Managing Storage Adapters

This chapter includes the following sections:

Self Encrypting Drives (Full Disk Encryption)

Cisco IMC supports self encrypting drives (SED). A special hardware in the drives encrypts incoming data and decrypts outgoing data in real-time. This feature is also called Full Disk Encryption (FDE).

The data on the drive is encrypted on its way into the drive and decrypted on its way out. However, if you lock the drive, no security key is required to retrieve the data.

When a drive is locked, an encryption key is created and stored internally. All data stored on this drive is encrypted using that key, and stored in encrypted form. Once you store the data in this manner, a security key is required in order to un-encrypt and fetch the data from the drive. Unlocking a drive deletes that encryption key and renders the stored data unusable. This is called a Secure Erase. The FDE comprises a key ID and a security key.

The FDE feature supports the following operations:

- Enable and disable security on a controller
- Create a secure virtual drive
- Secure a non-secure drive group
- Unlock foreign configuration drives
- Enable security on a physical drive (JBOD)
- Clear secure SED drives
- Clear secure foreign configuration

Scenarios to consider While Configuring Controller Security in a Dual or Multiple Controllers Environment

Note Dual or Multiple controllers connectivity is available only on some servers.

Controller security can be enabled, disabled, or modified independently. However, local and remote key management applies to all the controllers on the server. Therefore security action involving switching the key management modes must be performed with caution. In a scenario where both controllers are secure, and you decide to move one of the controllers to a different mode, you need to perform the same operation on the other controller as well.

Consider the following two scenarios:

- Scenario 1—Key management is set to remote; both controllers are secure and use remote key management. If you now wish to switch to local key management, switch the key management for each controller and disable remote key management.

- Scenario 2—Key management is set to local; both controllers are secure and use local key management. If you now wish to switch to remote key management, enable remote key management and switch the key management for each controller.

If you do not modify the controller security method on any one of the controllers, it renders the secure key management in an unsupported configuration state.

Create Virtual Drive from Unused Physical Drives

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from Unused Physical Drives**.

The **Create Virtual Drive from Unused Physical Drives** dialog box displays.

Step 5 In the **Create Virtual Drive from Unused Physical Drives** dialog box, select the RAID level for the new virtual drives:

This can be one of the following:

- **Raid 0**—Simple striping.
- **Raid 1**—Simple mirroring.
- **Raid 5**—Striping with parity.
- **Raid 6**—Striping with two parity drives.
- **Raid 10**—Spanned mirroring.
- **Raid 50**—Spanned striping with parity.
- **Raid 60**—Spanned striping with two parity drives.

Note You must have multiple drive groups available to create virtual drives for certain RAID levels. While creating drives for these RAID levels, the create drive option is available only if the required number of drives are selected.

Step 6 Optionally, select the **Enable Full Disk Encryption** checkbox.

This enables disk encryption on the drive group and allows you to secure it.

Step 7 In the **Create Drive Groups** area, choose one or more physical drives to include in the group.

Use the >> button to add the drives to the **Drive Groups** table. Use the << button to remove physical drives from the drive group.

Note The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.

Step 8 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 9 Click **Create Virtual Drive**.

Create Virtual Drive from an Existing Drive Group

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from an Existing Virtual Drive Group**.

The **Create Virtual Drive from an Existing Virtual Drive Group** dialog box displays.

Step 5 In the **Create Virtual Drive from an Existing Virtual Drive Group** dialog box, select the virtual drive whose drive group you want to use to create a new virtual drive.

Step 6 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Name	Description
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 7 Click **Create Virtual Drive**.

Setting a Virtual Drive to Transport Ready State

You can move a virtual drive from one MegaRAID controller to another using the **Set Transport Ready** feature. This allows all the pending IOs of the virtual drive to complete their activities, hide the virtual drive from the operating system, flush cache, pause all the background operations, and save the current progress in disk data format, allowing you to move the drive. When you move a virtual drive, all other drives belonging to the same drive group inherit the same change as the moved drive.

When the last configured physical drive on the group is removed from the current controller, the drive group becomes foreign and all foreign configuration rules apply to the group. However, the Transport Ready feature does not change any foreign configuration behavior.

