



Table of Contents

- 1. About This Release..... 3
 - 1.1. Release Identification..... 3
 - 1.2. Files Included in this Release..... 3
- 2. What's New?..... 5
 - 2.1. Fixes and Enhancements..... 5
 - 2.2. Limitations..... 11
- 3. Updating the Controller Firmware..... 15
 - 3.1. Updating Controllers to Latest Firmware..... 15
- 4. Revision History..... 16
- Microchip Information..... 17
 - Trademarks..... 17
 - Legal Notice..... 17
 - Microchip Devices Code Protection Feature..... 18

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	3.4.2
Package release date	December 4, 2024
Firmware version	3.01.33.44
UEFI/Legacy BIOS	2.16.4/2.16.3
Driver versions	<p>Windows Drivers:</p> <ul style="list-style-type: none"> Windows 2025, 2022, 2019, Windows 11, 10: 1016.10.0.1004 <p>Linux SmartPQI:</p> <ul style="list-style-type: none"> Rocky Linux 9: 2.1.32-035 RHEL 7/8/9: 2.1.32-035 SLES 12/15: 2.1.32-035 Ubuntu 20/22/24: 2.1.32-035 Oracle Linux 7/8/9: 2.1.32-035 Citrix Xenserver 8: 2.1.32-035 Debian 11/12: 2.1.32-035 <p>VMware:</p> <ul style="list-style-type: none"> VMware ESX 7.0/8.0: 4704.0.108 <p>FreeBSD:</p> <ul style="list-style-type: none"> FreeBSD 14/13: 4570.0.1006
ARCCONF/maxView	4.23.00.27147
PLDM	6.45.7.0

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

Table 1-4. Windows Drivers

OS	Version
Server 2025, 2022, 2019, Windows 11, 10	x64

Table 1-5. Linux Drivers

OS	Version
RHEL 9.5 ¹ (inbox only), 9.4, 9.3, 8.10, 8.9, 7.9	x64
SLES 12 SP5	x64
SLES 15 SP6, SP5	x64
Ubuntu 20.04.6, 20.04	x64
Ubuntu 24.04.1, 24.04, 22.04.5, 22.04.4, 22.04	x64
Oracle Linux 7.9 UEK6U3	x64
Oracle Linux 9.4, 9.3, 8.10, 8.9, UEK7U2	x64
Debian 12.6, 11.10	x64
Fedora 40 (inbox)	x64
Citrix XenServer 8.2.1	x64
Rocky Linux 9.4, 9.3	x64
SLE-Micro 6.0, 5.5 (inbox only)	x64

Note:

1. New OS is minimally tested with inbox driver. Full support is expected in the next release.

Table 1-6. FreeBSD and VMware Drivers

OS	Version
ESX 8.0 U3/U2, 7.0 U3/U2	x64
FreeBSD 14.1, 13.3	x64

Note:

1. New OS is minimally tested with inbox driver. Full support is expected in the next release.

Note: Though provided driver bundle includes drivers for several other OSes, only versions mentioned above have been QA tested and are officially supported in this release.

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 arccconf_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.

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 3.01.33.44

This release includes the following fixes and enhancements:

- Added support for transferring controller Serial Output Buffer (SOB) log using PLDM Type 7 command.
- Added support to ignore unsupported drive attached to UBM backplane.
- Added support to reduce UEFI load time.
- Added support to allow configuring internal connector's PCIe PHY rate.
- Added support to log device information that caused a 0x1ABx lockup in the controller event log.
- Fixed an issue where continuous prints were observed in the UART in the presence of an Otherwise Owned Locked SED drive.
 - *Root cause:* Since Otherwise Owned SED is in locked state, any IOs accessing the drive will cause the SED to return a Small Computer System Interface (SCSI) error. Firmware displays the drive error when processing the failure.
 - *Fix:* To reduce the number of errors reported, firmware will print the error in a decreasing frequency over time until it reaches a predefined threshold value.
 - *Risk:* Low
- Fixed an issue where fault LED was not blinking for controller-based erase operation.
 - *Root cause:* On a controller-based erase operation, the firmware code controlling the LED checks the wrong value.
 - *Fix:* To ensure the fault LED blinks consistently throughout the erase operation and until its completion, the firmware will check the right variable.
 - *Risk:* Low
- Fixed an issue where the controller has a lockup after a power cycle to JBOD.
 - *Root cause:* During the power cycle of the JBOD, the firmware issued management commands and waited indefinitely, causing a deadlock.
 - *Fix:* The firmware has been updated to eliminate indefinite waiting on management commands to a JBOD.
 - *Risk:* Low
- Fixed an issue where SATA Drive removed within 10 seconds after link reset due to internal firmware timer.
 - *Root cause:* An internal firmware timer value based on which a drive under reset will be immune from other PHY or port related activities is not inline with the reset wait timer, which will monitor the link reset response.
 - *Fix:* Increased internal firmware timer to 45 seconds for SATA drives, which is same duration as link reset wait timer value.
 - *Risk:* Medium

