', 'KMS CA Certificate Upload' (highlighted), and 'Test Network Connection'. The main area displays a table of certificate details and a two-step process.

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 7 20:52:08 2021 GMT	Valid To	Nov 5 20:52:08 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.

[Upload KMS CA Certificate](#)

Step 4 of 5

[Cancel](#) [Back](#) [Next](#) [Finish](#)

Figure 27. KMS CA certificate upload

A message indicates that the upload operation has succeeded.

4. Go to **Test Network Connection** and verify that the connection is successful.
5. Click **Finish** to go to the Job Queue page and ensure that the job ID is marked successfully completed.

The screenshot shows the 'Job Queue' page with a 'Delete' button and a table of jobs.

ID	Job	Status
<input type="checkbox"/> RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
<input type="checkbox"/> RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
<input type="checkbox"/> RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
<input type="checkbox"/> JID_925070986474	SEKM Status Change	Completed (100%)

Figure 28. Job queue

iDRAC SEKM configuration with CipherTrust Manager is complete.

Viewing iDRAC key ID on CipherTrust Manager

You will not see a key generated for your iDRAC until you enable SEKM on a supported storage device. For information about how to enable SEKM on supported storage device, see the related section for your storage device.

THALES CipherTrust Manager

Products

Access Management

Keys

CA

Alarms

Records

Admin Settings

Keys

Name Supports wildcards: '*', '?'

Filters Basic Raw

Types Size Status

Latest Version Only

Key Name	Version	Owner
ks-a1f21db64d4347838768fc285a94185a57c31bc6850...	0	local X004_R840
ks-7f59ea6bc0384aebddf568301c1e00821af969a26dd...	0	local X004_R840

Figure 29. Keys

IBM Secure Guardium Key Lifecycle Manager

Topics:

- IBM Secure Guardium Key Lifecycle Manager (SGKLM) prerequisites
- Set up SEKM on IBM SGKLM
- Generate CSR for Server Certificate
- Sign CSR with external CA
- Upload signed CSR to IBM SGKLM
- Set up SEKM on iDRAC
- Configure SEKM using the iDRAC GUI
- Get the CSR file signed by an external CA
- Register Client on IBM SGKLM
- Upload the signed CSR for iDRAC to IBM SGKLM
- Import external CA into IBM SGKLM
- Download the external CA and upload to iDRAC
- Viewing iDRAC key ID on IBM SGKLM
- Audit and debug on IBM SGKLM

IBM Secure Guardium Key Lifecycle Manager (SGKLM) prerequisites

Before you set up iDRAC SEKM support, you must fulfill the following prerequisites:

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 that supports SEKM

IBM SGKLM 4.1 Prerequisites

- Access to a valid external Certificate Authority to sign the server certificate.
- Register a new client that represents iDRAC on the CLIENTS page in the KMS.

Set up SEKM on IBM SGKLM

The following sections describe the IBM SGKLM features that are supported by iDRAC. For information about all other features, see the Product Overview documentation available on the [IBM support site](#).

Generate CSR for Server Certificate

1. Log in to IBM SGKLM.
2. Go to **Advanced Configuration > Server Certificates**.

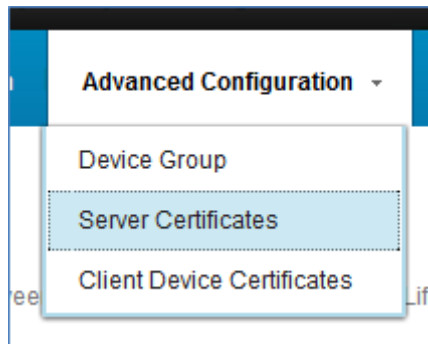


Figure 30. Advanced configuration dropdown menu

3. Click the **Add** icon and select **Request Certificate from a third-party provider**.

Figure 31. Add TLS/KMIP certificate

NOTE: It is mandatory to enter the KMS server IP address or hostname in the **Certificate description** field.

4. After entering or selecting all necessary information, click **Add Certificate**.

Figure 32. Add certificate

A CSR file is generated in the following location where IBM SGKLM is installed:

- **Windows:** C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data
- **Linux:** /opt/IBM/WebSphere/Liberty/products/sklm/data

This CSR can also be downloaded from the **Advanced Configuration > Server Certificates** page. The last column provides an option to download.

Sign CSR with external CA

1. Copy the CSR content and get it signed by an external Certificate Authority (CA).

NOTE: This signed CSR is for the server certificate on the KMS.

2. Copy the signed CSR file to the same location where IBM SGKLM is installed:
 - **Windows:** C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data
 - **Linux:** /opt/IBM/WebSphere/Liberty/products/sklm/data
3. The signed CSR can also be uploaded from the GUI. For more information, see [Upload signed CSR to IBM SGKLM](#).

Upload signed CSR to IBM SGKLM

1. Go to the Welcome page.
2. Click **Third-party certificates pending import** under **Key Groups and Certificates**.

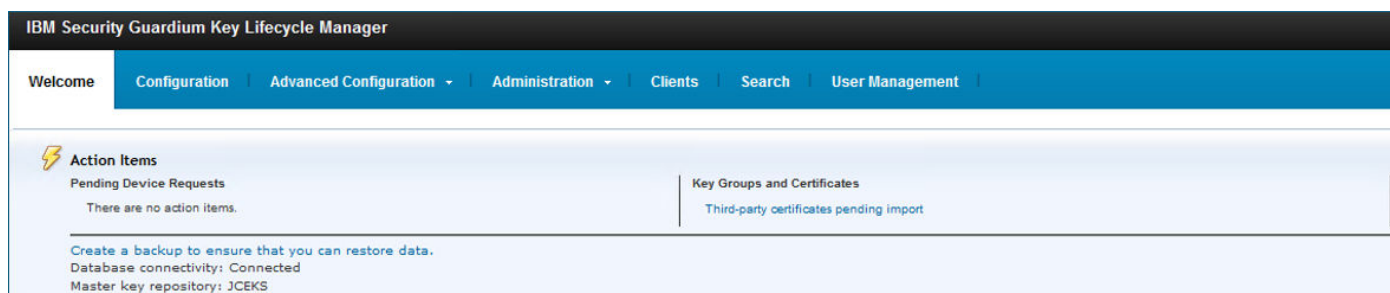


Figure 33. Welcome page

3. Double-click the certificate that you generate from the list of pending certificates.

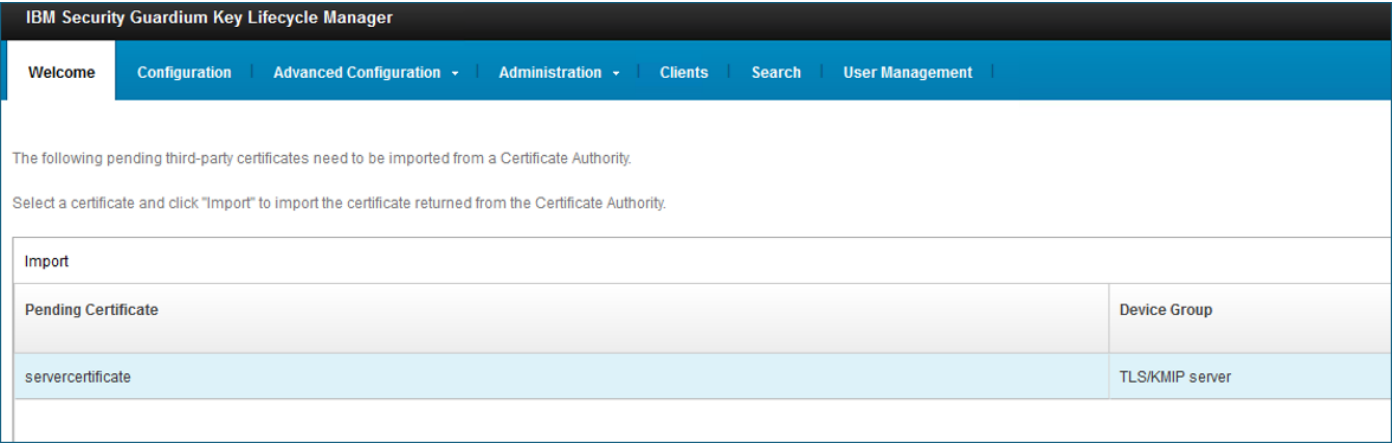


Figure 34. Pending certificates

4. Browse and search for the signed CSR from the previous step.

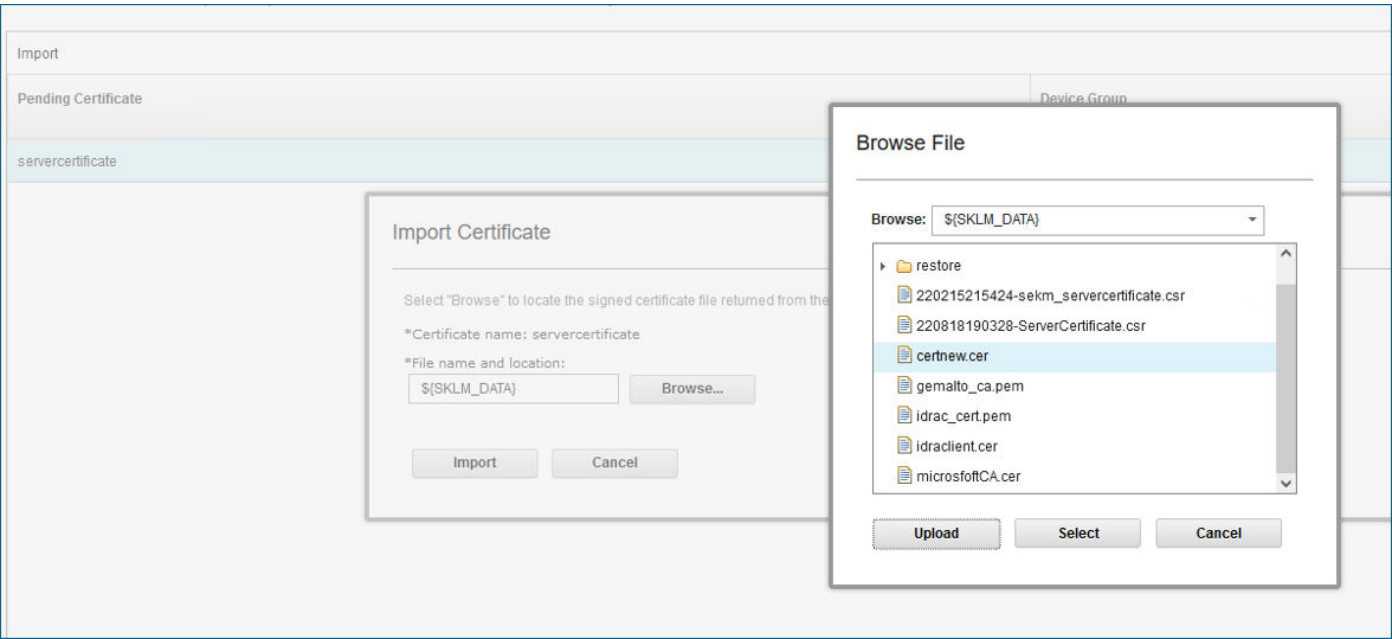


Figure 35. Browse to the signed CSR

5. If the file is not present in the list, then use the Upload button to upload the signed CSR from the previous step, then select the file.
6. Click **Import**.
7. Go to **Advanced Configuration > Server Certificates** and verify that the box in the **Status** column has changed to green.

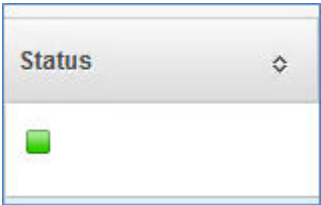


Figure 36. Valid status

8. On the **Server Certificates** page, double-click the certificate and select the **Current certificate in use** check box.
9. Click **Modify Certificate**.

The screenshot displays the 'Modify TLS/KMIP Certificate' window in the IBM Security Guardium Key Lifecycle Manager. The left-hand navigation pane shows the 'Certificates' section with a list containing 'sekm_servercertificate' and 'servercertificate', the latter being selected. Below the list, it indicates 'Total: 2 Selected: 1' and provides a 'Return home' link. The main panel contains several input fields: '*Certificate label in keystore:' with the value 'servercertificate', '*Certificate description (common name):' with '100.64.41.42', '*Validity period of certificate (in days):' with '1096', and '*Algorithm:' with 'RSA'. A checkbox labeled 'Current certificate in use' is checked. An expandable section titled 'Optional Certificate Parameters' is visible below the main fields. At the bottom of the dialog are two buttons: 'Modify Certificate' and 'Cancel'.

Figure 37. Modify certificate

Set up SEKM on iDRAC

See [Set up SEKM on iDRAC](#).

Configure SEKM using the iDRAC GUI

See [Configure SEKM using the iDRAC GUI](#).

Get the CSR file signed by an external CA

Get the CSR signed by your supported Certificate Authority.

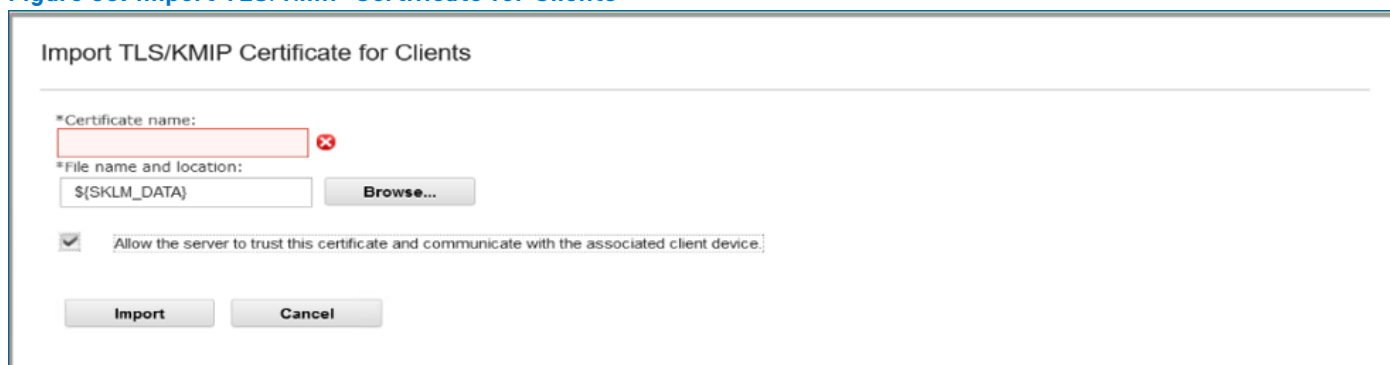
Register Client on IBM SGKLM

1. Copy the iDRAC Client certificate and the corresponding external CA used to sign the iDRAC CSR to the following location where IBM SGKLM is installed.
 - **Windows:** C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data
 - **Linux:** /opt/IBM/WebSphere/Liberty/products/sklm/data
2. Alternatively, the above certificates can be uploaded from the IBM SGKLM GUI. Further details can be found in the following sections.

Upload the signed CSR for iDRAC to IBM SGKLM

1. In the IBM SGKLM, navigate to **Advanced Configuration > Client Device Certificates**.
2. Click **Import**.
3. Browse through the list of files and upload the signed SEKM SSL certificate.
4. Select the uploaded certificate.
5. Select the **Allow the server to trust this certificate** check box, then click **Import**.

Figure 38. Import TLS/KMIP Certificate for Clients



NOTE: The certificate name should be the same as the common name used while generating iDRAC CSR.

Import external CA into IBM SGKLM

1. Go to **Configuration > Truststore** and click **Add**.
2. Browse through the list of files and upload the external CA used to sign the iDRAC CSR.
3. Select the uploaded certificate and click **Add Certificate**.

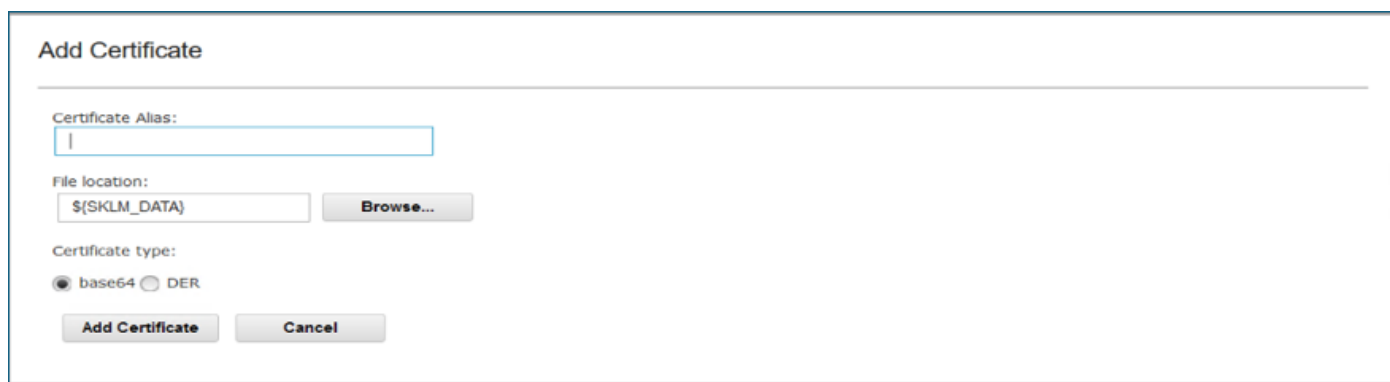


Figure 39. Add Certificate

Download the external CA and upload to iDRAC

- 1. Download your external CA, then go to the KMS CA Certificate section in iDRAC.
- 2. Click **Upload KMS CA Certificate**.

Figure 40. KMS CA Certificate

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

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 7 20:52:08 2021 GMT	Valid To	Nov 5 20:52:08 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.

Upload KMS CA Certificate

Step 4 of 5

Cancel

Back

Next

Finish

Upload

A message displays, indicating that the upload is successful.

- 3. Go to **Test Network Connection** and verify that the connection is successful.
- 4. Click **Finish** to go to the **Job Queue** page and ensure that the job ID is marked "Completed."

Job Queue			
<div>Delete</div>			
<input type="checkbox"/>	ID <input type="text"/>	Job	Status
<input checked="" type="checkbox"/>	RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
<input checked="" type="checkbox"/>	RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
<input checked="" type="checkbox"/>	RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
<input checked="" type="checkbox"/>	JID_925070986474	SEKM Status Change	Completed (100%)

Figure 41. Job Queue

iDRAC SEKM configuration with IBM SGKLM is now complete.

Viewing iDRAC key ID on IBM SGKLM

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

- 1. Go to the **Clients** tab.
- 2. Double-click the required iDRAC client from the list.
- 3. Select the **Add Objects** tab.
- 4. Double-click **SYMMETRIC_KEY** under **Object Type**.

Figure 42. Modify Client

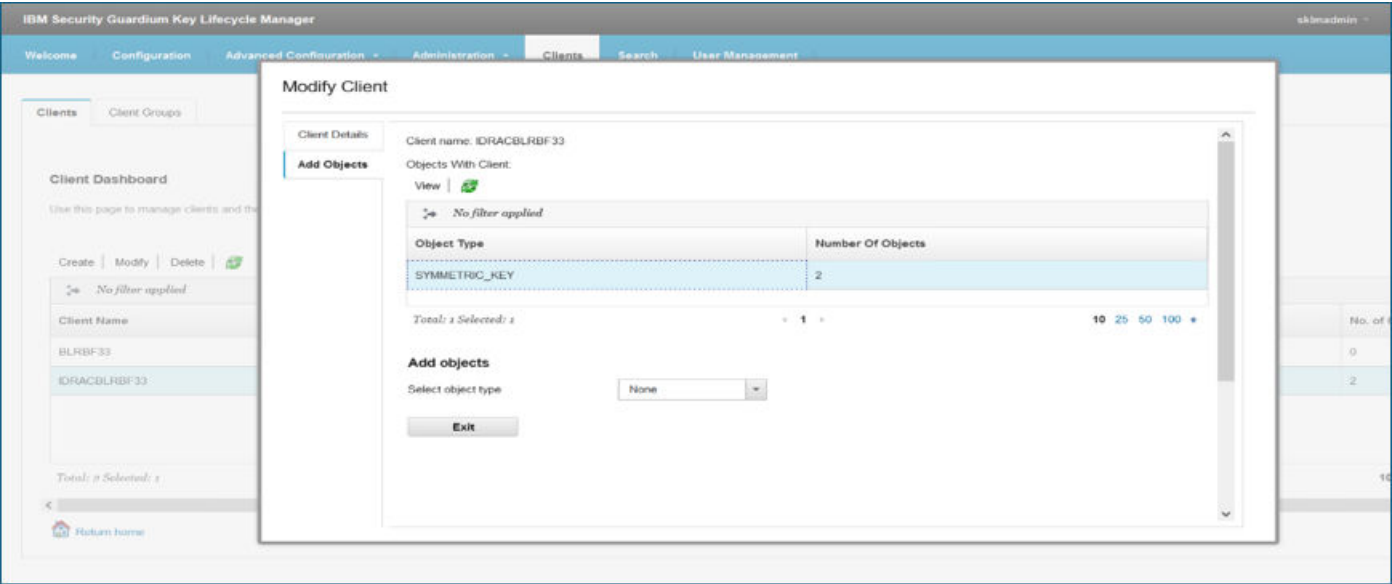
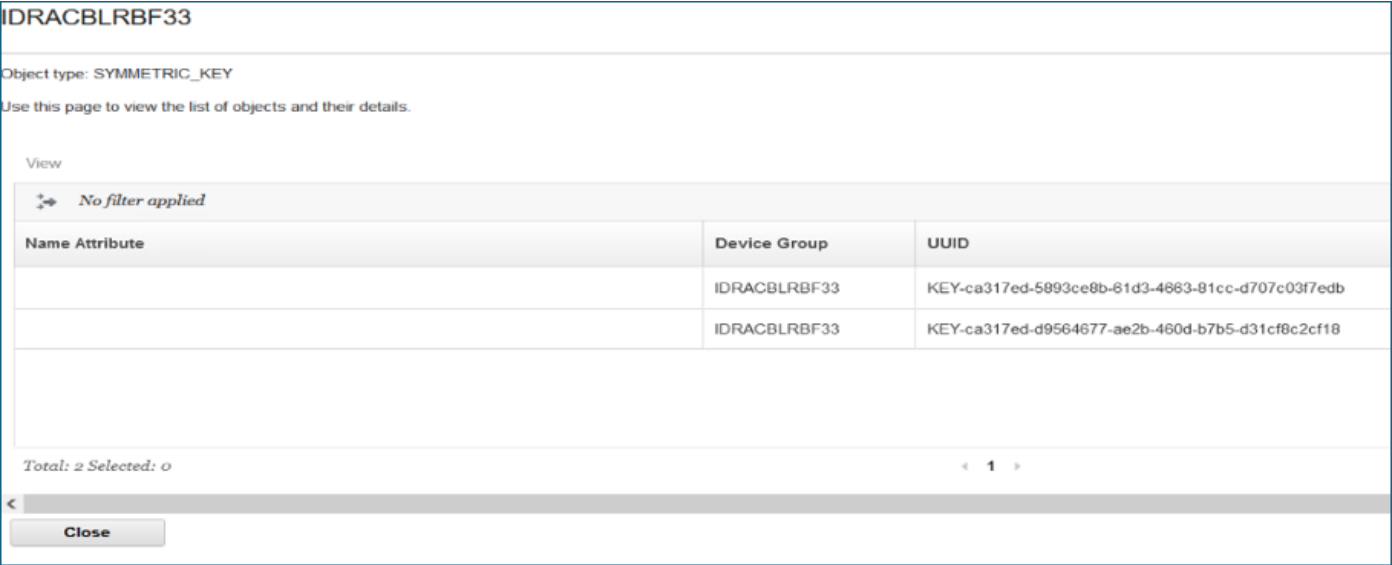


Figure 43. Detailed Key ID information



- 5. Double-click the required key ID for a detailed view.

Audit and debug on IBM SGKLM

- 1. Go to **Configuration > Audit and Debug**.
- 2. Select the **Enable Debug** check box to log further activities.

Figure 44. Audit and Debug

IBM Security Guardium Key Lifecycle Manager

Welcome | Configuration | Advanced Configuration | Administration | Clients | Search | User Management

TLS/KMIP

Audit and Debug

Key Serving Ports

Key Serving Parameters

Truststore

[Audit](#)

Use this page to specify your audit and debug settings. Before you redirect the audit information to the syslog server over TLS, en...

Audit level:

☐ Low - Failure outcomes for all event types

☐ Medium - Failure outcomes for all event types, and success outcomes for runtime, authorization, key management, and res

☒ High - Failure and success outcomes for all event types

☐ Use syslog format

Syslog server host:

Syslog server port:

☐ Use TLS

[Debug](#)

Apply the Debug settings: Enabling Debug will create debug log in logs folder.

☒ **Enable Debug**

[Download log files](#)

3. Log files can be downloaded from the **Download log files** link. Alternatively, log files can be found at the following locations where IBM SGKLM is installed.
 - **Windows:** C:\Program Files\IBM\WebSphere\AppServer\products\sklm\logs
 - **Linux:** /opt/IBM/WebSphere/Liberty/products/sklm/logs

Topics:

- [Utimaco prerequisites](#)
- [Set up SEKM on Utimaco](#)
- [Set up SEKM on iDRAC](#)
- [Configure SEKM using the iDRAC GUI](#)
- [Get the CSR file signed on Utimaco](#)
- [Download the server CA file from Utimaco and upload to iDRAC](#)
- [View iDRAC key ID on Utimaco](#)

Utimaco prerequisites

Before you set up iDRAC SEKM support, you must fulfill the following prerequisites:

PowerEdge Server prerequisites:

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

Key Management Server (KMS) prerequisites:

- Set up a valid CA to sign the iDRAC CSR
- A user account that represents the iDRAC on the KMS
- Authentication settings on the KMIP Service of the KMS

Set up SEKM on Utimaco

This section describes the Utimaco features that are supported by iDRAC.

SSL certificate

When creating an SSL certificate request, you must include the IP address of the KMS in the **Subject Alternative Name** field.

