HBA 1200 Software/Firmware Release Notes

© 2023 Microchip Technology Inc. and its subsidiaries

Table of Contents

© 2023 Microchip Technology Inc. and its subsidiaries

1. About This Release

The release described in this document includes firmware, OS drivers, tools, and host management software for the HBA 1200 solutions from Microchip.

1.1 Release Identification

The firmware, software, and driver versions for this release are shown in the following table.

Table 1-1. Release Summary

Solutions release	3.2.4
Package release date	March 15, 2023
Firmware version	3.01.20.48
UEFI/Legacy BIOS	2.6.2/2.6.2
Driver versions	**Windows Drivers**: • Windows 2022, 2019, 2016, Windows 11, 10: 1010.64.0.1037 **Linux SmartPQI**: • RHEL 7/8/9: 2.1.22-040 • SLES 12/15: 2.1.22-040 • Ubuntu 18/20/22: 2.1.22-040 • Oracle Linux 7/8/9: 2.1.22-040 • Citrix Xenserver 8: 2.1.22-040 • Debian 10/11: 2.1.22-040 **VMware**: • VMware ESX 7.0/8.0: 4440.0.124 **FreeBSD/Solaris**: • FreeBSD 12/13: 4390.0.1010 • Solaris: 11: 11.4120.0.1005
ARCCONF/maxView	4.11.00.25823
PLDM	6.20.8.0

1.2 Files Included in this Release

This section details the files included in this release.

Table 1-2. Firmware Files

Component	Description	Pre-Assembly Use	Post-Assembly Use
SmartFWx200.bin	Production-signed programmable NOR Flash File. Use to program NOR Flash for boards that are already running firmware.		X

Table 1-3. Firmware Programming Tools

Tool	Description	Executable
ARCCONF	ARCCONF CLI Utility	ARCCONF BXXXXX.zip
maxView	maxView Utility	MAXVIEW XXX BXXXXX.zip

Driver Files

© 2023 Microchip Technology Inc. and its subsidiaries

Table 1-4. Windows Drivers

OS	Version
Server 2022, 2019, 2016, Windows 11, 10	x64

Table 1-5. Linux Drivers

OS	Version
RHEL 9.1, 9.0[2], 8.7, 8.6, 8.5, 7.9	x64
SLES 12 SP5, SP4	x64
SLES 15 SP4, SP3, SP2	x64
Ubuntu 20.04.5, 20.04.4, 20.04, 18.04.5, 18.04.4	x64
Ubuntu 22.04.2, 22.04.1, 22.04	x64
Oracle Linux 7.9 UEK6U3	x64
Oracle Linux 9.1, 9.0, 8.7, 8.6 UEK7	x64
Debian 11.5, 10.13	x64
Fedora 37 (inbox)	x64
Citrix XenServer 8.2.1	x64

Notes:

1. New OS support—minimally tested drivers in this release. Fully supported drivers are expected in the next release.
2. Support based off August 2022 RHEL 9.0 ISO refresh.

Table 1-6. FreeBSD, Solaris, and VMware Drivers

OS	Version
ESX 8.0, 7.0 U3/U2	x64
FreeBSD 13.1, 12.4	x64
Solaris 11.4	x64

Host Management Software

Table 1-7. maxView™ and ARCCONF Utilities

Description	OS	Executable
ARCCONF Command Line Utility	Windows x64 Linux x64 VMware 7.0 and above XenServer UEFI support	See the arcconf_B#####.zip for the installation executables for the relevant OS.
maxView™ Storage Manager	Windows x64 Linux x64 VMware 7.0 and above XenServer	See the maxview_linux_B#####.zip, maxview_win_ B#####.zip,and the maxview_vmware_B#####.zip for the installation executables.
maxView™ vSphere Plugin	VMware 7.0 and above	See the maxview_vmware_B#####.zip for the installation executables.
Boot USB (offline or pre-boot) for ARCCONF and maxView Storage Manager	Linux x64	See the maxview_offline_bootusb_B#####.zip for the .iso file.

© 2023 Microchip Technology Inc. and its subsidiaries

2. What's New?

This section shows what's new in this release.

2.1 Fixes and Enhancements

This section shows the fixes and enhancements for this release.

2.1.1 Firmware Fixes

This section shows the firmware fixes and enhancements for this release.

2.1.1.1 Fixes and Enhancements for Firmware Release 03.01.20.48

This release includes the following fixes and enhancements.

