

Configure self-encrypting disks (SEDs)

Published: 2024-07-16

This guide explains how to configure self-encrypting disks (SEDs) in the EDA 9300 or 10300 sensor.

SEDs continuously encrypt data written to the drive. Data on these drives is protected by requiring a key to unlock the encrypted drives before retrieving data. The drives are only protected from theft when the disks are secured.

You can configure security for virtual disks on SEDs either upon or after virtual disk creation. Secure virtual disks cannot be unsecured without erasing all data on the drive.

There are two options available for enabling security and encryption on installed drives:

Local Key Management (LKM)

Enable security from the PowerEdge RAID Controller (PERC) and configure a security key and passphrase that is stored locally on the controller. This method protects data in the event of physical drive theft, but not entire system theft. For more information on configuring LKM, see [Security key and RAID management](#).

Secure Enterprise Key Management (SEKM)


Manage keys from a key management service and enable security on installed drives from the iDRAC9. Because keys are stored externally on a key management service, data on these drives is protected in the event of system theft. For more information on configuring SEKM, see the "PowerEdge RAID Controller (PERC)" section in the [SEKM configuration and deployment guide](#).

After you enable either LKM or SEKM, you must encrypt your existing virtual disks.


Configure LKM on the RAID controller from the iDRAC web interface

If you prefer to secure the system with Local Key Management (LKM), you can enable security from the RAID controller.

1. Start iDRAC from any supported browser.
2. From the iDRAC web interface, click **Storage**, and then click **Overview**.
3. Click **Controllers**.
4. In the Controllers section, click **Edit** from the Actions list next to the controller that you want to configure.

 **Note:** There are two controllers: one for the internal disks, which store firmware and configuration, and one for Extended Storage Units (ESUs), which store packets.

5. In the Controller Properties section, click **Security**.
6. From the **Security (Encryption)** list, click **Create Security Key**.
7. Click **Next**.
8. For the **Security Key Identifier**, type the key ID that will be required to secure virtual disks.
9. For the **Security Key Passphrase**, type the password that will be required to secure the virtual disks.

 **Note:** The passphrase is case-sensitive. The minimum character length is 8, and the maximum is 32 characters. Ensure that the characters contain at least one number, one lower case letter, one upper case letter, and one nonalphanumeric character.

10. For the **Confirm Security Key Passphrase**, type the password again.
11. Click **Add to Pending**.

Next steps

Next, [encrypt an existing virtual disk](#).

Configure SEKM for drive encryption from the iDRAC web interface

Before you begin

Before you configure Secure Enterprise Key Management (SEKM), be sure to configure your external Key Management Server (KMS), which manages keys that can lock and unlock storage drives through iDRAC. For more information, see the specific section for your KMS in the [SEKM configuration and deployment guide](#).

If you prefer to secure the system with SEKM, you can configure security from the RAID controller.

1. Start iDRAC from any supported browser.
2. From the iDRAC web interface, click **Storage**, and then click **Overview**.
3. Click **Controllers**.
4. In the Controllers section, click **Edit** from the Actions list next to the controller that you want to configure.



Note: There are two controllers: one for the internal disks, which store firmware and configuration, and one for Extended Storage Units (ESUs), which store packets.

5. In the Controller Properties section, click **Security**.
6. From the **Security (Encryption)** list, click **Secure Enterprise Key Manager**.
7. Click **Add to Pending**.
8. Click **At Next Reboot**.
A message displays indicating that the job ID is created.
9. Go to the **Job Queue** page and ensure that this job ID is marked as **Scheduled**.
10. Restart the server to run the configuration job.
11. Go to the **Job Queue** page to view the scheduled job.

After restarting the server, the configuration job runs in the Automated Task Application to enable SEKM on the PERC. The server restarts automatically.

Next steps

Next, [encrypt an existing virtual disk](#).

Encrypt a virtual disk

You can configure security for virtual disks on existing SEDs. Secure virtual disks cannot be unsecured without erasing all data on the drive.

1. Start iDRAC from any supported browser.
2. From the iDRAC web interface, click **Storage**, and then click **Overview**.
3. Click **Virtual Disks**.
4. Click **Encrypt Virtual Disk** from the Actions list for the virtual disk to be encrypted.
5. Click **Add to Pending**.
6. Click **Apply Now**.