The IP address must be entered in the format that is indicated in the sample screenshot here:

Create Certificate

Certificate Name:	ESKMServerCert
Common Name:	ESKM
Organization Name:	Organization
Organizational Unit Name:	Information Security
Locality Name:	Campbell
State or Province Name:	CA
Country Name:	US
Email Address:	infosec@organization.com
Subject Alternative Name:	IP:XXX.XXX.XXX.XXX
Algorithm:	RSA-2048 ▼
Creation Type:	<input type="radio"/> Certificate Request - to be signed by external CA <input checked="" type="radio"/> Certificate Signed by Local CA
Local CA:	ESKMCA (maximum 3598 days) ▼
Certificate Purpose:	Server ▼

Create

Figure 45. Create Certificate

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 that are created by one iDRAC from being accessed by another. If the keys must be shared between iDRACs, it is recommended to create a group and add all iDRAC usernames that must share keys to that group.

Authentication

The authentication options that are supported by the Utimaco KMS are shown in this sample screenshot:

KMIP Server Configuration

KMIP Server Settings

IP:	100.65.89.6
Port:	5696
Server Certificate:	KMIPServerCertificate
Local CA Certificate for Certify/Re-certify:	KMIPCertificateAuthority
Connection Timeout (sec):	360
Default number of items returned in Locate:	100
Maximum number of items returned in Locate:	1000

Edit

KMIP Server Authentication Settings

Client Certificate Authentication:	enable
Trusted CA List Profile:	Default

Edit

Figure 46. KMIP Server Configuration settings

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 the Client Certificate Authentication 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](#).

Username field in client certificate

It is recommended to set the username field 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, the SEKM stops functioning until the SSL certificates are set up again. If this option is enabled, ensure that the same option is also enabled on iDRAC, as explained later in [Set up SEKM on iDRAC](#).

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 be installed first, and then the iDRAC firmware be updated to a version that supports SEKM. This is because an iDRAC firmware update is always required after the SEKM license is installed, regardless of whether the existing firmware version supports SEKM or not. The existing interface methods for installing the 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, 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

While many of the CSR properties are standard and straightforward, here are a few important guidelines to keep in mind:

If the **Username Field in Client Certificate** option the KMS is enabled, ensure that the iDRAC account username on the KMS is entered in the correct field (CN, OU, or KMS user ID) that matches the value that is selected in the KMS.

If the **Require Client Certificate to Contain Source IP** field is enabled on the KMS, enable the "iDRAC IP address in CSR" IP address during the CSR generation.

Configure SEKM using the iDRAC GUI

1. Start iDRAC using any supported browser.
2. Click **iDRAC Settings > Services**.
3. Expand the **iDRAC Key Management** menu and select **SEKM** for Key Management Service.
4. Go to **SEKM Configuration**.
5. Enter the KMS IP address and iDRAC KMS user ID and password fields if applicable.

Configuration Secure Enterprise Key Manager (SEKM)

?

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

KMS (IP Address or FQDN)*

Port Number*

5696

Redundant KMS Information

Port Number

5696

Redundant KMS 1 (IP Address or FQDN)

+ Add Redundant KMS

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.

Step 2 of 5

Cancel

Back

Next

Finish

Figure 47. SEKM configuration

NOTE: The user ID and password fields must match the user that you created on Utimaco in the above steps.

6. Click **Next**.
7. Click **Generate CSR**.

44 Utimaco

Configuration Secure Enterprise Key Manager (SEKM)

?

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1

Generate a Certificate Signing Request (CSR)

Generate CSR

Download 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.

Upload Signed CSR

i

Step 3 of 5

Cancel

Back

Next

Finish

Figure 48. SEKM certificate

NOTE: The **Download CSR** option is available after generating a CSR.

8. Enter the certificate information in the **Generated Certificate Signing Requests (CSR)** dialog box.

Utimaco 45

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)*

idrac-HC02502

Country Code (CC)

United States ▼

Locality (L)*

Round Rock

Organization Name (O)*

Dell

Organization Unit (OU)*

ISG

State*

Texas

Email

Subject Alternative Names

i

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-HC02502

iDRAC IP Address in CSR

☒ Include

Cancel

Generate

Figure 49. Generate CSR

NOTE: It is recommended to include both user ID and iDRAC IP address options in the CSR field.

9. Click **Generate** to generate the CSR file.
10. Save it to your system.

Get the CSR file signed on Utimaco

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVUZShhcZETMBEG
A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbnBFTUMxDTALBgNVBAsMBFRl
```

```
c3QxGTAXBgNVBAMMEGlkcMfjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWd3Rlc3RlcBkZwxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOLJcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjQmGmRhIdnINI6Ya+lWVi/OyLyeJ711SKnu4UpUGF1jcpYubDSpt11ZZ5bw3LotBklrbLqlHpY1c9kGgnjaeLPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFACqp0z76vqTYAVn73oyinMW8p5hchyoThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCCGCSqGSIb3DQEJJDjEaMBGwCQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7NaV3t5LGma/I3sPYl4baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aHlcTuBhpm5XiP/IUmvGf1AEplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3ykjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp36A=
-----END CERTIFICATE REQUEST-----
```

1. Click **Security > Local CAs.**
2. Click **Sign Request.**

Home
Security
Device

Keys & KMIP Objects

- Keys
- KMIP Objects
- Authorization Policies

Users & Groups

- Local Users & Groups
- LDAP

Certificates & CAs

- Certificates
- Trusted CA Lists
- Local CAs
- Known CAs

Advanced Security

- High Security
- SSL Options
- SSH Options
- FIPS Status Server

Security / Local CAs

Certificate and CA Configuration

Local Certificate Authority List

CA Name	CA Information
<input checked="" type="radio"/> ESKMCA2	Common: ESKMLocalCA Issuer: Organization Expires: Jul 2 11:22:24 2032 GMT

Edit
Delete
Download
Properties
Sign Request
Show Signed Certs

Create Local Certificate Authority

Certificate Authority Name:

ESKMCA

Common Name:

ESKMLocalCA

Organization Name:

Organization

Organizational Unit Name:

Information Security

Locality Name:

Campbell

State or Province Name:

CA

Country Name:

US

Email Address:

infosec@organization.com

Algorithm:

RSA-2048

☒ Self-signed Root CA

CA Certificate Duration (days):

3650

Maximum User Certificate Duration (days):

3650

☐ Intermediate CA Request

Create

Figure 50. Sign request

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

Home

Security

Device

Keys & KMIP Objects

Keys

KMIP Objects

Authorization Policies

Users & Groups

Local Users & Groups

LDAP

Certificates & CAs

Certificates

Trusted CA Lists

Local CAs

Known CAs

Advanced Security

High Security

SSL Options

SSH Options

FIPS Status Server

Security / Local CAs

Certificate and CA Configuration

Sign Certificate Request

Sign with Certificate Authority:

ESKMCA2 (maximum 3613 days)

Certificate Purpose:

Server

Client

Server and Client

Certificate Duration (days):

3613

Certificate Request:

5VWdVJ+m2ILLNyKC+9MCAwEAAApMCCGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7NaV3t5LGma/I3sPY14baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYYldH3+ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF7840sVaJiyAXFhcaB33Sdtc4Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvGf1AEplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3ykiw+SxEos6JnYpT9yxJSCj2Rmddb56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD2lp36A=

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

Sign Request

Back

Figure 51. Sign certificate request with Client purpose

- After the request is signed, click **Download** to save the signed CSR file to your system.
- To upload the file that is signed on Gemalto or Utimaco, access the iDRAC GUI, go to the SEKM Certificate page, and click **Upload Signed CSR**. A message is displayed to indicate the successful upload.

NOTE: You must upload this signed certificate as the KMIP client certificate for your assigned user on Utimaco.

Download the server CA file from Utimaco and upload to iDRAC

- On the Utimaco GUI, click **Security Tab > Local CAs**. Select the server CA that you are using and click **Download**. The file is saved to your local system.

Enterprise Secure Key Manager

[Home](#)
[Security](#)
[Device](#)

Keys & KMIP Objects

- Keys
- KMIP Objects
- Authorization Policies

Users & Groups

- Local Users & Groups
- LDAP

Certificates & CAs

- Certificates
- Trusted CA Lists

[Security](#) / [Local CAs](#)

Certificate and CA Configuration

Local Certificate Authority List

CA Name	CA Information
<input checked="" type="radio"/> ESKMCA2	Common: ESKMLocalCA Issuer: Organization Expires: Jul 2 11:22:24 2032 GMT

[Edit](#)
[Delete](#)
[Download](#)
[Properties](#)
[Sign Request](#)
[Show Signed Certs](#)

Figure 52. Download local CA

- Go to the KMS CA Certificate section and click **Upload KMS CA Certificate**.

Configuration Secure Enterprise Key Manager (SEKM)

SEKM Rekey
SEKM Configuration
SEKM Certificate
KMS CA Certificate Upload
Test Network Connection

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 7 20:52:08 2021 GMT	Valid To	Nov 5 20:52:08 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.

Upload KMS CA Certificate

Step 4 of 5

[Cancel](#)
[Back](#)
[Next](#)
[Finish](#)

Figure 53. Upload KMS CA certificate

A message is displayed to indicate that the upload was successful.

- Click **Finish** to go to the **Job Queue** page and ensure that the job ID is marked "Completed."

Job Queue				
<div> Delete </div>				
<input type="checkbox"/>	ID	Job		Status
	<input type="checkbox"/> RID_919130367938	Reboot: Power cycle		Reboot Completed (100%)
	<input type="checkbox"/> RID_919007247652	Reboot: Power cycle		Reboot Completed (100%)
	<input type="checkbox"/> RID_919000641413	Reboot: Power cycle		Reboot Completed (100%)
	<input type="checkbox"/> JID_925070986474	SEKM Status Change		Completed (100%)

Figure 54. Job Queue

The iDRAC SEKM configuration with Utimaco is complete.

View iDRAC key ID on Utimaco

1. Log in to the Utimaco GUI.
2. Click **Security > KMIP Objects**.

Enterprise Secure Key Manager

utimaco®

Home > Security > Device

Keys & KMIP Objects

Keys

KMIP Objects

Authorization Policies

Users & Groups

Local Users & Groups

LDAP

Certificates & CAs

Certificates

Trusted CA Lists

Local CAs

Known CAs

Security / KMIP Objects

KMIP Object Configuration

KMIP Objects

Query: [All KMIP Keys]

Run Query

Items per page: 10

Submit

UUID	Object Name	Owner	Object Type	State	Creation Date
<input checked="" type="radio"/> 32d76a3c-a075-4073-8dc3-bec7cb95fd67	-	idrac-F20Q643	SymmetricKey	Active	2022-07-20 01:16:23

Delete

Properties

Purge Destroyed Objects

1 - 1 of 1

Figure 55. KMIP object configuration

Utimaco

51


Fortanix Data Security Manager

Topics:

- [Fortanix prerequisites](#)
- [Set up SEKM on Fortanix](#)
- [Set up SEKM on iDRAC](#)
- [Configure SEKM using the iDRAC UI](#)
- [Get the CSR file signed](#)
- [Download the CA and upload it to iDRAC](#)

Fortanix prerequisites

The following sections describe the Fortanix features that are supported by iDRAC. For information about deployment and all other features, see the Fortanix guide.


 **NOTE:** Fortanix DSM is deployed with a server certificate that is signed by an internal Certificate Authority. The server certificate must contain the IP address of the KMS in the Subject Alternative Name (SAN) field.

Set up SEKM on Fortanix

Fortanix DSM supports KMIP client authentication using the Apps feature.

1. On the Fortanix DSM user interface, log in and go to the **Apps** tab on **Fortanix DSM**.
2. Click **Create New App**.
3. Enter an **App Name**, select **KMIP Interface**, and select **API Key** for **Authentication Method**.
4. Assign the app to a group and click **Save**.

Once the app is created, select the detailed view of the app and note the app's UUID and password.

 **NOTE:** If you select **Client Certificate** as the Authentication Method, then the KMS username and password fields on iDRAC are optional.

The UUID and password values on Fortanix are the KMS username and password credentials on iDRAC.

 **NOTE:** When generating the iDRAC CSR, the UUID must match the Common Name (CN) field.

Set up SEKM on iDRAC

Licensing and firmware update

SEKM is a licensed feature that requires the iDRAC Enterprise license as a pre-requisite. To avoid an additional iDRAC firmware update, install the SEKM license first, and then update the iDRAC firmware to a version that supports SEKM. This is necessary because an iDRAC firmware update is always required after the SEKM license is installed, regardless of whether the existing firmware version supports SEKM. You can use the existing interface methods for installing the license and firmware updates for SEKM.

Set up SSL certificate

The SEKM solution mandates two-way authentication between the iDRAC and the KMS. For iDRAC authentication, you must generate a CSR on the iDRAC, get it signed by a trusted CA on the KMS, and upload the signed certificate to iDRAC. For KMS authentication, you must upload the KMS CA certificate to the iDRAC.

Configure SEKM using the iDRAC UI

- 1. Start iDRAC using any supported browser.
- 2. Click **iDRAC Settings > Services.**
- 3. Expand the **iDRAC Key Management** menu and select **SEKM** for **Key Management Service.**
- 4. Go to **SEKM Configuration.**
- 5. Enter the KMS IP address and iDRAC KMS user ID and password fields if applicable.

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

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)

+ Add Redundant KMS

iDRAC Account on KMS

Setup your iDRAC account on the Key Management Server. Provide information a

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.

Figure 56. SEKM configuration

NOTE: The user ID and password fields must match the Fortanix-generated UUID and password if applicable.

- 6. Click **Next.**
- 7. Click **Generate CSR.**

Fortanix Data Security Manager 53

Configuration Secure Enterprise Key Manager (SEKM)

?

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1

Generate a Certificate Signing Request (CSR)

Generate CSR

Download 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.

Upload Signed CSR

i

Step 3 of 5

Cancel

Back

Next

Finish

Figure 57. SEKM certificate

NOTE: The Download CSR option is available after generating a CSR.

- In the **Generate Certificate Signing Requests (CSR)** dialog box, enter the client certificate information.
- Click **Generate**. The CSR file generates.
- Save the file to your system.

Get the CSR file signed

Using OpenSSL, get the CSR signed by Fortanix's internal Certificate Authority.

Download the CA and upload it to iDRAC

- Click the padlock icon in your web browser to view and export the Certificate Authority file from Fortanix.
- Upload the same certificate to iDRAC as the KMS server CA.
- Go to **Text Network Connection** and verify that the connection is successful.

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

Test Network Connection

Perform a test on the network connection for the configured SEKM settings

Test Network Connection

Step 5 of 5

Cancel

Back

Next

Finish

Figure 58. Test network connection

- Click **Finish** to go to the **Job Queue** page and ensure that the job ID is marked "Complete."

Job Queue

 Delete






<input type="checkbox"/>	ID 	Job	Status
	<input type="checkbox"/> RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
	<input type="checkbox"/> RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
	<input type="checkbox"/> RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
	<input type="checkbox"/> JID_925070986474	SEKM Status Change	Completed (100%)

Figure 59. Job queue

iDRAC SEKM configuration with SEKM is now complete.

Entrust KeyControl

Topics:


- [Entrust KeyControl prerequisites](#)
- [Set up SEKM on Entrust](#)
- [Set up SEKM on iDRAC](#)
- [Configure SEKM using the iDRAC GUI](#)
- [Get the CSR file signed](#)
- [Download the CA and upload to iDRAC](#)

Entrust KeyControl prerequisites

The following sections describe the Entrust KeyControl features that are supported by iDRAC. For information about deployment and all other features, see the [Entrust KeyControl guide](#).

Set up SEKM on Entrust

1. Log in to Vault Management and click **Create Management**.
2. Select **KMIP** for vault type, then provide a name for the vault.
3. Once your vault is created, you are prompted with a URL to your newly created vault along with the admin credentials.

 **NOTE:** You will be prompted to change the password after the first login.

Set up SEKM on iDRAC

Licensing and firmware update

SEKM is a licensed feature that requires the iDRAC Enterprise license as a prerequisite. To avoid an additional iDRAC firmware update, install the SEKM license first, then update the iDRAC firmware to a version that supports SEKM. This is necessary because an iDRAC firmware update is always required after the SEKM license is installed, regardless of whether the existing firmware version supports SEKM. You can use the existing interface methods for installing the license and firmware updates for SEKM.

Set up SSL certificate

The SEKM solution mandates two-way authentication between the iDRAC and the KMS. For iDRAC authentication, you must generate a CSR on the iDRAC, get it signed by a trusted CA on the KMS, and upload the signed certificate to iDRAC. For KMS authentication, you must upload the KMS CA certificate to the iDRAC.


Configure SEKM using the iDRAC GUI

1. Start iDRAC using any supported browser.
2. Click **iDRAC Settings > Services**.
3. Expand the iDRAC Key Management menu and select **SEKM for Key Management Service**.
4. Go to **SEKM Configuration**.
5. Enter the KMS IP address.

The screenshot shows a web interface for SEKM Configuration. On the left is a sidebar with three items: 'SEKM Configuration' (highlighted in blue), 'SEKM Certificate', 'KMS CA Certificate Upload', and 'Test Network Connection'. The main content area is titled 'KMS Information' and contains the following sections:

- KMS Information**: Subtitle 'Set-up upstream communications with the Key Management Server.' It includes a text input for 'KMS (IP Address or FQDN)*' and a text input for 'Port Number*' with the value '5696' entered.
- Redundant KMS Information**: It includes a text input for 'Port Number' with the value '5696' entered and a text input for 'Redundant KMS 1 (IP Address or FQDN)'. Below these is a blue button with a plus icon and the text '+ Add Redundant KMS'.
- iDRAC Account on KMS**: Subtitle 'Setup your iDRAC account on the Key Management Server. Provide information a' (truncated). Below this is a text input for 'User ID' and a text input for 'Password'. A small note below the password field reads: 'Provide password if Password based authentication has been enabled on the Key Management Server.'

Figure 60. KMS information

 **NOTE:** Entrust KeyControl does not support KMS User ID and Password fields on iDRAC.

6. Click **Next**.
7. Click **Generate CSR**.

Configuration Secure Enterprise Key Manager (SEKM)

?

SEKM Rekey

SEKM Configuration

SEKM Certificate

KMS CA Certificate Upload

Test Network Connection

SEKM Certificate

Generate and Sign CSR by the Key Management Server Certifying Authority

STEP 1

Generate a Certificate Signing Request (CSR)

Generate CSR

Download 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.

Upload Signed CSR

i

Step 3 of 5

Cancel

Back

Next

Finish

Figure 61. SEKM Certificate

NOTE: The **Download CSR** option is available after generating a CSR.

8. In the **Generate Certificate Signing Requests (CSR)** dialog box, enter the client certificate information.
9. Click **Generate**. The CSR file generates.
10. Save the file to your system.

Get the CSR file signed

1. Log into your newly created vault on Entrust, then select **Security > Client Certificates**.
2. Click the plus icon to upload a CSR from iDRAC.

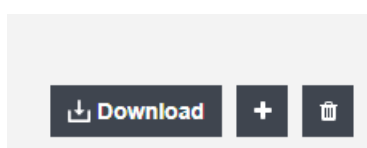


Figure 62. Plus icon

- 3. The client certificate will be signed by Entrust’s internal Certificate Authority and is available for download after creating the certificate.
- 4. Download the certificate, which is a zip file containing the signed client certificate and the certificate authority.
- 5. Upload the signed client certificate to iDRAC.

Download the CA and upload to iDRAC

- 1. Upload the certificate authority from the previous step as the KMS server CA.
- 2. Go to **Test Network Connection** and verify that the connection is successful.

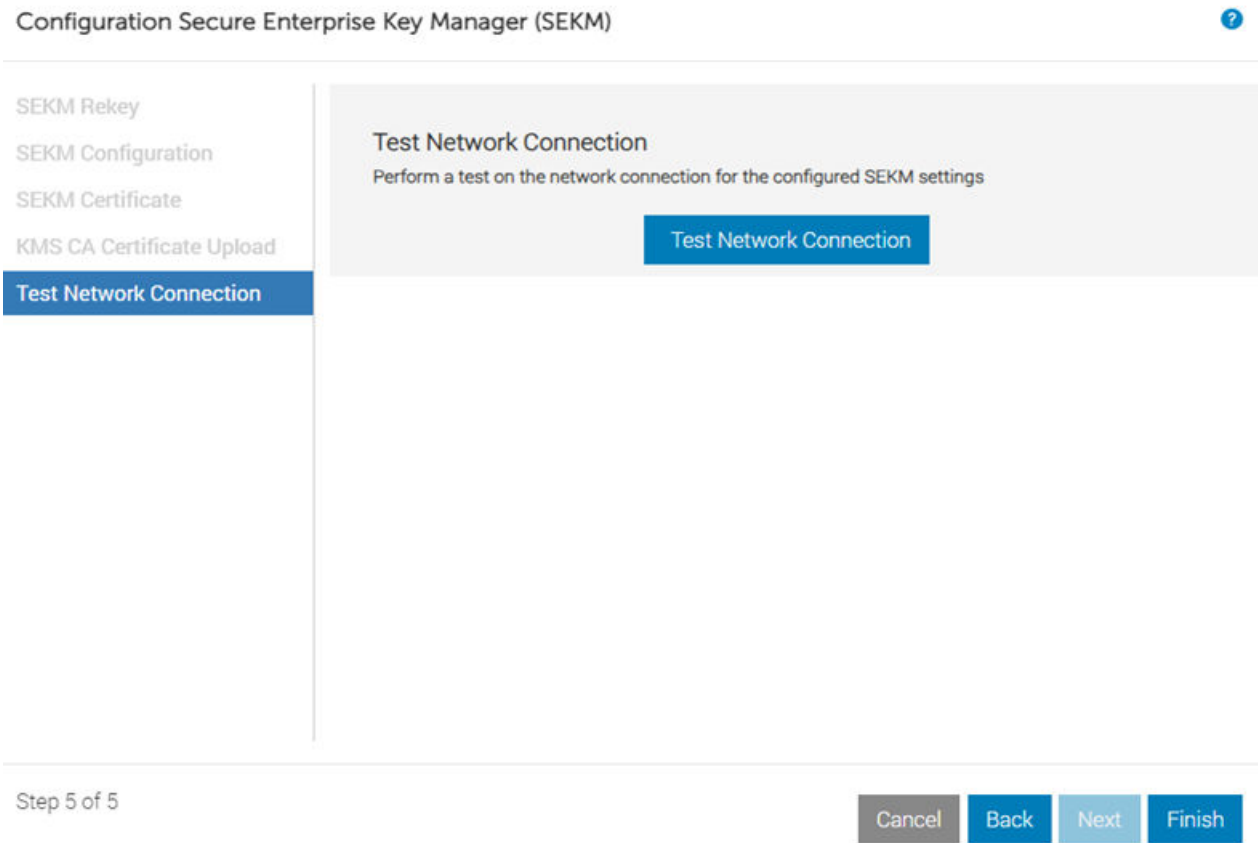


Figure 63. Test Network Connection

- 3. Click **Finish** to go to the **Job Queue** page and ensure that the job ID is marked "Complete."

Job Queue

Delete

<input type="checkbox"/>	ID ▼	Job	Status
+ <input type="checkbox"/>	RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
+ <input type="checkbox"/>	RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
+ <input type="checkbox"/>	RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
+ <input type="checkbox"/>	JID_925070986474	SEKM Status Change	Completed (100%)

Figure 64. Job Queue

4. The iDRAC SEKM configuration with Entrust KeyControl is now complete.

Configure SEKM on iDRAC

The sections above demonstrate how to configure SEKM on iDRAC using the UI. This section shows how to configure SEKM using Redfish, RACADM, and Server Configuration Profile (SCP).

Topics:

- [Configure SEKM using Redfish](#)
- [Configure SEKM using RACADM](#)
- [Configure SEKM using Server Configuration Profile](#)

Configure SEKM using Redfish

For more information about Redfish calls, see the [Redfish guide](#).

Set SEKM certificate attributes

Command: PATCH

URI: `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1`

Header: `content-type application/json`

Auth: Basic

Body: `{"Attributes": {"SEKMCert.1.CommonName": "idrac-PTC8502"}}`

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

NOTE: The following fields are optional when generating a CSR: `SEKMCert.1.SubjectAltName`, `SEKMCert.1.UserId`

Generate a CSR

Command: POST

URI: `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DelliDRACCardService/Actions/DelliDRACCardService.GenerateSEKMCSR`

Header: `content-type application/json`

Auth: Basic

Body: `{}`

Take the CSR and get it signed by the Certificate Authority on your supported Key Management Server.

Upload SEKM certificates to iDRAC

Command: POST

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

Header: content-type application/json

Auth: Basic

Body for KMS server certificate: {"CertificateType": "KMS_SERVER_CA", "CertificateFile": "certificate_authority.pem"}

Body for signed SEKM SSL certificate: {"CertificateType": "SEKM_SSL_CERT", "CertificateFile": "signed_certificate.pem"}

Set KMS attributes

Command: PATCH

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Header: content-type application/json

Auth: Basic

Body: {"Attributes": {"KMS.1.PrimaryServerAddress": "192.168.0.120", "KMS.1.iDRACUserName": "idrac-PTC8502", "KMS.1.iDRACPassword": "P@ssw0rd"}}

Set SEKM attributes

Command: PATCH

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Header: content-type application/json

Auth: Basic

Body: {"Attributes": {"SEKM.1.AutoSecure": "Enabled", "SEKM.1.IPAddressInCertificate": "Enabled", "SEKM.1.KMSKeyPurgePolicy": "Keep All Keys", "SEKM.1.KeyCachingPolicy": "No Caching"}}

Enable SEKM


Command: POST

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DelliDRACCardService/Actions/DelliDRACCardService.EnableSEKM

Header: content-type application/json

Auth: Basic

Body: {}

 **NOTE:** In the **Headers** output, the **Location** property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Verify SEKM status

Command: GET

URI: `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1?$select=Attributes/SEKM.1.SEKMStatus`

Auth: `Basic`

Expected attribute if SEKM is enabled: `{SEKM.1.SEKMStatus": "Enabled"}`

Expected attribute if SEKM is disabled: `{SEKM.1.SEKMStatus": "Disabled"}`

Disable SEKM


Command: `POST`

URI: `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DelliDRACCardService/Actions/DelliDRACCardService.DisableSEKM`

Header: `content-type application/json`

Auth: `Basic`

Body: `{}`

 **NOTE:** In the **Headers** output, the **Location** property returns a job ID URI. Run GET on the URI to monitor the job status until it is marked "Complete."

FIPS compliance descriptor


Command: `GET`

URI: `/redfish/v1/Systems/System.Embedded.1/Storage/CPU.1/Drives/Disk.Bay.14:Enclosure.Internal.0-2`

Auth: `Basic`

Body:

```
{ "Oem": {
  "Dell": {
    "FIPS140ComplianceDescriptor": {
      "ComplianceDescriptorType": "FIPS140",
      "ComplianceDescriptorVersion": "2.3",
      "ComplianceRelatedStandard": "FIPS140-3",
      "ComplianceOverallSecurityLevel": "32h",
      "ComplianceHardwareVersion": "SC10",
      "ComplianceDescriptorModuleName": "Micron(R) 7400 SSD
Controller Security Subsystem"
    }
  }
}
```

 **NOTE:** The FIPS compliance descriptor is only available through the Redfish interface.

Configure SEKM using RACADM

For more information about RACADM commands, see the [RACADM guide](#).

Set SEKM certificate attributes

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

2. To set each attribute, run the SET command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --nocertwarn set
idrac.sekmcert.StateName Texas
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
```

Generate a CSR

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sslcsrgen -g -t 3 -f
sekm_csr
CSR generated and downloaded from RAC successfully
```

1. Get the CSR contents signed by a trusted CA on the Key Management Server.
2. Download the signed file, then upload it back to iDRAC.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sslcertupload -t 6 -f
signed_sekm_ssl_cert.pem
```

Certificate successfully uploaded to the RAC.