- Added support for improving secure erase time for disks supporting the WRITE SAME command.
- Added support for switching persistent event log policy without clearing the existing event logs.
- Added support for custom controller cards and backplanes.
- Disabled Min Power Mode.
- Fixed an issue where the controller is not found during system boot.
  - *Root cause*: The firmware's processing of a PCIe Configuration Write cycle to change the PCIe Maximum Payload Size value may take longer than 10 milliseconds and result in the Host system determining the controller is unresponsive. If the boot disk is attached to the controller, the host will not boot into the OS; otherwise, the OS may not report the controller in the PCIe device listings.
  - *Fix*: Firmware will ensure that PCIe Configuration cycles are completed within the PCIe Specification requirement of 10 milliseconds.
  - *Risk*: Medium
- Fixed an issue where a controller may not be found during boot and may result in a PSOD or RSOD.
  - *Root cause*: UART output by the firmware was causing a delay in processing the PCIe Configuration Write cycles leading to an Unsupported Request response sent to the host. The Unsupported Request response may result in a PSOD or RSOD by the host.
  - *Fix*: Firmware will write the log information into internal memory rather than outputting to the UART.
  - *Risk*: Low
- Fixed an issue where the required reason for controller reboot is not getting updated for the sanitize policy change.
  - *Root cause*: When the sanitize policy is changed, the firmware updates the NVRAM content of the controller with the new sanitize policy. On the next boot, the firmware uses the NVRAM content to update the current sanitize policy. However, firmware is not updating the reboot required reason for this sanitize policy change.
  - *Fix*: Firmware will update reboot required reason when the sanitize policy is changed.
  - *Risk*: Low
- Fixed an issue where, in a rare case, the controller would not be detected at bootup.
  - *Root cause*: The controller was trying to write to flash upon bootup and this was causing PCIe calls from the host to timeout.
  - *Fix*: Only write to the flash if needed and delay writing to the flash until after host boot has completed.
  - *Risk*: Low
- Fixed an issue flashing controller firmware from VMware VM, when running firmware is not the same as reported version.
  - *Root cause*: If flash from VM and reboot VM only (not server), this will result in a flash failure, yet the reported version was the new version.

© 2023 Microchip Technology Inc. and its subsidiaries

  - *Fix*: Improved logic at bootup to correctly determine which firmware version is running at bootup.
  - *Risk*: Medium
- Fixed an issue where the controller reports sanitizing complete on a hot-removed and hot-plugged back in HDD that happens while sanitize is being performed.
  - *Root cause*: There was a race condition where the sanitize status was cleared when a hot plug was detected.
  - *Fix*: Mark status of the hot plug device and do not resume sanitize if that status is set.
  - *Risk*: Low
- Fixed an issue where the spare rebuilding is not happening when a global dedicated spare is assigned for multiple arrays.
  - *Root cause*: When an array is failed or the user deletes the array, for which the spare drive is already activated, firmware failed to deactivate and update the spare drive availability to other arrays to which the global spare is assigned. Due to this, the spare drive rebuild is not started on the degraded arrays even though the spare drive is free.
  - *Fix*: Fixed the conditional checks in firmware to deactivate the spare from failed or deleted arrays.
  - *Risk*: Low
- Fixed an issue where on reboot after panic shutdown, Ownership or Revert of the drive is unsuccessful.
  - *Root cause*: When “Take Ownership” occurs, several administrative pins are changed from MSID to the new master pin (key). Similarly, when “Revert to OFS (Original Factory State)” occurs, several administrative pins are changed from existing master pin to default MSID.
  - *Fix*:
    - When Take Ownership or Revert is occurring on the drive, track the start and complete steps of the Ownership or Revert process. On boot, if the tracking information is valid, then revert the drive using the master key.
    - For enterprise drive, during Revert for the change of master pin, if the session authentication fails with STATUS NOT AUTHORIZED, then retry using the other pin (MSID).
  - *Risk*: Low
- Fixed an issue where a hot-added Managed SED is reported to the host before it is fully ready.
  - *Root cause*: Firmware is reporting a hot-added Managed SED to the host before the process of unlocking the drive is complete.
  - *Fix*: Firmware will report the Managed SED to the host when the drive is completely ready.
  - *Risk*: Low
- Fixed an issue where the failed SED drive is found during drive spin-up.
  - *Root cause*: During discovery, a locked SED drive was in Idle Power state, and when trying to spin up, it failed with access denied because the drive was locked.
  - *Fix*: Do not fail the locked SED drive so there is a chance to unlock it after device discovery has completed.
  - *Risk*: Low
- Fixed an issue of power surge when too many SATA drives are spinning up simultaneously.
  - *Root cause*: During boot, multiple SATA drives were spun up almost simultaneously during RAID metadata read; causing power surge.
  - *Fix*: Instead of Test Unit Ready command, use the ATA passthrough command with the Check Power mode command to check the power condition to determine whether to spin up the drive or not.
  - *Risk*: Low
- Fixed an issue of the Managed SED adapter password internal lockout wait timeout being reset on system reboot.