You can also clear a virtual drive from the Transport Ready state. This makes the virtual drive available to the operating systems.

Following restrictions apply to a transport ready virtual drive:

- Only a maximum of 16 transport ready drive groups are currently supported.
- This feature is not supported on high availability.
- A virtual drive cannot be set as transport ready under these conditions:
  - When a virtual drive of a drive group is being reconstructed
  - When a virtual drive of a drive group contains a pinned cache

- When a virtual drive of a drive group is marked as cacheable or associated with a cachecade virtual drive
- If a virtual drive is a cachecade virtual drive
- If a virtual drive is offline
- If a virtual drive is a bootable virtual drive

Setting a Virtual Drive as Transport Ready

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be in optimal state to enable transport ready.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA Controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want set as transport ready.

Step 5 In the **Actions** area, click **Set Transport Ready**.

The **Set Transport Ready** dialog box displays.

Step 6 Update the following properties in the dialog box:

Name	Description
Initialize Type drop-down list	Allows you to select the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following: • **Exlude All**— Excludes all the dedicated hot spare drives. • **Include All**— Includes any exclusively available or shared dedicated hot spare drives. • **Include Dedicated Hot Spare Drive**— Includes exclusive dedicated hot spare drives.
Set Transport Ready button	Sets the selected virtual drive as transport ready.
Cancel button	Cancels the action.

Note When you set a virtual drive to transport ready all the physical drives associated with it are displayed as **Ready to Remove**.

Clearing a Virtual Drive from Transport Ready State

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be transport ready.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive to set as transport ready.

Step 5 In the **Actions** area, click **Clear Transport Ready**.

This reverts the selected transport ready virtual drive to its original optimal state.

Importing Foreign Configuration

When a set of physical drives hosting a secured drive group are inserted into a different server or controller (or the same controller but whose security-key has been changed while they were not present), they become foreign configurations. Since they are secured, these foreign configurations must be unlocked by verifying their security key information before they can be imported.

Complete the following steps to verify the security key for a foreign configuration and import the configuration:

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Import Foreign Config**.

This action opens the **Secure Key Verification** dialog box. Review the following information before proceeding:

Table 1: Secure Key Verification Area

Name	Description
Security Key field	Unique key ID assigned to a controller.
Verify button	Verifies if the key you entered matches the stored key information. If the secure key is verified to be correct, the requested action is completed.
Cancel button	Cancels the action.

Step 5 Click **OK** to confirm.

Clearing Foreign Configuration

Important This task clears all foreign configuration on the controller. Also, all configuration information from all physical drives hosting foreign configuration is deleted. This action cannot be reverted.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Controller Info** tab.
Step 4 In the **Actions** area, click **Clear Foreign Config**.
Step 5 Click **OK** to confirm.

Clearing a Boot Drive

Important This task clears the boot drive configuration on the controller. This action cannot be reverted.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Controller Info** tab.
Step 4 In the **Actions** area, click **Clear Boot Drive**.
Step 5 Click **OK** to confirm.

Enabling a JBOD

Note You can enable Just a Bunch Of Disks (JBOD) only on some UCS C-Series servers.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage Adapters** pane, click the appropriate **MegaRAID** controller.
Step 3 On the **Work** pane, click **Controller Info** tab.
Step 4 In the **Actions** area, click **Enable JBOD**.
Step 5 Click **Ok** to confirm.

Disabling a JBOD

Note This option is available only on some UCS C-Series servers.

Before you begin

JBOD option must be enabled for the selected controller.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage Adapters** pane, click the appropriate **MegaRAID** controller.
Step 3 On the **Work** pane, click **Controller Info** tab.

Step 4 In the **Actions** area, click **Disable JBOD**.

Step 5 Click **Ok** to confirm.

Preparing a Drive for Removal

Note You can perform this task only on physical drives that display the **Unconfigured Good** status.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the drive you want to remove.

Step 5 In the **Actions** area, click **Prepare for Removal**.

Step 6 Click **OK** to confirm.

Retrieving TTY Logs for a Controller

This task retrieves the TTY logs for the controller and places it in the `/var/log` location. This ensures that this log data is available when Technical Support Data is requested.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Get TTY Log**.

