CHAPTER 10

# System Administration

When you click the **System Admin** button in the navigation pane, you are taken to the Configure Cache page. The navigation bar across the top contains links to this section's subpages.

- **Cache** links to Configure Cache
- **Alarm** links to Audible Alarm
- **Enclosure Config** links to Configure Enclosures
- **Reboot** links to Reboot System
- **Rebuild Rate** links to Configure Rebuild Priority
- **Verify Config** links to Verify RAID Arrays
- **System Mode** links to System Mode
- **Settings** links to Download/Upload System Settings
- **Update Firmware** links to Update Firmware

## Configure Cache

Clicking **System Admin** takes you to the Configure Cache page, which allows you to configure settings for the unit's cache memory.

Cache memory holds data that is being written to one or more disks, which enables the RAID Controller to confirm that a command has been completed before the data has been written to disk.

In the event of a power interruption during an unfinished write operation, the cache memory has a battery backup which allows the cache to hold data for up to 72 hours. When the power is restored to the unit, the RAID Controller will automatically complete any write operations using the data held in the cache.

The Configure Cache page displays the current cache settings and lets you configure them:

- **Current write cache state**: Shows whether the cache is currently enabled or disabled, mirrored, and in streaming mode, plus its "force unit access" (FUA) status and the size of the cache in megabytes (MB) for each RAID Controller.
- Manually override current write cache status: Normally, when the cache is enabled or disabled, the unit must be rebooted for it to take effect. Using this check box, you can force the cache to become Enabled (if it is disabled) or Disabled (if it is enabled) without rebooting the system.
- Desired write cache state: By default, this is **Enabled**. Select the desired setting (**Enabled** or **Disabled**).

- **Allow attached host to override write cache configuration**: Some hosts can issue commands that force the cache to not be used. To allow this, check this check box. To prevent it, leave the box unchecked (the default setting).
- **Ignore force unit access (FUA) bit**: Some SCSI commands contain a "force unit access" (FUA) bit, which forces the unit to bypass cache memory and perform read and write operations directly from and to the disks. Check this check box to ignore the FUA bit and always use the cache memory for command execution. Uncheck it (the default setting) to allow the FUA bit to bypass cache memory.
- **Enable cache mirroring**: On Cisco Video Surveillance Storage System components in a dual-controller active-active failover mode (see System Mode, page 10-6), this setting is enabled by default. It tells the system to duplicate the contents of the cache of one RAID Controller to the other, thus ensuring that cache contents are not lost in the event of a controller failure. Uncheck the box to disable cache mirroring (not recommended).

**Caution** If cache mirroring is turned off, data stored in the write cache may be lost if a RAID Controller fails.

- **Write/Read cache streaming mode**: When the cache streaming mode is active, the system continuously flushes the cache memory, which provides maximum cache buffering to protect against delayed command responses. When the streaming mode is not active, the system runs with a full cache, which helps reduce disk access and maximizes random I/O performance.

  Check this box to activate streaming mode. Uncheck it (the default) to deactivate streaming mode.
- **Cache optimization setting**: Select the cache setting that fits the kind of data and method of data access that your system uses most often:
  - **Random access**: This setting is best for systems that access a large number of files or many different areas of its volumes, such as systems with many individual users or that house frequently accessed databases.
  - **Mixed sequential/random** (default): This setting is best for systems that are "mixed use", sometimes accessing many smaller files and sometimes accessing a few larger files.
  - **Sequential access**: This setting is best for systems that access a small number of large files sequentially, such as an archive of manuscripts or videos.

  This setting can be changed in real-time. We encourage you to experiment with this setting to determine which configuration works best for your environment.

When you have selected the desired settings, click the **Save settings** button. A message is displayed, informing you that the settings have been updated. Click the **Back** button to be returned to the Configure Cache page.