© 2023 Microchip Technology Inc. and its subsidiaries

  - *Root cause*: When a user is in Locked Out state, a message instructs user to either wait for 15 minutes or reboot the system. On reboot, firmware was resetting timer to 15 minutes.
  - *Fix*: Clear the countdown timer upon reboot to allow the user to enter the adapter password..
  - *Risk*: Low

2.1.2 UEFI/Legacy BIOS Fixes

This section shows the UEFI/Legacy BIOS fixes and enhancements for this release.

2.1.2.1 Fixes and Enhancements for UEFI Build 2.6.2/Legacy BIOS Build 2.6.2

This release includes the following fixes and enhancements:

- Added HII option, Configure Controller UEFI Driver Health Reporting in the Configure Controller Settings menu to enable or disable reporting controller configuration errors and information using driver health protocol.
- Added an HII option to unset, temporarily suspend and resume controller password options for controller based encryption settings
- The Device Information menu under Disk Utilities is enhanced with multi-LUN information such as WWID and size of multi-LUN devices.
- Added a new HII menu, Configuration, under Configure Controller Settings that permits setting the PCIe maximum read request size and also shows current values of PCIe Max Read Request Size and Max Payload Size.
- Enhanced the temperature sensor location information display under controller information menu to show as location strings.
- Fixed an issue where the **Import Foreign Local Key** option for Managed SED encryption setting appears even when no foreign devices are present.
  - *Root cause*: Eligibility check for foreign import was missing when the controller is in Locked state.
  - *Fix*: Added an appropriate eligibility check for foreign import when the controller is in Locked state.
  - *Risk*: Low
- Fixed an issue where system freezes during boot after enabling IOMMU remapping.
  - *Root cause*: UEFI driver communication queues and interfaces were using the DMA-mapped address instead of the host address.
  - *Fix*: Changed the UEFI driver communication queues to use the host allocated and mapped address.
  - *Risk*: Medium
- Fixed an issue where an incorrect value is set for the VDM Discovery option under out of band settings menu.
  - *Root cause*: The VDM Discovery option under out of band settings menu was considering incorrect values for enable and disable options.
  - *Fix*: Corrected the values per controller's expectations for the VDM Discovery option.
  - *Risk*: Low

2.1.3 Driver Fixes

This section shows the driver fixes and enhancements for this release.

2.1.3.1 Windows Driver Fixes

This section shows the Windows driver fixes and enhancements for this release.

2.1.3.1.1 Fixes and Enhancements for Windows Driver Build 1010.64.0.1037

Enter a short description of your topic here (optional).

This release includes the following fixes and enhancements.

- Fixed an issue where the Dual-Actuator device is inaccessible after receiving a Report LUN command with an allocation length less than eight.
  - *Root cause*: The driver failed to verify whether the allocation length of the Report LUN command was less than eight and updated an invalid LUN number for the Dual-Actuator device.

© 2023 Microchip Technology Inc. and its subsidiaries

  - *Fix*: The driver will not update the LUN number for the Dual-Actuator device when the allocation length of the Report LUN command is less than eight.
  - *Risk*: Low
- Fixed an issue where BSOD SYSTEM_THREAD_EXCEPTION_NOT_HANDLED is observed in systems containing a significantly large number of CPUs with BIOS setting (Sub-NUMA) SNC4 enabled.
  - *Root cause*: The BIOS SNC4 (sub NUMA cluster) switch changes the max CPU group value returned by the OS that exceeds the driver's max group count and causes a buffer overrun. The buffer overrun results in the driver accessing out of range memory triggering a SYSTEM_THREAD_EXCEPTION_NOT_HANDLED BSOD.
  - *Fix*: Dynamically get the max CPU group value from the OS to avoid the buffer overrun.
  - *Risk*: Low

2.1.3.2 Linux Driver Fixes

This section shows the Linux driver fixes and enhancements for this release.