Step 5 Click **OK** to confirm.

Important Retrieving TTY logs for a controller could take up to 2-4 minutes. Until this process is complete, do not initiate exporting technical support data.

Modifying Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Modify Drive Security**.

The **Modify Drive Security** dialog box appears.

Step 5 In the **Modify Drive Security** dialog box, review the following information:

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **Enabled**— Controller security is enabled. • **Disabled**— Controller security is disabled.
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.
Confirm Security Key field	Re-enter the security key.
Modify Security Key check box	**Note** This option appears only for remote key management. If you select this option the security key on the KMIP server is modified.
Suggest button	Suggests the security key or key ID that can be assigned.
Save button	Saves the data.

Name	Description
Cancel button	Cancels the action.

Disabling Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Disable Drive Security**.

Click **Yes** or **No** at the prompt.

Enabling Controller Security

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Enable Drive Security**.

The **Enable Drive Security** dialog box appears.

Step 5 In the **Enable Drive Security** dialog box, review the following information:

Table 2: Secure Key Configuration Area

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **True**— Controller security is enabled. • **False**— Controller security is disabled.
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.
Confirm Security Key field	Re-enter the security key.
Suggest button	Suggests the security key or key ID that can be used.
Save button	Saves the data.
Cancel button	Cancels the action.

What to do next

Undo Preparing a Drive for Removal

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 On the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.
Step 5 In the **Actions** area, click **Undo Prepare for Removal**.
Step 6 Click **OK** to confirm.

Making a Dedicated Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the physical drive you want to make a dedicated hot spare.

Step 5 In the **Actions** area, click **Make Dedicated Hot Spare**.

The **Make Dedicated Hot Spare** dialog box displays.

Step 6 In the **Virtual Drive Details** area, update the following properties:

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.
Virtual Drive Name field	The name of the selected virtual drive.
Physical Drive Number field	The number of the physical drive.

Step 7 Click **Make Dedicated Hot Spare** to confirm.

Making a Global Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the physical drive you want to make a global hot spare.

Step 5 In the **Actions** area, click **Make Global Hot Spare**.

Removing a Drive from Hot Spare Pools

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.

Step 5 In the **Actions** area, click **Remove From Hot Spare Pools**.

Toggling Physical Drive Status

Before you begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the drive you want to set as unconfigured good.

Step 5 In the **Actions** area, click **Set State as Unconfigured Good**.

Step 6 Click **OK** to confirm that the JBOD mode be disabled.

The **Set State as JBOD** option is enabled.

Step 7 To enable the JBOD mode for the physical drive, click **Set State as JBOD**.

Step 8 Click **OK** to confirm.

The **Set State as Unconfigured Good** option is enabled.

Setting a Physical Drive as a Controller Boot Drive

Before you begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to set as boot drive for the controller.
Step 5 In the **Actions** area, click **Set as Boot Drive**.
Step 6 Click **OK** to confirm.

Enabling Full Disk Encryption on a Physical Drive

Before you begin

- You must log in with admin privileges to perform this task.
- The physical drive must be a JBOD.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Enable Full Disk Encryption**.

Clearing a Secure Physical Drive

Before you begin

- You must log in with admin privileges to perform this task.

- You must enable full disk encryption on a physical drive.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Clear Secure Drive**.

Clearing Secure Foreign Configuration Drive

If the security key used to lock a foreign configuration is lost, the data cannot be retrieved. You then have the option of either discarding the HDD or clearing the foreign configuration.

Note Clearing a foreign configuration erases all data from the drive.

Before you begin

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Clear Secure Foreign Config Drive**.

Initializing a Virtual Drive

All data on a virtual drive is lost when you initialize the drive. Before you run an initialization, back up any data on the virtual drive that you want to save.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want to initialize.

Step 5 In the **Actions** area, click **Initialize**.

The **Initialize Virtual Drive** dialog box displays.

Step 6 Choose the type of initialization you want to use for the virtual drive.

This can be one of the following:

- **Fast Initialize**—This option allows you to start writing data to the virtual drive immediately.
- **Full Initialize**—A complete initialization is done on the new configuration. You cannot write data to the new virtual drive until the initialization is complete.