**Note** If at any time you wish to return the Configure Cache page to its initial state, click **Reset**.

# Audible Alarm

Clicking **System Admin > Alarm** takes you to the Audible Alarm page, which allows you to silence or sound the audible alarm on the unit.

If the alarm is sounding, click **Silence the Audible Alarm** to silence the alarm. (To find out why the alarm is sounding, click the notification in the upper right corner to be taken to the Problem Summary page. See Summary of System Problems, page 5-7 for more information.)

**Note** If further problems occur, the audible alarm will sound again.

If the alarm is not sounding, click **Re-Sound the Audible Alarm** to sound the alarm (if a problem is present—see Summary of System Problems, page 5-7).

# Configure Enclosures

Clicking **System Admin > Enclosures Config** takes you to the Configure Enclosures page, which allows you to name each unit in your storage system.

To change the name of a unit, enter the new name in the **Friendly Name** field and click **Submit**. A message is displayed, informing you that the new name is saved. Click the **Back** button to return to the Configure Enclosures page.

Clicking the **Beacon** button causes the LEDs on the front of the unit to flash for one minute. This can help in locating a specific unit in a large installation where multiple Cisco Video Surveillance Storage System components are located.

# Reboot System

Clicking **System Admin > Reboot** takes you to the Reboot System page, which enables you to restart or shut down the system.

## Reboot RAID

The Reboot RAID System section has three options:

- **Rolling Restart**: For dual-controller units with certain configurations, this allows you to restart the RAID Controllers without losing host connectivity or data transfer capability. During a rolling restart, each RAID Controller reboots individually.

  For a rolling restart to be performed, both RAID Controllers must be fully operational and have the same firmware version (see Update Firmware, page 10-9), and the system must be in mode that supports controller failover (Active-Active or All Ports All LUNs—see System Mode, page 10-6). If one or more of these conditions is not met, the **Rolling Restart** option is grayed out.

  **Note** In order to avoid host connection timeout during a rolling restart, disk timeouts for all hardware and virtual servers should be set to 150 seconds.

  **Note** On single-controller units, this option does not appear.

- **System Reboot** (default): This option executes a full restart of the system. While the system is rebooting, the unit is offline, and arrays and volumes are inaccessible. Therefore, hosts should be safely shut down or disconnected before performing a System Reboot. After the system has finished rebooting, the arrays and volumes are once again accessible.

- **System Shutdown**: This option flushes the cache data to the disks and shuts down the system. Therefore, hosts should be safely shut down or disconnected before performing a System Shutdown. System Shutdown does NOT turn the system completely off; the power supply units (PSUs) are still active, and fans may still run. To completely power off the system, or to bring the system back on line after a shutdown, follow the instructions in the system's Hardware Manual.

To perform a reboot or shutdown:

**Step 1** Select the desired reboot option.

**Step 2** Check the confirmation box.

**Step 3** Click **Execute NOW** to reboot the system.

A message is displayed, informing you that the reboot or shutdown sequence is in progress.

**Step 4** When the unit is back online, click the **Back** button to return to the Reboot System page.

**Note** While a rolling restart or reboot operation is in progress, the system status icon may indicate a FAILURE. The FAILURE message will clear once the system is fully restarted.

# Controller Maintenance

The Controller Maintenance section allows you to take a RAID Controller offline for maintenance or diagnostic purposes. It also allows you to test failover settings (see System Mode, page 10-6) before deploying the system into your production environment. The RAID Controller that is currently being used to access the Cisco Video Surveillance Storage System Management Console is noted by the text "(current)" after it.

**Note** Taking the "current" RAID Controller offline can cause the Management Console to become unresponsive for up to a minute as the host connections are passed to the other controller.

To take a RAID Controller offline:

**Step 1** Select the RAID Controller to be taken offline.

**Step 2** Check the confirmation box.

**Step 3** Click **Execute NOW**.

The selected RAID Controller is taken offline, and control of the arrays is passed to the other RAID Controller (if the unit has two controllers and is in an Active-Active or All Ports All LUNs mode—see System Mode, page 10-6).