2.1.3.2.1 Fixes and Enhancements for Linux Driver Build 2.1.22-040

This release includes the following fixes and enhancements.

- Fixed an issue of sending a command to physical devices during device discovery.
  - *Root cause*: The smartPQI driver was sending a SCSI TEST UNIT READY command to physical devices during device discovery. The driver's device discovery thread hung if a physical device failed to complete this command.
  - *Fix*: The driver no longer sends a SCSI TEST UNIT READY command to physical devices during device discovery. It uses a different method to detect sanitize/erase in progress.
  - *Risk*: Low
- Fixed an issue where the OS crashes on aarch64 servers using the out-of-box driver during driver initialization.
  - *Root cause*: The driver attempts to communicate with the controller firmware using a `writew()` kernel call to a byte aligned address. This works on x86_64 servers but fails on aarch64 systems.
  - *Fix*: Change the `writew()` to two `writeb()` calls.
  - *Risk*: Medium
- Fixed an issue where the OS crashes when a drive is hot removed during I/O stress test.
  - *Root cause*: An I/O request pointer can be invalid if the block layer provides incorrect multi-queue host tag. This can lead to invalid I/O request pointer deference.
  - *Fix*: Validate the block layer provided host tag and handle the I/O request pointer properly if an invalid host tag is received.
  - *Risk*: Low
- Fixed an issue with the driver not mapping full length of PCI BAR 0.
  - *Root cause*: The driver is only mapping the controller registers up to and including the PQI standard registers.
  - *Fix*: Update the length to include the full size of PCI BAR.
  - *Risk*: Low

2.1.3.3 VMware Driver Fixes

This section shows the VMware driver fixes and enhancements for this release.

2.1.3.3.1 Fixes and Enhancements for VMware Driver Build 4440.0.124

There are no known fixes for this release.

2.1.3.4 FreeBSD/Solaris Driver Fixes

This section shows the FreeBSD/Solaris driver fixes and enhancements for this release.

© 2023 Microchip Technology Inc. and its subsidiaries

2.1.3.4.1 Fixes and Enhancements for FreeBSD Driver Build 4390.0.1010

This release includes the following fixes and enhancements.

- Fixed an issue where a wrong LUN is reset when LUN RESET TMF is issued.
  - *Root cause*: While issuing LUN RESET TMF to the second LUN of the Dual-Actuator drive, the first LUN is also reset. In the current code, LUN address and LUN number fields are not updated in `tmf req struture` for multi-LUN devices.
  - *Fix*: Added changes in IOBypass/RAID TMF structures to send `tmf request` for multi-LUN devices.
  - *Risk*: Low
- Fixed an issue where the partition information for all LUNs of a multi-actuator drive is reported to be the same after hot-removal and hot-reinsertion of the drive.
  - *Root cause*: For a multi-actuator drive, the partition information for LUN1 is reported with the information from LUN0 after a hot-removal and hot-reinsertion of the drive. After hot-reinserting a Multi-Actuator drive, I/O to LUNs is submitted using the RAID path. However, commands sent to Multi-Actuator drives through the RAID path are not handled correctly.
  - *Fix*: Added support to send commands to Multi-Actuator drives through the RAID path when needed.
  - *Risk*: Medium

2.1.3.4.2 Fixes and Enhancements for Solaris Driver Build 11.4120.0.1005

There are no fixes and enhancements for this version.

2.1.4 Management Software Fixes

This section shows the management software fixes and enhancements for this release.

2.1.4.1 maxView Storage Manager/ARCCONF

Fixes

This section shows the maxView Storage Manager/ARCCONF fixes and enhancements for this release.

2.1.4.1.1 Fixes and Enhancements for maxView Storage Manager/ARCCONF Build 25823

This release includes the following fixes and enhancements.

- Added the Desktop maxView Web Application support where the maxView process starts when the user opens the maxView GUI and the process stops when the user closes the maxView GUI.
- Added support for PCIe Maximum Read Request Size (MRRS) configuration.
- Added Multi-Actuator drive support where maxView and arcconf displays the additional LUN details.
- Added the user configurable option to prevent halting boot process on UEFI driver health.
- Deprecated support Minimum Power mode.
- Fixed an issue where ARCCONF was displaying the “Physical Block Size” as “Unknown” for the 16 kB physical block size drives
  - *Root cause*: The 16 kB physical block size was not included in the macro and the display string which caused ARCCONF to display the string as Unknown.
  - *Fix*: Added changes to include the 16 kB physical block size in the macro and the display string.
  - *Risk*: Low
- Fixed an issue where maxView was failing to upgrade or downgrade the expander firmware.
  - *Root cause*: maxView was not passing the Expander Upgrade mode which caused the operation to fail.
  - *Fix*: Added changes to update the User Provided Mode property while passing the expander firmware upgrade parameters.
  - *Risk*: Low

2.1.4.2 PLDM Fixes

This section shows the PLDM fixes and enhancements for this release.

