CF205R008 Release Notes

Product	Software Version: CF205R008 for StorNext QX-1200 and QX-2400 base systems
Operating Systems	• Microsoft Windows Server 2008 (IA32 and x64, Standard, Enterprise, and Datacenter editions) • Microsoft Windows Server 2008 R2 (x64, Standard, Enterprise, and Datacenter editions) • Microsoft Windows Server 2008 and 2008 R2 x64 Hyper-V • Red Hat Enterprise Linux 5.6, 5.7, 5.8, 6.1, 6.2 (IA32, x64) • SuSE Linux Enterprise Server 10.4 and 11 SP1 and SP2 (x64 and IA32) • VMware ESX 4.0, 4.1, and 5.0 • Solaris 10 (x86 only), Solaris 11 • Apple OS X (Snow Leopard 10.6 and 10.7)
Date	April 2015

Contents

Description

This CF205R008 firmware release applies to the StorNext QX-1200 and QX-2400 systems.

This firmware release fixes controller crashes, corrected total I/Os data transfer and response time when one controller is shut down, and corrected the number of supported initiators to 1024 total.

Recent Enhancements

This section provides recent enhancements for the following:

- CF205R008 Firmware
- CF100P002 Firmware
- CF100R038 Firmware
- CF100R036 Firmware

CF205R008 Firmware

The enhancements for CF205R008 include fixes for:

- Controller crashes
- Total I/Os data transfer and response time when one controller is shut down
- Initiators corrected back to 1024 total
- Degraded Disk Detection for drives that exhibit a trend of degrading quality of service.

- Parallel Disk Firmware Update enables loading firmware onto multiple disks in a single operation.

CF100P002 Firmware

There are no enhancements for the CF100P002 Firmware.

CF100R038 Firmware

The enhancements for CF100R038 include:

- Performance improvements.
- Eliminate I/O impact on getting logs.
- Changes to support 1024 initiators per port.
- Increase the system-wide PGR registration limit from 1024 to 32k.
- Added support for the CLI down disk command.
- Updated algorithm for Compact Flash diagnostic speed test for Tricor C1 P9 component.
- Disable PCIE Error stat checking.

CF100R036 Firmware

The enhancements for CF100R036 include:

- 23852: Eliminate I/O impact on getting logs.
- 27487: Changes to support 1024 initiators per port.
- 27375: Increase the system-wide PGR registration limit from 1024 to 32k.
- 27573: Added support for the CLI down disk command.
- 27643: Updated algorithm for Compact Flash diagnostic speed test for Tricor C1 P9 component.
- Disable PCIE Error stat checking.

Supported Configurations

The following summarizes the supported configurations for this firmware release. The supported configurations are:.

- QX-1200/QX-2400 base supports QX-1200/QX-2400 expansions

Important Firmware Notes

Always update controller firmware when:

- Installing a new system
- Adding disk expansion(s)
- Replacing a controller module(s) or expansion (IOM) module(s)
- Updating controller firmware with expansion modules active ensures that the controller firmware and expansion IOM firmware are at a compatible level.

Recent Fixes

This section provides recent fixes. This is the firmware release for the StorNext QX-1200 and QX-2400 systems. This section provides recent fixes as follows:

- CF205R008 Firmware
- CF100P002 Firmware
- CF100R038 Firmware
- CF100R036 Firmware

CF205R008 Firmware

Recent fixes for CF205R008 include:

- 32940: Controller crashes with `OSMAssertParam4`.
- 33445: Total I/Os, data transferred and response time are shown as 0 when one controller is shutdown.
- 35430: Initiators changed from 64 to 1024 total.
- Delete schedule doesn't work and hangs terminal, when the task was already deleted.
- Junk characters are observed in the event logs when a scheduled task is initiated.
- Disabled the HIO sequencer raw ctr QD debug information.
- Resolved a flaw in logic in setting Ethernet parameters during the boot up. It is not properly reading the existing settings so forcefully setting it to 10Mbps Half Duplex.
- The Help page was blank when using Internet Explorer 11.
- Fix for Drive FW upgrade failure.
- Fix for “disk detected error” message when rescan, shutdown, restart, firmware code load is performed on 3TB and 4TB SAS MDL drives.