3. Upload the server CA file to the iDRAC.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sslcertupload -t 7 -f
server_ca_new.pem
```

Certificate successfully uploaded to the RAC.

4. Configure Key Management Server settings on iDRAC.

NOTE: Ensure you have a user on the Key Management Server (KMS) you are using for key exchange with the iDRAC. For the username, ensure that it matches the same value in the CSR certificate property you selected for the KMIP username field in the client certificate authentication settings.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --nocertwarn set
idrac.kms.iDRACPassword Dell123!
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully
```

Enable SEKM

Run the following command to enable SEKM:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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 enables.]
Percent Complete=[100]
-----
```

Verify SEKM status

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get idrac.sekm
[Key=idrac.Embedded.1#SEKM.1]
AutoSecure=Enabled
#iLKMStatus=Disabled
IPAddressInCertificate=Disabled
KeyAlgorithm=AES-256
```

```
#KeyCreationPolicy=Key per iDRAC
#KeyIdentifierN= e401a33e1a7e477391326baaa4bafb27d484eabf68e646ffbd69c4b95246a00c
#KeyIdentifierNMinusOne=
KMSKeyPurgePolicy=Keep All Keys
#SecurityMode=None
#SEKMStatus=Enabled
#SupportStatus=Installed

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get idrac.sekmservices
[Key=idrac.Embedded.1#SEKMServices.1]
#BOSSStatus=Ready
#HBAStatus=Not Supported
#NVMeStatus=Ready
#OverallStatus=Ready
#PERCStatus=Ready
#VOSSStatus=Ready
```

NOTE: HBA12 is based on PERC and is tracked under PERCStatus. HBA 355i is only supported on VxRAIL platforms. The command above was run against a PowerEdge platform.

Disable SEKM

Run the following command to disable SEKM:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sekm disable
```

SEKM0213: The SEKM disable operation is successful.

Configure SEKM using Server Configuration Profile

For more information about Server Configuration Profile (SCP), see the [SCP Reference Guide](#).

Enable SEKM

For the signed SSL certificate, a CSR must be generated and signed on the KMS, then downloaded. The Server CA must also be downloaded from the KMS. In the SCP, copy the contents of the signed SSL certificate and Server CA as shown in the example SCP file below. This SCP file has been edited to show 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
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEADAOBgNVBACjB0JlBGNhbXAxEADA
BgNVBAoTB0dlbWFSdG8xGjAYBgNVBAMTEutleVNlY3VyZSBSb290IENBMB4XDTIx
MDYyMzE0MDU0N1oXDTMxMDYyMTE0MDU0N1owWjELMAkGA1UEBhMCVVMxGjAxBgNV
BAgTAK1EMRAwDgYDVQQHEWdCZWxjYW1wMRwDgYDVQQKEWdHZW1hbnHRvMRRowGAYD
VQQDEwFLZXNlZlZWN1cmUgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADgIPADCC
AgoCggIBANbjXWXRloVYosJlwxpSz2fCXGLWQQfULFCEwUPFw+R8fAD29lSo6tHa
sQ3Tx+QMz1FEa9DaZbhcuOyQsoIUoG1V+oBpZSvx1+QTVcO6PRM8Tv3RD75xI36Y
KDQXxJoABB414laHM9pyAmk1ldnHs7wQhHBrb7PBW80l2+Qzk3CDAYaa4t/s332/
KldQs18JTBHceMnNEdXkG9rVcYmpjZXvrhjYHSvvVoGZWctzuKvszL6NOKj7ruUT
uq2WSSBRjiwPSysJntubcGNravyOm4FCgSNzi0v1bqKFTBq01XgamhScjYIHGKrfm
ao71vl0mDTjih7c69gtOQg+yvYCKPBNrxh5CvEU7yoJDwa1ak7TJaiYcZ12cvmDY2
3r9uFWdfem0E4EQ5kM5KvLXzygM8FxxZE3XkreKfw+6kOZuZmf0FoptQYATOAqPk
xGrTWGjlcAlnoQDgINGjZFD70y/mf01JkS/UWtdX0yZysw/iNDzqmH7ELy9dsR2s
PkXyM1AOVW/ydlFRcy+s32kMqRXlFKgy8vuyPMLhi/i/tMGnpvJ4N6vnjzHfDpsWK
d5n/T7tDMAf/zlmUsvwhTsHkMnXyCpPAR/uVW5DMwbf9d6TCJ57ofIFpsSptkw53
UDL7ThX9klq00WV5fbhGBlY1oFNmX6L1wJ+V3AlVVNFNlYxCUTA/AgMBAAGjQzBB
MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB4GA1UdEQQXMBWBE3N1
cHBvcnRAZ2VtYXx0by5jb20wDQYJKoZIhvcNAQELBQADggIBANFZGyBqQ6u26G/C
P2vhIr5i3UrlOyLFC+erX2LGu68GFloHF26ZKBej3kAkF16naThR3vj01j2crM6+
PzlyW/JTpmBa0AvfyfVlKyTUmKXXM27bPheeBInDPOffgJROG7xiMfMKRdDwMJ+B
iYX+rH08xc72e7FUnF7kYd0n1AK+2sLvaFSdWYwQ/Aj2Dm5qXxRqW3YptToax3ml
c+O3Wb5jCW01s+7w+E74CPRCiFISRsP23qDJV3xGbMF7pTwJEDzIQTtrXT5DXOXa
o7yJm9UyW5QF589agesVybH8KsJJZLN+wW75NHUp+OnTuC/gY8viccaYzCCXuqGH
R3aX/k9UBka0cAI9M6bGhN7XwsJWKSyWHtsCqJKyGvo9+48kgg0dximWDwUBMBjx
tP0lmoMOLecG3xB72L2otPNZHLU/4w87sLVxPJyrdRT+ZnlzjFdBDGUdNEW2di+2
qWlXwoy8TQK/cOKC5/cMQVqrG4PriRTbhnU5WDSfQ/fuiyGmU+L9/LorjL9S2/8C
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-----
MIIEpTCCAO2gAwIBAgIQU0lUS/yDXsY8uGv+lxAuQDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxEADAOBgNVBACjB0JlBGNhbXAxEADA
BgNVBAoTB0dlbWFSdG8xGjAYBgNVBAMTEutleVNlY3VyZSBSb290IENBMB4XDTIx
MTAyMDE4MDUwMlloXDTIyMTAyMDE4MDUwMlloYysxGjAxBgNVBAYTA1VTMqB4DAYD
VQQIEwVUZlZlZWN1cmUgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADgIPADCC
AgoCggIBANbjXWXRloVYosJlwxpSz2fCXGLWQQfULFCEwUPFw+R8fAD29lSo6tHa
sQ3Tx+QMz1FEa9DaZbhcuOyQsoIUoG1V+oBpZSvx1+QTVcO6PRM8Tv3RD75xI36Y
KDQXxJoABB414laHM9pyAmk1ldnHs7wQhHBrb7PBW80l2+Qzk3CDAYaa4t/s332/
KldQs18JTBHceMnNEdXkG9rVcYmpjZXvrhjYHSvvVoGZWctzuKvszL6NOKj7ruUT
uq2WSSBRjiwPSysJntubcGNravyOm4FCgSNzi0v1bqKFTBq01XgamhScjYIHGKrfm
ao71vl0mDTjih7c69gtOQg+yvYCKPBNrxh5CvEU7yoJDwa1ak7TJaiYcZ12cvmDY2
3r9uFWdfem0E4EQ5kM5KvLXzygM8FxxZE3XkreKfw+6kOZuZmf0FoptQYATOAqPk
xGrTWGjlcAlnoQDgINGjZFD70y/mf01JkS/UWtdX0yZysw/iNDzqmH7ELy9dsR2s
PkXyM1AOVW/ydlFRcy+s32kMqRXlFKgy8vuyPMLhi/i/tMGnpvJ4N6vnjzHfDpsWK
d5n/T7tDMAf/zlmUsvwhTsHkMnXyCpPAR/uVW5DMwbf9d6TCJ57ofIFpsSptkw53
UDL7ThX9klq00WV5fbhGBlY1oFNmX6L1wJ+V3AlVVNFNlYxCUTA/AgMBAAGjQzBB
MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB4GA1UdEQQXMBWBE3N1
cHBvcnRAZ2VtYXx0by5jb20wDQYJKoZIhvcNAQELBQADggIBANFZGyBqQ6u26G/C
P2vhIr5i3UrlOyLFC+erX2LGu68GFloHF26ZKBej3kAkF16naThR3vj01j2crM6+
PzlyW/JTpmBa0AvfyfVlKyTUmKXXM27bPheeBInDPOffgJROG7xiMfMKRdDwMJ+B
iYX+rH08xc72e7FUnF7kYd0n1AK+2sLvaFSdWYwQ/Aj2Dm5qXxRqW3YptToax3ml
c+O3Wb5jCW01s+7w+E74CPRCiFISRsP23qDJV3xGbMF7pTwJEDzIQTtrXT5DXOXa
o7yJm9UyW5QF589agesVybH8KsJJZLN+wW75NHUp+OnTuC/gY8viccaYzCCXuqGH
R3aX/k9UBka0cAI9M6bGhN7XwsJWKSyWHtsCqJKyGvo9+48kgg0dximWDwUBMBjx
tP0lmoMOLecG3xB72L2otPNZHLU/4w87sLVxPJyrdRT+ZnlzjFdBDGUdNEW2di+2
qWlXwoy8TQK/cOKC5/cMQVqrG4PriRTbhnU5WDSfQ/fuiyGmU+L9/LorjL9S2/8C
RTsQzOmQC+1ADOXHedMFPhsRZcMTZgSWXThERrn46ZiuO+yvBvh5rfvNf6JH+LLL
uwpUDmwzRF3rmXqGzeuk0Ou620kQuylK4nnyii3GsCgq/ZOn6Gqz+afcUoCPN39n
6CTqqYiFHUXl4pZJrrXhQ+16gdtrd
-----END CERTIFICATE-----</Attribute>
<Attribute Name="SecurityCertificate.2#CertType">KMS_SSL_CERT</Attribute>
</Component>
</SystemConfiguration>
```

Disable SEKM

This SCP file has been edited to show 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">Disabled</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"> </Attribute>
  <Attribute Name="KMS.1#iDRACPassword"> </Attribute>
  <Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute>
  <Attribute Name="SEKMCert.1#CommonName"></Attribute>
  <Attribute Name="SEKMCert.1#OrganizationName"></Attribute>
  <Attribute Name="SEKMCert.1#OrganizationUnit"> </Attribute>
  <Attribute Name="SEKMCert.1#LocalityName"></Attribute>
  <Attribute Name="SEKMCert.1#StateName"></Attribute>
  <Attribute Name="SEKMCert.1#CountryCode"></Attribute>
  <Attribute Name="SEKMCert.1#EmailAddress"></Attribute>
  <Attribute Name="SEKMCert.1#SubjectAltName"/>
  <Attribute Name="SEKMCert.1#UserId"/>
  <Attribute Name="SecurityCertificate.1#CertData"></Attribute>
  <Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
  <Attribute Name="SecurityCertificate.2#CertData"></Attribute>
  <Attribute Name="SecurityCertificate.2#CertType">SEKM_SSL_CERT</Attribute>
</Component>
</SystemConfiguration>
```

1. Run the RACADM set command to import this SCP file from an HTTP share.
2. Ensure that the SCP import job is marked "Completed."

Auto Secure

To secure all supported SEDs, Auto Secure is available as part of SEKM enablement. This option is enabled by default.

NOTE: Auto Secure is not applicable for drives behind PERC, HBA 465i, BOSS-N1, and ROR-N1. To secure drives, perform manual operation.

Topics:

- [Configure Auto Secure using the iDRAC UI](#)
- [Configure Auto Secure using Redfish](#)
- [Configure Auto Secure using RACADM](#)
- [Configure Auto Secure using Server Configuration Profile](#)

Configure Auto Secure using the iDRAC UI

Go to the **iDRAC Dashboard > iDRAC Settings > Services > iDRAC Key Management**.

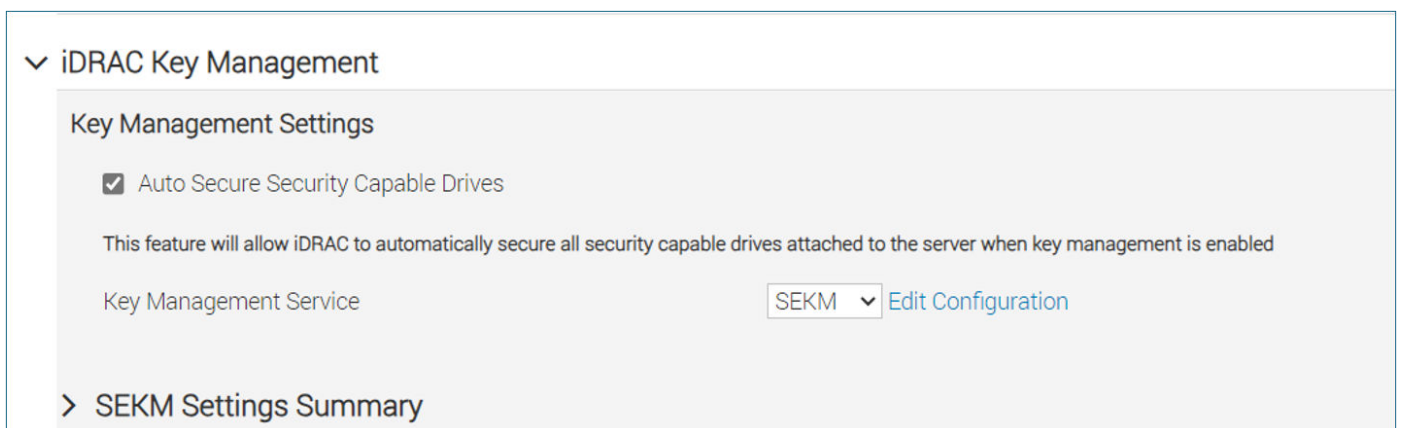


Figure 65. iDRAC Key Management

Configure Auto Secure using Redfish

Enable Auto Secure

Command:	PATCH
URI:	/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1
Header:	content-type application/json
Auth:	Basic
Body:	{"Attributes": {"SEKM.1.AutoSecure": "Enabled"}}

Verify Auto Secure status

Command: GET

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1?\$select=Attributes/SEKM.1.AutoSecure

Auth: Basic

Expected attributes if Auto Secure is enabled: "SEKM.1.AutoSecure": "Enabled"

Disable Auto Secure

Command: PATCH

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Header: content-type application/json

Auth: Basic

Body: {"Attributes": {"SEKM.1.AutoSecure": "Disabled"}}

Configure Auto Secure using RACADM

Enable Auto Secure

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set idrac.SEKM.AutoSecure "Enabled"
[Key=idrac.Embedded.1#SEKM.1]
Object value modified successfully
```

Verify Auto Secure status

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get idrac.SEKM.AutoSecure
[Key=idrac.Embedded.1#SEKM.1]
AutoSecure=Enabled
```

Disable Auto Secure

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set idrac.SEKM.AutoSecure "Disabled"
[Key=idrac.Embedded.1#SEKM.1]
Object value modified successfully
```

Configure Auto Secure using Server Configuration Profile

Enable Auto Secure

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

```
<Component FQDD="iDRAC.Embedded.1">  
<Attribute Name="SEKM.1#AutoSecure">Enabled</Attribute><Attribute  
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Ensure that the SCP import job is marked "Completed."

Disable Auto Secure

This SCP file has been edited to show only the configuration changes required to disable Auto Secure on iDRAC:

```
<Component FQDD="iDRAC.Embedded.1">  
<Attribute Name="SEKM.1#AutoSecure">Disabled</Attribute><Attribute  
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Ensure that the SCP import job is marked "Completed."

PowerEdge RAID Controller


Topics:

- [Overview](#)
- [Configure PERC using the iDRAC UI](#)
- [Configure PERC using Redfish](#)
- [Configure PERC using RACADM](#)
- [Configure PERC using Server Configuration Profile](#)

Overview

For more information about PERC features, see the PERC User's Guide.

- **PERC 12:** [Dell PowerEdge RAID Controller 12 User's Guide](#) PERC H965i Adapter, PERC H965i Front, PERC H965i MX, and PERC H965e Adapter
- **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

 **NOTE:** It is recommended to use real-time operations instead of staged for PERC 12 and newer generations.

Configure PERC using the iDRAC UI

1. Start iDRAC using any supported browser.
2. On the iDRAC GUI, click **Dashboard** > **Storage** > **Overview** > **Controllers**.
3. From the **Actions** drop-down menu of the PERC, select **Edit** > **Security** > **Secure Enterprise Key Manager**.

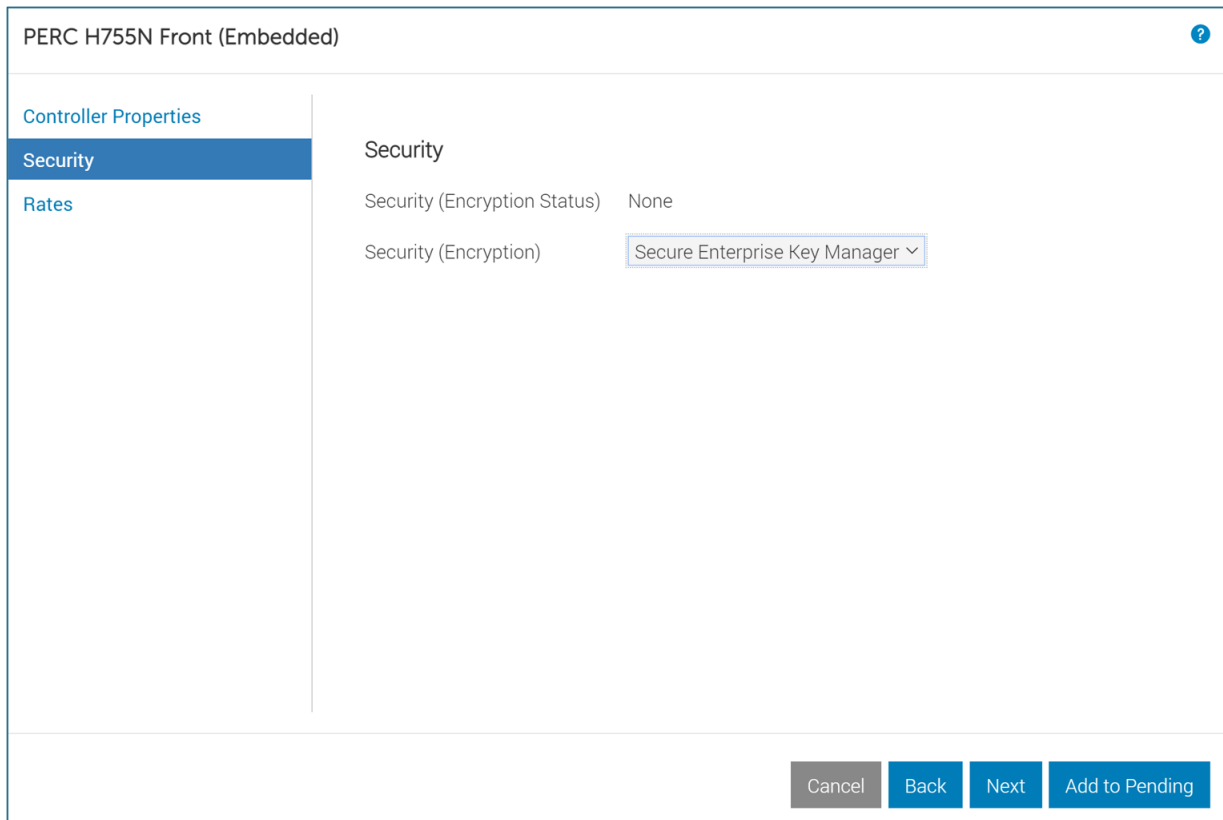


Figure 66. PERC security

NOTE: iDRAC9 is shown in the example above. The security options for PERC with iDRAC10 are “Enable Security” or “Disable Security”.

4. Click **Add to Pending**.

- Select **Apply Now** for PERC 12 and later generations.
- Select **At Next Reboot** for PERC 11 and earlier generations.

NOTE: The **Apply Now** feature is not supported for this operation on PERC 11 and older generations.

NOTE: If **At Next Reboot** is selected, a server power cycle (cold reboot) must be performed.

NOTE: If the **Apply Now** option is selected, the job runs in real time without a server reboot. Go to the **Job Queue**. This job should be marked "Running."

5. Go to the **Job Queue** page and ensure that this job ID has been marked "Completed."

Job Queue				
<div><div></div> Delete</div>				
	<input type="checkbox"/>	ID ▼	Job	Status
+	<input type="checkbox"/>	RID_919130367938	Reboot: Power cycle	Reboot Completed (100%)
+	<input type="checkbox"/>	RID_919007247652	Reboot: Power cycle	Reboot Completed (100%)
+	<input type="checkbox"/>	RID_919000641413	Reboot: Power cycle	Reboot Completed (100%)
+	<input type="checkbox"/>	JID_924369135049	Configure: RAID.Integrated.1-1	Completed (100%)
+	<input type="checkbox"/>	JID_924369003403	SEKM Status Change	Completed (100%)

Figure 67. Job Queue

6. On the iDRAC GUI, click **Dashboard > Storage > Overview > Controllers**.
7. Expand your storage controller and ensure that the security settings are correct, as shown in the sample screenshot:

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	3b8fc69932054dcc05c91ab76923303652a91be8b9240178045c8409d40c8ee
Support LKM to SEKM Transition	Supported

Figure 68. Security attributes

8. To disable SEKM on PERC, select **Delete Security Key** from the **Actions** drop-down menu.
9. Select **Add to Pending** and **Apply Now**.

NOTE: If the request to disable controller security fails, delete any existing volumes and perform cryptographic erase for each drive.


NOTE: For more information about cryptographic erase, see [Cryptographic erase](#).

Configure PERC using Redfish

Enable security on PERC

Command:	POST
URI:	/redfish/v1/Dell/Systems/System.Embedded.1/Oem/DellRaidService/Actions/DellRaidService.EnableControllerEncryption
Header:	content-type application/json

Auth: Basic
Body: {"Mode": "SEKM", "TargetFQDD": "RAID.Integrated.1-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Verify Encryption Mode on PERC


Command: GET
URI: /redfish/v1/Systems/System.Embedded.1/Storage/RAID.Integrated.1-1
Auth: Basic
iDRAC10 example: {"EncryptionMode": "Enabled"}
iDRAC9 example: {"EncryptionMode": "SecureEnterpriseKeyManager"}

Verify Encryption Status on SED behind PERC

Command: GET
URI: /redfish/v1/Systems/System.Embedded.1/Storage/RAID.SL.1-1/Drives/Disk.Bay.5:Enclosure.Internal.0-1:RAID.SL.1-1?\$select=EncryptionStatus
Header: content-type application/json
Auth: Basic
Body: {"EncryptionStatus": "Unlocked"}

Disable security on PERC

Command: POST
URI: /redfish/v1/Dell/Systems/System.Embedded.1/Oem/DellRaidService/Actions/DellRaidService.RemoveControllerKey
Header: content-type application/json
Auth: Basic

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Configure PERC using RACADM

Enable security on PERC

Run the following command to enable security on PERC:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage  
setencryptionmode:RAID.SL.1-1 -mode SEKM
```

STOR094: The storage configuration operation is successfully completed, and the change is in a 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 the jobqueue command, run the `racadm help jobqueue` command.

NOTE: PERC 12 and newer generations support enabling SEKM with a real time job.

NOTE: Enabling SEKM on PERC 11 and older generations requires a staged job.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create RAID.SL.1-1
--realtime -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_021549410134

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_021549410134
```

```
----- JOB -----
[Job ID=JID_021549410134]
Job Name=Configure: RAID.SL.1-1
Status=Running
Scheduled Start Time=[Now]
Expiration Time=[Not Applicable]
Actual Start Time=[Sat, 09 Dec 2023 14:49:02]
Actual Completion Time=[Not Applicable]
Message=[PR20: Job in progress.]
Percent Complete=[1]
-----
```

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_021549410134
```

```
----- JOB -----
[Job ID=JID_021549410134]
Job Name=Configure: RAID.SL.1-1
Status=Completed
Scheduled Start Time=[Now]
Expiration Time=[Not Applicable]
Actual Start Time=[Sat, 09 Dec 2023 14:49:02]
Actual Completion Time=[Sat, 09 Dec 2023 14:50:20]
Message=[PR19: Job completed successfully.]
Percent Complete=[100]
-----
```

Verify Encryption Mode on PERC

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get controllers -o
-p encryptionmode
RAID.SL.1-1
EncryptionMode = Secure Enterprise Key Manager
```

Verify Security Status on SED behind PERC

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p
securitystatus
Disk.Bay.0:Enclosure.Internal.0-1:RAID.SL.1-1
SecurityStatus = Secured
Disk.Bay.8:Enclosure.Internal.0-2:RAID.SL.1-1
SecurityStatus = Secured
```

Disable security on PERC

```
C:\>racadm -r 192.168.0.12 -u root -p P@ssw0rd --nocertwarn storage
deletesecuritykey:RAID.SL.1-1
```

STOR094: The storage configuration operation is successfully completed, and the change is in a 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 the `jobqueue` command, run the `racadm help jobqueue` command.

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_021542870002

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_021542870002
----- JOB -----
[Job ID=JID_021542870002]
Job Name=Configure: RAID.SL.1-1
Status=Completed
Scheduled Start Time=[Now]
Expiration Time=[Not Applicable]
Actual Start Time=[Sat, 09 Dec 2023 14:38:07]
Actual Completion Time=[Sat, 09 Dec 2023 14:39:26]
Message=[PR19: Job completed successfully.]
Percent Complete=[100]
-----
```

Configure PERC using Server Configuration Profile

Enable security on PERC

This SCP file displays only the SEKM configuration changes required to enable security on PERC:

```
<Component FQDD="RAID.SL.1-1">
<Attribute Name="EncryptionMode">Secure Enterprise Key Manager</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Disable security on PERC

This SCP file displays only the SEKM configuration changes required to disable security on PERC:

```
<Component FQDD="RAID.SL.1-1">
<Attribute Name="EncryptionMode">None</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Host Bus Adapter

Topics:

- [Overview](#)
- [Configure HBA using the iDRAC UI](#)
- [Configure HBA using Redfish](#)
- [Configure HBA using RACADM](#)
- [Configure HBA using Server Configuration Profile](#)

Overview

SEKM for HBA only supports SEDs that adhere to the TCG Enterprise Protocol. Below is an example of how to verify support using the Redfish interface.