© 2023 Microchip Technology Inc. and its subsidiaries

2.1.4.2.1 Fixes and Enhancements for PLDM Release 6.20.8.0

This release includes the following fixes and enhancements.

- Updated the Redfish resource and annotation schema dictionaries to their latest version available in the DMTF 2022.2 schema bundle. The updated schema dictionary versions are as follows:
  - Annotations: v1.1.1 → v1.2.0
  - Drive: v1.14.0 → v1.15.0
  - Event: v1.7.0 → 1.7.1
  - Port: v1.6.0 → 1.7.0
  - StorageController: v1.5.0 → v1.6.0
  - Storage: v1.12.0 → v1.13.0
  - Volume: v1.6.2 → v1.8.0
- Added the following Redfish annotation to the Drive resource:
  - @Redfish.WriteableProperties - LocationIndicatorActive and/or WriteCacheEnabled will conditionally be added to this annotation array depending on support and validation conditions.
- The SensorId field in the GetPDR response for the individual drive temperature NumericSensor PDRs will now be set to the drive's Redfish resourceId.
- Added support for updating the SEP firmware through PLDM Type 5 commands.
  Note: Self-contained activation of the SEP firmware updates is not currently supported with this release.
- Fixed an issue where an UpdateComponent request for a drive will still be accepted with an invalid ComponentImageSize.
  - *Symptom*: When sending an UpdateComponent request with a ComponentImageSize larger than the specified allowed maximum for a drive, the response's ComponentCompatibilityResponse value is that the component can be updated when it cannot be updated.
  - *Root cause*: No check in UpdateComponent for when a component image size is too large for a physical drive. The maximum component image size allowed for a drive is 16 MiB.
  - *Fix*: Added a component image size check for a physical drive in UpdateComponent.
  - *Risk*: Low
- Fixed an issue where DurableName associated with each LUN on a Multi-Actuator drive is published with incorrect values.
  - *Symptom*: Identifiers.DurableName for each LUN on a Multi-Actuator drive resource is the same.
  - *Root cause*: The API which fetches DurableName for Multi-Actuator drives was working incorrectly.
  - *Fix*: Fixed the API that fetches DurableName for Multi-Actuator drives.
  - *Risk*: Low
- Fixed an issue where an incorrect extended error message was sent when attempting a SecureErase ACTION on a SED that is not in its OFS.
  - *Symptom*: Attempting the Drive.#SecureErase ACTION on a SED that is not in OFS will fail with the extended error message ActionNotSupported instead of the expected ResourceInUse.
  - *Root cause*: A change in firmware behavior to strip support for the drive sanitize patterns from non-OFS SEDs' IDPD response caused a preemption of the non-OFS check in the SecureErase request validation code.
  - *Fix*: Added a check of SED status when no sanitize erase patterns are supported by the drive to help determine the most appropriate extended error to send.
  - *Risk*: Low
- Fixed an issue where the updateTime field in the GetPDRRepositoryInfo command response was not being updated correctly.