- Fixed an issue where a good drive could be labelled as a predictive fail drive incorrectly.
 - *Root cause:* There was a small scenario where an unconfigured drive could have old data and firmware used this data to mark the drive as a predictive fail.
 - *Fix:* Corrected logic to make sure the old data was not used.
 - *Fix Risk:* Low
- Fixed an issue where controller was reporting failed drives on a UBM backplane when drives were not present.
 - *Root cause:* The UBM FRU has different drive type support for different ports for different connector identities. The controller should not look at the ports that are for different connector identities, but it does, and it generates the wrong supported drive types and supported max link rate. This leads to the controller thinking the drive is present when it is not.
 - *Fix:* Only look at the ports for the connector identity when looking at supported drive types and supported max link rates.
 - *Fix Risk:* Low
- Fixed a drive firmware update failure due to drive report Sense command support.
 - *Root cause:* When host updates drive firmware through DOWNLOAD MICROCODE(0xE) command, after transferring all the microcode chunks, drive responds with Status with Sense Data Available. Controller on receiving the status from the drive sends REQUEST SENSE command to retrieve the Sense Data. Drive responds with CHECK CONDITION with Sense Data filled as 06: 3F: 01 - Microcode has been changed. Since CHECK CONDITION is set for REQUEST SENSE command, FATAL_ERROR is returned to upper layer hence firmware download to the drive is failed.
 - *Fix:* When drive reports KCQ Value 06: 3F: 01 - Microcode Has been changed for REQUEST SENSE command, send success to upper layer so that firmware downloaded can be activated.
 - *Risk:* Low
- Fixed a controller failure to boot when inserted into PCIe Gen 6 system.
 - *Root cause:* During boot, the controller waits for a handshake message with PCIe Gen 4 configuration details from the host. As the host device is PCIe Gen6 capable, the controller does not get the PCIe Gen 4 configuration details and waits indefinitely resulting in the controller not being found during system boot up.
 - *Fix:* Corrected the handshake message handling to work irrespective of the PCIe generation supported by the host.
 - *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 2.16.4/Legacy BIOS Build 2.16.3

This release includes the following fixes and enhancements:

- Added support to show drive location information in the driver health message if a previous controller lockup is detected that is caused due to a drive.
- Added a menu to configure the connector PCIe data rate and SAS Phy link rate.

2.1.3 Driver Fixes

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

2.1.3.1 Linux Driver Fixes

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

2.1.3.1.1 Fixes and Enhancements for Linux Driver Build 2.1.32-035

This release includes the following fixes and enhancements:

- Fixed an issue where drives are not taken offline when the controller is offline. Drives are listing in `sg_map` and `lsblk` output after controller lockup.
 - *Root cause:* During a controller lockup, the physical and logical drives under the locked up controller are still listed at the OS level. The controller is offline, but the status of each drive is running.
 - *Fix:* When the controller is unexpectedly taken offline, show its drives as offline.
 - *Risk:* Low

2.1.3.2 Windows Driver Fixes

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

2.1.3.2.1 Fixes and Enhancements for Windows Driver Build 1016.10.0.1004

This release includes the following fixes and enhancements:

- Added support for Windows Server 2025.
- Added support to enable DMA remapping feature for Windows Server 2025. Kernel DMA Protection is a Windows security feature that protects against external peripherals from gaining unauthorized access to memory. Added a registry entry "DmaRemappingCompatible" under the SmartPQI services to declare the compatibility/support of the driver to the DMA protection feature.

2.1.3.3 FreeBSD Driver Fixes

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

2.1.3.3.1 Fixes and Enhancements for FreeBSD Driver Build 4570.0.1006

There are no known fixes for this release.