**Step 4** Click the **Back** button to be returned to the Reboot System page.

To re-enable the RAID Controller:

**Step 1** Click the button next to **Re-enable controller *N***.

**Step 2** Check the confirmation box.

**Step 3** Click **Execute NOW**.

The RAID Controller is put back on line.

**Step 4** Click the **Back** button to return to the Reboot System page.

## Power Restoration Policy

On CPS-SS-4RU units, the Power Restoration Policy section controls how the unit behaves after A/C power has been restored after an interruption (due to power failure or the removal of the power cords).

- **Boot immediately after power is restored**: After power is restored, the unit automatically starts up. This is the default setting.
- **Remain unpowered until the controller push-switch (SW0) is pressed**: After power is restored, the unit will not start up until the **SW0** switch on either RAID Controller is pressed. This switch must be pressed for approximately 4 seconds to start the unit, then released as soon as the unit begins to power up.

Select the desired power restoration policy and click **Save Configuration**. A message is displayed, informing you that the settings has been saved. Click the **Back** button to return to the Reboot System page.

# Configure Rebuild Priority

Clicking **System Admin > Rebuild Rate** takes you to the Configure Rebuild Priority page, which lets you customize the amount of system I/O time dedicated to rebuilding critical arrays.

There are five rebuild rates, arranged from **Lowest** to **Highest**. The default setting is **Medium**.

When there is high host activity, less spare I/O time is available, which can result in longer rebuild times. In this situation, it may become necessary to increase the rebuild priority so that arrays are rebuilt more quickly.

Select the desired rebuild rate and click **Set Rebuild Priority**. A message is displayed, informing you that the setting has been saved. Click the **Back** button to return to the Configure Rebuild Priority page.

**Caution** Your data is vulnerable while an array is critical. Depending on RAID level, any further disk failures could mean your data becomes unavailable to your host.

# Verify RAID Arrays

Clicking **System Admin > Verify Config** takes you to the RAID Array Verify page, which lets you configure the method and frequency of RAID array verification.

### Schedule RAID Array Verification

To set up a RAID array verification schedule, configure the following settings:

- **Select verify utility to use**: There are two different verification utilities available: **Surface scan** and **Parity scrub**.
  - **Surface scan** (default) reads all blocks on each disk drive in the array to ensure their integrity. If it encounters a bad block, it will quarantine that block and rebuild it using mirrored data (for RAID 1 or 10) or parity data (for RAID 4, 5 or 6).

    **Note** NOTE: If bad data blocks occur on arrays configured as RAID 0, Surface scan will not be able to rebuild the data.

  - **Parity scrub** (available for RAID 4, 5, and 6) reads all array data and ensures that the parity data is intact. If it encounters a parity inconsistency, it will correct the inconsistency. **Parity scrub** also rebuilds bad data blocks in a similar fashion to **Surface scan**.

  If you do not wish RAID array verification to be scheduled, select **None**.
- **Verify interval**: This settings tells the unit how often to automatically run the selected verification utility. You can select **1 week** (the default), **2 weeks**, or **4 weeks**.
- **Verify schedule**: Use the drop-down lists to select the day of the week and the time of day to begin running the selected verification utility. This allows you to schedule the verification for a time when data activity is low.

When you have configured the verification schedule, click **Save Settings**. A message is displayed, informing you that the settings have been updated. Click the **Back** button to return to the RAID Array Verify page.

When a verification utility is running, you can check its progress on the RAID Array Utility Progress page (see RAID Array Utility Progress, page 4-3).

#### Start or Stop RAID Array Verification Immediately

- To perform a RAID array verification immediately, select the verification tool (**Surface scan** or **Parity scrub**) and click **Execute verify utility NOW**. A message is displayed, informing you that the verification utility will begin shortly. Click the **Back** button to return to the RAID Array Verify page.