Command: GET

URI: /redfish/v1/Systems/System.Embedded.1/Storage/{controller ID}/Drives/{disk ID}/Oem/Dell/DellDrives/{disk ID}?\$select=EncryptionProtocol

Auth: Basic

Expected value: "EncryptionProtocol": "TCGEnterpriseSSC"

For more information about HBA features, see the [HBA User Guide](#).

Configure HBA using the iDRAC UI

NOTE: An Identity Module is required for SEKM HBA 355i support on VxRail platforms. This can be uploaded through the manual update page (**Maintenance > System Update**).

1. Start iDRAC using any supported browser.
2. On the iDRAC UI, click **Dashboard > Storage > Overview > Controllers**.
3. Go to the HBA controller and open the **Actions** drop-down menu. Go to **Edit**, then **Security**. Here, you can choose to either **Enable** or **Disable** security.
4. Click **Add to Pending**.
5. Select **At Next Reboot**, then restart the server if necessary.

NOTE: HBA 12 and later generations support the **Apply Now** option for changes to the controller security state.

6. Go to the **Job Queue** page and ensure that this job ID is marked "Completed."
7. On the iDRAC UI, click **Dashboard > Storage > Overview > Controllers** to view your storage controller security properties:

Security	
Security Status	Security Key Assigned
Encryption Mode	Enabled
Encryption Capable	Capable
Key ID	979d719fa856488b87f3b1139a95588a6d626f8e919e4215a49857cf48b07a8f
Support LKM to SEKM Transition	Not Supported

Figure 69. Security attributes

NOTE: Security properties above are applicable to HBA 465i when security is enabled on the controller. See [Supported storage devices](#) to see all supported properties.

If the request to disable controller security fails, ensure that you reset the controller to remove any VDs. Then, perform PSID revert or cryptographic erase depending on the state of the supported drives behind HBA.

For more information about PSID revert and cryptographic erase, see [PSID revert](#) and [Cryptographic erase](#).

NOTE: The `ConvertToRAID OEM` action is required before you can erase supported drives behind HBA 465i from all supported interfaces.

NOTE: The `ConvertToNonRAID OEM` action is required before you can secure supported drives behind HBA 465i from all supported interfaces.

Configure HBA using Redfish

Enable security on HBA

Command: POST

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

Header: `content-type application/json`

Auth: Basic

Body: `{"TargetFQDD": "NonRAID.SL.8-1"}`

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

ConvertToNonRAID on supported SED behind HBA 12

Expected status code: 202 Accepted

Command: POST

URI: `/redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.ConvertToNonRAID`

Header: `content-type application/json`

Auth: Basic

Body:

```
{
  "PDArray": [
    "Disk.Bay.2:Enclosure.Internal.0-1:NonRAID.SL.8-1",
    "Disk.Bay.3:Enclosure.Internal.0-1:NonRAID.SL.8-1"
  ]
}
```

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Enable security on SED behind HBA


Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": " Disk.Bay.7:Enclosure.Internal.0-1:NonRAID.SL.8-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Verify Security Status on HBA

Command: GET

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

Auth: Basic

Body: {"EncryptionMode": "Enabled"}

Verify Encryption Status on SED behind HBA

Command: GET

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

Auth: Basic

Body: {"EncryptionStatus": "Unlocked"}

Disable security on HBA


Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"ControllerFQDD": "NonRAID.SL.8-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

ConvertToRAID on supported SED behind HBA 12

Expected status code: 202 Accepted

Command: POST

URI: /redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.ConvertToRAID

Header: content-type application/json

Auth: Basic

Body:

```
{
  "PDArray": [
    "Disk.Bay.2:Enclosure.Internal.0-1:NonRAID.SL.8-1"
  ]
}
```

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Configure HBA using RACADM

NOTE: HBA 12 and later generations support the real time option for changes to the controller security state.

Enable security on HBA

Run the following command to enable security on HBA:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:NonRAID.SL.8-1 -enable
```

RAC1040: The storage configuration operation has been successfully accepted.

- 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 P@ssw0rd --nocertwarn jobqueue create
NonRAID.SL.8-1 -r pwrcycle -s TIME_NOW
```

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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]
-----
```

Enable security on SED behind HBA

Run the following command to enable security on SED behind HBA:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
encryptpd:Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1
```

STOR094: The storage configuration operation has been successfully completed, and the change is in a 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 the `jobqueue` command, run the `racadm help jobqueue` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
NonRAID.SL.8-1 --realtime -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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.]
-----
```

Verify Security Status on HBA

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get controllers -o
-p securitystatus
NonRAID.SL.8-1
SecurityStatus = Enabled
```

Verify Encryption Status on SED behind HBA

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p
securitystatus
Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1
SecurityStatus = Secured
```

Disable security on HBA

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:NonRAID.SL.8-1 -disable
```

RAC1040: The storage configuration operation has been successfully accepted.

- To apply the configuration operation, create a configuration job, 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 P@ssw0rd --nocertwarn jobqueue create
NonRAID.SL.8-1 -r pwr cycle -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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]
-----
```

Configure HBA using Server Configuration Profile

Enable security on HBA

This SCP file only displays the SEKM configuration changes required to enable security on HBA:

```
<Component FQDD="NonRAID.SL.8-1">
  <Attribute Name="EncryptionMode">Enabled</Attribute>
  <Component FQDD="Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
  <Component FQDD="Disk.Bay.1:Enclosure.Internal.0-1:NonRAID.SL.8-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
</Component>
```

- Run the command to import this SCP file from an HTTP share.
- Confirm that the SCP import job is marked "Completed."

Disable security on HBA

This SCP file displays only the SEKM configuration changes required to disable security on HBA:

```
<Component FQDD="NonRAID.SL.8-1">
  <Attribute Name="EncryptionMode">Disabled</Attribute>
```

```
<Component FQDD="Disk.Bay.0:Enclosure.Internal.0-1:NonRAID.SL.8-1">
  <Attribute Name="LockStatus">Encryption Capable</Attribute>
<Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
<Component FQDD="Disk.Bay.1:Enclosure.Internal.0-1:NonRAID.SL.8-1">
  <Attribute Name="LockStatus">Encryption Capable</Attribute>
<Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
</Component>
```

CPU Attached NVMe SEDs

Topics:

- Configure CPU attached NVMe SED using iDRAC UI
- Configure CPU attached NVMe SED using Redfish
- Configure CPU attached NVMe SED using RACADM
- Configure CPU attached NVMe SED using Server Configuration Profile

Configure CPU attached NVMe SED using iDRAC UI

1. Start iDRAC using any supported browser.
2. On the iDRAC UI, click **Dashboard > iDRAC Settings > Services > iDRAC Key Management**.
3. Select the **Auto Secure** option.

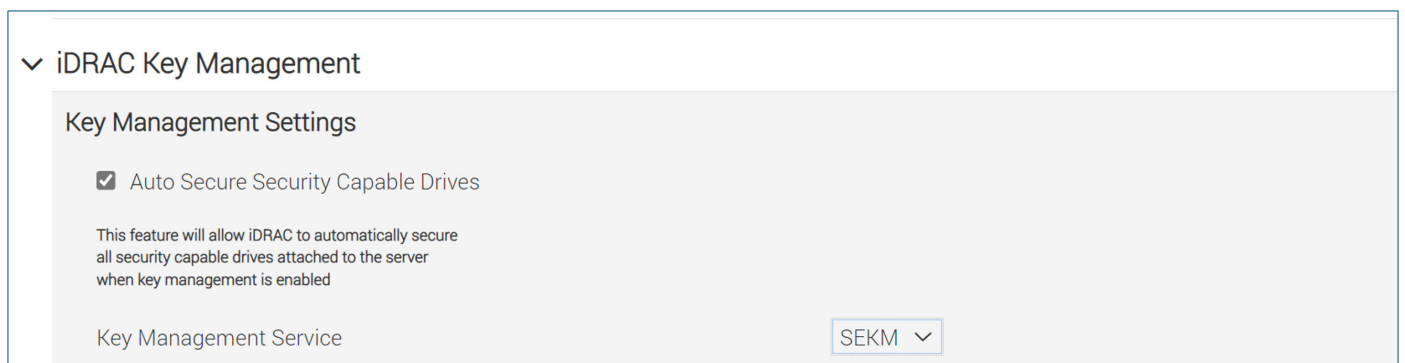


Figure 70. iDRAC Auto Secure

NOTE: If Auto Secure is enabled while enabling SEKM on iDRAC, then iDRAC tries to secure NVMe SEDs in a single job. This job completes with errors when non-SEDs are present in the system. This is to ensure that users are warned and aware of nonsecured drives in the system.

4. View the security status of supported drives by clicking **Dashboard > Storage > Overview > Physical Disks** on the iDRAC UI.

Physical Disks									
Filter Drives									
<div> <div>Blink</div> <div>Unblink</div> <div>Create Virtual Disk</div> </div>									
	<input type="checkbox"/>	Status	Name	State	Slot Number	Size	Bus Protocol	Security Status	Encryption Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	PCIe SSD in Slot 1 in Bay 1	Ready	1	1788.5 GB	PCIe	Secured	Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	PCIe SSD in Slot 2 in Bay 1	Ready	2	1788.5 GB	PCIe	Secured	Capable

Figure 71. Physical Disks

NOTE: The **Secure Drive** option is also available in the **Actions** drop-down menu.

5. Select **Secure Drive** and click **Apply Now** to secure the drive in real-time without restarting the server.

Physical Disks										
Filter Drives										
	<input type="checkbox"/> Status	Name	State	Slot Number	Size	Bus Protocol	Media Type	Hot Spare	Security Status	Actions
+	<input checked="" type="checkbox"/>	PCIe SSD in Slot 13 in Bay 2	Ready	13	2980.82 GB	PCIe	SSD	Not Applicable	Encryption Capable	Secure Drive
+	<input checked="" type="checkbox"/>	PCIe SSD in Slot 14 in Bay 2	Ready	14	1490.42 GB	PCIe	SSD	Not Applicable	Encryption Capable	Action
+	<input checked="" type="checkbox"/>	PCIe SSD in Slot 16 in Bay 2	Ready	16	894.25 GB	PCIe	SSD	Not Applicable	Encryption Capable	Prepare to remove
+	<input checked="" type="checkbox"/>	PCIe SSD in Slot 17 in Bay 2	Ready	17	894.25 GB	PCIe	SSD	Not Applicable	Encryption Capable	Cryptographic Erase
										Secure Drive
										Collect Logs
										View Enclosures

Figure 72. Secure drive option

NOTE: To disable security on a supported SED, you must perform the PSID revert or cryptographic erase operation based on the state of the drive.

For more information about PSID revert and cryptographic erase, see [PSID revert](#) and [Cryptographic erase](#).

Configure CPU attached NVMe SED using Redfish

Enable security on CPU attached NVMe SED

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": "Disk.Bay.12:Enclosure.Internal.0-1"}

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Verify Encryption Status on CPU attached NVMe SED

Command: GET

URI: /redfish/v1/Systems/System.Embedded.1/Storage/CPU.1/Drives/Disk.Bay.12:Enclosure.Internal.0-2?\$select=EncryptionStatus

Auth: Basic

Body: "EncryptionStatus": "Unlocked"

Configure CPU attached NVMe SED using RACADM

Enable security on CPU attached NVMe SED

Run the following command to enable security on CPU attached NVMe SED:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
encryptpd:Disk.Bay.15:Enclosure.Internal.0-1
```

STOR094: The storage configuration operation is successfully completed, and the change is in a 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 the `jobqueue` command, run the `racadm help jobqueue` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
Disk.Bay.15:Enclosure.Internal.0- 1 --realtime -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384841257680

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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]
-----
```

Verify Security Status on CPU attached NVMe SED

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p
securitystatus
Disk.Bay.15:Enclosure.Internal.0-1
SecurityStatus = Secured
```

Configure CPU attached NVMe SED using Server Configuration Profile

Enable security on CPU attached NVMe SED

This SCP file displays only the SEKM configuration changes required to enable security on supported NVMe SED:

```
Component FQDD="Disk.Bay.18:Enclosure.Internal.0-2">
  <Attribute Name="LockStatus">Secured</Attribute>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Boot Optimized Storage Solution

For more information about Boot Optimized Storage Solution (BOSS-N1) features, see the [BOSS-N1 User's Guide](#).

NOTE: Supported M.2 SEDs behind BOSS-N1 is automatically secured when security is enabled on BOSS-N1, regardless of the iDRAC Auto Secure setting.

NOTE: To disable BOSS-N1 security, stack cryptographic erase and disable security on the controller into a single job.

Related information

[Crypto-Erase All Drives in a Single Operation](#)

Topics:

- [Configure BOSS-N1 using the iDRAC UI](#)
- [Configure BOSS-N1 using Redfish](#)
- [Configure BOSS-N1 using RACADM](#)
- [Configure BOSS-N1 using Server Configuration Profile](#)

Configure BOSS-N1 using the iDRAC UI

1. Start iDRAC using any supported browser.
2. On the iDRAC UI, click **Dashboard > Storage > Overview > Controllers**.
3. From the **Actions** drop-down menu of the BOSS-N1 controller, select **Edit > Security > Enable Security**.

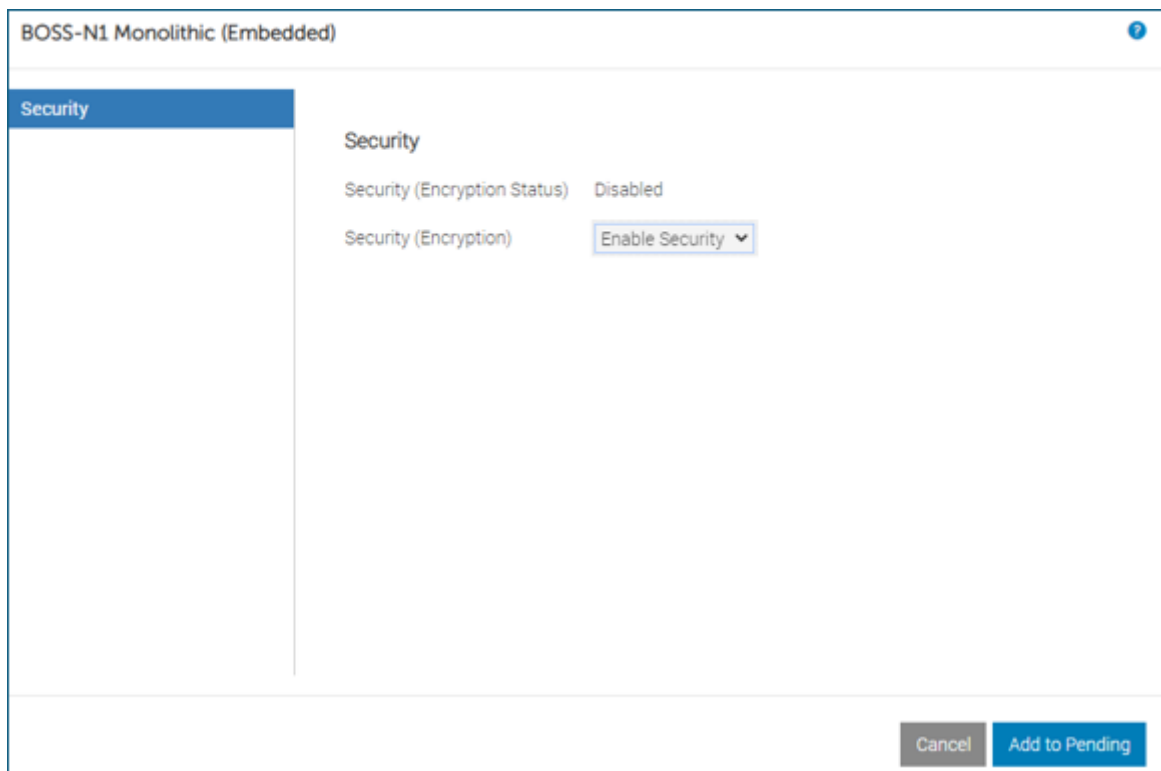


Figure 73. BOSS-N1 security

4. Click **Add to Pending**.

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

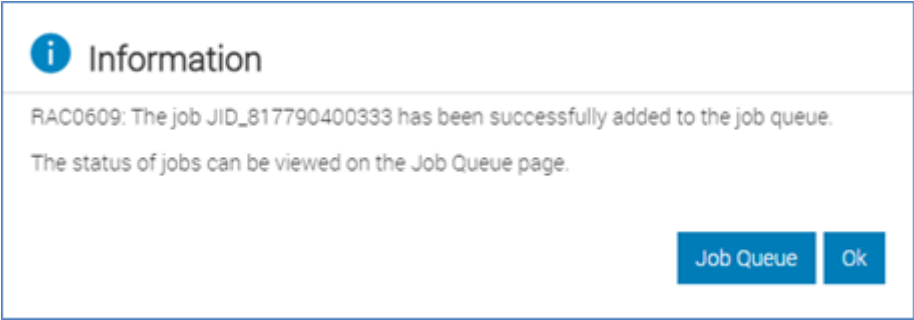


Figure 74. Job information

8. Go to the Job Queue to view the scheduled job.
9. 9. After restarting the server, the configuration job runs in the **Automated Task Application** to enable SEKM security on BOSS. The server is then automatically restarted.
10. 10. After the POST or Collecting Inventory operation completes, ensure that the job ID has been marked "Completed" on the **Job Queue** page.

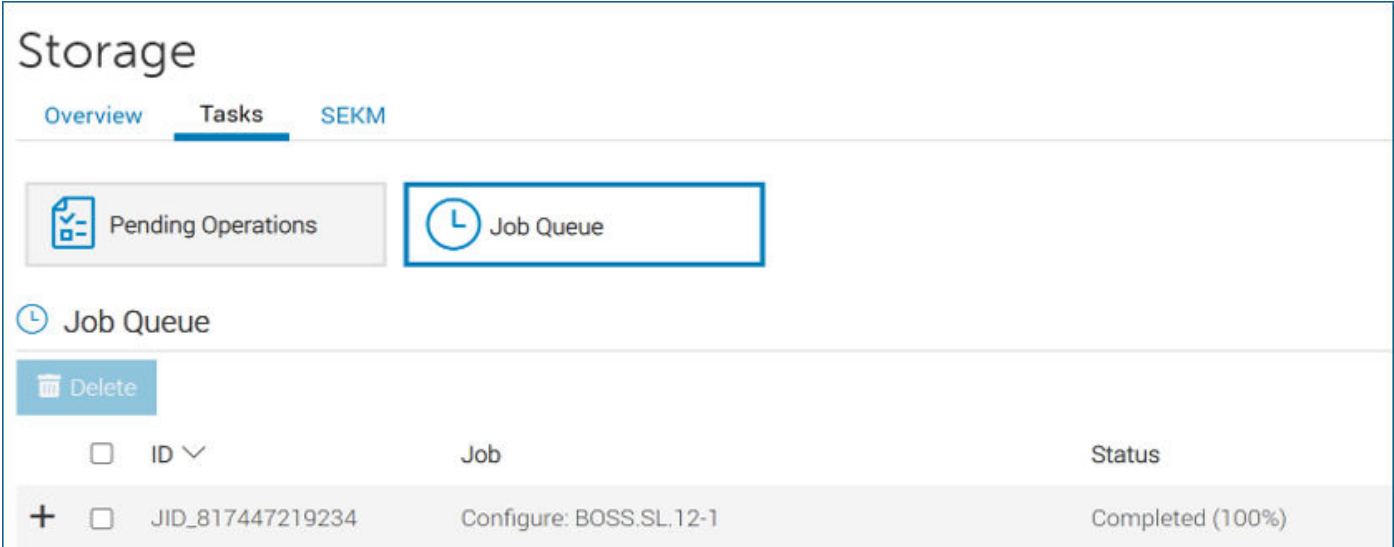


Figure 75. Job queue

11. On the iDRAC UI, click **Dashboard > Storage > Overview > Controllers**.
12. 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

Figure 76. Security properties

13. To disable security on BOSS-N1, select the "Disabled" option from the **Actions** drop-down menu, then select **Add to Pending** and **At Next Reboot**.

NOTE: If the request to disable controller security fails, ensure that you delete any volumes and perform PSID revert or cryptographic erase depending on the state of the drives.

For more information about PSID revert and cryptographic erase, see [PSID revert](#) and [Cryptographic erase](#).

Configure BOSS-N1 using Redfish

Enable security on BOSS-N1

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": "BOSS.SL.12-1"}

NOTE: The request body allows you to specify when the operation completes. @Redfish.OperationApplyTime supports OnReset and Immediate values. OnReset does not run the job until the server is rebooted. Immediate performs a graceful OS shutdown with power cycle once the reboot job timeout completes. Examples are shown below.

Enable security on BOSS-N1 (OnReset)

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": "BOSS.SL.12-1", "@Redfish.OperationApplyTime": "OnReset"}

Enable security on BOSS-N1 (Immediate)

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": "BOSS.SL.12-1", "@Redfish.OperationApplyTime": "Immediate"}

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Verify Security Status on BOSS-N1

Command: GET

URI: /redfish/v1/Systems/System.Embedded.1/Storage/BOSS.SL.12-1

Auth: Basic


Expected attributes "SecurityStatus": "Enabled"
if iLKM security is enabled on BOSS-N1:

Verify Security Status on SED behind BOSS-N1

Command: GET
URI: /redfish/v1/Systems/System.Embedded.1/Storage/BOSS.SL.12-1/Drives/Disk.Direct.0-0:BOSS.SL.12-1?\$select=EncryptionStatus
Auth: Basic
Expected attributes "EncryptionStatus": "Unlocked"
if iLKM security is enabled on SED behind BOSS-N1:

Disable security on BOSS-N1

Command: POST
URI: /redfish/v1/Systems/System.Embedded.1/Oem/Dell/DellRaidService/Actions/DellRaidService.DisableSecurity
Header: content-type application/json
Auth: Basic
Body: {"ControllerFQDD":"BOSS.SL.12-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Configure BOSS-N1 using RACADM

Enable security on BOSS-N1


Run the following command to enable security on BOSS-N1:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage security:BOSS.SL.12-1 -enable
```

RAC1040: The storage configuration operation has been successfully accepted.

- 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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create BOSS.SL.12-1 -r pwr cycle -s TIME_NOW
```

 **NOTE:** A staged job must be scheduled for this operation. A host reboot is required for the security mode change to occur.

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i JID_384818826920
```

```

----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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]
-----

```

Verify Security Status on BOSS-N1

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get controllers -o
-p securitystatus
BOSS.SL.12-1
SecurityStatus                = Enabled

```


Verify Security Status on SED behind BOSS-N1

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p
securitystatus
Disk.Direct.0-0:BOSS.SL.12-1
SecurityStatus                = Secured
Disk.Direct.1-1:BOSS.SL.12-1
SecurityStatus                = Secured

```

Disable security on BOSS-N1

 **NOTE:** To disable security, stack cryptographic erase and disable security on the controller into a single job. An example using RACADM is shown below.

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Direct.1-1:BOSS.SL.14-1

```

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.

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Direct.0-0:BOSS.SL.14-1

```

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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:BOSS.SL.14-1 -disable
```

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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
BOSS.SL.14-1 -r pwr cycle -s TIME_NOW
```

RAC1024: Successfully scheduled a job.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_436090034200

Reboot JID: RID_436090035531

NOTE: A staged job must be scheduled for this operation. A host reboot is necessary for the security mode change to occur.

An example showing RACADM command to disable security on BOSS-N1 as a standalone operation from RACADM is shown below.

Run the following command to disable security on BOSS-N1:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:BOSS.SL.12-1 -disable
```

RAC1040: The storage configuration operation has been successfully accepted.

- 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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
BOSS.SL.12-1 -r pwr cycle -s TIME_NOW
```

NOTE: A staged job must be scheduled for this operation. A host reboot is required for the security mode change to occur.