2.1.3.4 VMware Driver Fixes

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

2.1.3.4.1 Fixes and Enhancements for VMware Driver Build 4704.0.108

There are no known fixes for this release.

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 27147

This release includes the following fixes and enhancements for ARCCONF/maxView:

- Fixed an issue where ARCCONF was not displaying the "S.M.A.R.T" and "S.M.A.R.T warning" property value correctly.
 - *Root cause:* Mapping of the "S.M.A.R.T" and "S.M.A.R.T warning" property value with the firmware provided values was not done correctly.
 - *Fix:* Value for S.M.A.R.T. mapped with "Supported" and "Not Supported" and S.M.A.R.T. warning value mapped with "Yes" or "No".
 - *Risk:* Low
- Fixed an issue where the maxView was not allowing to secure erase the 4K drives.
 - *Root cause:* maxView was blocking the secure erase operation for the 4K drive type.

- *Fix:* Enabled the secure erase operation for the 4K drives in maxView.
- *Risk:* Low
- Fixed an issue in ARCCONF where 'Negotiated Physical Link Rate' was incorrectly displayed instead of 'Physical Link Rate', and 'Negotiated Logical Link Rate' was shown instead of 'Logical Link Rate'.
 - *Root cause:* The ARCCONF tool was incorrectly displaying the 'Negotiated Physical Link Rate' instead of the actual 'Physical Link Rate' and the 'Negotiated Logical Link Rate' instead of the 'Logical Link Rate'.
 - *Fix:* Updated the property name 'Negotiated Physical Link Rate' to 'Physical Link Rate' and 'Negotiated Logical Link Rate' to 'Logical Link Rate'.
 - *Risk:* Low

2.1.4.2 PLDM Fixes

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

2.1.4.2.1 Fixes and Enhancements for PLDM Release 6.45.7.0

This release includes the following fixes and enhancements:

- Added support for PLDM Type 7 (File I/O) compliance with final release versions of DMTF specifications
- Made the following changes to PLDM Base (Type 0) commands to comply with v1.2.0 of the PLDM base specification (DSP0240).
 - Implemented the PLDM Type 0 command `GetMultipartTransferSupport` to provide which Multipart Transfer commands the specified PLDM Type at the specified version are supported.
 - The PLDM Type 0 command `GetPLDMCommands` has been updated to report `GetMultipartTransferSupport` as a supported command.
- Made the following changes to PLDM Platform Monitoring and Control (Type 2) commands to comply with v1.3.0 of the PLDM Platform Monitoring and Control Specification (DSP0248).
 - The `PDRType` value for the File Descriptor PDR has been updated to 30 from the draft spec value of 25.
 - The `CrashDumpFile FileClassification` value for the File Descriptor PDR has been updated to 5 from the draft spec value of 4.
 - The supported state set values for the Device File State Sensors have been updated to conform to v1.2.0 of the PLDM State Set Specification (DSP0249).
 - The `FatalHigh` threshold value for file size Numeric Sensors is now set to the maximum file size.
- Made the following changes to PLDM File I/O (Type 7) commands to comply with v1.0.0 of the PLDM for File Transfer Specification (DSP0242).
 - Added support for the metacommand `DfReadMultipartReceive (0x20)`. This command is not intended to be issued by File Clients; its only purpose is to allow the `GetPLDMCommands` command to indicate that the Type 0 command `MultipartReceive` may be used as a data transfer mechanism for PLDM Type 7.
 - Implemented the PLDM Type 7 command `DfProperties` to provide the maximum number of mediums supported and the total number of File Descriptors supported.
 - The command code for the Type 7 command `DfHeartbeat` has been updated to 0x03 from the draft spec value of 0x06.
 - Added the PLDM Type 7 completion codes `UNABLE_TO_OPEN_FILE (0x8A)` and `ZEROLENGTH_NOT_ALLOWED (0x82)`.