  Progress can monitored on the RAID Array Utility Progress page (see RAID Array Utility Progress, page 4-3).
- To stop a RAID array verification in progress (for instance, if it is negatively impacting host I/O performance), click the **Stop Verification** button. A message is displayed, informing you that the verification will soon be stopped. Click the **Back** button to return to the RAID Array Verify page.

# System Mode

Clicking **System Admin > System Mode** takes you to the System Mode page, where you can configure the failover mode for the unit.

"Failover" is the term used for when one RAID Controller takes over the host connections and array control of the other RAID Controller when that controller fails. There are several ways to implement failover, depending on whether the storage area network (SAN) uses switches, multiple host ports, and/or hostbased multipathing software.

**Caution** If the unit is in Single Controller or Dual Controller Non-Redundant (DCNR) mode, or if cache mirroring is not enabled (see Configure Cache, page 10-1), data stored in the write cache may be lost if a RAID Controller fails.

**Note** If the System Mode is changed, volumes may become temporarily inaccessible. If this occurs, you must remap them (see Map Logical Volumes, page 7-4).

The possible settings for System Mode are:

- **Single Controller mode** (default): In this mode, only one RAID Controller is active, and failure of this controller makes all arrays and volumes inaccessible. This is the only possible setting on single-controller units, but it is possible to set a dual-controller unit to Single Controller mode.
- **Dual Controller Non-Redundant mode (DCNR)**: In this mode, both controllers are active, but each controller operates as an independent node, and all ports are independent from each other. Volumes can only be mapped to ports on the controller that owns the array. They become inaccessible if the controller fails.

  **Note** NOTE: Although DCNR mode does not allow failover, overall system performance may increase slightly.

- **2-port Active-Active mode (2 ports active)**: In this mode, each controller operates as an independent node, but only one port is active on each controller. The second port operates in passive mode. Port **0** is active on controller 0, and port **1** is active on controller 1. Volumes are mapped to the active port on their owning controller. When one controller fails, the passive port on the other controller activates and takes over the host port functions of the failed controller. In a switched environment, failover is completely transparent to the hosts. This mode is suitable for customers who want to be able to handle controller failover, but do not have multipathing software.

  **Note** For failover to occur, hosts must be connected to the same numbered port on both controllers.

  **Note** iSCSI connections (1Gb/s and 10Gb/s) do not failover in this mode. Should a controller fail, volumes accessed through an iSCSI network will become inaccessible. To configure failover for iSCSI, use **All Ports All LUNs mode**.

- **4-port Active-Active mode (4 ports active)**: In this mode, each controller operates as an independent node, and all ports are active. Port **0** is the primary port on controller 0, and port **1** is the primary port on controller 1. Volumes must be mapped to at least one port on its owning controller and to the secondary port on the other controller. When one controller fails, the secondary port on the other controller takes on the host address of the primary port on the failed controller, allowing host I/O to continue; the host sees the storage become active through its second path.

  **Note** For failover to occur, hosts to be connected to both ports on their owning controller and to the secondary port on the other controller.

**Note** If a host is connected to both ports on any one controller, the host must be running multipathing software.

**Note** iSCSI connections (1Gb/s and 10Gb/s) do not failover in this mode. Should a controller fail, volumes accessed through an iSCSI network will become inaccessible. To configure failover for iSCSI, use **All Ports All LUNs mode**.

- **All Ports All LUNs mode (all ports active)**: In this mode, the entire system operates as a single node. Volumes can be mapped to any or all ports on both controllers. When a controller fails, the ports on that controller become inaccessible. However, if the volumes are mapped to ports on the other controller as well, they remain accessible to the host, which sees the storage become active through its second path.

**Note** For hosts to continue to have access to the LUNs after a controller failure or during a rolling restart, each volume should be mapped to at least one port on each controller (see Map Logical Volumes, page 7-4) and each host must have an active path to at least one port on each controller. Volumes mapped to only one controller become inaccessible if that controller fails or if a rolling restart is executed.