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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]
-----
```

Configure BOSS-N1 using Server Configuration Profile

Enable security on BOSS-N1

This SCP file displays only the SEKM configuration changes required to enable security on BOSS-N1:

```
<Component FQDD="BOSS.SL.12-1">
  <Attribute Name="SecurityStatus">Enabled</Attribute>
  <Component FQDD="Disk.Direct.0-0:BOSS.SL.12-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
  <Component FQDD="Disk.Direct.1-1:BOSS.SL.12-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Disable security on BOSS-N1

This SCP file displays only the SEKM configuration changes required to disable security on BOSS-N1:

```
<Component FQDD="BOSS.SL.12-1">
  <Attribute Name="SecurityStatus">Disabled</Attribute>
  <Component FQDD="Disk.Direct.0-0:BOSS.SL.12-1">
    <Attribute Name="LockStatus">Encryption Capable</Attribute>
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
  <Component FQDD="Disk.Direct.1-1:BOSS.SL.12-1">
    <Attribute Name="LockStatus">Encryption Capable</Attribute>
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

RAID on RISER

NOTE: Supported M.2 SEDs associated with RAID on RISER (ROR-N1) are automatically secured when security is enabled on ROR-N1, regardless of the iDRAC Auto Secure setting.

NOTE: To disable ROR-N1 security, stack cryptographic erase and disable security on the controller into a single job.

Topics:

- [Configure ROR-N1 using the iDRAC UI](#)
- [Configure ROR-N1 using Redfish](#)
- [Configure ROR-N1 using RACADM](#)
- [Configure ROR-N1 using Server Configuration Profile](#)

Configure ROR-N1 using the iDRAC UI

1. Start iDRAC using any supported browser.
2. Go to the **iDRAC Dashboard > Storage > Overview > Controllers.**
3. From the **Actions** drop-down menu of the ROR-N1 controller, select **Edit > Security > Enable Security.**

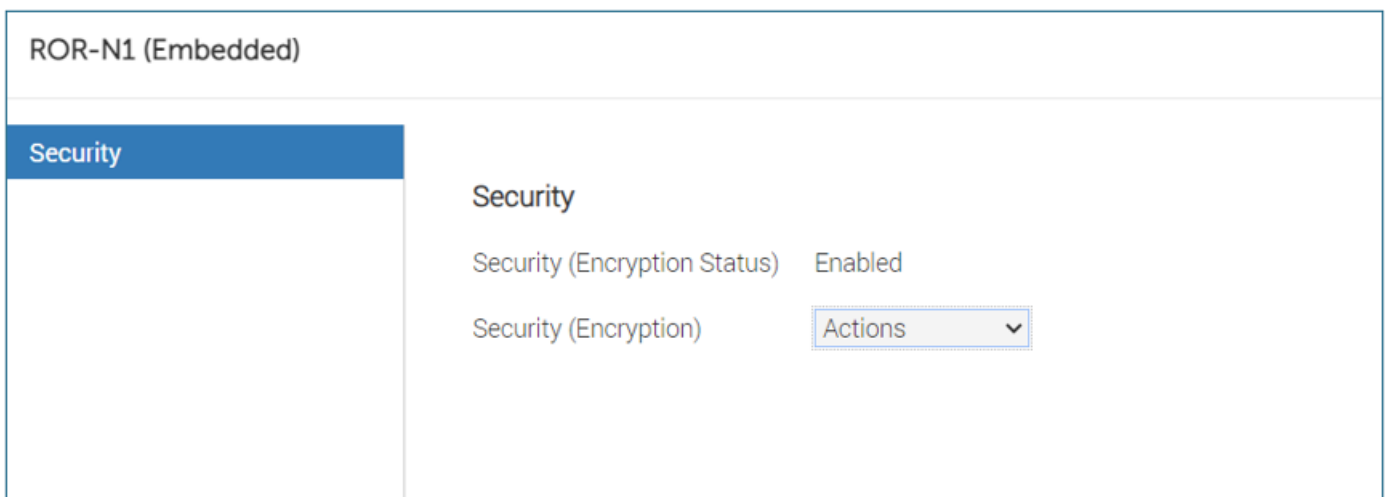


Figure 77. ROR-N1 security

4. Click **Add to Pending.**
5. Select **At Next Reboot.** A message displays, indicating that the job ID is created.
6. Go to the **Job Queue** page and ensure that this job ID is marked "Scheduled."
7. Restart the server to run the configuration job.

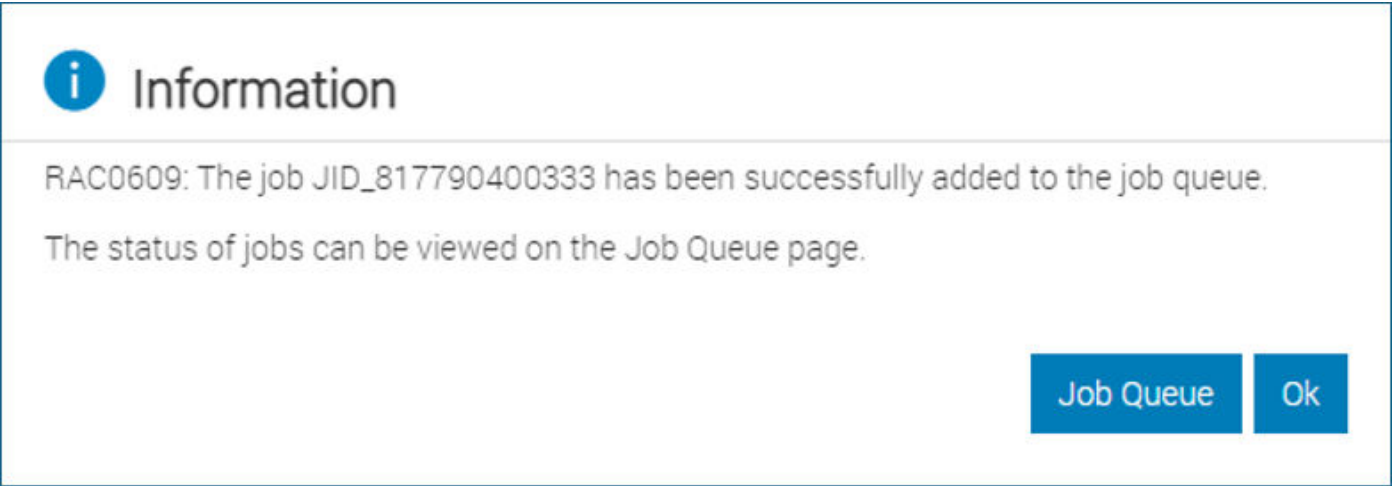


Figure 78. Job information

- 8. After restarting the server, the configuration job runs in the **Automated Task Application** to enable SEKM security on ROR-N1. The server will automatically restart.
- 9. After the POST or Collecting Inventory operation completes, ensure that the job ID has been marked “Completed” on the Job Queue page.

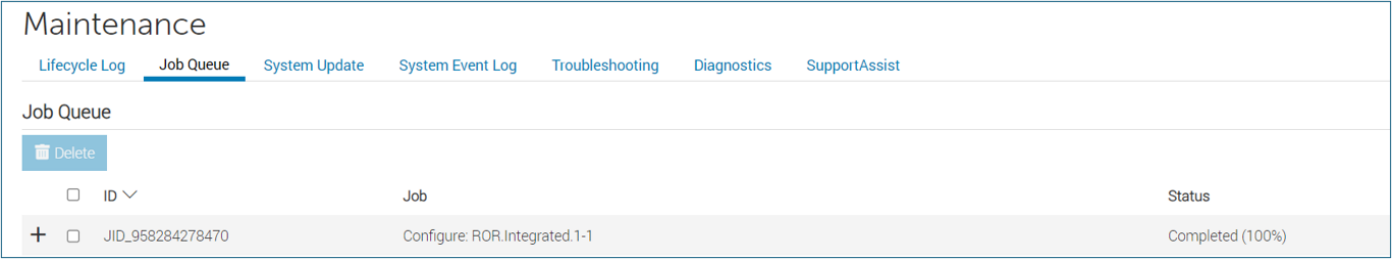


Figure 79. Job queue

- 10. On the iDRAC UI, click **Dashboard > Storage > Overview > Controllers**.
- 11. Expand your storage controller and ensure the following:

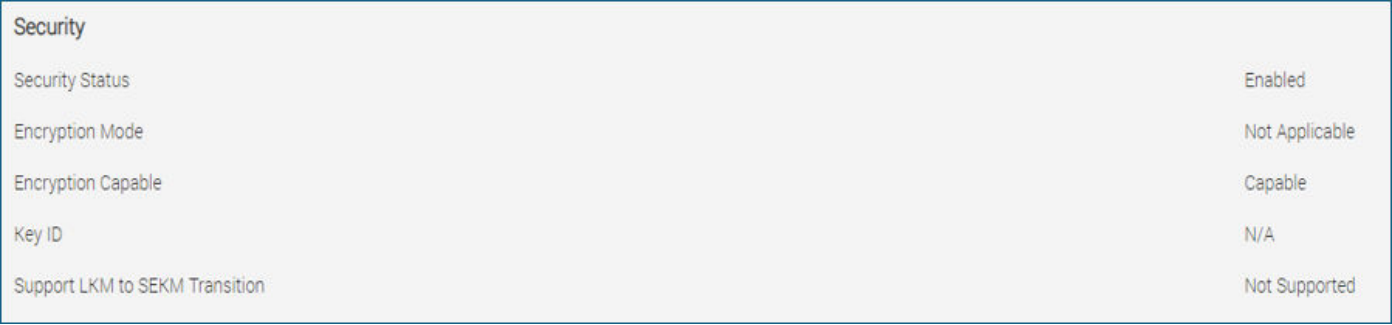


Figure 80. Security properties

NOTE: If the request to disable controller security fails, ensure you delete any volumes and PSID revert or cryptographic erase depending on the state of the drives.

For more information about PSID revert and cryptographic erase, see [PSID revert](#) and [Cryptographic erase](#).

Configure ROR-N1 using Redfish

Enable security on ROR-N1


Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"TargetFQDD": "ROR.Integrated.1-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Verify Security Status on ROR-N1

Command: GET

URI: /redfish/v1/Systems/System.Embedded.1/Storage/ROR.Integrated.1-1

Auth: Basic

Expected attributes if iLKM security is enabled on ROR-N1: "SecurityStatus": "Enabled"

Verify Encryption Status on SED behind ROR-N1

Command: GET

URI: /redfish/v1/Systems/System.Embedded.1/Storage/ROR.Integrated.1-1

Auth: Basic

Expected attributes if iLKM security is enabled on SED behind ROR-N1: "EncryptionStatus": "Unlocked"

Disable security on ROR-N1


Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"ControllerFQDD": "ROR.Integrated.1-1"}

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Configure ROR-N1 using RACADM

Enable security on ROR-N1

Run the following command to enable security on ROR-N1:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:ROR.Integrated.1-1 -enable
```

RAC1040: The storage configuration operation has been successfully accepted.

- To apply the configuration operation, create a configuration job, then restart the server.
- To create the required commit and reboot jobs, run the `jobqueue` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
ROR.Integrated.1-1 -r pwrcycle -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:ROR.Integrated.1-1
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:ROR.Integrated.1-1
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]
-----
```

Verify Security Status on ROR-N1

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get controllers -o
-p securitystatus
ROR.Integrated.1-1
SecurityStatus = Enabled
```

Verify Security Status on SED behind ROR-N1

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p securitystatus
Disk.Direct.0-0:ROR.Integrated.1-1
SecurityStatus = Secured
Disk.Direct.1-1:ROR.Integrated.1-1
SecurityStatus = Secured
```

Disable security on ROR-N1

NOTE: To disable security, stack cryptographic erase and disable security on the controller into a single job. An example using RACADM is shown below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Direct.0-0:ROR.Integrated.1-1
```

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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Direct.1-1:ROR.Integrated.1-1
```

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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:ROR.Integrated.1-1 -disable
```

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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
ROR.Integrated.1-1 -r pwrcycle -s TIME_NOW
```

RAC1024: Successfully scheduled a job.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_436090034200

Reboot JID: RID_436090035531

NOTE: A staged job must be scheduled for this operation. A host reboot is necessary for the security mode change to occur.

An example showing RACADM command to disable security on ROR-N1 as a standalone operation from RACADM is shown below.

Run the following command to disable security on ROR-N1:

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
security:ROR.Integrated.1-1 -disable
```

RAC1040: The storage configuration operation has been successfully accepted.

- To apply the configuration operation, create a configuration job, then restart the server.

- To create the required commit and reboot jobs, run the `jobqueue create` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
ROR.Integrated.1-1 -r pwr cycle -s TIME_NOW
```

NOTE: A staged job must be scheduled for this operation. A host reboot is required for the security mode change to occur.

RAC1024: Successfully scheduled a job.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:ROR.Integrated.1-1
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:ROR.Integrated.1-1
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]
```

Configure ROR-N1 using Server Configuration Profile

Enable security on ROR-N1

This SCP file displays only the SEKM configuration changes required to enable security on ROR-N1:

```
<Component FQDD="ROR.Integrated.1-1">
  <Attribute Name="SecurityStatus">Enabled</Attribute>
  <Component FQDD="Disk.Direct.0-0:ROR.Integrated.1-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
  <Component FQDD="Disk.Direct.1-1:ROR.Integrated.1-1">
    <Attribute Name="LockStatus">Secured</Attribute>
  </Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Disable security on ROR-N1

This SCP file displays only the SEKM configuration changes required to disable security on ROR-N1.

```
<Component FQDD="ROR.Integrated.1-1">
  <Attribute Name="SecurityStatus">Disabled</Attribute>
  <Component FQDD="Disk.Direct.0-0:ROR.Integrated.1-1">
    <Attribute Name="LockStatus">Encryption Capable</Attribute>
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
  <Component FQDD="Disk.Direct.1-1:ROR.Integrated.1-1">
    <Attribute Name="LockStatus">Encryption Capable</Attribute>
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Software Defined Persistent Memory

NOTE: A personality module is required to enable SDPM. This module can be applied to iDRAC by going to **Maintenance > System Update**.

NOTE: The **SEKM.1.VossSdpmReducedRebootSupport** attribute is available from supported interfaces and is read-only. If this value reports "Supported," security can be disabled on SDPM configurations with reduced server reboots.

Topics:

- [Configure SDPM using the iDRAC UI](#)
- [Configure SDPM using Redfish](#)
- [Configure SDPM using RACADM](#)
- [Configure SDPM using Server Configuration Profile](#)

Configure SDPM using the iDRAC UI

1. Start iDRAC using any supported browser.
2. On the iDRAC UI, click **Dashboard > Configuration > BIOS Settings > Memory Settings > Persistent Memory**.
3. To enable SDPM, select any nonzero value from the **SDPM Default Memory Size** dropdown list, then click **Apply**. This value is listed under **Pending Value**. Values vary based on system configuration. To disable SDPM, select **0GB**.
4. Enable **Sanitize All NVDIMMs**, then click **Apply**. This value is listed under **Pending Value**.

NOTE: You must manually enable the **Sanitize** operation. SDPM will be initialized to the selected size after the **Sanitize All NVDIMMs** operation.

NOTE: SDPM Current Size is read-only from all supported interfaces.

NOTE: When iDRAC is in SEKM mode with SDPM enabled, VOSS drives are automatically secured regardless of the Auto Secure setting on iDRAC. VOSS drives can still be manually secured without a server reboot, but only from [Redfish](#) or [RACADM](#) interfaces.

▼ Persistent Memory

	Current Value	Pending Value
Sanitize All NVDIMMs	Disabled ▼	Enabled

▼ Software Define Persistent Memory

	Current Value	Pending Value
SDPM Current Size	0GB (Disabled)	
SDPM Default Memory Size	0GB (Disabled) ▼	160GB
SDPM Vault Drive 0 path B/D/F/P	536870912	
SDPM Vault Drive 1 path B/D/F/P	553648128	
SDPM Vault Drive 2 path B/D/F/P	570425344	
SDPM Battery 1	Present	
SDPM Battery 2	Present	

Apply

Discard

Figure 81. Persistent memory

5. Select **Apply and Reboot** on the **Bios Settings** page.

- > System Profile Settings
- > System Security
- > Redundant OS Control
- > Miscellaneous Settings

Apply And Reboot

At Next Reboot

Discard All Pending

Figure 82. BIOS settings

6. Go to the **Job Queue** to view the scheduled job.
7. After the server is restarted, the BIOS configuration job is run in the **Automated Task Application** mode to apply the selected settings. The server automatically restarts.
8. After the POST or Collecting Inventory operation completes, ensure that the job ID has been marked “Completed” on the Job Queue page.

Job Queue			
<div><div><div></div></div><div>Delete</div></div>			
<input type="checkbox"/>	ID ▼	Job	Status
<div><div><div></div></div><div>+</div></div> <input type="checkbox"/>	JID_818619816924	Configure: BIOS.Setup.1-1	Completed (100%)

Figure 83. Job queue

9. On the iDRAC UI, click **Dashboard > Storage > Overview > Physical Disks**.

10. Verify the security status for VOSS drives.

<input type="checkbox"/>	Status	Name	State	Slot Number	Size	Bus Protocol	Media Type	Hot Spare	Security Status	Encryption Capable	
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	NVMe 1	Online	1	447.13 GB	PCIe	SSD	No	Not Capable	Not Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	PCIe SSD in Slot 8 in Bay 1	Ready	8	1788.5 GB	PCIe	SSD	Not Applicable	Not Capable	Not Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VOSS PCIe SSD in SL 11 Index 0	Ready	NA	894.25 GB	PCIe	SSD	Not Applicable	Secured	Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VOSS PCIe SSD in SL 11 Index 1	Ready	NA	894.25 GB	PCIe	SSD	Not Applicable	Secured	Capable
+	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VOSS PCIe SSD in SL 11 Index 2	Ready	NA	894.25 GB	PCIe	SSD	Not Applicable	Secured	Capable

Figure 84. Security status

NOTE: An additional server power-cycle operation may be required to secure VOSS drives.

NOTE: To disable security on a supported VOSS SED, you must perform a PSID revert or cryptographic erase operation depending on the state of the drive.

For more information about PSID revert and cryptographic erase, see [PSID revert](#) and [Cryptographic erase](#).

Configure SDPM using Redfish

Enable SDPM

NOTE: This step can be skipped if the SDPM Current Size already reports a nonzero value.

Command: PATCH

URI: /redfish/v1/Systems/System.Embedded.1/Bios/Settings

Header: content-type application/json

Auth: Basic

Body:

```
{"@Redfish.SettingsApplyTime": {"ApplyTime": "OnReset"},  
"Attributes": {"SdpmDefaultSize": "SdpmMem32",  
"NvdimFactoryDefault": "NvdimFactoryDefaultEnable"}}
```

NOTE: Supported values for **SdpmDefaultSize** vary based on system configuration.


NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Enable security on VOSS SED

Command: POST

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

Header: content-type application/json
Body: {"TargetFQDD": "VOSS.SL.11-2"}

 **NOTE:** This job runs in real-time without a server reboot. In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Verify SDPM current size


Command: GET
URI: /redfish/v1/Systems/System.Embedded.1/Bios?\$select=Attributes/
SdpmCurrentSize
Header: content-type application/json
Auth: Basic

Verify attribute SdpmCurrentSize

Verify Encryption Status on VOSS SED


Command: GET
URI: /redfish/v1/Systems/System.Embedded.1/Storage/VOSS.SL.11-C/Drives/
VOSS.SL.11-2?\$select=EncryptionStatus
Auth: Basic
Expected attributes if iLKM security is enabled on VOSS SED: "EncryptionStatus": "Unlocked"

Disable SDPM

 **NOTE:** This step can be skipped if the SDPM Current Size already reports zero.

Command: PATCH
URI: /redfish/v1/Systems/System.Embedded.1/Bios/Settings
Header: content-type application/json
Auth: Basic
Body:

```
{"@Redfish.SettingsApplyTime": {"ApplyTime": "OnReset"},  
"Attributes": {"SdpmDefaultSize": "SdpmMem0", "NvdimmFactoryDefault":  
"NvdimmFactoryDefaultEnable"}}
```

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Configure SDPM using RACADM

Enable SDPM


 **NOTE:** This step can be skipped if the **SDPM Current Size** already reports a nonzero value.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set
BIOS.SdpmSetting.SdpmDefaultSize SdpmMem32
```

RAC1017: The object value has been successfully modified, and the change is in a pending state.

- To apply a modified value, create a configuration job and reboot the system.
- To create the commit and reboot jobs, use the `jobqueue` command.
- For more information about the `jobqueue` command, see [RACADM help](#).

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set
BIOS.PersistentMemorySetting.NvdimmmFactoryDefault NvdimmmFactoryDefaultEnable
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
BIOS.Setup.1-1 -r pwr cycle -s TIME_NOW
```

 **NOTE:** A staged job must be scheduled for this operation. A host reboot is required to set the SDPM current size.

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.


Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:BIOS.Setup.1-1
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]
```

Enable security on VOSS SED

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
encryptpd:VOSS.SL.11-0
```

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

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 the `jobqueue` command, run the `racadm help jobqueue` command.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
VOSS.SL.11-0 --realtime -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384841257680

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: VOSS.SL.11-0
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: VOSS.SL.11-0
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]
-----
```


Verify SDPM current size

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get Bios.SdpmSetting
[Key=BIOS.Setup.1-1#SdpmSetting]
#SdpmBbu1Pres=Present
#SdpmBbu2Pres=Present
#SdpmCurrentSize=SdpmMem0
SdpmDefaultSize=SdpmMem0
#SdpmVaultDrivePath0=536870912
#SdpmVaultDrivePath1=553648128
#SdpmVaultDrivePath2=570425344
```

Verify Security Status on VOSS SED

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage get pdisks -o -p
securitystatus
VOSS.SL.11-0
SecurityStatus = Secured
VOSS.SL.11-1
SecurityStatus = Secured
```

Disable SDPM

 **NOTE:** This step can be skipped if the SDPM Current Size already reports zero.

RAC1017: The object value has been successfully modified, and the change is in a pending state.

- To apply a modified value, create a configuration job and reboot the system.
- To create the commit and reboot jobs, use the `jobqueue` command.

- For more information about the `jobqueue` command, see [RACADM help](#).

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set
BIOS.PersistentMemorySetting.NvdimmmFactoryDefault NvdimmmFactoryDefaultEnable
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
BIOS.Setup.1-1 -r pwrccycle -s TIME_NOW
```

NOTE: A staged job must be scheduled for this operation. A host reboot is required to set the SDPM current size.

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:BIOS.Setup.1-1
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]
-----
```

Configure SDPM using Server Configuration Profile

Enable SDPM

This SCP file displays only the configuration changes required to enable SDPM:

```
<Component FQDD="BIOS.Setup.1-1">
<Attribute Name="NvdimmmFactoryDefault">NvdimmmFactoryDefaultEnable</Attribute>
<Attribute Name="SdpmDefaultSize">SdpmMem32</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Disable SDPM

This SCP file displays only the configuration changes required to disable SDPM:

```
<Component FQDD="BIOS.Setup.1-1">
<Attribute Name="NvdimmmFactoryDefault">NvdimmmFactoryDefaultDisable</Attribute>
<Attribute Name="SdpmDefaultSize">SdpmMem32</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Cryptographic Erase

Topics:

- [Overview](#)
- [Cryptographic Erase using the iDRAC UI](#)
- [Cryptographic Erase using Redfish](#)
- [Cryptographic Erase using RACADM](#)
- [Cryptographic Erase using Server Configuration Profile](#)

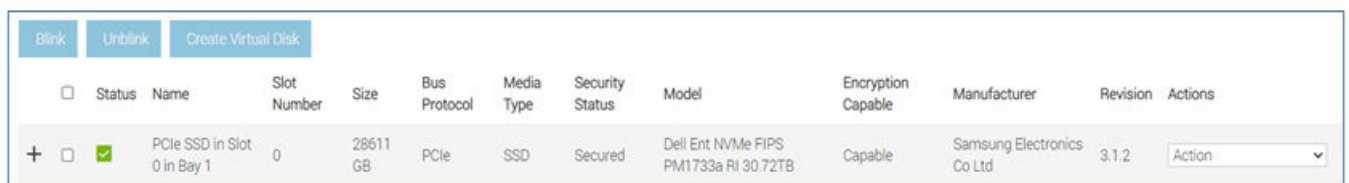
Overview

Cryptographic erase permanently deletes data on encryption-capable drives and resets security attributes. It works with CPU-attached NVMe and SEDs linked to PERC, HBA, BOSS-N1, ROR-N1, and M.2 SEDs in the SDPM solution. For more on Instant Scramble Erase (ISE), see [Instant Scramble Erase](#).

- NOTE:** If Auto Secure is enabled, CPU-attached NVMe SEDs secure again on the next boot. Disable Auto Secure before erasing a SED. This does not apply to drives behind BOSS-N1, ROR-N1, or SDPM solution. If security is enabled on the controller, drives behind BOSS-N1 and ROR-N1 will always auto-secure.
- NOTE:** For cryptographic erase to work, the drive cannot be in a RAID volume. If using PERC, BOSS-N1, or ROR-N1, delete the volume first.
- NOTE:** Schedule a staged job for secured CPU-attached NVMe and SEDs behind BOSS-N1 and ROR-N1.

Cryptographic Erase using the iDRAC UI

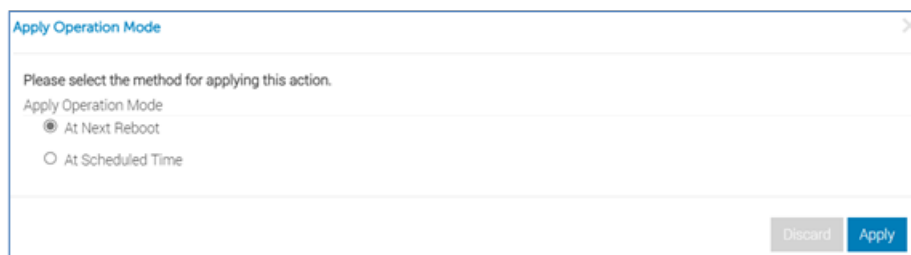
1. Start iDRAC using any supported browser.
2. On the iDRAC UI, click **Dashboard > Storage > Physical Disks**.
3. From the **Actions** drop-down menu of the supported drive, select the **Cryptographic Erase** option.



	Status	Name	Slot Number	Size	Bus Protocol	Media Type	Security Status	Model	Encryption Capable	Manufacturer	Revision	Actions
+	<input checked="" type="checkbox"/>	PCIe SSD in Slot 0 in Bay 1	0	28611 GB	PCIe	SSD	Secured	Dell Ent NVMe FIPS PM1733a RI 30.72TB	Capable	Samsung Electronics Co Ltd	3.1.2	Action

Figure 85. Physical disk options

4. Select **At Next Reboot** and click **Apply**.



Apply Operation Mode

Please select the method for applying this action.

Apply Operation Mode

☒ At Next Reboot

☐ At Scheduled Time

Discard Apply

Figure 86. Apply Operation Mode

5. Go to the **Job Queue** to view the scheduled job.

- Restart the server to run the configuration job.
- After restarting the server, the configuration job runs in the **Automated Task Application** mode to perform cryptographic erase on the selected drive.
- After the POST or Collecting Inventory operation completes, ensure that the job ID has been marked "Completed" on the **Job Queue** page.

Cryptographic Erase using Redfish

NOTE: Specify your supported SED FQDD in the URI below.

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {}

NOTE: You must pass in an empty body.

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

Cryptographic Erase using RACADM

Specify your supported SED FQDD in the commands below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Bay.12:Enclosure.Internal.0-1
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.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
Disk.Bay.12:Enclosure.Internal.0-1 -r pwr cycle -s TIME_NOW
```

RAC1024: A job has been successfully scheduled.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure:Disk.Bay.12: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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
```

```

Job Name=Configure:Disk.Bay.12: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]
-----

```

NOTE: The example above is performing cryptographic erase on a CPU attached NVMe SED. If you are performing cryptographic erase on a drive behind a storage controller, you must pass in the supported drive FQDD to the cryptographic erase command, then pass in the storage controller FQDD to create a job.

An example of a supported SED behind BOSS-N1 is shown below.

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
cryptographicerase:Disk.Direct.1-1:BOSS.SL.12-1

```

RAC1040: Successfully accepted the storage configuration operation.

```

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
BOSS.SL.12-1 -r pwr cycle -s TIME_NOW

```

RAC1024: Successfully scheduled a job.

- Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_384818826920

Reboot JID: RID_384818827401

```


C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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 P@ssw0rd --nocertwarn jobqueue view -i
JID_384818826920
----- JOB -----
[Job ID=JID_384818826920]
Job Name=Configure: BOSS.SL.12-1
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]
-----

```

Cryptographic Erase using Server Configuration Profile

This SCP file displays only the SEKM configuration changes required to erase supported drives:

NOTE: For CPU attached NVMe and VOSS SEDs, set **PCleSSDsecureErase** to “True.”

 **NOTE:** For SEDs behind PERC, BOSS-N1, and ROR-N1, set `Cryptographic Erase` to "True."

```
Component FQDD="Disk.Bay.18:Enclosure.Internal.0-2">
  <Attribute Name="PCIeSSDsecureErase">True</Attribute>
</Component>
<Component FQDD="Disk.Direct.0-0:BOSS.SL.12-1">
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
<Component FQDD="VOSS.SL.11-0">
  <Attribute Name="PCIeSSDsecureErase">True</Attribute>
</Component>
<Component FQDD="Disk.Direct.0-0:ROR.Integrated.1-1">
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

PSID Revert

Topics:

- [Overview](#)
- [PSID revert using the iDRAC UI](#)
- [PSID revert using Redfish](#)
- [PSID revert using RACADM](#)
- [PSID revert using Server Configuration Profile](#)

Overview

Use PSID revert when iDRAC cannot unlock a drive that is secured by an authentication key. This feature permanently erases all user data, making the drive available for resecuring. To access data, unlock the drive on the original system.

This feature works on CPU-attached NVMe and SEDs behind HBA, BOSS-N1, ROR-N1, and SDPM. For PERC-attached SEDs, use the legacy cryptographic erase instead of PSID revert.

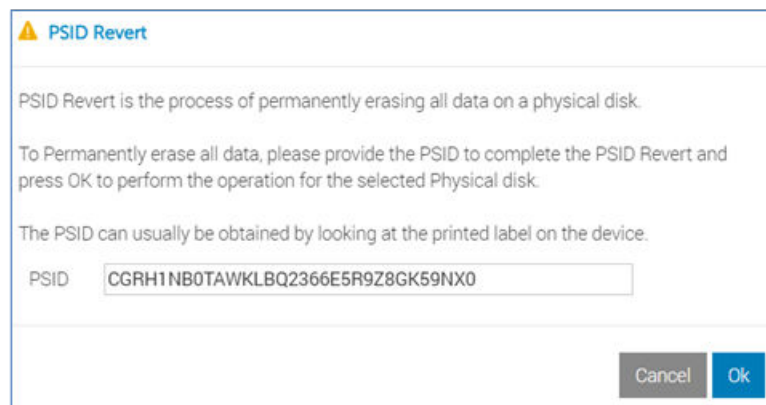
Users can select an individual SED and perform a PSID revert operation by using the methods below.

NOTE: The PSID is printed on the physical label of the drive and is not displayed in iDRAC drive inventory.

NOTE: This operation can be performed in real-time without a server reboot.

PSID revert using the iDRAC UI

1. Start iDRAC using any supported browser.
2. Go to the **iDRAC Dashboard > Storage > Physical Disks**.
3. From the **Actions** dropdown for your supported drive, select the **PSID Revert** option.



PSID Revert

PSID Revert is the process of permanently erasing all data on a physical disk.

To Permanently erase all data, please provide the PSID to complete the PSID Revert and press OK to perform the operation for the selected Physical disk.

The PSID can usually be obtained by looking at the printed label on the device.

PSID

Figure 87. PSID Revert option

4. Select **Ok** to add the pending operation for the selected disk.

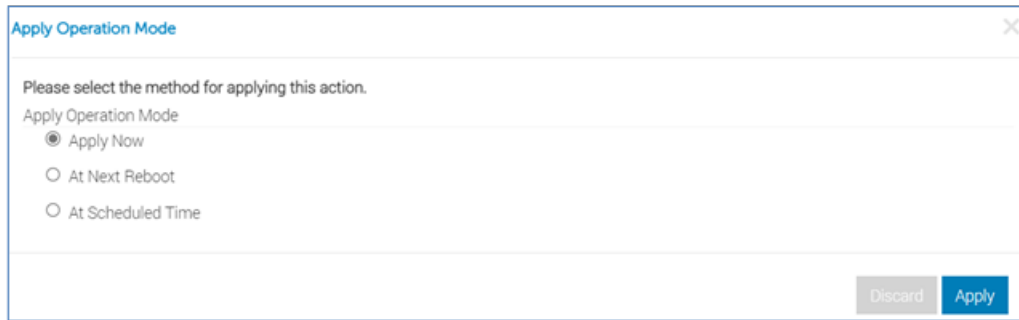


Figure 88. Apply Operation Mode

5. Select **Apply Now**, then click **Apply** to run the operation.
6. Go to the **Job Queue** to monitor the status of the job and ensure it has been marked "Completed."

PSID revert using Redfish

NOTE: Specify your supported SED FQDD and PSID in the URI below.

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"DriveFQDD": "Disk.Bay.12:Enclosure.Internal.0-1", "PSID": "CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0"}

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

PSID revert using RACADM

NOTE: Specify your supported SED FQDD in the commands below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage cryptographicerase:Disk.Bay.12:Enclosure.Internal.0-1 -psid CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0
C:\>racadm -r 192.168.0.120 -u P@ssw0rd -p P@ssw0rd --nocertwarn jobqueue create Disk.Bay.12:Enclosure.Internal.0-1 --realtime -s TIME_NOW
```


NOTE: The example above performs a PSID revert on a CPU attached NVMe SED. If you are performing a PSID revert on a drive behind a storage controller, you must pass in the supported drive FQDD to the PSID revert command, and then pass in the storage controller FQDD to create a job.


An example of a supported SED behind BOSS-N1 is shown below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage cryptographicerase:Disk.Direct.1-1:BOSS.SL.12-1 -psid CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create BOSS.SL.12-1 --realtime -s TIME_NOW
```

PSID revert using Server Configuration Profile

This SCP file displays only the SEKM configuration changes required to PSID revert supported drives:

 **NOTE:** For CPU attached NVMe and VOSS SEDs, set PCIeSSDsecureErase to “True.”

 **NOTE:** For SEDs behind BOSS-N1 and ROR-N1, set Cryptographic Erase to “True.”

```
Component FQDD="Disk.Bay.18:Enclosure.Internal.0-2">
  <Attribute Name="PCIeSSDsecureErase">True</Attribute>
<Attribute Name="PSID">CGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0</Attribute>
</Component>
<Component FQDD="Disk.Direct.0-0:BOSS.SL.12-1">
  <Attribute Name="Cryptographic Erase">True</Attribute>
<Attribute Name="PSID">DGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0</Attribute>
</Component>
<Component FQDD="VOSS.SL.11-0">
  <Attribute Name="PCIeSSDsecureErase">True</Attribute>
<Attribute Name="PSID">EGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0</Attribute>
</Component>
<Component FQDD="Disk.Direct.0-0:ROR.Integrated.1-1">
  <Attribute Name="Cryptographic Erase">True</Attribute>
<Attribute Name="PSID">FGRH1NB0TAWKLBQ2366E5R9Z8GK59NX0</Attribute>
</Component>
```

1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked “Completed.”

PERC LKM to SEKM Transition

Topics:

- [Overview](#)
- [PERCM LKM to SEKM transition using the iDRAC UI](#)
- [PERC LKM to SEKM transition using Redfish](#)
- [PERC LKM to SEKM transition using RACADM](#)
- [PERC LKM to SEKM transition using Server Configuration Profile](#)

Overview

The PERC LKM to SEKM migration feature provides PERC LKM users with the ability to transition to SEKM once it is enabled on iDRAC. This enhancement ensures a seamless and secure transition process.

A new property, `SupportsLKMtoSEKMTransition`, has been added. A value of "Yes" indicates that PERC supports the transition from LKM to SEKM. SEKM must be enabled on iDRAC before requesting a PERC LKM to SEKM transition. Users can request this transition through any iDRAC interface. For security reasons, the PERC LKM passphrase is required when requesting the transition.

If using PERC 11 or older, a staged job must be scheduled for this operation. For PERC 12 or newer generations, a real-time job can be initiated. Once PERC is in SEKM mode, transitioning back to LKM mode is not allowed. Also, the PERC LKM to SEKM transition is not allowed while the system is in lockdown mode.

PERCM LKM to SEKM transition using the iDRAC UI

1. Start iDRAC using any supported browser.
2. Go to the **iDRAC Dashboard > Storage > Controllers**.
3. Select the **Actions** dropdown for your supported PERC, then click **Edit**.
4. Go to **Security**, then select **Secure Enterprise Key Manager** from the **Security** dropdown.

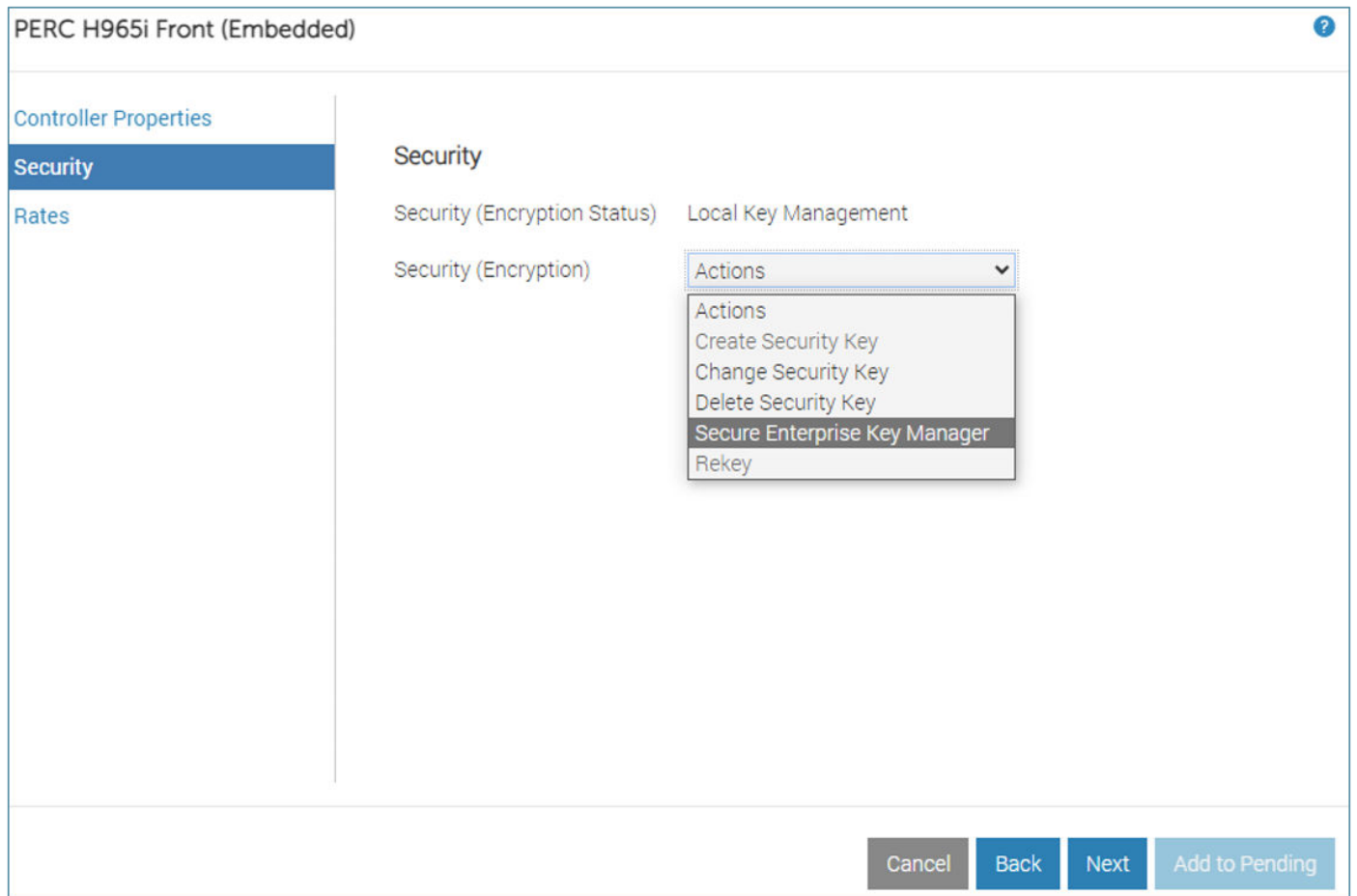


Figure 89. LKM to SEKM security

5. Click **Next**.
6. Enter your **Security Key Passphrase**.

PERC H965i Front (Embedded) ?

Controller Properties
Security
Rates

Security

Security (Encryption Status) Local Key Management

Security (Encryption)

Security Key Identifier test_ID

Security Key Passphrase*

Instruction: Provide the Local Key Management "Security Key Passphrase" to perform the LKM to SEKM transition.

Cancel
Back
Next
Add to Pending

Figure 90. Security passphrase

- Click **Add to Pending**.

✓ Pending Operation Created ✕

You have successfully created pending operation on Controller
PERC H965i Front (Embedded)

Order ▼	Component Type	Component Name	Operation
0	Controller	PERC H965i Front (Embedded)	Create Security Key

Apply Later
Apply Now
At Next Reboot
At Scheduled Time
Discard All Pending

Figure 91. Pending Operation

- Select **Apply Now** for PERC 12 and newer generations.
- Select **At Next Reboot** for PERC 11 and older generations.

i **NOTE:** The **Apply Now** option is not supported for this operation on PERC 11 and older generations.

i **NOTE:** If the **Apply Now** option is selected, the job runs in real-time without a server reboot. Once you go to the **Job Queue**, this job should be marked "Running."

- Ensure that this job has been marked "Completed."

PERC LKM to SEKM transition using Redfish

Command: POST

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

Header: content-type application/json

Auth: Basic

Body: {"Key": "Dell123!", "Mode": "LKM_TO_SEKM", "TargetFQDD": "RAID.SL.3-1"}

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

PERC LKM to SEKM transition using RACADM

NOTE: Use the same passphrase that was used to enable LKM on PERC.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn storage
setencryptionmode:RAID.Integrated.1-1 -mode SEKM -passphrase Dell123!
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --nocertwarn storage
setencryptionmode:RAID.Integrated.1-1 -mode SEKM -passphrase Test123
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn jobqueue create
RAID.Integrated.1-1 -s TIME_NOW -realtime
```

Verify the job status using the `racadm jobqueue view -i JID_XXXXXX` command.

Commit JID: JID_385106379901

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --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 P@ssw0rd --nocertwarn storage get controllers -o
-p encryptionmode,keyid
RAID.Integrated.1-1
```

```
EncryptionMode      =      Secure Enterprise Key Manager
KeyID                =      9DC2F2F0D42DDE89AD9FFD5F3B68239195FE32DF2F75BFB73B44BD61B7A01E39
```

PERC LKM to SEKM transition using Server Configuration Profile

This SCP file displays only the SEKM configuration changes required to transition from LKM to SEKM on PERC:

```
<Component FQDD="RAID.SL.1-1">
<Attribute Name="EncryptionMode">Secure Enterprise Key Manager</Attribute>
<Attribute Name="OldControllerKey">Dell123!</Attribute>
</Component>
```

1. Run the command to import this SCP file that is on an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

iDRAC Initiated KMS Key Purge

Topics:

- [Overview](#)
- [Configure Key Purge Policy using Redfish](#)
- [Configure Key Purge Policy using RACADM](#)
- [Configure Key Purge Policy using Server Configuration Profile](#)
- [Disable Key Purge on SEKM](#)

Overview

iDRAC purges unused keys at the Key Management Server (KMS) as part of SEKM. When iDRAC rekeys secured storage devices on the server, it generates a new key at the KMS each time. This can lead to a buildup of unused keys, especially with multiple iDRACs enabled for SEKM.

To manage this, iDRAC offers a policy setting to purge old unused keys at the KMS during a Rekey operation. Users can set the iDRAC attribute KMSKeyPurgePolicy to one of the following values:

- **Keep All Keys:** This is the default setting, where iDRAC leaves all keys on the KMS untouched.
- **Keep N and N-1 keys:** iDRAC deletes all keys at the KMS except the current (N) and previous key (N-1).

After a Rekey operation, iDRAC verifies the policy, purges keys accordingly, and logs a message to Lifecycle logs to indicate success or failure.

Here is an example of a Lifecycle log entry after a Rekey operation with the Purge policy set to "Keep N and N -1 keys":


Table 6. Lifecycle log entry example

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

Configure KMIP to delete keys

Enable this setting on CipherTrust Manager KMS to delete both the key and its metadata when iDRAC requests it. Without this setting, the key is deleted, but the key ID remains visible at the KMS.


Configure KMIP

☒ Enable hard delete 
☒ Auto Registration

Registration Token *

qaPpOzZ93m1XbXEx36ypjDf3nWl2gQa3T0


Figure 92. Configure KMIP

 **NOTE:** This setting is not required on other supported Key Management Servers.

Purge old keys

After setting the iDRAC key purge policy, iDRAC tags the keys it generates with the server service tag for identification and purging. For older keys without a service tag, users can enable the `KMSPurgeOldKeys` attribute. When enabled, iDRAC deletes all old keys without a service tag during a Rekey operation and then resets the attribute to "Disabled."

 **WARNING:** If users share keys between different iDRACs, or if keys from other iDRACs are in the same KMS Domain, all such keys are deleted.

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

Configure Key Purge Policy using Redfish

Command: PATCH

URI: `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1`

Header: `content-type application/json`

Auth: Basic

Body: `{"Attributes": {"SEKM.1.KMSKeyPurgePolicy": "Keep N and N-1 keys", "SEKM.1.KMSPurgeOldKeys": "Enable"}}`

Configure Key Purge Policy using RACADM

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --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 P@ssw0rd --nocertwarn set
idrac.sekm.kmspurgeoldkeys Enable
[Key=idrac.Embedded.1#SEKM.1]
Object value modified successfully

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get
idrac.sekm.kmspurgeoldkeys
[Key=idrac.Embedded.1#SEKM.1]
KMSPurgeOldKeys=Enable

C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get
idrac.SEKM.KMSKeyPurgePolicy
KMSKeyPurgePolicy=Keep N and N-1 keys
```

Configure Key Purge Policy using Server Configuration Profile

Enable Key Purge policy

This SCP file displays only the SEKM configuration changes required to configure the Key Purge Policy:


```
<Component FQDD="iDRAC.Embedded.1">
<Attribute Name="SEKM.1#KMSKeyPurgePolicy">Keep N and N-1 Keys</Attribute>
</Component>
```


1. Run the command to import this SCP file from an HTTP share.
2. Confirm that the SCP import job is marked "Completed."

Disable Key Purge on SEKM

When SEKM is disabled on iDRAC, it can leave unused keys at the KMS when SEKM is disabled. To address this, iDRAC allows the deletion of these keys.

The `-purgeKMSKeys` option has been added to the `racadm sekm disable` command, enabling users to purge keys at the KMS when SEKM is disabled. iDRAC checks this option, purges keys that are tagged with the server service tag, and logs the result. To delete old keys without a service tag, enable the `KMSPurgeOldKeys` attribute.

 **NOTE:** To purge old keys with SEKM already disabled, re-enable SEKM, then disable it using the `-purgeKMSKeys` option.

 **NOTE:** This setting is not available from the iDRAC UI.

Key Purge on SEKM disabled using RACADM

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sekm disable -purgeKMSKeys
```

SEKM0213: The SEKM disable operation is successful.

iDRAC Volatile Key Caching

Topics:

- [Overview](#)
- [Configure VKC using Redfish](#)
- [Configure VKC using RACADM](#)
- [VKC guidelines and limitations](#)

Overview

iDRAC Volatile Key Caching (VKC) provides an option for iDRAC to cache the SEKM authentication key in volatile memory. This feature is useful in scenarios where iDRAC cannot connect to the external Key Management Server (KMS) to fetch the key. It does not require a new license and is available with the existing SEKM license.

Prerequisites

- iDRAC Data Center or Enterprise license
- iDRAC SEKM license
- iDRAC firmware which supports SEKM VKC
- Supported storage devices updated to SEKM supported firmware
- SEKM enabled on iDRAC

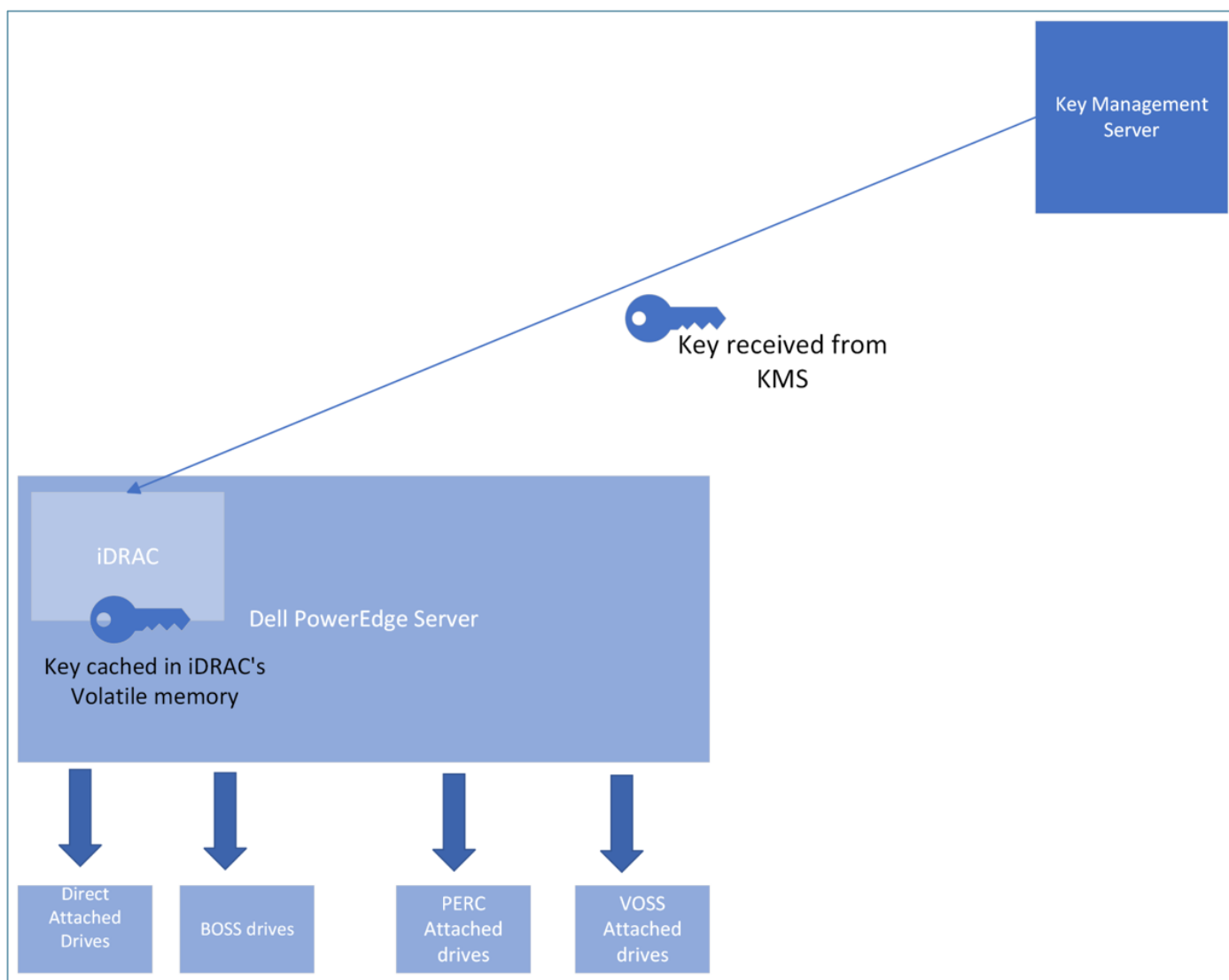


Figure 93. Solution architecture

Enable volatile key caching by setting `KeyCachingPolicy` on iDRAC. iDRAC fetches the key from the KMS, encrypts it with its Hardware Root Key and a random initialization vector, and stores it in volatile memory. This cached key unlocks drives when iDRAC cannot connect to the KMS. iDRAC always tries to connect to the KMS first. On host reboot, the cached key unlocks the secured devices. The key can unlock, secure, or erase a device but cannot rekey it. When rekeyed, iDRAC gets a new key from the KMS and caches it.

`KeyCachingPolicy` is available under the SEKM attributes group. This property can be set to define the key caching policy for SEKM. Here are the supported values for this attribute:

- **No Caching:** Default value
- **Cache in Volatile Memory**

`KeyCachingStatus` is available under the SEKM attributes group. This property can be checked to see if the key has been cached or not. Here are the supported values for this attribute:

- **Key Not Cached:** Indicates iDRAC does not have the key that is cached in volatile memory
- **Key Cached in Volatile Memory:** Indicates iDRAC has the key that is cached in volatile memory

Below are example Lifecycle (LC) log entries that are related to VKC:

Table 7. Lifecycle log examples

Key	Message
SEKM005	The SEKM setting KeyCachingPolicy is changed from "No Caching" to "Cache in Volatile Memory."
SEKM100	iDRAC has used the cached key because iDRAC could not connect to the Key Management Server.
SEKM101	iDRAC has deleted the cached key because either the SEKM or the key caching feature was disabled.
SEKM102	iDRAC has deleted the cached key because Key Management Server rejected a request to get the key.
SEKM103	iDRAC has successfully obtained the key e401a33e1a7e477391326baaa4bafb27d484eabf68e646ffbd69c4b95246a00c from the Key Management Server, and then locally cached it.
SEKM104	iDRAC is unable to cache the key e401a33e1a7e477391326baaa4bafb27d484eabf68e646ffbd69c4b95246a00c because iDRAC could not obtain the key from the Key Management Server.

Configure VKC using Redfish

Enable VKC

Command: PATCH

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Header: content-type application/json

Auth: Basic

Body: {"Attributes": {"SEKM.1.KeyCachingPolicy": "Cache in Volatile Memory"}}

Verify VKC attributes

Command: GET

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Auth: Basic

Response example:

```
{"SEKM.1.KeyCachingPolicy": "Cache in Volatile Memory"}
{"SEKM.1.KeyCachingStatus": "Key cached in Volatile Memory"}
```

Disable VKC

Command: PATCH

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1

Auth: Basic

Body: {"Attributes": {"SEKM.1.KeyCachingPolicy": "No caching"}}

Configure VKC using RACADM

Enable VKC

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set
idrac.sekm.KeyCachingPolicy "Cache in Volatile Memory"
[Key=idrac.Embedded.1#SEKM.1]
Object value modified successfully
```

Verify VKC

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn get idrac.sekm
[Key=idrac.Embedded.1#SEKM.1]
AutoSecure=Disabled
#iLKMStatus=Disabled
IPAddressInCertificate=Enabled
KeyAlgorithm=AES-256
KeyCachingPolicy=Cache in Volatile Memory
#KeyCachingStatus=Key cached in Volatile Memory
#KeyCreationPolicy=Key per iDRAC
#KeyIdentifierN=e401a33e1a7e477391326baaa4bafb27d484eabf68e646ffbd69c4b95246a00c
#KeyIdentifierNMinusOne=
KMSKeyPurgePolicy=Keep All Keys
#SecurityMode=SEKM
#SEKMStatus=Enabled
#SupportStatus=Installed
```

Disable VKC

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn set
idrac.sekm.KeyCachingPolicy "No caching"
[Key=idrac.Embedded.1#SEKM.1]
Object value modified successfully
```

VKC guidelines and limitations

When **KeyCachingPolicy** is enabled, iDRAC automatically caches the key. A host reboot is not required and does not delete the cached key. The encrypted key is stored in the iDRAC's volatile RAM as part of the KMIP client's data segment, making it inaccessible to other processes within iDRAC or to iDRAC users, and it is not displayed by any interfaces. iDRAC deletes the cached key from volatile memory in the following scenarios:

- KeyCachingPolicy is disabled
- SEKM is disabled
- iDRAC can connect to the KMS but unable to fetch the key (for example, key that is deleted at KMS or modified key permission)
- Loss of power to server or iDRAC reset
- Systems erase

KeyCachingStatus is a read-only attribute and cannot be modified.

- VKC is supported only through RACADM or Redfish interfaces, and while SCP export will list key caching attributes, SCP import of these attributes is not supported. The cached key will no longer be available after an iDRAC reset. If the KMS is down once iDRAC comes back up from reset, any secured drives will become locked after a server reboot. To unlock the drives, iDRAC must reestablish a connection with the KMS and cache a new key.

All iDRAC actions related to key caching are available in Lifecycle logs. The SEKM103 message string references the key ID, not the actual key. A user can boot a system even when the connection to the KMS is not available if `KeyCachingPolicy` is enabled. However, if `KeyCachingPolicy` is disabled, the user cannot boot the system without a connection to the KMS.

Import Pre-Generated Host Certificate and Private Key into iDRAC using Redfish

Topics:

- [Overview](#)
- [Custom Certificate](#)
- [Custom PEM certificate](#)

Overview

SEKM_CUSTOM_CERT and SEKM_CUSTOM_PEM_CERT include a signed client certificate and private key. These certificates can replace SEKM_SSL_CERT, eliminating the need to generate a CSR for each iDRAC and allowing the same client certificate to be uploaded to multiple iDRACs.

NOTE: It is the system's administrator's responsibility to store and maintain the CSR since it is not stored on iDRAC.

NOTE: The KMS_SERVER_CA certificate must still be uploaded to iDRAC for a successful connection to your supported Key Management Server.

NOTE: SEKM_CUSTOM_CERT and SEKM_CUSTOM_PEM_CERT can only be imported from the Redfish interface.

You must generate a CSR and private key using OpenSSL. The workflow below demonstrates the process of creating a .p12 certificate bundle for SEKM_CUSTOM_CERT on a Linux system and importing the certificate using Redfish.

```
[root@localhost certs]# openssl genpkey -algorithm RSA -out privatekey.pem -aes256
.....+++++
.....+++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
[root@localhost certs]# openssl req -new -key privatekey.pem -out csr.pem
Enter pass phrase for privatekey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Texas
Locality Name (eg, city) [Default City]:Round Rock
Organization Name (eg, company) [Default Company Ltd]:Dell
Organizational Unit Name (eg, section) []:ISG
Common Name (eg, your name or your server's hostname) []:idrac-CP09511
Email Address []:tester@dell.com


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:P@ssw0rd
An optional company name []:Dell
[root@localhost certs]# cat signed_client_csr.pem privatekey.pem > certificate_and_private_key.pem
[root@localhost certs]# openssl pkcs12 -export -out client_certificate.p12 -in certificate_and_private_key.pem
Enter pass phrase for certificate_and_private_key.pem:
Enter Export Password:
Verifying - Enter Export Password:
[root@localhost certs]# openssl base64 -in client_certificate.p12 -out base64encoded
```

Figure 94. SEKM custom certificate

Take the contents of base64encoded and pass it into CertificateFile in the Redfish request body, as shown in the next section.

Custom Certificate

This section demonstrates how to install and view the custom SEKM certificate.

 **NOTE:** The certificate file in the request body can be generated using OpenSSL, which is shown in the previous section.

Upload certificate

Expected status code:	200 OK
Command:	POST
URI:	/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DelliDRACCardService/Actions/DelliDRACCardService.ImportCertificate
Header:	content-type application/json
Auth:	Basic
Body:	<pre>{ "CertificateType": "SEKM_CUSTOM_CERT", "CertificateFile": "MIILWQIBAzCCCx8GCSqGSIB3DQEHAaCCCxAEggsMMIILCDDCCBb8GCSqGSIB3DQEH BqCCBbAwggWsAgEAMIIFpQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIUf9J zX4eaasCAggAgIIFeMLhVO6jo0lndlRTnhDKkcE6s0cAPyXd3+NXs5noY+dU9yAy sOkfm+YSZOJDBdKHxqgbI83YjY80S7NzRpuaHexliIeQQaOHPEqs3s2v17EBIggH dsc32f2qt7+Wb4aHyORL10k5YW+FEAwVMV2isIt0K/Powrt97L3sAqhVHZrmwkDr m9HJqS6B2JVwaiOysYTWgJb/n6jcpqQBONbZtLkHNN6ESE/Pp438g/0j/6k0/jsJ oRAEUvjEuTaAZe58uAV9cBlSe6euinAOXYRHv5PHMQPkb+trFY/pWzTgGttB5WsX 6LskKQY5bnL84F02S72M7cvHLPkj4/wv7ttILCzFS6+ORTdkBY5JJtaD7/AW9RRW hAGV8AeZjwWGRKbZAWReebIBjeqGxuARYYgZpP9cB4FU/vuApKdH5336X+4PxLSs AE3rAMOE/zxyTbYv3s7S/2lNvrQxNiWv6BJxD/vxdmHANOUxb4bqgQcMNLMT0Q82 2C2a3hA/5+qfYhze/qSMPnRBRXwVDDmqZ0dUVAaWIFZLYU1flkJOkZgsnKP1JtwZ Q/BezVDYvnmDMkBCfak5V5fHzndVGQ9acsuNn0IKrua5poK/veCSu5arEZPWq7M9 NknJFMeU00/knY6+onYbgwIXVJ9WImZjYinwgVSqiom+bdL3ozXpWKByTybng1VZ rU/ii3+l9s4gJMQ9n/ZcgN8CD+amKUmden3D6CZ2ifVprhx37G0Rd5AP538Ew0x 1WntfEN2bLpbuH4tbOyFn/LL0OMnshfSxSR0PH4CJm6kB4soqRbuDKoKQKlytka +fzOoo6NULi7U/tppyhc3qT7z5Diq34+e0dPlCwRpy3zSjUr0ClyH3M5zaPGAavO w4Ec1OdshZlpFjixb+dI14hp7sErNhdDjZZK1NfW/xOXCcORoJjDyJ1hS8DwIg2n 63VEMwBY+U7FmGsdnqldKxvPE1X5LFGSQuq6+Yv23/jLa/yVaskxH1EzzGpr0jl 3/0GtKvObbqMp7rbWoAOM6NNIvmXPlnvQPKI4LSyGwdYmgRWUFXWE3fCL2nToT4 yEpl08PWVXSti+sQYwwO9+7Xx1bkiKvLRC7r6B0ZI2oNSJW/sFAsuKjahs9BkjEC agdKz+QAJ7tJuok+X7gToz0HhYrP4t9QE2WbV89eN9/BOj9i/OOcCuEox1NOuvyR yZcUuwvRptnPD3Rr2eG5+tSO/mPnBHkWS/gCcYkorrgMBfMYg2se9Kf3zpc9hTz 18R17labyZviGk2sFmfJ+b2mhyxqdbXjJGF7Z3r51L0tjGqY3L0yy6GHeQLtJ3k /XTfSOheRyE7fmP7UdBL0X05iJRaRC3nx+VANOXnu7Mq0LppRYjFnlynD4EKI3r7 hPwAPzE1funkt/9tYlRUCX1JPnZ+/8pBphVT9kyGPYunB5DtfE447AQIEy+YrLd6y cYoj9jy5rffOYS/G0w8EzgcMWE5+NeyqThi3/pPVk7/B4WjwRYUeov3NpLuiLcma /LqjW1kBw/D0ci93HO+i2cXjM/4sqId5bcgrMfHOSsd21ljMba1hgyIwVE069Pre iWhdAvml0TXIxnAgCrexleakVw5W3Y81xDZWY6valG105XbQ2k7SDT2zjjLsBimh liF4o+rXUYsFviLsvuRrOR9TdZBWR6E5f/TkMDp/ahbvIM3+KWommP9Wct62zgun NjHEov63J+3SQSc8iyvcvEFLQZGRneEx/haGkDRD/AzmXsN2FtjF3s0o/BjjIp0e tJ2yJZmYuy23l6E/RfRf1AkSLw5kgdZgT0y0DMDOnM4mDP4Ah1Sb5uBoqqbd5mlo 7/LdjBRIH03NwwJfL9dniLkYDnRCMIIFQQYJKoZIhvcNAQcBoIIFMgSCBS4wggUq MIIFJgYlKoZIhvcNAQwKAQKgggTuMIIE6jAcBgoqhkiG9w0BDAEDMA4ECNtnIm14 RylgAgIIAASCBMhNWTgLoCm3Dm5Tj1fZ+Ip+3Sz+c3LYagscYAqXUaQMAUcayzNf Q5JjSdd4ngSyOp/RKOEK8p6PoF3ZI+cQ432afCszLu8xj7CdEaTVXiBIEQIfPZPg e5zLNR5sweAlgNook6Mnwftiq4gNufjkwDJH3VPNe53R2EG7FkgfOQl9MntBBN6B kpRtZVL1surV3uJpL94iSrDYk+8k45IuCOQ5nYPyL7/vkBsux1APR+qd/L0wz3ss aF+liDqC6hT3ncmK+aia2EYSWGv4H/Q3ClVyrGwTxb68oEfmab6M60gdXGW2X3+L Us1BYtGiYNOJKg/wRMIEZV08JULzubG3IDJ87P+TD2un8lQLSUelidJW3HsZNWNn /AuzT9PqYgJruPtI32PRFgQnmmd/b0qxnP+VNAJNDEOpGfi9MzteE7IYICAMc9m 3ysaeaklNuKki4nbXBHfsuM1ff9+f9v2bPKODhFgyo0FBjTm02x/cyM4uiUUBXXb B+9//jEE+jEbZqVhlpYp70/qltdmttFiyIEGkWHZiD3FaHO+ab1v8y3aIw4CGFNQ</pre>

```
yOkpdW9FOdv7CaTPLVh9WyXa/ng7Ew14VZI9aOAGtACXXYqPkK2NjrzPRVd4XFYC
5JWlXbITYG9nWW1SsHjmlXnxJOFObvqhItL+zEub79SxyulB9w4pbsjuly/OaXH/
V2XdN6ennlyqymh/iwF5ngT6he8deqCeHZQpKbopLS8SGhlwo4++/TWckbwO9LTT
3apxVgUKPf+fBBqWEZuu2/M4L2km16Hq33MvKdE/AE1Yub+Oto59kx4KawgBUjlo
t86BdJqYy0jGKf/tEgVgyQ/hlc9MqSoileG99hNvDPccb5+lgd6CN57nDXGmJrXV
wkGS0oq+RdG4D+ghxDJ+rjlfowl0I1mIPE20FTq97dpnEZJ4S/s9EUiRoJWmk5Xy
mC+5U+IYD9uff3bpfB46QXeHoWn1vhzr2+HcNQofMPgGK+pHVDcdQXt9qkPegkQ2
W/fsz5BMOqKD8LMihpWSjgf2i/fuFsD4Ikyc8KijXq1+kzkbP/AJuzvsc006IhEH
x4DmHwBwVRit0Shz68QCS2j7GAvYhUjSABRg1YQk2htipwgBkXmfB11Jw8AMoz6r
fPEb3tBoarRlqajhSiA0INF/2h9+YB4Q1Evflg7bybeaq4hmDa1il200A4Eoqlv3
eg1AXcSXGPsDQcALSPrHYAILZ9gAv63J1eBmrRgDJLJURCKrbWoWmCz72847N2LZ
uy0HwSE9rEB44J2g4Dv8D2xHprNTdx+XlFZjfcYnsb6Jx1UtQm4Wwdl3Ps/Zz5F9
3ATT+mRonuDbOGqbAjG8E3SW/GvVbza7DoX+gmIGsJbz+oiJBjeS1Dpc8ID/Ks3b
tlaV4IHZGDvpTvtbYrjagBby6qwxZwuzUjebJAvKwpBmPGukzTJG3LTiNb5a9bU
vfMrJDFrvHggn8EJRMbBhYKS/2RM+sL2JyqfjTAn6BcfLjh8oc5ddK3Iz3h8f4b
6910crnW5y6PPoi/mEpKFAV/FHRvid3Pl9u9gvGDIkUT+TSWlXMC8J9zrcPCAvkJ
rs/Sji/c40tutMlwlPoHzJ6uEQW3aKQwsHBYiShb06tz0E4xJTAjBgkqhkiG9w0B
CRUxFgQUfomfKgGgPP02k9rLy5kyhjmkwMTAhMAkGBSsOAwIaBQAIEFPgBsOyk
DsLC5mk65Y7i12ww5B1oBAjd7AVglUoauAICCAA=", "Passphrase": "P@ssw0rd"}
```

View certificate

NOTE: The custom SEKM certificate can only be viewed from the RACADM interface using the command below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sslcertview -t 6
Serial Number          : 0A
Subject Information:
Country Code (CC)      : US
State (S)              : TX
Locality (L)           : Round Rock
Organization (O)        : Dell
Organizational Unit (OU) : Validation
Common Name (CN)       : iDRAC-12345

Issuer Information:
Country Code (CC)      : US
State (S)              : TX
Locality (L)           : Round Rock
Organization (O)        : Dell
Organizational Unit (OU) : Solutions Group
Common Name (CN)       : Certificate Authority
Valid From              : Apr 29 17:00:08 2024 GMT
Valid To                : Apr 29 17:00:08 2025 GMT
```

Custom PEM certificate

This section demonstrates how to install and view the custom SEKM PEM certificate.

NOTE: The process to create the custom PEM certificate is similar to that of the custom certificate. However, instead of converting to PKCS12, you can directly use the PEM content in the request body as shown below.

NOTE: A passphrase is optional.

Upload certificate

Expected status code:	200 OK
Command:	POST
URI:	/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DelliDRACCardService/Actions/DelliDRACCardService.ImportCertificate

Header: content-type application/json

Auth: Basic

Body:

```
{"CertificateType": "SEKM_CUSTOM_PEM_CERT",
 "CertificateFile": "-----BEGIN CERTIFICATE-----
MIIFSzCCAzOgAwIBAgIRAPijjq2DNNkNM69MLxaTUdYwDQYJKoZIhvcNAQELBQAw
WjELMAkGA1UEBhMCVVMxMzA5BjBGA1UEAwwbZm9udCBkdDQTAeFw0y
DgYDVQQKEwdHbWVhbnRvMR0wGAYDVQQDEwFLZX1tZW50cmUgUm9vdCBkdDQTAeFw0y
NDA0MTcxNDA5MjhaFw0yNTA0MTgxNDA5MjhaMIGTMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCMVFGxZARBgNVBAClJvdW5kIFJvY2sIZAhBgNVBAoTGlZhbHVlZCBE
YXRhRG9tYWluIGN1c3RvbWVwYmRYwFAYDVQQDEw1pZHZhYy1uZ3gwM1NUMSUwIwYJ
KoZIhvcNAQkBDDBZzdXB3J0QGRhdGFkb21haW4uY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg21heHVHLSaKrsaQXAY8ZuoRFmdgbfoSZd2RKQyhe
kCrkegUOOExADEJJDO4V6sEz/s5re/YbIoBhHPgHCkqJ0LfgXLBjrr0SnSuw1Vv
nW5ffRuf9TKRg3TqBgr68aiyXgHdeXBjvJAoK7w1wiFLYtanmgxu6FCEi4eyfYZr
dUqA1Qhm+1LXQnRjp3o+kRrajRizjHhf2GK53OrD8AdZKwThtgBJ1k26ba/ynee
CswcfhPqiMkteQCHUPpxhDvUKXWrvUYDf/LTpXnhLVcLA/fJsqYrew10mXRq5nhK
6ZytvE0Zjh090GZ1GFs4k/MScj9RZA+arTUYMazRPAhKtwIDAQABo4HRMIHOMA4G
A1UdDwEB/wQEAwIDiDATBgNVHSUEDDAKBggrBgEFBQcDAjAMBGNVHRMBaf8EAjAA
MB8GA1UdIwQYMBAAAFBjEjD1OTc+PjJMjCgzmE2PeXaBCMBGGA1UdEQQRMA+CDTEw
MC42NC40MC4yMzMwXgYDVR0fBFcwVTBToFGgT4ZNAHR0cDovL2NpcGhlcnRydXN0
bWFuYWdlci5sb2NhbC9jcmxzL2I0YzkwMDc4LTRjMjQtdNDYxNy1hNGY1LTlTYxNGE5
NjYwNTY3MS5jcmwwDQYJKoZIhvcNAQELBQADggIBAHHr9udux97beCCfzYh48X++
VSgJ9EGPj14e6KUU6r9bK5f7Q3oTfkNyctuC+8zPz7vDb1QQ1SXA3/xgK2LGisjo
98pprjlGlu+WXcX/7T+/kDY4b8njxr3C3GHGcCkjpgfSSXDbXJctOhE/cgHCqh1
UdE5Q0LVB2HiVptctyQ+7CdTI3hVj8mbOq8A47aGaFhzszCeM2LinKrEm1CwsKpK
9s0nO30/1+AIRpvrRrL1lks7LiCgA9jjveb2KXL0Z9+n3XRYKZxUt7BVk40LR2wm
XZ71LLrhiMwrisXMOrotLNBWJbfBj5hJMuU3oilDelvHEBwH8tLyAL16Zw6Rwter
nHBQLQIwpIv9UjUeQ69mp6P8f3W6iR+OpYzbxHneyUwxQAN+tiq0gdd5ZcD7Nflw
6pV8wMF7+i3Eu6gUA+5H7TRreka6CxWmU5gPLxAmJQ3yIDSKcFyJjU7H0Uar/h6k
2vprf76NGxcm44v/trXRbB3/zQdMWiFm4BQzXNHXDqPva7di2jXzhTBLADf4meLc
Hz9UHYwkJO3UP/MTp85AuDpNuL9Z88lvz/M/zJAFdRC19PqWFM90ZBs97qwdj0BE
lWvzWBAEDnMVOKA12Gro6mGQrgLVMRF9y4rjVHiES01E3rhOntp7J9LyXAZBvGg0
K7UQWkZXqYKrj+eYQQQe
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAg21heHVHLSaKrsaQXAY8ZuoRFmdgbfoSZd2RKQyhekCrkegU
OOExADEJJDO4V6sEz/s5re/YbIoBhHPgHCkqJ0LfgXLBjrr0SnSuw1VvnW5ffRuf
9TKRg3TqBgr68aiyXgHdeXBjvJAoK7w1wiFLYtanmgxu6FCEi4eyfYZrdUqA1Qhm
+1LXQnRjp3o+kRrajRizjHhf2GK53OrD8AdZKwThtgBJ1k26ba/yneeCswcfhPq
iMkteQCHUPpxhDvUKXWrvUYDf/LTpXnhLVcLA/fJsqYrew10mXRq5nhK6ZytvE0Z
jh090GZ1GFs4k/MScj9RZA+arTUYMazRPAhKtwIDAQABaoIBACBChD4z68IOZ7i+
OzpmHgXL9I0/xQDNN5sd2AxeiSDFfMQHZY7Sgfl8R1kdt0og79Xn1BHsedDrI5/2
Ym1KPdmHlyH4KE+gjqPz701rbYa115hmk3KEIqgXX1blyBWkbnT0auZiHSxeAIFC
eOgdgpxsAtZVkgv8gqlzTt6aZix7GqEJqqe7mPVBZJx29GyzR9pDd6CGdZyLW26j
jFjDxBM2S8YMeDI0PbWm7DYQ+ktSSMuxCgvXt797NRpECRFTHRdn1VgTfD551014
QhvekRN9W5ubD2QFFoyFdn0JJdpaSQUE34ExZgUwtdv0oedS8pb+1/yf8t1Zmrcv
gnhPipkCgYEA5HZczD2+0eM9aFC2v+68okYeBOuYd6g7fE3s5r5qkfkyLuFL5BML
cfhpTiZ1EeMr1oJMpTDjTFKM7OAGmt+9LCjtcCUPNKQLR/f2yTD1gG1IDHVCYOn
fKrijBMnqV8aDwnXSgOVJ7AFrPuSwGnmtdqfFhQ3783JXsUafOuj8gEMCgYEAwBcX
zEer4KfBGo+V31Q5DYGCgutkQLfNkcAVR1HiruLbs6V64UNakOXfU8BsJJHO+ZOJ
4EyXEoxplg018Y6sz9hpUeJAznHVM2P1D2PCWsyJW16SCT4maySj+fnwV30ES1fl
ganJmWi3MGA+tH2EbqjgJyPIexf7mkfgyii+Dn0CgYAOaFfX/00E10YDc5E1yJnck
8LER9F2gJi7iLvPitV15KTMEit7DWMXBIZ5YwobuAtqP45W70TJ0bLxQb+xaTgNz
Fn2kRt9HotTHTB73HyxMVddiWcBdJT1Zwlkgwy8RLAa6nLWSxWL9DDXcOIXWLZfR
VclCE9iwyKQ5HGcbYvepiwKBgGVni3uelmB5jppb9G16Q8gadzmIzFrR7SalNVZ6
GSwhvIPAtvbWHKhjgZrv+ObxRkdAmMedBx+WmmLJRJHplNcAUtEUVmVnEfrYKNVf
/4j5cwWWDhftBFEJfbsIM9WrvKkWB6UZQQoKWrKiDFgx7siQRAZFeh9pULxod4Wh
LnvTAoGBAL24/183zdryS37AS33+Metib1aYG3j94H5PCYRqITPIeQ3fdPHbZH/F
uid35BB/p41/BYv8R5iuklVgBY/TZabPg1NdpMvKfLH4YGu5e+0ynrhTSnSIFTqV
lMXE5lvzMQ/Ryux6UdRV2ZiETHrPQ6R0e+MldFevVYRygoJ3/ol
-----END RSA PRIVATE KEY-----}"}
```

View certificate

 **NOTE:** The custom SEKM PEM certificate can only be viewed from the RACADM interface using the command below.