- Added changes to the CLI set led command to properly turn on and turn off the of enclosure, controller A, and controller B LEDs.
- When trying to set the start “time range” value in the vdisk performance statistics tab, “start time” was forwarded to 15 minutes prior to the user-specified value.
- Fixed MC NOT TALKING issue after changing the IP Address of the Controllers.
- Scheduled task did not start drive shutdown. .
- Unable to modify user interfaces from WBI.
- Warning/error message is not displayed in the same screen for the password setup field if invalid characters are given.
- While collecting logs from FTP, getting invalid/ misleading error messages.
- Show the complete information of a drive in a disk detected error event message.
- Removed unsupported CHAP commands.
- Removed DMS-related commands and help since DMS software features are not supported in this product.
- Drive scrub status percentage is updating correctly in CLI.
- Fixed problems with using a forward slash in a password.
- Removed Independent Cache Mode option
- Prevent RAID1 scrubs from starting until cache has completed destaging data that was previously interrupted by a power failure.
- User with Monitor role is able to change system settings.
- Modified the code to correctly find the number of partitions associated with a specific container while force-changing the preferred owner of the container.
- Unable to create an SNMP V3 user with auth type:none and privacy type:DES.
- Log messages erroneously indicating an MC is missing or down.

CF100P002 Firmware

Recent fixes for CF100P002 include:

- Removed the OpenSSL CVE-2014-0160 (Heartbleed) vulnerability, and applied a nwly issued SSL certificate to the array.

  Fixed problem where CLI restore users and restore defaults commands did not work when connected directly to the USB port.
- Fixed an MTO issue with PCIE Link Recovery.

CF100R038 Firmware

Recent fixes for CF100R038 include:

- Heart Bleed bug fix
- Message Timeout (MTO, issue with PCIe link recovery) fix

- Correct the event reporting mechanism for correctable ECC errors.
- Eliminate a page fault caused by a metadata locking conflict during global spare drive allocation.
- Improve Compact Flash error handling to prevent a controller crash.
- Implement a chip supplier's recommended timing change to prevent a rare SAS chip failure during initialization.

CF100R036 Firmware

The fixes for CF100R036 include:

- 25303: Correct the event reporting mechanism for correctable ECC errors.
- 26776: Eliminate a page fault caused by a metadata locking conflict during global spare drive allocation.
- 27852: Improve Compact Flash error handling to prevent a controller crash.
- 28014: Implement a chip supplier's recommended timing change to prevent a rare SAS chip failure during initialization.

Installation Instructions

The following sections discuss installing firmware:

- Installation Notes and Best Practices
- Installation Troubleshooting
- Installation Instructions Using the GUI
- Updating Expansion Module Firmware Using the GUI
- Installing Firmware Using FTP

Installation Notes and Best Practices

WARNING: Do not cycle power or restart devices during a firmware update. If the update is interrupted or there is a power failure, the module could become inoperative. If this occurs, contact technical support. The module may need to be returned to the factory for re-programming.

Caution: Before upgrading firmware, ensure that the system is stable and is not being re-configured or changed in any way. If changes are in progress, monitor them and wait until they are completed before proceeding with the upgrade.

- As with any firmware upgrade, it is a recommended best practice to ensure that you have a full backup prior to the upgrade.
- When planning for a firmware upgrade, schedule an appropriate time to perform an online upgrade.

  - For single domain systems, I/O must be halted.
  - For dual domain systems, because the online firmware upgrade is performed while host I/Os are being processed, I/O load can impact the upgrade process. Select a period of low I/O activity to ensure the upgrade completes as quickly as possible and avoid disruptions to hosts and applications due to timeouts.
- When planning for a firmware upgrade, allow sufficient time for the update.
  - In single-controller systems, it takes approximately 10 minutes for the firmware to load and for the automatic controller restart to complete.
  - In dual-controller systems, the second controller usually takes an additional 20 minutes to update, but may take as long as one hour.
- During the installation process, monitor the system to determine update status and know when the update is complete.
- After the installation process is complete and all controllers have automatically restarted, verify system status in the GUI or the CLI and confirm that the new firmware version is displayed as running on all controllers.
- Updating array controller firmware may result in new event messages that are not described in earlier versions of documentation. For comprehensive event message documentation, see the current version of the System Event Descriptions Reference Guide.

Installation Troubleshooting

If you experience issues during the installation process, do the following:

1. When viewing system version information in the StorNext Disk Storage Management Utility System Overview panel, if an hour has elapsed and the components do not show that they were updated to the new firmware version, refresh the web browser. If version information is still incorrect, proceed to the next troubleshooting step.
2. If version information does not show that the new firmware has been installed, even after refreshing the browser, restart all system controllers. For example, in the CLI, enter the **restart mc both** command. After the controllers have restarted, one of three things happens:
   - Updated system version information is displayed, and the new firmware version shows that it was installed.
   - The Partner Firmware Update process automatically begins and installs the firmware on the second controller. When complete, the versions should be correct.
   - System version information is still incorrect. If system version information is still incorrect, proceed to the next troubleshooting step.
3. Verify that all system controllers are operating properly. For example, in the CLI, enter the **show disks** command, and read the display to confirm that the displayed information is correct.
   - If the **show disks** command fails to display the disks correctly, communications within the controller have failed. To re-establish communication, cycle power on the system, and repeat the **show disks**

command. (Do not restart the controllers; cycle power on the controller enclosure.)