**Note** Because this mode presents up to eight paths to configured volumes, the host must be running multipathing software.

**Note** This is the only mode in which redundancy is available for all network types (Fibre Channel, SAS, 10GbE iSCSI, and 1GbE iSCSI).

Select the desired System Mode and click **Save System Mode**. A message is displayed, informing you that the setting has been saved.

When the setting is saved, click **System Admin > Reboot** and perform a **System Reboot** (see Reboot System, page 10-3).

**Note** If the System Mode setting is changed, but the system is not rebooted, the new mode will not take effect until the unit is next rebooted.

**Note** NOTE: If the System Mode is changed, volume mappings may also change. Always check the volume mappings (see Configured Logical Volumes, page 4-3) after changing the System Mode.

# Download/Upload System Settings

Clicking **System Admin > Settings** takes you to the Download & Upload System Settings page, where you can download a file with the current controller settings or upload a new controller settings file to the system.

**Caution** Because improper or incorrect settings in the settings file can prevent the unit from being accessible on the network, *always* verify the contents of a settings.dat file—both manually (by opening it as a text file) and by using the **Verify Settings File** button—before uploading and installing it.

To download the current settings.dat file, click the **Click to download controller settings** link and save the file to your computer according to the method of your operating system.

To upload a new settings.dat file to the system, do the following:

**Step 1** Click **Browse** and navigate to the file according to the method of your operating system. (If you select a wrong file, click **Clear Selection** and try again.)

**Step 2** When the file's path is displayed in the **Select file** field, click **Verify Settings File** to validate the settings.dat file.

**Note** If you wish to see more detail, check the **Advanced debugging mode** check box before clicking **Verify Settings File**.

A Settings File Processing Report is displayed. Errors are shown in red text.

**Step 3** If there are errors, fix them in the settings.dat file and repeat Step 1.

**Step 4** Click **Upload and Install Settings**.

The settings.dat file is automatically installed, although some settings will only take effect after a system restart (see Reboot System, page 10-3).

# Update Firmware

Clicking **System Admin > Update Firmware** takes you to the Update Firmware page, which allows you to upload new RAID Controller firmware and emergency firmware.

Firmware updates are periodically released to introduce new features or to solve firmware-related issues.

To upload a new firmware file, do the following:

**Step 1** Ensure that both RAID Controllers on the unit are up and running (if applicable).

**Step 2** On the Update Firmware page, click **Browse** and navigate to the extracted firmware file according to the method of your operating system. (If you select the wrong file, click **Clear File Selection** and try again.)

**Step 3** When the file's path is displayed in the **Select file** field, click **Upload Firmware**.

**Note** The firmware file may take several minutes to be sent over the network. You will see NO response from the browser while this is happening.

**Step 4** If the progress window is not displayed automatically, click the **Click this text ...** link.

The progress bar shows the progress of the installation. When the installation is complete, the message "Firmware update finished, status - 'Microcode Updated OK'" is displayed:

**Step 5** Click the **Return to GUI** button to be taken to the Reboot System page (see Reboot System, page 10-3).

**Step 6** Restart the system using a **Rolling Restart** (if available) or a **System Reboot**.

**Step 7** When the reboot has completed, verify that the update was successful:

**a.** Go to **System Information > System Info** and check that the **Firmware revision** and **Build Loader revision** for both controllers are updated.

**b.** If hosts were shut down or disconnected for the system reboot (see Reboot System, page 10-3), reconnect them to the storage unit.

**c.** Ensure that your volumes are visible and working as expected.

**Step 8** Update the emergency firmware, if required:

**Note** This does not require a reboot and can safely be carried out at any time.

**a.** Check your current **Emergency revision** on the System Information > System Info page.

**b.** If an emergency firmware update is required, upload it using Step 2 through Step 5.