



Exos[®] CORVAULT[™]

S120R003 Release Notes

Part Number 205071100-02, A • April 2025

Description

This package delivers S120R003 firmware for Exos CORVAULT storage enclosures.

Update recommendation

This is a recommended firmware update.

Supported upgrade paths

You may upgrade *to* this firmware bundle from S100R014-02 or S120R002-02. Direct upgrade from controller firmware below S100R014-02 is not supported. If you have controller firmware below S100R014-02, please contact Seagate Support to determine the required steps to upgrade to this S120R003.

NOTE After updating to S120, downgrading to S100 firmware is not supported.

Supported downgrade paths

You may downgrade *from* this firmware bundle to S120R002-02.

Operating systems

Supported operating systems include:

- Windows 2022 Hyper-V, Windows Server 2022, Windows Server 2019
- Ubuntu 20.04 LTS, 22.04 LTS
- Debian 11, 12
- CentOS 7.90, 8.5
- Redhat RHEL 8.7, 9.1
- SuSe 12.5, 15.4
- VMWare ESXi 7.0, 8.0
- Rocky Linux 9.1

Installation instructions

To install this firmware by using either the Storage Management Console or the SFTP/FTP interface, see the *Seagate Exos CORVAULT Storage Management Guide*.

New features or enhancements in S120R003

- Changed system to use DHCP addressing instead of static addressing by default.

Issues fixed in S120R003

- Fixed an issue where replacing a SAS expander left it in a fault state.
- Fixed an issue where ADR didn't complete on all drives.
- Fixed an issue for SATA systems where event 358 was improperly logged for a missing drive in the 10-drive bay.
- Fixed an issue that resulted in Management Controller memory exhaustion or restarts.
- Fixed an issue that prevented the EULA from being displayed in the Storage Management Console.
- Fixed an issue where after replacing a failed drive, multiple drives in the same disk group were left in a fault state.
- Fixed an issue that left 12 drives in a failed state after the controller tried to recover from a potential drive-channel failure.
- Fixed an issue where the ADR queue was blocked by single drives, when the first drive in the queue failed but was not removed from the queue.
- Fixed an issue that occurred when multiple ADR (remanufacture) operations were issued over time to the same drive. The drive reported that it exceeded the number of remanufacture operations instead of reporting that ADR failed.
- Fixed an issue where controller A crashed while controller B was performing ADR for an ADAPT disk group.
- Implemented a change to save the ADR drive queue across power-cycle and shutdown-restart operations.
- Fixed an issue where if both controllers were simultaneously running ADR operations with queued operations behind them, a drive in that queue could be marked leftover and cause the queue to end up in failed state.
- Fixed an issue where after a shutdown-restart, some drive slots were reported as degraded even though they were healthy.
- Provided help for the `abort disk-firmware-update` CLI command.
- Implemented security improvements.

Known issues and workarounds

 **IMPORTANT** The Intelligent Drive Firmware Update feature has known issues and it is recommended not to use this feature.

Firmware update
Issue: In rare cases, a system firmware bundle update operation can error out with error "BP: Error: Fatal".
Workaround: Wait 15 minutes after seeing this error and check whether the update succeeded. If it did not succeed, retry the codeload.
Issue: In rare occasions, system firmware bundle update will fail with error "EXCEPT: timeout – timed out".
Workaround: Wait 15 minutes and then check whether the update eventually succeeded. If it did not succeed, retry the codeload.