- DfClose can now respond with the PLDM base completion code `ERROR_INVALID_DATA` (0x02).
 - Support for the PLDM Type 7 draft spec completion code `EXCLUSIVE_OWNERSHIP_REQUIRED` (0x87) has been removed.
 - The value of the PLDM Type 7 completion code `MAX_NUM_FDS_EXCEEDED` has been updated to 0x88 from the draft spec value of 0x89.
 - Added changes to long-running task support for storage resource RDE action operations.
 - All RDE ACTION requests for a Storage resource will now result in the operation being carried out via a long-running task. BMCs are now expected to set both the `action_supported` and `events_supported` bits of the `MCFeatureSupport` field in a `NegotiateRedfishParameters` request in order for a RDE ACTION request for a Storage resource to be allowed by the RDE device.
 - Added support transfer of the controller Serial Output Buffer (SOB) log file through PLDM Type 7.
 - Added a contained entity to the Entity Association PDR having `entityType = 0x09` (Device File) and `entityInstanceNumber = 2` representing the controller SOB log Device File.
 - Added a File Descriptor PDR with `FileClassification = 0x02` (`SerialTxFIFO`) to provide a file identifier for the controller SOB log device file.
 - Added file size numeric sensor and device file state sensor PDRs to provide size and state information for the controller SOB log device file.
 - Updated the Type 7 command `DfOpen` to support handling for the `DfOpenRegFIFO` bit of the `DfOpenAttributes` field. When sending `DfOpen` for a device file that requires transmission as streaming FIFO, not setting this bit will result in a `INVALID_DF_ATTRIBUTE` error completion code in the response.
 - Updated `MultipartReceive` for type 7 to support files classified as `SerialTxFIFO`. The following rules and requirements apply when issuing a `MultipartReceive` request on a `SerialTxFIFO` file:
 - Seeking is not supported. `MultipartReceive RequestedSectionOffset` shall be set to zero.
 - Single part per section. `TransferOperation` shall not be set to `XFER_NEXT_PART`.
 - A `MultipartReceive` response where the data length is less than the negotiated part size indicates that all the available data has been transferred.
 - The response to a `MultipartReceive` request for an empty `SerialTxFIFO` file will have a `SUCCESS` completion code.
 - A `MultipartReceive` request restarting a section of a FIFO file that has wrapped will result in new data. Data overwritten by new wrapped data will not be preserved.
- The following error completion codes will be returned by `MultipartReceive` for FIFO files:
- `INVALID_DATA_TRANSFER_HANDLE` if request `DataTransferHandle` is not ZERO
 - `INVALID_REQUESTED_SECTION_OFFSET` if request `RequestedSectionOffset` is not ZERO
 - `INVALID_DATA` if request `RequestedSectionLengthBytes` is ZERO or greater than the negotiated size
- Fixed an issue where the `GetPDR` command can sometimes fail to retrieve the requested PDR when no drives are connected to the targeted controller.
 - *Root cause:* RedfishAction PDRs for Drive resources were being internally allocated in error when no drives were present, causing a failure when an MC attempted to fetch the PDR with the `GetPDR` command.

- *Fix:* Modified the logic for allocating RedfishAction PDR(s) for Drive resources to require at least one drive to be connected prior to the allocation.
 - *Risk:* Low
- Fixed an issue where with a given a configuration ExternalKey encryption is enabled and SED is controller owned and KMS is unavailable. RDE READ on the controller SED publishes Status.State and Status.Health as Enabled and OK respectively.
 - *Root cause:* The logic that sets a Drive's State and Health did not account for the case when KMS is unavailable or inactive and the Drive is a controller owned SED.
 - *Fix:* Added logic so that an RDE READ on a controller owned SED will publish Status.State and Status.Health as StandByOffline and Warning respectively when KMS is not available or inactive.
 - *Risk:* Low
- Fixed an issue where the [Links.Enclosures@odata.count](#) and [Links.Enclosures@odata.id](#) properties were missing from the Redfish storage resource.
 - *Root cause:* The [Links.Enclosures@odata.count](#) and [Links.Enclosures@odata.id](#) properties were not added to the Redfish Storage resource.
 - *Fix:* The [Links.Enclosures@odata.count](#) and [Links.Enclosures@odata.id](#) properties have been added to the Redfish Storage resource. [Links.Enclosures@odata.count](#) will contain the number of chassis resources of type enclosure being managed by the controller. [Links.Enclosures@odata.id](#) will an contain links to chassis resources of type enclosure.
 - *Risk:* Low.
- Fixed an issue for which the GetPDR for the File Descriptor PDR representing the controller crash dump did not have the Polled bit of the file capabilities field set as required by the Type 2 spec.
 - *Root cause:* The implementation of the File Descriptor PDR was based on a pre-release draft of the most recent version of the Type 2 spec, and the requirements for setting the file capabilities bits were changed during subsequent development of the spec.
 - *Fix:* Updated GetPDR to set the Polled access bit in the File Capabilities field for the controller crash dump File Descriptor PDR.
 - *Risk:* Low
- Fixed an issue in which DfOpen returns EXCLUSIVE_OWNERSHIP_NOT_AVAILABLE when opening crash dump file while it is already opened.
 - *Root cause:* Logic exists to capture this error case, but the incorrect response completion code was assigned to be returned.
 - *Fix:* Updated the error logic to send the correct completion code MAX_NUM_FDS_EXCEEDED as defined in the Type 7 spec.
 - *Risk:* Low
- Fixed an issue in which after reading the LAST_PART of a section in a file, the NEXT_PART command to read the initial part of the section must not get executed. Instead, the initial part of the section is sent and received.
 - *Root cause:* There was no check to determine if the transfer of a section was completed.
 - *Fix:* Handle the situation where the file client requests the NEXT_PART after the section has been transferred.
 - *Risk:* Low
- Fixed an issue in which the @odata.id property retrieved from an RDE READ on a drive resource representing an empty bay in a chassis resource did not match the URI given in the Chassis child drive PDR.