- If the **show disks** command from all controllers is successful, perform the firmware update process again.

Installation Instructions Using the GUI

Note: It takes approximately 10 minutes for the firmware to load and for the automatic restart to complete. Progress messages are displayed in the FTP interface during that time. Wait for the progress messages to specify that the firmware load has completed. If the system **Partner Firmware Update** (PFU) option is enabled, allow an additional 20 minutes for the partner controller to be updated. No messages are displayed in the FTP interface during PFU.

A controller enclosure can contain one or two controller modules. In a dual-controller system, both controllers should run the same firmware version. Storage systems in a replication set must run the same firmware version. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

If you have a dual-controller system and the Partner Firmware Update option is enabled, when you update new controller the system automatically updates the partner controller. If Partner Firmware Update is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

Firmware update is supported from any of the following versions: CF205R002, CF100R003-02, CF100R036, CF100R038.

To update controller-module firmware:

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to the system before you start the firmware update.
3. Restart the Management Controller (MC) in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers.
4. Do one of the following:
   - In the banner click the system panel and select **Update Firmware**.
   - In the System topic select **Action > Update Firmware**.

   The Update Firmware panel opens. The Update Controller Modules tab shows versions of firmware components that are currently installed in each controller.
5. Click **Choose File** and select the firmware file to install.
6. If you have a dual-controller system and want firmware to be automatically updated in both controllers, under Partner Firmware Upgrade select the Enabled check box and click **Set**. (PFU is enabled by default.) Otherwise, if PFU is disabled, after updating firmware on one controller you must log into

the partner controller and perform this firmware update on that controller also.

7 Click **OK**. A panel shows firmware-update progress.

The process starts by validating the firmware file:

- If the file is invalid, verify that you specified the correct firmware file. If you did, try downloading it again from the source location.
- If the file is valid, the process continues.

Firmware updates typically take 10 minutes for a controller with current CPLD firmware, or 20 minutes for a controller with down-level CPLD firmware. If the controller enclosure has connected enclosures, allow additional time for each expansion module's enclosure management processor (EMP) to be updated. This typically takes or 3 minutes for each EMP in an expansion enclosure.

If the Storage Controller cannot be updated, the update operation is canceled. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

When firmware update on the local controller is complete, users are automatically signed out and the MC restarts. Until the restart is complete, sign-in pages say that the system is currently unavailable.

When this message is cleared, you may sign in again.

If PFU is enabled, allow 10 to 20 minutes for the partner controller to be updated.

8 Clear your web browser cache, then sign in to the GUI. If PFU is running on the controller you sign in to, a panel shows PFU progress and prevents you from performing other tasks until PFU is complete.

Updating Expansion Module Firmware Using the GUI

An expansion enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

Expansion-module firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion module by loading a firmware file obtained from the enclosure vendor.

To update expansion module firmware:

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to the system before you start the firmware update.
3. Do one of the following:
   - In the banner click the system panel and select **Update Firmware**.
   - In the System topic select **Action > Update Firmware**.

   The Update Firmware panel opens.

4 Select the **Update Expansion Modules** tab. This tab shows information about each expansion module in the system.

5 Select the expansion modules to update.

6 Click **Choose File** and select the firmware file to install.

7 Click **OK**. Messages show firmware-update progress.

It typically takes 3 minutes to update each EMP in an expansion enclosure. Wait for a message that the code load has completed.

Verify that each updated expansion module has the new firmware version.

Installing Firmware Using FTP

Note: It takes approximately 10 minutes for the firmware to load and for the automatic restart to complete. Progress messages are displayed in the FTP interface during that time. Wait for the progress messages to specify that the firmware load has completed. If the system **Partner Firmware Update** (PFU) option is enabled, allow an additional 20 minutes for the partner controller to be updated. No messages are displayed in the FTP interface during PFU.

A controller enclosure can contain one or two controller modules. In a dual-controller system, both controllers should run the same firmware version. Storage systems in a replication set must run the same firmware version. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

If you have a dual-controller system and the Partner Firmware Update option is enabled, when you update one controller the system automatically updates the partner controller. If Partner Firmware Update is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

Firmware update via FTP is supported from any of the following versions: CF205R002, CF100R003-02, CF100R036, CF100R038.

