HBA 1100 Software/Firmware Release Notes

Table of Contents

1. About This Release

The solution release described in this document includes firmware, OS drivers, tools, and host management software for the 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	2.9.2
Package Release Date	December 12, 2024
Firmware Version	7.41 B0[1]
UEFI Driver Version	2.16.4
Legacy BIOS	2.16.3
Driver Versions	Windows SmartPQI: • Windows Server 2019/2022/2025: 1016.10.0.1004 • Windows 10/11: 1016.10.0.1004 Linux SmartPQI: • RHEL 7/8/9: 2.1.32-035 • SLES 12/15: 2.1.32-035 • Ubuntu 20/22/24: 2.1.32-035 • Debian 11/12: 2.1.32-035 • Oracle Linux 7/8/9: 2.1.32-035 • Citrix XenServer 8: 2.1.32-035 • BC Linux 7: 2.1.32-035 • OpenEuler 22/24: 2.1.32-035 VMware SmartPQI: • VMware 7.0/8.0: 4704.0.108 FreeBSD SmartPQI: • FreeBSD 13/14: 4570.0.1006
arcconf/maxView™	4.23.00.27147
PLDM	6.45.7.0

Note:

1. Downgrading to 1.04 B0 or older builds from this release or prior 1.29 releases may cause the board to not boot or have supercap errors due to an incompatibility in SEEPROMs between this release and prior releases. See section "Updating the Controller Firmware".

1.2 Components and Documents Included in this Release

Download the firmware, drivers, host management software, and supporting documentation for your HBA1100 controller solution from the Microchip Web site at https://start.adaptec.com

1.3 Files Included in this Release

This release consists of the files listed in the following tables:

Firmware Files

Table 1-2. Firmware Files

Component	Description	Pre-Assembly Use	Post-Assembly Use
SmartFWx100.bin	Programmable NOR Flash File Use to program NOR Flash for boards that are already running firmware.	—	X
SmartFWx100.fup	Programmable NOR Flash File Used for PLDM type 5 firmware flashing for boards that are already running firmware.	—	X

Table 1-3. Firmware Programming Tools

Tool	Description	Executable
Arcconf romupdate	The command allows to upgrade/downgrade the firmware and BIOS image to the controller.	Refer to Table 1-8
maxView™ firmware upgrade wizard	The firmware upgrade wizard allows to upgrade/downgrade the firmware and BIOS image to one or more controller(s) of same model in the system.	Refer to Table 1-8

Driver Files

Table 1-4. Windows Storport Miniport SmartPQI Drivers

Drivers	Binary	Version
Server 2025, 2022 and 2019 Windows 10 (version 22H2) and 11 (version 24H2)	SmartPqi.sys	x64
	SmartPqi.inf	x64
	smartpqi.cat	x64

Table 1-5. Linux SmartPQI Drivers for Arm

Drivers	Version
Red Hat Enterprise Linux 9.4, 8.10	Arm®
SuSE Linux Enterprise Server 12 SP5	Arm
SuSE Linux Enterprise Server 15 SP6, SP5	Arm
Ubuntu 24.04.1, 22.04.5, 20.04.5	Arm
BC Linux 7.7	Arm
OpenEuler 24.03 LTS, 22.03 SP4 LTS	Arm

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

Table 1-6. Linux SmartPQI Drivers for Intel/AMD x64

Drivers	Version
Red Hat Enterprise Linux 9.5 (inbox only)[1], 9.4, 9.3, 8.10, 8.9, 7.9	x86_64
SuSE Linux Enterprise Server 12, SP5	x86_64
SuSE Linux Enterprise Server 15 SP6, SP5	x86_64
Oracle Linux 7.9 UEK6U3	x86_64
Oracle Linux 9.4, 9.3, 8.10, 8.9, UEK7U2	x86_64
Ubuntu 24.04.1, 22.04, 22.04.5, 22.04.4, 22.04	x86_64

...........continued

Drivers	Version
Ubuntu 20.04.6, 20.04	x86_64
Debian 12.6, 11.10, 11.9	x86_64
Citrix xenServer 8.2.1	x86_64
Fedora 40 (inbox only)	x86_64
OpenEuler 24.03 LTS	x86_64
OpenEuler 22.03 SP4 LTS	x86_64
SLE-Micro 6.0, 5.5 (Inbox only)	x86_64

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

Table 1-7. FreeBSD and VMware SmartPQI Drivers

Drivers	Version
FreeBSD 14.1, 13.3	x64
VMware 8.0 U3/U2, 7.0 U3/U2	x64

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

Host Management Software

Table 1-8. Host Management Utilities

Description	OS	Executable
ARCCONF Command Line Utility	Windows® x64 Linux® x64 VMware 7.0 and above XenServer FreeBSD x64 Linux ARM	See the Arcconf download package for the OS-applicable installation executable.
ARCCONF for UEFI	—	Included as part of the firmware downloadable image.
maxView™ Storage Manager	Windows x64 VMware 7.0 and above Linux x64 XenServer	See the maxView Storage Manager download package for the OS-applicable installation executable.
maxView™ vSphere Plugin	VMware 7.0 and above	See the VMware maxView Storage Manager download package for the OS-applicable installation executable.
Boot USB (offline or pre-boot) for ARCCONF and maxView Storage Manager	Linux x64	See the maxView BootUSB download package for the .iso file.