```
C:\>racadm -r 192.168.0.120 -u root -p P@ssw0rd --nocertwarn sslcertview -t 6
Serial Number           : 0A
Subject Information:
Country Code (CC)       : US
State (S)               : TX
Locality (L)            : Round Rock
Organization (O)        : Dell
Organizational Unit (OU) : Validation
Common Name (CN)        : iDRAC-12345

Issuer Information:
Country Code (CC)       : US
State (S)               : TX
Locality (L)            : Round Rock
Organization (O)        : Dell
Organizational Unit (OU) : Solutions Group
Common Name (CN)        : Certificate Authority
Valid From              : Apr 29 17:00:08 2024 GMT
Valid To                 : Apr 29 17:00:08 2025 GMT
```

Periodic Sync with Key Management Server

Periodic Sync with KMS automatically updates encryption keys based on a KMS schedule. iDRAC scans the KMS for new keys and rekeys all SEKM-secured devices with any new key it finds. Activate this feature on the KMS first, then configure it on iDRAC using any supported interface. For more details, see your KMS administrator guide.

NOTE: Periodic Sync is only supported with CipherTrust Manager (k170v) Key Management Server.

NOTE: Periodic Sync is only supported through the Redfish interface.

NOTE: Periodic Sync can be disabled by running a manual rekey command. This will also delete any jobs that are scheduled by Periodic Sync.

The default pattern for the recurrence job is once daily. Since the KMS cannot notify iDRAC about key rotations, iDRAC checks the KMS daily for any new keys. If no new key is found, the rekey operation does not occur.

NOTE: While enabling key rotation on the KMS, you must also enable the option to deactivate the old key. This ensures that the new key is activated once created and the old key is deactivated at the scheduled timer expiry.

Enable Periodic Sync

Command: POST

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellIDRACCardService/Actions/DellIDRACCardService.PeriodicSyncWithKMS

Header: content-type application/json

Auth: Basic

Body: {}

Verify Rekey mode

Command: GET

URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1?\$select=Attributes/SEKM.1.RekeyMode

Auth: Basic

Example: "SEKM.1.RekeyMode": "Periodic Sync with KMS"

View Periodic Sync schedule

Command: GET

URI: /redfish/v1/JobService/Jobs/Auto7c5292ab

Auth: Basic

Expected response code: 200 OK

Example response:

```
{
  "@odata.context": "/redfish/v1/$metadata#Job.Job",
  "@odata.id": "/redfish/v1/JobService/Jobs/Auto7c5292ab",
  "@odata.type": "#Job.v1_2_4.Job",
  "Description": "Represent a job in Redfish",
  "Id": "Auto7c5292ab",
  "Name": "Recurring Job",
  "Steps": {
    "@odata.id": "/redfish/v1/JobService/Jobs/Auto7c5292ab/Steps"
  },
  "Schedule": {
    "MaxOccurrences": 6953,
    "InitialStartTime": "20240904143900.000000+000+00:00",
    "RecurrenceInterval": "P1D",
    "EnabledDaysOfWeek": [
    ],
    "EnabledDaysOfMonth": [
    ]
  }
}
```

NOTE: The RecurrenceInterval value "P1D" indicates "per 1 day."

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed."

Scheduled Rekey

SEKM Scheduled Rekey sends a new key generation request from iDRAC based on a user-configured recurrence interval. The rekey can be scheduled daily, on specific days of the week, or monthly. Examples are shown below.

NOTE: Scheduled Rekey is available on all supported Key Management Servers.

NOTE: Scheduled Rekey is only supported through the Redfish interface.

NOTE: Scheduled Rekey can be disabled by running a manual rekey command. This deletes any Scheduled Rekey jobs.

Enabled Scheduled Rekey (daily)

Command: POST
URI: /redfish/v1/JobService/Jobs
Header: content-type application/json
Auth: Basic
Body:

```
{
  "Payload": {
    "TargetUri": "/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/
DelliDRACCardService/Actions/DelliDRACCardService.Rekey"
  },
  "Schedule": {
    "RecurrenceInterval": "P1D"
  }
}
```

Enabled Scheduled Rekey (specific days of the week)

Command: POST
URI: /redfish/v1/JobService/Jobs
Header: content-type application/json
Auth: Basic
Body:

```
{
  "Payload": {
    "TargetUri": "/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/
DelliDRACCardService/Actions/DelliDRACCardService.Rekey"
  },
  "Schedule": {
    "EnabledDaysOfWeek" : ["Monday", "Wednesday", "Friday"]
  }
}
```

Enabled Scheduled Rekey (monthly)

Command: POST
URI: /redfish/v1/JobService/Jobs
Header: content-type application/json
Auth: Basic
Body:

```
{
  "Payload": {
    "TargetUri": "/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellIDRACCardService/Actions/DellIDRACCardService.Rekey"
  },
  "Schedule": {
    "EnabledDaysOfMonth": [10]
  }
}
```

Verify Rekey mode


Command: GET
URI: /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1?\$select=Attributes/SEKM.1.RekeyMode
Auth: Basic
Example: "SEKM.1.RekeyMode": "Scheduled Rekey"

View Scheduled Rekey schedule

Command: GET
URI: /redfish/v1/JobService/Jobs/Auto7c5292ab
Auth: Basic
Expected response code: 200 OK
Example response:


```
{
  "@odata.context": "/redfish/v1/$metadata#Job.Job",
  "@odata.id": "/redfish/v1/JobService/Jobs/Auto8e034526",
  "@odata.type": "#Job.v1_2_4.Job",
  "Description": "Represent a job in Redfish",
  "Id": "Auto8e034526",
  "Name": "Recurring Job",
  "Steps": {
    "@odata.id": "/redfish/v1/JobService/Jobs/Auto8e034526/Steps"
  },
  "Schedule": {
    "MaxOccurrences": 6953,
    "InitialStartTime": "20240904145300.000000+000+00:00",
    "RecurrenceInterval": null,
    "EnabledDaysOfWeek": [
      "Wednesday",
      "Friday"
    ],
    "EnabledDaysOfMonth": [
    ]
  }
}
```

 **NOTE:** In the example above, Scheduled Rekey operation runs on Wednesday and Friday.

 **NOTE:** In the Headers output, the Location property returns a job ID URI. Run `GET` on this URI to view recurring job details.

Easy Restore

Easy Restore employs its own flash memory to create a backup of the system data. Upon replacing the motherboard and initiating the system, the BIOS communicates with the iDRAC and offers the option to restore the backup. The initial BIOS screen provides prompts to restore the service tag, iDRAC licenses, SupportAssist, and Identity Module (if applicable). The subsequent BIOS screen offers prompts to restore the system configuration settings (iDRAC, BIOS, and NIC). However, SEKM certificates are not copied to flash memory, and must be installed again manually.

 **NOTE:** The Identity Module is restored first before other system settings (iDRAC, BIOS, and NIC).

For more general information about Easy Restore, see the iDRAC User Guide.

The steps below outline the process to enable SEKM on the new motherboard:

- **Restore licenses:** iDRAC Datacenter, iDRAC Enterprise, and SEKM licenses are restored as part of Easy Restore.
- **Update firmware:** After the Easy Restore process completes, update the iDRAC firmware update to ensure KMIP functionality on the new iDRAC.
- **Reupload certificates:** Manually reupload the SEKM certificates. Enable SEKM using the same iDRAC KMS user credentials from the original system.
- **Unlock devices:** Once SEKM is enabled, iDRAC can unlock any previously locked supported device.

Crypto-Erase All Drives in a Single Operation

`ControllerDrivesDecommission` deletes all virtual disks, securely erases all supported drives, and disables security on the storage controller in a single stacked operation.

NOTE: This feature is only supported through the Redfish interface.

NOTE: This feature is only supported on BOSS-N1 and HBA 465i storage controllers.

Command: POST

URI: `/redfish/v1/Systems/System.Embedded.1/Storage/{controller ID}/Actions/Oem/DellStorage.ControllerDrivesDecommission`

URI example: `/redfish/v1/Systems/System.Embedded.1/Storage/BOSS.SL.14-1/Actions/Oem/DellStorage.ControllerDrivesDecommission`

Header: `content-type application/json`

Auth: Basic

Body: `{"DisableControllerSecurity": true}`

Expected response code: 202 ACCEPTED

`DisableControllerSecurity` is a boolean property that indicates whether security is disabled on the storage controller. A value of `true` results in disabling security on your supported storage controller.

NOTE: In the Headers output, the Location property returns a job ID URI. Run GET on this URI to monitor the job status until it is marked "Completed." If the job stops in a "Scheduled" state, a server reboot is required to run the job.

The `ControllerDrivesDecommission` action also supports the `@Redfish.OperationApplyTime` parameter in the request body. An example request body is shown below:

OnReset

```
{
  "@Redfish.OperationApplyTime" : "OnReset",
  "DisableControllerSecurity": true
}
```

The `OnReset` option does not run the job until the server has rebooted.

Immediate

```
{
  "@Redfish.OperationApplyTime" : "Immediate",
  "DisableControllerSecurity": true
}
```

The `Immediate` option will perform a graceful OS shutdown with power cycle after the reboot job timeout completes.

Troubleshooting

This section discusses some of the common issues that are encountered while setting up SEKM.

Topics:

- SEKM license installed but cannot enable on iDRAC
- SEKM SSL certificates uploaded but cannot enable SEKM
- Cannot switch PERC to SEKM mode
- SEKM failed for PERC encryption mode
- SEKM status shows "Unverified Changes Pending"
- SEKM status shows "Failed" after changing KMIP authentication settings
- SED shows as Locked and Foreign after moving to another SEKM-enabled PERC
- SEKM failed after moving SEKM-enabled PERC to another server
- Key size and algorithm used by KMS
- New PERC encryption mode is "None" after replacement
- New key generated after replacing SEKM-enabled PERC
- New BOSS-N1 security status after replacement
- Rollback of iDRAC firmware blocked
- Restoring SEKM mode on PERC after network outage
- Changing keys on a PERC
- PERC encryption mode still shows SEKM after system erase
- Cannot switch PERC to SEKM mode from LKM mode
- SED shows as Locked and Foreign after migrating from LKM to SEKM mode
- Cannot switch PERC to SEKM from eHBA personality mode
- Information on SEKM setup failures, key exchange issues, successful exchanges, or rekey operations
- SEKM key exchange after deleting SEKM license
- SEKM key exchange after an iDRAC reset
- SEKM key exchange failed after a warm reboot, but secured volume drives are still online and secured
- Auto Secure not enabling security on HBA or PERC
- Hot-plugged SED not showing up in the OS
- Cannot disable SEKM on iDRAC
- Cannot disable security on HBA or BOSS controller
- Confirming IP address in the KMS certificate SAN field
- Recovering from a key exchange failure after changing the iDRAC IP
- Updating PERC or HBA 12 firmware to version 12.2 or later

SEKM license installed but cannot enable on iDRAC

Q: I installed the SEKM license but cannot enable it on iDRAC. Any suggestions?

A: Ensure you update the iDRAC firmware after you install the SEKM license. This is required even if you had a SEKM-supported iDRAC firmware version before installing the SEKM license.

SEKM SSL certificates uploaded but cannot enable SEKM

Q: I set up the KMS info and uploaded SEKM SSL certificates, but still cannot enable SEKM on iDRAC. Any tips?

A: 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 the following:
 - Primary and Secondary KMIP port numbers are correct.
 - The KMS CA certificate is the same as the one used to sign the KMS Server certificate.
 - The CA used to sign the iDRAC CSR is in the Trusted CA list on the KMS server.
 - The SSL Timeout value is large enough to allow iDRAC to be able to establish the SSL connection to the KMS.
 - The 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).
- Ensure that the iDRAC CSR has the option to include IP address in the CSR selected.

Cannot switch PERC to SEKM mode

Q: I cannot switch PERC to SEKM mode. Any advice?

A: Ensure the following:

- The PERC firmware has been upgraded to a version that supports SEKM.
- The SEKM status on iDRAC is enabled. You can use the `racadm sekm getstatus` command to see the current SEKM status.

SEKM failed for PERC encryption mode

Q: I set up SEKM on iDRAC and PERC, rebooted the host, but PERC shows 'SEKM Failed' for Encryption Mode. Any ideas?

A: The primary reason for this is that the PERC could not get the key from the iDRAC. In this case, the iDRAC SEKM status changes to "Failed." See the troubleshooting tips mentioned earlier and ensure iDRAC can communicate with the KMS.

SEKM status shows "Unverified Changes Pending"

Q: The SEKM status on iDRAC shows "Unverified Changes Pending." What does that mean?

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

SEKM status shows "Failed" after changing KMIP authentication settings

Q: I changed the KMIP authentication settings on the KMS, and now the iDRAC SEKM status shows "Failed." Any solutions?

A: If you changed the username or password of the iDRAC account on the KMS, ensure you update the corresponding properties on the iDRAC and enable SEKM.

If you changed the value of the "Username field in the Client Certificate" option on the KMS, generate a new CSR from iDRAC by setting the appropriate CSR property to the username, get the CSR signed by the KMS CA, and 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," 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, 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.

SED shows as Locked and Foreign after moving to another SEKM-enabled PERC

Q: I moved a SED from a SEKM-enabled PERC to another, and now the drive shows as Locked and Foreign. How do I unlock it?

A: Because each iDRAC is represented on the KMS by a separate user account, the keys that are created by one iDRAC are not accessible to another iDRAC by default. 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 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 group, click **Add** in **Local Groups**.
3. Select the newly created group and click **Properties**.
4. In the **User List** section, click **Add**, then add both the iDRAC usernames to this group.
5. After the group is created, click **Security Keys**.
6. Identify the key that is created by the first iDRAC using the iDRAC unique username.
7. Select the key and click **Properties**.
8. Click the **Permissions** tab, then click **Add** under **Group Permissions**.
9. Enter the name of the newly created group in step 2.
10. Remove and insert the drive to initiate a key exchange.
11. Now, the second iDRAC can get the key and provide it to PERC to successfully unlock the drive. The SEDs appear as Foreign and Unlocked.
12. Import or clear the foreign configuration of the drive. The steps for the CipherTrust Manager k170v are:
 - a. Log in to the **CipherTrust Manager** and click **Keys and Access Management > Groups**.
 - b. To create a group, enter the name of your new group in the **Create New Group** section, then click **Add**.
 - c. Select your newly created group and add the required users to the group.
 - d. After the group is created and the users are added, click **Keys** to identify the key you want to be shared between iDRACs.
 - e. Select the required key, click **Edit**, identify your newly created group, and add the key to the group. Click **Update**.

SEKM failed after moving SEKM-enabled PERC to another server

Q: I moved a SEKM-enabled PERC to another server, and now the encryption mode shows “SEKM Failed.” How do I enable SEKM on the PERC?

A: Follow the steps outlined in [SED shows as Locked and Foreign](#) after moving to another SEKM-enabled PERC and restart the host.

Key size and algorithm used by KMS

Q: What key size and algorithm does the KMS use to generate the key?

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

New PERC encryption mode is “None” after replacement

Q: I replaced a SEKM-enabled PERC with another, but the new PERC encryption mode is “None.” Why is it not “SEKM”?

A: On a part replacement, iDRAC sets the encryption mode of the new PERC to SEKM only if the firmware version of the new PERC is SEKM-capable. Ensure that the replacement PERC has a firmware version that supports SEKM. If not, perform a firmware update of the PERC to a version that supports SEKM and then check the PERC encryption mode.

New key generated after replacing SEKM-enabled PERC

Q: I replaced a SEKM-enabled PERC, and now iDRAC has generated a new key. Why was the original key not used?

A: Each PERC needs its own key for SEKM. When a PERC is replaced, the new PERC requests a new key from iDRAC, use the old key to unlock the drives, and then rekey them with its new key.

New BOSS-N1 security status after replacement

Q: I replaced a SEKM-enabled BOSS-N1 with another, but the security status of the new BOSS-N1 is “Disabled.” Why is it not enabled?

A: On a part replacement, iDRAC sets the security status of the new BOSS-N1 to “Enabled” only if the firmware version of the new BOSS-N1 supports SEKM. If not, perform a firmware update of the BOSS-N1 to a version that supports SEKM, then check the BOSS-N1 security status. This is also applicable to ROR-N1.

Rollback of iDRAC firmware blocked

Q: I cannot roll back iDRAC firmware. Why might the rollback be blocked?

A: Ensure that there are no storage devices in SEKM mode. If there are any storage devices in SEKM mode, iDRAC blocks rollbacks to versions that do not support SEKM. This is to prevent data lockout, since iDRAC cannot provide keys to the storage devices to be unlocked after rollback.

Restoring SEKM mode on PERC after network outage

Q: I rebooted the host, and key exchange failed due to a network outage, putting PERC in SEKM failed state. The outage is resolved—how do I restore SEKM mode on PERC?

A: Ideally, you do not have to do anything because iDRAC periodically tries to connect to the KMS. After the network is restored, iDRAC can connect to the KMS, get the keys and provide them to PERC, and put it back in the SEKM mode. If the PERC is still in SEKM failed state after five minutes, reboot the host and check if the key exchange is successful.

Changing keys on a PERC

Q: Can I change the keys on a PERC?

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

PERC encryption mode still shows SEKM after system erase

Q: I did a system erase, but PERC encryption mode still shows SEKM. Why?

A: This is expected behavior, as 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.”

Cannot switch PERC to SEKM mode from LKM mode

Q: I cannot switch PERC to SEKM mode from LKM mode. Any advice?

A: Update to the latest iDRAC and PERC firmware.

SED shows as Locked and Foreign after migrating from LKM to SEKM mode

Q: I migrated an SED from LKM mode to SEKM mode, but the drive shows as Locked and Foreign. Why was not it unlocked?

A: This is expected behavior. Because a PERC locks the SED in LKM mode, it must be unlocked manually by the LKM passphrase using any of the iDRAC interfaces. After unlocking, the foreign configuration the drive is imported, then the SEKM key locks the drive.

Cannot switch PERC to SEKM from eHBA personality mode

Q: I cannot switch PERC to SEKM mode from eHBA personality mode. Any tips?

A: This is expected behavior. The SEKM encryption mode is not supported in eHBA personality mode.

Information on SEKM setup failures, key exchange issues, successful exchanges, or rekey operations

Q: Where can I find information about SEKM setup failures, key exchange issues, successful exchanges, or rekey operations?

A: In all these cases, see the iDRAC Lifecycle logs for detailed log entries. In addition to checking iDRAC Lifecycle logs for detailed log entries, review the logs on the Key Management Server for any key exchange activity.

SEKM key exchange after deleting SEKM license

Q: Will the SEKM key exchange still work after deleting the SEKM license?

A: Yes, SEKM key exchange continues to work even if the SEKM license has been deleted.

i NOTE: Updating the iDRAC firmware or performing an iDRAC reset without a SEKM license causes iDRAC to lose SEKM functionality. To recover this functionality, reinstall the SEKM license and update the iDRAC firmware again.

SEKM key exchange after an iDRAC reset

Q: Will the SEKM key exchange still work after an iDRAC reset?

A: SEKM key exchange will continue to work after a racreset if the SEKM attributes and certificates on iDRAC are still valid.

i NOTE: `racresetcfg` is blocked while SEKM is enabled. To perform a `racresetcfg` operation, you must disable SEKM on iDRAC first.

SEKM key exchange failed after a warm reboot, but secured volume drives are still online and secured

Q: SEKM key exchange that is failed after a warm reboot, but my secured volume drives are still online and secured. Why?

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

Auto Secure not enabling security on HBA or PERC

Q: I enabled Auto Secure, but security was not enabled on HBA or PERC. Why?

A: Controllers such as PERC and HBA are not auto secured and must be manually secured.

Hot-plugged SED not showing up in the OS

Q: I hot-plugged a SED, but the drive is not showing up in the OS. Why?

A: Rescan the drive in the OS after it is reported in iDRAC storage inventory as secured.

Cannot disable SEKM on iDRAC

Q: I cannot disable SEKM on iDRAC. Any advice?

A: Ensure that security is disabled on all storage devices before attempting to disable SEKM on iDRAC.

Cannot disable security on HBA or BOSS controller

Q: I cannot disable security on the HBA or BOSS controller. Any advice?

A: Ensure all supported drives behind the controller have security that is disabled.

Confirming IP address in the KMS certificate SAN field

Q: How can I confirm that the IP address is in the SAN field for the KMS certificate?

A: Go to the **iDRAC9 UI > Storage > SEKM** page to determine KMS information.

The screenshot shows the 'SEKM Status' as 'Enabled' with a green clock icon. Below this is the 'KMS Information' section with the instruction 'Set-up upstream communications with the Key Management Server.' There are two input fields: 'KMS (IP Address or FQDN)*' containing '100.64.40.230' and 'Port Number*' containing '5696'.

SEKM Status	Enabled
KMS Information Set-up upstream communications with the Key Management Server.	
KMS (IP Address or FQDN)*	100.64.40.230
Port Number*	5696

Figure 95. KMS information

1. Open a web browser that can reach the KMS server and enter the IP and port number in the address bar (Mozilla Firefox was used in example below). Example: `https://XXX.XXX.XXX.XXX:5696`.

NOTE: This does not open a valid webpage, since the port is not for a webservice.

2. Click the address bar site information to see page information and view the certificate.

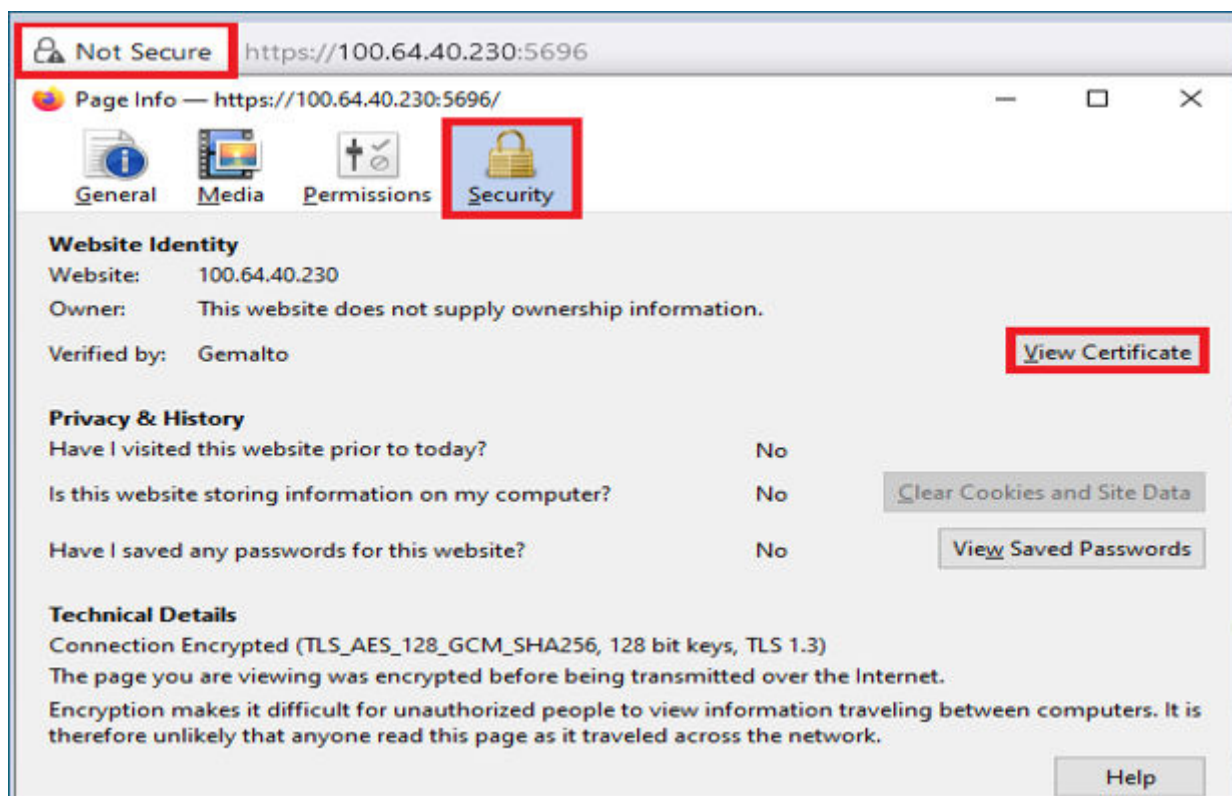


Figure 96. View certificate

3. On the Certificate Details page, go to Subject Alt Names and confirm that the IP address is included.

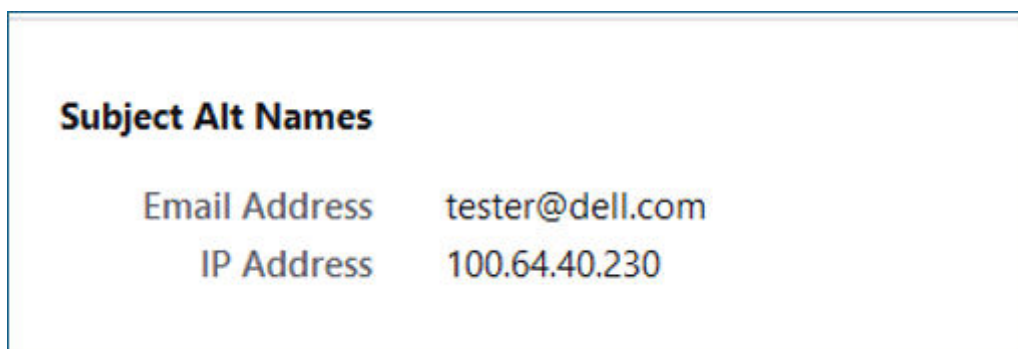


Figure 97. Subject Alt Names

NOTE: If the IP address is not included within the Subject Alt Name field, a new CSR must be generated on the KMS.

Information on including the IP address in KMS CSR is in each supported KMS section.

Recovering from a key exchange failure after changing the iDRAC IP

Q: How do I recover from a key exchange failure after changing the iDRAC IP?

A: If your iDRAC IP changes after you have enabled the “Require Client Certificate to Contain Source IP” setting on your supported KMS and included the iDRAC IP when generating a CSR, you must regenerate a CSR and upload the signed certificate with the new iDRAC IP in the request.

Updating PERC or HBA 12 firmware to version 12.2 or later

Q: What should I do after updating PERC or HBA 12 firmware to version 12.2 or later?

A: After updating PERC or HBA FW to 12.2 or later, perform a cold reboot instead of a warm reboot. This ensures that supported drives are unlocked and prevent any locked-out conditions.

Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.