To update controller-module firmware:

1 Obtain the appropriate firmware file and download it to your computer or network.

2 Place the downloaded firmware package in a temporary directory.

3 Locate the firmware file in the extracted folder.

4 In the Disk Management Utility, prepare to use FTP:

  a Determine the network-port IP addresses of the system controllers.

  b Verify that the system FTP service is enabled.

  c Verify that the user you will log in as has permission to use the FTP interface and has manage access rights.

5 In single-domain environments, halt I/O to vdisks before starting the firmware update.

6 Restart the Management Controller (MC) in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers.

7 Open a command prompt (Windows) or a terminal window (UNIX), and navigate to the directory containing the firmware file to load.

   a Enter a command using the following syntax: `ftp <controller-network-address>`.

   b Log in as an FTP user (user = `ftp`, password = `flash`).

   c Enter a command using the following syntax: `put <firmware-file> flash`.

8 If needed, repeat these steps to load the firmware on additional modules.

9 Quit the FTP session.

If the Storage Controller cannot be updated, the update operation is canceled. If the FTP prompt does not return, quit the FTP session and log in again. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

When firmware update on the local controller is complete, the message Operation Complete is printed, the FTP session returns to the ftp> prompt, and the FTP session to the local MC is closed.

10 Clear your web browser's cache and then sign in to the GUI. In the GUI display, verify that the proper firmware version appears for each module. If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

Note: If you attempt to load an incompatible firmware version, the message `*** Code Load Fail. Bad format image. ***` is displayed and after a few seconds the FTP prompt is redisplayed. The code is not loaded.

Note: If you are using a Windows FTP client, during firmware update a client-side FTP application issue can cause the FTP session to be aborted. If this issue persists, try using Storage Management Console to perform the update, use another client, or use another FTP application.

Note: After firmware update has completed on both controllers, if the correct version does not appear for a component or if the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

Rebranding Instructions

After applying the firmware, follow the steps in this section to rebrand the QX arrays to ensure that the Quantum-branded splash screen displays properly.

This procedure involves FTPing the `QUANTUMSTORNEXT.bin` binary file (available on CSWeb) onto each controller. This binary file **must** be applied through FTP, and cannot be applied through the GUI.

1. If you did not already download the binary file `QUANTUMSTORNEXT.bin` when you downloaded the firmware, do so now.
2. Apply the Quantum branding .bin file:
   a. **`ftp <ArrayIP>`**
   b. **`put QUANTUMSTORNEXT.bin flash`**
3. Repeat the procedure for the second controller, using that controller's IP address.
4. Reboot the storage controller, and then clear the browser cache.
5. Confirm that Quantum-branded splash screen and GUI appear.

Known Issues

This section describes known issues for the following:

- CF205R008 Firmware
- CF100P002 Firmware
- CF205R002 Firmware
- CF100R038 Firmware

CF205R008 Firmware

There are no known issues for CF205R008 firmware.

CF100P002 Firmware

There are no known issues for CF100P002 firmware.

CF205R002 Firmware

Known issues and workarounds for CF205R002 firmware include:

Issue	Workaround
A drive FW updated success message pop-up window occurs continuously.	Reset the MC.
The CLI show redundancy-mode command reports a controller is operational when it is down.	None

Issue	Workaround
When replacing a controller while logged in to the other controller, the CLI session is disconnected with no warning other than a "Killed" message.	After a brief wait, log back in to the controller. If that session is killed, wait before logging back in.
In a VMware environment, if no LUN 0 exists host drivers might be unable to find a LUN to which they should have access.	Use the CLI set advanced-settings command or RAIDar's Advanced Settings to set Missing LUN Response to illegal (Illegal Request).
Cannot use both controller FC ports at the same time when Independent Cache mode is enabled.	Disable independent cache.

CF100R038 Firmware

Known issues and workarounds for CF100R038 firmware include:

Issue	Workaround
In a VMware environment, if no LUN 0 exists host drivers might be unable to find a LUN to which they should have access.	Use the CLI set advanced-settings command or Disk Management Utility's Advanced Settings to set Missing LUN Response to illegal (Illegal Request).
Cannot use both controller FC ports at the same time when Independent Cache mode is enabled.	Disable independent cache.

Contacting Quantum

More information about this product is available on the Service and Support website at http://www.quantum.com/ServiceandSupport/Index.aspx. The Service and Support Website contains a collection of information, including answers to frequently asked questions (FAQs). You can also access software, firmware, and drivers through this site.

For further assistance, or if training is desired, contact the Quantum Customer Support Center:

United States	1-800-284-5101 (toll free) +1-720-249-5700
EMEA	+800-7826-8888 (toll free) +49-6131-3241-1164
APAC	+800-7826-8887 (toll free) +603-7953-3010
For worldwide support: http://www.quantum.com/ServiceandSupport/Index.aspx	