2. What's New?

This section shows what’s new in this release.

2.1 Features

The following table highlights major features supported by each Solutions Release.

Table 2-1. Feature Summary

Feature		Supported Release
Added support to reduce UEFI load time.		2.9.2
Arcconf command to check Nand and NOR Flash type		2.9.0
Redfish Resource to Publish SuperCap Properties Support		2.8.2
Arcconf and Redfish Support in Secureboot ESXi Environment		2.8.2
Remote Key Management of Managed SED		2.8.0
Multi-Actuator Drive Support Enhancements		2.7.4
Managed SED Adapter Password Support		2.7.2
Managed SED Local Mode Support		2.7.0
Multi-Actuator Drive Support		2.7.0
Persistent Event Logging Support		2.6.2
Out of Band Interface Selection Support of MCTP or PBSI		2.5.2
MCTP BMC Management		2.4.8
SMR Drive Support	Enumeration, Unrestrected Command Flow-Through	2.3.0
	SATL Translation for HA/HM SMR Management	
	Identify all Drive Types	
Driver OS Certification Where Applicable		2.3.0
SNMP Management Software Support		2.3.0
4Kn, 512e and 512n Support		2.3.0
Legacy Boot Support		2.3.0
UEFI Driver, Boot Support		2.3.0

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 7.41

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 reduce UEFI load time.
- Added support to log device information that caused a 0x1ABx lockup in the controller event log.
- Fixed an issue where expander cannot be detected during first power on.
  - Root Cause: Due to PHY down and up events during boot time, firmware might mistakenly remove the expander device that attached to the controller.
  - Fix: Firmware will do a soft reset during POST to rescan devices only after the Test Unit Ready (TUR) issued to expander has failed.
  - Risk: Low

- Fixed an issue where erase command keeps on changing between Write Same 16 and Write Same 10.
  - Root Cause: The firmware logic that decides whether Write Same 16 (0x93) or Write Same 10 (0x41) is based on a value that was not initialized.
  - Fix: For erase iteration, initialize the value to the drive number which is getting erased.
  - Risk: Low
- 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 a MCTP communication issue between BMC and controller during AC power cycle test.
  - Root Cause: During an Intel 4 socket server, AC power cycle test, the BMC is not able to communicate to the controller. This is due to the host not sending a response for a MCTP command and the host proceeded with the next command. Meanwhile, the controller firmware retried the MCTP command for which the response is not received and that stopped MCTP communication between the host and controller.
  - Fix: Firmware will not retry the MCTP command for which the response is not received if the MCTP communication path is already established. The MCTP specification allows the host to not send a response to one MCTP command (due to its internal state) and still proceed with establishing communication.
  - Risk: Low
- Fixed a MCTP communication issue between BMC and controller in AMD Turin server.
  - Root Cause: In AMD Turin server there are two processors. The controller firmware sent a MCTP response, but it went to the incorrect processor and not to the processor with the BMC. The routing table in the controller firmware for the MCTP communication was incorrect.
  - Fix: Fixed the MCTP routing table in firmware so that the response is sent to the corresponding processor which is requesting the information from controller.
  - Risk: Low
- Fixed issue for handling controller 0x1ABD lockup when a timeout occurs with an expander attached SATA drive.

  - Root Cause: A 0x1ABD controller lockup was observed when a timeout occurs during an IO operation with an expander attached SATA drive. The controller SAS hardware notifies the firmware about the timeout condition, but the firmware did not handle the timeout correctly which led to the 0x1ABD lockup.
  - Fix: The firmware will handle the SAS hardware timeout notification correctly by triggering NCQ error mode handling to flush the queued-up commands and resolve the lockup.
  - Risk: Low
- Fixed an issue with checking support for secure erase command.
  - Root Cause: When host sends secure erase command, firmware fails it with an error. The firmware checked if the drive supported both SCT Write Same and SCT DATA Tables command. If both were supported, then firmware would allow the secure erase command. However, if SCT DATA Tables command was not supported then firmware would fail the secure erase command.
  - Fix: Firmware will only check if the drive supports for SCT Write Same command to allow secure erase commands.
  - 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 to report 24G link rate for expander PHYs.
  - Root Cause: The firmware did not properly report 24G link rates for expander PHYs and listed them as a maximum value of 12G.
  - Fix: Updated firmware to allow reporting of 24G link rates for expander PHYs.
  - Fix Risk: Medium

2.2.2 UEFI Fixes

Note: Microsoft signed and secure boot is supported**.**

2.2.2.1 Fixes and Enhancements for UEFI Driver 2.16.4/Legacy BIOS 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.

2.2.3 Driver Fixes

2.2.3.1 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 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

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4570.0.1006

There are no known fixes for this release.