- *Root cause:* The logic to generate the empty bay drive resource @odata.id property was incorrect.
- *Fix:* The empty bay resource @odata.id property is now being calculated using the correct logic.
- *Risk:* Low
- Fixed an issue in which incorrect severity warning was reported for the drive when sanitize erase operation is in progress on drive. The severity should be OK, and therefore the condition should not be shown.
 - *Root cause:* The severity for the offline condition was using the drive health. There was no check to determine if the drive was being erased.
 - *Fix:* When determining whether a condition should be shown for an offline drive, the check has been updated to match the check performed for an event. An offline condition will only be shown when the drive health is Warning, and the drive is not in a predictive failure state. So, when the drive is being erased and is in a predictive failure state, the offline condition will not be shown.
 - *Risk:* Low
- Fixed an issue where HealthRollup shows a warning when there is no warning on a lower level component.
 - *Root cause:* Storage.Status.HealthRollup was not factoring in StorageController.Status.Health.
 - *Fix:* Update Storage.Status.HealthRollup to factor in StorageController.Status.Health.
 - *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 3.01.33.44

This release includes the following firmware limitations:

- Persistent Event Logs (PEL) are getting cleared when:
 - 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.
- Firmware downgrade from firmware version 3.01.30.106 to any older firmware version is blocked if Managed SED is enabled.

- *Workaround:* Disable Managed SED and try firmware downgrade.
- Managed SED cannot be enabled on the controller when reboot is pending after firmware downgrade from firmware version 3.01.23.72 to any older firmware version.
 - *Workaround:* Reboot the controller and enable the Managed SED.

2.2.3 UEFI/Legacy BIOS Limitations

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

2.2.3.1 Limitations for UEFI Build 2.16.4/Legacy BIOS Build 2.16.3

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 Linux Driver Limitations

This section shows the Linux driver limitations for this release.

2.2.4.1.1 Limitations for Linux Driver Build 2.1.32-035

This release includes the following limitations:

- SL-Micro 6.0 fails to boot after installation on 4Kn drives.
 - *Workaround:* This is a SUSE issue and only workaround is to use non-4Kn drives.
- On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, SLES15SP3, OpenEuler 20.03LTS, and 22.03LTS including SP releases), the driver injection (DUD) install will hang if an attached drive (either HBA mode or Logical Volume) has Write Cache enabled.
 - *Workaround:* There are two workarounds for this issue:
 - Ensure that the Write Cache is disabled for any attached drive.
 - For RHEL7.9/8.2/8.3 and OpenEuler 20.03LTS, 22.03LTS, add `rd.driver.blacklist=smartpqi` to the grub entry along with `inst.dd`.
- Unable to do a driver injection (DUD) install on RHEL 8.7 when NVMe drives are attached to the system. This is a multipath issue with the OS install process.
 - *Workaround:* Edit grub to include the boot argument "nompath". So replace "inst.dd" with "nompath inst.dd" for DUD install.
- RHEL driver injection (DUD) install where OS ISO is mounted as virtual media on BMC based servers (non-ILO). Installer will hang after driver injection. It is reported on RHEL 8.5, 8.6, 9.0 to 9.4.
 - *Workaround:*
 - Load the OS from USB device instead of virtual media.
 - Load the OS from virtual media but initiate ISO verification (media test) during the installation followed by ESC to cancel the media test.
 - Edit grub to include the boot argument "nompath". Replace "inst.dd" with "nompath inst.dd" for DUD install.
- Oracle 9 UEK 7 kernel causes SmartPQI rpm dependency failures. This is an issue with how the kernel package was created by Oracle. Correct UEK7 kernel for Oracle 9, which is expected in the mid-October UEK7 release, version number is still pending.