Step 7 Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.

Step 8 To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.

The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive from which the controller must boot.

Step 5 In the **Actions** area, click **Set as Boot Drive**.

Step 6 Click **OK** to confirm.

Editing a Virtual Drive

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage Adapters pane**, click **LSI MegaRAID SAS 9266-8i**.

Step 3 On the **Work** pane, click **Virtual Drive Info** tab.

Step 4 In the **Actions** area, click **Edit Virtual Drive**.

Step 5 Review the instructions, and then click **OK**.
The Edit Virtual Drive dialog box displays.

Step 6 From the **Select RAID Level to migrate** drop-down list, choose a RAID level.

See the following table for RAID migration criteria:

Name	Description
Select RAID Level to migrate drop-down list	Select the RAID level to which you want to migrate. Migrations are allowed for the following RAID levels: • **RAID 0** to **RAID 1** • **RAID 0** to **RAID 5** • **RAID 0** to **RAID 6** • **RAID 1** to **RAID 0** • **RAID 1** to **RAID 5** • **RAID 1** to **RAID 6** • **RAID 5** to **RAID 0** • **RAID 6** to **RAID 0** • **RAID 6** to **RAID 5** When you are migrating from one raid level to another, the data arms of the new RAID level should be equal to or greater than the existing one. In case of RAID 6, the data arms will be number of drives minus two, as RAID 6 has double distributed parity. For example, when you create RAID 6 with eight drives, the number of data arms will be 8 – 2 = 6. In this case, if you are migrating from RAID 6 to RAID 0, RAID 0 must have a minimum of six drives. If you select lesser number of drives then **Edit** or **Save** button will be disabled. If you are adding, you can migrate to RAID 0 as you will not be deleting any drives. **Note** RAID level migration is not supported in the following cases: • When there are multiple virtual drives in a RAID group. • With a combination of SSD/HDD RAID groups.

Step 7 From the **Write Policy** drop-down list in the **Virtual Drive Properties** area, choose one of the following:

- **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache.
- **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure.
- **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Step 8 Click **Save Changes**.

Securing a Virtual Drive

You can secure a virtual drive only after enabling full disk encryption on that drive. You can complete this action while creating a virtual drive from an unused physical drive. Since it is a physical drive that performs encryption, when a virtual drive in the drive group is secured, all the virtual drives in the drive group are secured. Virtual drives inherit the security setting of the drive group.

Before you begin

- You must log in with admin privileges to perform this task.
- You must enable full disk encryption on a virtual drive.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, select the drive you want to secure.
Step 5 In the **Actions** area, click **Secure Virtual Drive**.

Deleting a Virtual Drive

Important This task deletes a virtual drive, including the drives that run the booted operating system. So back up any data that you want to retain before you delete a virtual drive.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, select the virtual drive you want to delete.
Step 5 In the **Actions** area, click **Delete Virtual Drive**.
Step 6 Click **OK** to confirm.

Enabling Auto Learn Cycle for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Enable Auto Learn Mode**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Disabling Auto Learn Cycle for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Disable Auto Learn Mode**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Starting Learn Cycles for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.
Step 4 From the **Actions** pane, click **Start Learn Cycle**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Toggling Locator LED for a Physical Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 From the **Status** area, select **Turn On** or **Turn Off** radio button for the **Locator LED** field.

Viewing Storage Controller Logs

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click **Storage Log** tab and review the following information:

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Description column	A description of the event.

Viewing SSD Smart Information for MegaRAID Controllers

You can view smart information for a solid state drive. Complete these steps:

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Smart Information** area, review the following information:

Name	Description
Power Cycle Count field	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours field	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left field	The number of write cycles remaining in a solid state drive (SSD). For instance, if an SSD is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%.

Name	Description
Wear Status in Days field	The number of days an SSD has gone through with the write cycles. SSD vendors provide a finite number of writes per day on the SSD, based on which, you can calculate the total number of years the SSD would continue to work.
Operating Temperature field	The current temperature of the drive at which the selected SSD operates at the time of selection.