Issue: While drive firmware is being updated with the Intelligent Drive Firmware Update (IDFU) feature, drive firmware can still be updated using the single drive firmware update method. Workaround: If the <code>show firmware-update-status</code> command shows IDFU In-Progress, do not perform any other drive firmware updates. Further, it is not recommended to use IDFU in this release.
Issue: In very rare cases, codeload can fail due to the midplane experiencing an I²C failure. In this case, the MC on the controller experiencing the I²C failure will be down. Workaround: Reboot the controller that experienced the I²C failure.
Issue: Disks' unrecoverable read error thresholds do not update after upgrading to code with different thresholds. Workaround: After firmware upgrade, reboot the controllers to make the new disk thresholds take effect.
Issue: When two Exos E 4U106 expanders running GEM 5.2 replaced two CORVAULT expanders in a system running newer firmware, only one of the two expanders was updated to the newer firmware version. Workaround: Follow the procedure to replace a SAS expander. If the expanders do not show up, disable PFU and re-load the firmware onto one controller and wait for expander firmware to update, then repeat the process on the other controller. Power cycle and the expander firmware will be loaded.
Shutdown/restart
Issue: In rare cases, a controller will crash on boot during host channel diagnostics. Workaround: Within an applicable service window where downtime is acceptable, power cycle the system. If the issue persists, replace the controller.
Issue: In rare cases, a controller can crash on boot during diagnostic tests. Workaround: The controller will automatically recover after 3-4 minutes.
Drive pull
Issue: If a Degraded disk is pulled and replaced while its owning disk group is undergoing Reconstruct, the slot status for 5 to 11 other drives will briefly show as Degraded. Workaround: Wait 3 minutes for the Degraded drive slot status to clear.
Issue: When multiple drive models are present in the system and multiple disk firmware bundles are loaded to the system, the bundles will incorrectly show as Active in the CLI and WBI. Workaround: To activate one of the disk firmware bundles, ignore that the bundle status shows Active and run the <code>activate firmware</code> CLI command on the bundle.
Crash/hang
Issue: The Management Controller can hang resulting in failed logins via the WBI, Telnet, and FTP. Workaround: Wait 6 minutes for the Management Controller to auto-recover.
Issue: In the rare case of an expander firmware crash, some drives' Usage will show Leftover (LEFTOVR). Workaround: Clear the metadata on the Leftover drives and add them back into a disk group.
Issue: In rare cases, a controller can crash with a page fault after this sequence of operations: create a disk group, run <code>trust</code> on the disk group, and then map volumes on the disk group. Workaround: From the partner controller, run the <code>unfail controller</code> CLI command to restore the failed controller.
FRU replacement
Issue: If a power-supply unit (PSU) is removed, old version information for the removed PSU remains displayed even though the health is reported as Fault and there is a warning for the PSU being missing or not operational. Workaround: Replace the missing PSU.

Issue: After online expander replacement, one or more disks in a disk group become Leftover (`LEFTOVR`). Subsequent actions depend on whether the disk group has moved into a quarantined state.

- If the disk group is *not* quarantined (sufficient disks remain in the disk group for data integrity), the storage system will use the spare capacity to reconstruct the disk group and then rebalance the disk group. After rebalancing is complete, run the `clear disk-metadata` CLI command to clear the metadata on the Leftover disks, which will enable the disk group to automatically incorporate those disks.
- If the disk group is quarantined, run the `rescan` CLI command to recover the disk group with no data integrity issues.

If you have questions about these procedures, contact technical support.

Workaround: None.

ADR

Issue: After ADR completion, the usage of a disk in a disk group was reported as `AVAIL` instead of `LINEAR POOL`.

Workaround: In the SMCOr CLI, perform a rescan to update the usage value.

© 2025 Seagate Technology LLC or its affiliates. All rights reserved. Seagate, Seagate Technology, and the Spiral logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. CORVAULT and Exos are either trademarks or registered trademarks of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. When referring to drive capacity, one gigabyte (GB) equals one billion bytes, one terabyte (TB) equals one trillion bytes, and one petabyte (PB) equals one thousand terabytes. Your computer's operating system may use a different standard of measurement and report a lower capacity. In addition, some of the listed capacity is used for formatting and other functions, and thus will not be available for data storage. Actual data rates may vary depending on operating environment and other factors, such as chosen interface and drive capacity. The export or re-export of Seagate hardware or software is regulated by the U.S. Department of Commerce, Bureau of Industry and Security (for more information, visit www.bis.doc.gov), and may be controlled for export, import and use in other countries. All coded instruction and program statements contained herein remain copyrighted works and confidential proprietary and trade secret information of Seagate Technology LLC or its affiliates. Any use, derivation, disassembly, reverse engineering, dissemination, reproduction, or any attempt to modify, prepare derivative works, reproduce, distribute, disclose copyrighted material of Seagate Technology LLC, for any reason, in any manner, medium, or form, in whole or in part, if not expressly authorized, is strictly prohibited. Seagate reserves the right to change, without notice, product offerings or specifications.

For the latest regulatory and compliance information see www.seagate.com/support. Scroll down to the Compliance section.