# Table of Contents

Manage encryption with System Manager .............................................................. 1
  Encrypt stored data using software-based encryption ........................................ 1
  Encrypt stored data using self-encrypting drives ........................................... 1
Manage encryption with System Manager

Encrypt stored data using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

Steps
1. Click Cluster > Settings.
2. Under Encryption, click to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click Storage > Volumes.
4. On the desired volume, click and then click Edit.
5. Select Enable encryption.

Encrypt stored data using self-encrypting drives

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

Steps
1. Under Encryption, click to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click , and then click Rekey Disks.