© 2023 Microchip Technology Inc. and its subsidiaries

  - *Symptom*: The update time fields in the GetPDRRepoInfo response are empty.
  - *Root cause*: The update time was not maintained by PLDM.
  - *Fix*: Added code to track the update time as well as fill in the update time fields in the response.
  - *Risk*: Low
- Fixed an issue where duplicate entries for an expander were seen in the Type 5 downstream device inventory.
  - *Symptom*: The value for the 'Box' portion of the ServiceLabel identifier for a Storage Enclosure Processor (SEP) is being reported incorrectly.
  - *Root cause*: The APIs that were being used to determine SEP location were designed primarily for use with drives instead of SEPs.
  - *Fix*: Modified the construction of the ServiceLabel identifier to use the appropriate APIs to fetch the Port and Box segments.
  - *Risk*: Low
- Fixed an issue where a DriveOffline Redfish alert is not sent when a Drive resource begins a sanitize operation.
  - *Symptom*: When a Drive resource is in the Predictive Failure state and the drive is undergoing a sanitize operation, a DrivePredictiveFailure alert is generated, but a DriveOffline alert is not generated.
  - *Root cause*: When the drive is sanitizing, the logic to push a DriveOffline alert was not hit if the Drive resource is also in a Predictive Failure state.
  - *Fix*: Corrected the logic such that a DrivePredictiveFailure alert will be generated along with DriveOffline alert with a severity of OK.
    This fix also adds the following changes:
    - DrivePredictiveFailureCleared alert will now be generated along with a DriveOfflineCleared alert.
    - DriveOK alert will be now be generated along with DriveOffline alert with a severity of OK when the Drive's health changes from something other than OK to OK.
  - *Risk*: Medium
- Fixed an issue where incorrect CapabilitiesDuringUpdate flags were set for UBM PICs which do not support firmware updates.
  - *Symptom*: PLDM type 5 GetDownstreamFirmwareParameters command returns CapabilitiesDuringUpdate with CAN_BE_UPDATED bit set for UBM backplane PICs which cannot be updated.
  - *Root cause*: There was no logic to check if the UBM PIC firmware can be updated or not when sending the response for the GetDownstreamFirmwareParameters command.
  - *Fix*: Added logic to return ComponentActivationMethods and CapabilitiesDuringUpdate to be ZERO when the UBM firmware PIC cannot be updated.
  - *Risk*: Low
- Fixed an issue where an unflashable SMP PSOC device was appearing in the Type 5 downstream device inventory.
  - *Symptom*: QueryDownstreamIdentifiers and the other associated Type 5 downstream device inventory commands erroneously return a device for the enclosure SEP with the device number 380 when this device number is reserved for an unflashable SMP PSOC.
  - *Root cause*: The enclosure SEP enumeration did not have appropriate logic in place to filter out devices that were not of a type other than SEP.
  - *Fix*: Revised the SEP enumeration to not return device numbers that point to devices other than enclosure SEPs.
  - *Risk*: Low
- Fixed an issue where hot-removed SEPs could prevent other remaining SEPs from being included in the Type 5 downstream device inventory.

© 2023 Microchip Technology Inc. and its subsidiaries

  - *Symptom*: The SEP inventory returned by the Type 5 downstream device inventory commands did not agree with the SEP count returned by the controller firmware.
  - *Root cause*: Hot-removed SEPs persist in the controller firmware response as a zeroed slot. When this occurred at the beginning of the array in the firmware response, enumeration of any other SEP device numbers in the array was prevented.
  - *Fix*: Added logic to ignore zeroed entries in the firmware response when enumerating SEPs. This allows subsequent non-zero entries to be returned by the enumeration API.
  - *Risk*: Low
- Fixed an issue where a controller firmware update through PLDM fails if the final requested image segment is smaller than the spec-defined minimum transfer size.
  - *Symptom*: When updating controller firmware through PLDM Type 5, certain firmware images fail the image size validation check performed when the Type 5 State Machine is in the VERIFY state.
  - *Root cause*: The RequestFirmwareData command used to download the firmware image data from the Update Agent has a minimum transfer size of 32 bytes. If the last transfer request needs less than this amount of image data, a padded transfer is requested so that 32 bytes of image + padding is received. In cases where this condition is met, an error in the calculation of the size of the last image transfer to the controller's collect buffer caused more data to be sent to the buffer than expected.
  - *Fix*: Corrected the calculation of the final collect buffer transfer size to correctly omit the final transfer padding.
  - *Risk*: Low

2.2 Limitations

This section shows the limitations for this release.

2.2.1 General Limitations

This release includes the following general limitations.

- The following are the limitations of Multi-Actuator:
  - Supports only:
    - HBA drive
    - Windows/Linux/VMware
    - Intel/AMD
    - UEFI mode (for multi-LUN display)

2.2.2 Firmware Limitations

This section shows the firmware limitations for this release.

2.2.2.1 Limitations for Firmware Release 03.01.20.48

This release includes the following limitations.

- A NVME drive may be seen as hot removed if the host tries to change the PCIe Maximum Payload Size during system boot.
  - *Workaround*: Reboot the server to see if all the drives are found. If the drives are still not found, then contact Microchip Support.
- Persistent Event Logs (PEL) will be cleared under the following conditions:
  - Upgrading from firmware releases prior to 03.01.17.56 to 03.01.17.56 or later firmware releases.
  - Downgrading from firmware releases 03.01.17.56 or later to firmware releases prior to 03.01.17.56.