2.2.3.3 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.

2.2.3.4 Fixes and Enhancements for VMware Driver Build 4704.0.108

There are no known fixes for this release.

2.2.4 Management Software Fixes

2.2.4.1 Fixes and Enhancements for Arcconf/maxView™ Build 4.23.00.27147

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

2.2.4.2 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

2.3 Limitations

2.3.1 General Limitations

This release includes the following general limitation:

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

2.3.2 Firmware Limitations

2.3.2.1 Limitations for Firmware Release 7.41

This release includes the following firmware limitations:

- Persistent Event Logs (PEL) are getting cleared when:
  - Upgrading from firmware releases prior to 5.61 to 5.61 or later firmware releases.
  - Downgrading from firmware releases 5.61 or later to firmware releases prior to 5.61.
- Firmware downgrade from firmware version 7.11 B0 and newer to any firmware version before 7.11 B0 is blocked if Managed SED is enabled.
  - Workaround: Disable Managed SED and try firmware downgrade.
- Managed SED cannot be enabled on the controller, where reboot is pending after firmware downgrade from firmware version 6.22 B0 to any older firmware version.
  - Workaround: Reboot the controller and enable the Managed SED.

2.3.2.2 Limitations for Firmware Release 1.32 Build 0

- Firmware release 1.32b0 may become unresponsive while attempting to flash firmware or execute other RAID logical drive operations.
  - Description: Refer to entry "Fixed an issue where firmware may become unresponsive while attempting to flash firmware or execute other RAID logical drive operations" in the Firmware fixes section.
  - A fix for this issue is available in the 1.60 B0 firmware release. If a firmware flash failure is occurring, try the following workarounds:
    - Workaround: If there are no target devices (expanders or drives) attached to the controller, attach a target device to the controller and try the host management operation again.
    - Workaround: If the system is operating using UEFI, the HII tool can be used to flash the firmware to this release as outlined in the *Microchip SmartIOC 2100/SmartROC 3100 Installation and User's Guide (ESC-2170577),* appendix entry “Updating the SmartIOC 2100/SmartROC 3100 Controller Firmware”.
    - Workaround: If there are target devices attached to the controller and this issue occurs or none of the workarounds can be used, contact Microchip Support.

2.3.3 UEFI Limitations

2.3.3.1 Limitations for UEFI Build 2.16.4/Legacy BIOS Build 2.16.3

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 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`.
- 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.
- 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.

2.3.4.2 Limitations for Windows® Driver Build 1016.10.0.1004

This release includes the following limitation:

- 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.

2.3.4.3 Limitations for FreeBSD Driver Build 4570.0.1006

This release includes the following limitations:

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

2.3.4.4 Limitations for VMware Driver Build 4704.0.108

There are no known limitations for this release.

2.3.5 Management Software Limitations

2.3.5.1 Limitations for Arcconf/maxView Build 4.23.00.27147

There are no known limitations for this release.

2.3.5.2 Limitations for PLDMC Release 6.45.7.0

There are no known limitations for this release.

2.3.6 Hardware Limitations

This release includes the following hardware limitations:

- Two Wire Interface (TWI) address conflicts can cause system DDR memory to not be discovered.
  - Description: The HBA1100 boards include two TWI targets on the host-facing SMBUS interface with the following slave addresses:
    - 0xA0 – Field Replaceable Unit (FRU) SEEPROM
    - 0xDE – PBSI (default)

      According to the JEDEC specification, the default TWI addresses for the DDR SPD is 0xA0-0xAE (the spec uses 7 bit addressing which is 0x50-0x57). On platform system board designs with SMBUS wiring that has both PCIe slots and DDR slots shared on the same TWI bus, the TWI devices for the DDR and Smart controller are exposed to address conflicts which can result in the system memory not being discovered. The Smart controller PBSI interface defaults to a value of 0xDE (0x6F in 7-bit addressing) and is not a problem unless it is changed to an address that conflicts with the JEDEC defined values. The Smart controller FRU SEEPROM is hardwired to 0xA0.
  - Workaround: None available. If this issue is encountered, contact your Microchip support engineer to determine the next steps for your system.
  - Performance with workaround: Not applicable
  - Performance without workaround: Not applicable

3. Updating the Controller Firmware

This section describes how to update the board's firmware components to the latest release.