Note: This does not affect Oracle 8 UEK 7.

 - *Workaround:* Install the rpm using "`--nodeps`" when dependency failures occur.
 - Update:
 - For SmartPQI driver versions > 2.1.20-020 and UEK7 kernels >= 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm will install normally.

For UEK7 kernels < 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm needs to be installed using the "--nodeps".

- On AMD systems, the system might crash or hang due to a bug in the IOMMU module. For details, see lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/.
 - *Workaround:* Disable the IOMMU setting option in BIOS.
- When multiple controllers are in a system, udev(systemd) can timeout during kdump/kexec resulting in an incomplete kdump operation. The usual indication of the timeout is the console log entry: "scsi_hostX: error handler thread failed to spawn, error = -4".
 - *Workaround:* The workaroud for this issue involves extending the udev(systemd) timeout during a kdump operation.
 - The steps to increase the timeout for udev(systemd) are:
 1. vi /etc/sysconfig/kdump
 2. Add udev.event-timeout=300 to KDUMP_COMMANDLINE_APPEND
 3. systemctl restart kdump
 4. systemctl status kdump
- On some distributions (including RHEL 9.0/Oracle Linux 9.0), you are unable to inject the OOB driver (DUD) during install when a multi-actuator drive is attached.
 - *Workaround:* Install using the inbox driver, complete OS installation, then install the OOB driver.

2.2.4.2 Windows Driver Limitations

This section shows the Windows driver limitations for this release.

2.2.4.2.1 Limitations for Windows Driver Build 1016.10.0.1004

This release includes the following limitations:

- A system crash may occur when hibernating a system installed on a Dual Actuator drive.
 - *Workaround:*
 - Avoid hibernating the system while running heavy I/Os to multiple Dual Actuator drives.
 - Stop running the I/Os to the drives and then hibernate the system.
 - Reboot the server to recover the system.

2.2.4.3 FreeBSD Driver Limitations

This section shows FreeBSD driver limitations for this release.

2.2.4.3.1 Limitations for FreeBSD Driver Build 4570.0.1006

This release includes the following limitation:

- FreeBSD 13.2 and later OS Installations will fail with the out of box driver.
 - *Workaround:* Install with inbox driver then update to latest.

2.2.4.4 VMware Driver Limitations

This section shows VMware driver limitations for this release.

2.2.4.4.1 Limitations for VMware Driver Build 4704.0.108

This release includes the following limitations:

- A controller lockup may occur when using VMDirectPath on a single-processor AMD system. These lockups have been seen with VMs running Linux and Windows. If a lockup of a passed-through controller occurs, a reboot of the ESXi server may be required to clear the lockup condition and restore the virtual machine to working condition.
 - *Workaround:* No known workaround at this time.

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 27147

There are no known limitations for this release.

2.2.5.2 PLDM Limitations


This section shows the PLDM limitations for this release.

2.2.5.2.1 Limitations for PLDM Release 6.45.7.0

There are no known limitations for this release.

3. Updating the Controller Firmware

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

 **Important:** When downgrading firmware, there may be cases when newer hardware is not supported by an older version of firmware. In these cases, attempting to downgrade firmware will be prevented (fail). It is recommended to regularly qualify newer firmware versions, to ensure that newer hardware is supported in your system(s)

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.

4. Revision History

Table 4-1. Revision History

Revision	Date	Description
R	12/2024	Updated for SR 3.4.2 release.
Q	07/2024	Updated for SR 3.4.0 release.
P	02/2024	Updated for SR 3.3.4 release.
N	11/2023	SR 3.3.0 patch release with maxView™ version B26068.
M	11/2023	SR 3.2.0 patch release with maxView™ version B25339.
L	11/2023	Updated for SR 3.3.2 release.
K	08/2023	Updated for SR 3.3.0 release.
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.

Microchip Information

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, 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, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, 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, Clockstudio, 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, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, 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, Trusted Time, 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, and Symmcom 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.

© 2024, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 979-8-3371-0223-8

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 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.

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.