2.2.3 UEFI/Legacy BIOS Limitations

This section shows the UEFI/Legacy BIOS limitations for this release.

© 2023 Microchip Technology Inc. and its subsidiaries

2.2.3.1 Limitations for UEFI Build 2.6.2/Legacy BIOS Build 2.6.2

There are no known limitations for this release.

2.2.4 Driver Limitations

This section shows the driver limitations for this release.

2.2.4.1 Windows Driver Limitations

This section shows the Windows driver limitations for this release.

2.2.4.1.1 Limitations for Windows Driver Build 1010.64.0.1037

There are no known limitations for this release.

2.2.4.2 Linux Driver Limitations

This section shows the Linux driver limitations for this release.

2.2.4.2.1 Limitations for Linux Driver Build 2.1.22-040

There are no known limitations for this release.

2.2.4.3 VMware Driver Limitations

This section shows VMware driver limitations for this release.

2.2.4.3.1 Limitations for VMware Driver Build 4440.0.124

There are no known limitations for this release.

2.2.4.4 FreeBSD/Solaris Driver Limitations

This section shows FreeBSD/Solaris driver limitations for this release.

2.2.4.4.1 Limitations for FreeBSD Driver Build 4390.0.1010

There are no known limitations for this release.

2.2.4.4.2 Limitations for Solaris Driver Build 11.4120.0.1005

There are no known limitations for this release.

2.2.5 Management Software Limitations

This section shows management software limitations for this release.

2.2.5.1 maxView Storage Manager/ARCCONF Limitations

This section shows the maxView Storage Manager/ARCCONF limitations for this release.

2.2.5.1.1 Limitations for maxView Storage Manager/ARCCONF Build 25823

There are no known limitations for this release.

2.2.5.2 PLDM Limiations

This section shows the PLDM limitations for this release.

2.2.5.2.1 Limitations for PLDM Release 6.20.8.0

There are no known limitations for this release.

© 2023 Microchip Technology Inc. and its subsidiaries

3. Updating the Controller Firmware

This section describes how to update the controller firmware to the latest release.

3.1 Updating Controllers to Latest Firmware

If running firmware is 3.01.00.006 or lower, please contact Adaptec Apps team at ask.adaptec.com.

3.1.1 Upgrading to 3.0X.XX.XXX Firmware

1. For controllers running 3.01.02.042 or higher firmware, flash with 3.0X.XX.XXX version of firmware "SmartFWx200.bin" provided in this package using maxview or ARCCONF utility.
2. Power cycle the server.

© 2023 Microchip Technology Inc. and its subsidiaries

4. Revision History

Table 4-1. Revision History

Revision	Date	Description
J	03/2023	Updated for SR 3.2.4 release.
H	11/2022	Updated for SR 3.2.2 release.
G	07/2022	Updated for SR 3.2.0 release.
F	02/2022	VMware driver version changed from 4250.0.120 to 4252.0.103.
E	02/2022	Updated for SR 3.1.8 release.
D	12/2021	Updated for SR 3.1.6.1 release. Updated Fixes and Enhancements for maxView Storage Manager/ARCCONF section for log4j vulnerabilities.
C	11/2021	Updated for SR 3.1.6 release.
B	08/2021	Updated for SR 3.1.4 release.
A	06/2021	Document created.