Important:

- If Managed SED is enabled, do not downgrade firmware to version 5.00 or earlier because they do not support Managed SED capabilities. Disable Managed SED if downgrading to firmware versions 5.00 or earlier.
- 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 the Controller Firmware

This procedure describes how to prepare your board to be programmed with the latest firmware.

Note:

1. Complete these procedures exactly as described for proper functionality. If you do not follow all of the steps correctly, you could encounter unusual runtime behavior.

Flashing the board to the latest firmware:

This section describes how to update all the firmware components on HBA 1100 Adapter boards to the latest release.

If the controller is currently running 1.60 b0 firmware or newer, follow these steps:

1. **Mandatory:** Flash the target with the provided " SmartFWx100.bin" image with arcconf/maxView software.
2. **Mandatory:** Use the OS shutdown/restart operation to gracefully reboot the system to complete the firmware update process.

Note:
After completing the firmware update, if the firmware version is still showing the prior version, retry the firmware update steps.

If the controller is currently running 1.32 b0 firmware, follow these steps:

1. **Mandatory:** Flash the target with the provided “SmartFWx100.bin" image with arcconf/maxView software.
   - If the arcconf/maxView software becomes unresponsive or hangs then power cycle the system to recover and refer to firmware limitation section Limitations for Firmware Release 1.32 Build 0.
2. **Mandatory:** If flashing completes, use the OS shutdown/restart operation to gracefully reboot the system to complete the firmware update process.

Note:
After completing the firmware update, if the firmware version is still showing the prior version, retry the firmware update steps.

If the controller is currently running 1.04 b0 firmware, follow these steps:

1. **Mandatory:** Flash the controller with the provided “SmartFWx100_ v1.29_b314.bin" image with arcconf/maxView software.

2. **Mandatory:** Reboot the system to refresh all components**.**
3. **Mandatory**: Flash the target with the provided " SmartFWx100.bin" image with arcconf/maxView software.
4. **Mandatory**: Use the OS shutdown/restart operation to gracefully reboot the system to complete the firmware update process.

At this point, the controller would be updated and would be ready to use. Install the SmartPQI driver and the latest version of the Arcconf/maxView management utility to monitor and configure the controller.

Note: Downgrading firmware could lead to unexpected behavior due to an incompatibility in SEEPROMs between this release and the prior release.

4. Installing the Drivers

See the "*Microchip Adaptec® HBA 1100 Series Host Bus Adapters Installation and User's Guide* (DS00004281D, previously ESC-2161232)" for complete driver installation instructions.

5. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision	Date	Description
P	12/2024	SR 2.9.2 Production Release.
N	07/2024	SR 2.9.0 Production Release.
M	03/2024	SR 2.8.4 Production Release.
L	12/2023	SR 2.8.0 Patch Release with maxView version B26068
K	11/2023	SR 2.7.0 Patch Release with maxView version B25339
J	11/2023	SR 2.8.2 Production Release
H	07/2023	SR 2.8.0 Production Release
G	03/2023	SR 2.7.4 Production Release
F	11/2022	SR 2.7.2 Production Release
E	08/2022	SR 2.7.0 Production Release
D	03/2022	VMware driver version updated from 4250.0.120 to 4252.0.103
C	02/2022	SR 2.6.6 Production Release
B	12/2021	SR 2.6.4.1 Patch Release with maxView™ version B24713. Updated Fixes and Enhancements for maxView Storage Manager/ARCCONF section for log4j vulnerabilities.
A	11/2021	SR 2.6.4 with VMware driver version 4230.0.103 (previously ESC-2162192)
22	08/2021	SR 2.6.2 with VMware driver version 4150.0.119
21	04/2021	SR 2.6.1.1 with VMware driver version 4054.2.118
20	03/2021	SR 2.6.1 with VMware driver version 4054.1.103
19	02/2021	SR 2.6 Production Release
18	10/2020	SR 2.5.4 Production Release
17	08/2020	SR 2.5.2.2 Production Release with Firmware 3.00
16	02/2020	Update for SR 2.5.2
15	10/2019	Update for SR 2.5
14	08/2019	Update for SR 2.4.8 Release
13	03/2019	Update for SR 2.4.4 Release
12	01/2019	SR2.4 Production Release
11	10/2018	SR2.3 firmware update with Cavium/ARM support and Ubuntu driver.
10	06/2018	SR2.3 Production Release
8	10/2017	Update supported OSs
8	10/2017	First Production Release
1-7	10/2016 to 07/2017	Pre-Production Release.

Microchip Information

Trademarks

ISBN: 979-8-3371-0269-6

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 products are 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.