© 2023 Microchip Technology Inc. and its subsidiaries

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local

© 2023 Microchip Technology Inc. and its subsidiaries

Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-5224-9556-7

© 2023 Microchip Technology Inc. and its subsidiaries

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

© 2023 Microchip Technology Inc. and its subsidiaries

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office	**Australia - Sydney**	**India - Bangalore**	**Austria - Wels**
2355 West Chandler Blvd.	Tel: 61-2-9868-6733	Tel: 91-80-3090-4444	Tel: 43-7242-2244-39
Chandler, AZ 85224-6199	**China - Beijing**	**India - New Delhi**	Fax: 43-7242-2244-393
Tel: 480-792-7200	Tel: 86-10-8569-7000	Tel: 91-11-4160-8631	**Denmark - Copenhagen**
Fax: 480-792-7277	**China - Chengdu**	**India - Pune**	Tel: 45-4485-5910
Technical Support:	Tel: 86-28-8665-5511	Tel: 91-20-4121-0141	Fax: 45-4485-2829
www.microchip.com/support	**China - Chongqing**	**Japan - Osaka**	**Finland - Espoo**
Web Address:	Tel: 86-23-8980-9588	Tel: 81-6-6152-7160	Tel: 358-9-4520-820
www.microchip.com	**China - Dongguan**	**Japan - Tokyo**	**France - Paris**
Atlanta	Tel: 86-769-8702-9880	Tel: 81-3-6880- 3770	Tel: 33-1-69-53-63-20
Duluth, GA	**China - Guangzhou**	**Korea - Daegu**	Fax: 33-1-69-30-90-79
Tel: 678-957-9614	Tel: 86-20-8755-8029	Tel: 82-53-744-4301	**Germany - Garching**
Fax: 678-957-1455	**China - Hangzhou**	**Korea - Seoul**	Tel: 49-8931-9700
Austin, TX	Tel: 86-571-8792-8115	Tel: 82-2-554-7200	**Germany - Haan**
Tel: 512-257-3370	**China - Hong Kong SAR**	**Malaysia - Kuala Lumpur**	Tel: 49-2129-3766400
Boston	Tel: 852-2943-5100	Tel: 60-3-7651-7906	**Germany - Heilbronn**
Westborough, MA	**China - Nanjing**	**Malaysia - Penang**	Tel: 49-7131-72400
Tel: 774-760-0087	Tel: 86-25-8473-2460	Tel: 60-4-227-8870	**Germany - Karlsruhe**
Fax: 774-760-0088	**China - Qingdao**	**Philippines - Manila**	Tel: 49-721-625370
Chicago	Tel: 86-532-8502-7355	Tel: 63-2-634-9065	**Germany - Munich**
Itasca, IL	**China - Shanghai**	**Singapore**	Tel: 49-89-627-144-0
Tel: 630-285-0071	Tel: 86-21-3326-8000	Tel: 65-6334-8870	Fax: 49-89-627-144-44
Fax: 630-285-0075	**China - Shenyang**	**Taiwan - Hsin Chu**	**Germany - Rosenheim**
Dallas	Tel: 86-24-2334-2829	Tel: 886-3-577-8366	Tel: 49-8031-354-560
Addison, TX	**China - Shenzhen**	**Taiwan - Kaohsiung**	**Israel - Ra'anana**
Tel: 972-818-7423	Tel: 86-755-8864-2200	Tel: 886-7-213-7830	Tel: 972-9-744-7705
Fax: 972-818-2924	**China - Suzhou**	**Taiwan - Taipei**	**Italy - Milan**
Detroit	Tel: 86-186-6233-1526	Tel: 886-2-2508-8600	Tel: 39-0331-742611
Novi, MI	**China - Wuhan**	**Thailand - Bangkok**	Fax: 39-0331-466781
Tel: 248-848-4000	Tel: 86-27-5980-5300	Tel: 66-2-694-1351	**Italy - Padova**
Houston, TX	**China - Xian**	**Vietnam - Ho Chi Minh**	Tel: 39-049-7625286
Tel: 281-894-5983	Tel: 86-29-8833-7252	Tel: 84-28-5448-2100	**Netherlands - Drunen**
Indianapolis	**China - Xiamen**		Tel: 31-416-690399
Noblesville, IN	Tel: 86-592-2388138		Fax: 31-416-690340
Tel: 317-773-8323	**China - Zhuhai**		**Norway - Trondheim**
Fax: 317-773-5453	Tel: 86-756-3210040		Tel: 47-72884388
Tel: 317-536-2380			**Poland - Warsaw**
Los Angeles			Tel: 48-22-3325737
Mission Viejo, CA			**Romania - Bucharest**
Tel: 949-462-9523			Tel: 40-21-407-87-50
Fax: 949-462-9608			**Spain - Madrid**
Tel: 951-273-7800			Tel: 34-91-708-08-90
Raleigh, NC			Fax: 34-91-708-08-91
Tel: 919-844-7510			**Sweden - Gothenberg**
New York, NY			Tel: 46-31-704-60-40
Tel: 631-435-6000			**Sweden - Stockholm**
San Jose, CA			Tel: 46-8-5090-4654
Tel: 408-735-9110			**UK - Wokingham**
Tel: 408-436-4270			Tel: 44-118-921-5800
Canada - Toronto			Fax: 44-118-921-5820
Tel: 905-695-1980			
Fax: 905-695-2078			

© 2023 Microchip Technology Inc. and its subsidiaries