HBA 1100 Software/Firmware Release Notes

Table of Contents

1. About This Release

The development 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	2.7.2
Package Release Date	November 28, 2022
Firmware Version	5.61 B0[1,2]
UEFI Version	2.4.1
Legacy BIOS	2.4.3
Driver Versions	Windows SmartPQI: • Windows 2016/2019/2022: 1010.52.0.1012 • Windows 10/11: 1010.52.0.1012 Linux SmartPQI: • RHEL 7/8/9: 2.1.20-035 • SLES 12/15: 2.1.20-035 • Ubuntu 16/18/20/21/22: 2.1.20-035 • Debian 10/11: 2.1.20-035 • Oracle Linux 7/8/9: 2.1.20-035 • Citrix XenServer 8: 2.1.20-035 VMware SmartPQI: • VMware 7.0/8.0: 4380.0.108 FreeBSD/Solaris SmartPQI: • FreeBSD 12/13: 4330.0.1038 • Solaris 11: 11.4120.0.1005
Management Software (arcconf, maxView™, Event Monitor, BootUSB)	4.09.00.25611
PLDM	6.15.13.0

Notes:

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. Refer to the section "3. Updating the Controller Firmware" to downgrade an existing board.
2. 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.

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 2022, Server 2019 and Server 2016 Windows 10 (version 21H2) and 11	SmartPqi.sys	x64
	SmartPqi.inf	x64
	Smartpqi.cat	x64

Table 1-5. Linux SmartPQI Drivers for Intel/AMD x64

Drivers	Intel/AMD x64
Red Hat Enterprise Linux 9.1[1], 9.0[2], 8.7[1], 8.6, 8.5, 8.4, 7.9, 7.8	x64

.....continued

Drivers	Intel/AMD x64
SuSE Linux Enterprise Server 12 SP5, SP4	x64
SuSE Linux Enterprise Server 15 SP4, SP3, SP2	x64
Oracle Linux 7.9 UEK6U3	x64
Oracle Linux 9.0, 8.6 UEK7	x64
Ubuntu 22.04.1, 22.04, 21.04	x64
Ubuntu 20.04.5, 20.04.4, 20.04	x64
Ubuntu 18.04.5, 18.04.4, 18.04	x64
Ubuntu 16.04.5	x64
Debian 11.4, 10.12, 10.10	x64
Citrix xenServer 8.2.1, 8.2, 8.1, 8.0	x64
Fedora 36 (inbox only)	x64

Notes:

1. New OS is minimally tested with inbox driver. Full support is expected in the next release.
2. Support based off August 2022 RHEL 9.0 ISO refresh.

Table 1-6. Linux SmartPQI Drivers for Arm

Drivers	Cavium ThunderX2 Arm® x64
Red Hat Enterprise Linux 8.5, 8.4	X
SuSE Linux Enterprise Server 12 SP5	X
SuSE Linux Enterprise Server 15 SP3, SP2	X
Ubuntu 20.04.3, 20.04.2	X
BC Linux 7.7	X
OpenEuler 20.03 SP3 LTS, 22.03 LTS	X

Table 1-7. FreeBSD, Solaris, and VMware SmartPQI Drivers

Drivers	Version
FreeBSD 13.1, 12.3	x64
Solaris 11.4	x64
VMware 8.0, 7.0 U3/U2/U1	x64

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 Solaris x86 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 lists features supported for this release. Features to be supported in future releases or supported in current release are designated as “X”.

Table 2-1. Feature Summary

Feature		Supported in this Release	Future Release
UEFI Driver, Boot Support		X	
Legacy Boot Support		X	
Dynamic Power Management		X	
SMR Drive Support	Enumeration, Unrestricted Command Flow-Through	X	
	SATL Translation for HA/HM SMR Management	X	
	Identify All Drive Types	X	
Driver Support	Linux	X	
Out of Band interface selection support of MCTP or PBSI		X	
Flash Support		X	
MCTP BMC Management		X	
SED Local Key Management		X	

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 5.61 B0

This release includes the following fixes and enhancements:

- Added support for Managed SED adapter password.
- Added support for a new persistent event log policy that overwrites old events with the most recently occurred events.
- Fixed an issue that caused PLDM code to assert.
  - Root Cause: Non-ASCII values in extended drive buffer causes PLDM code to assert.
  - Fix: Validate the buffer data for ASCII characters before saving part number and serial number values.
  - Risk: Low
- Fixed an issue where failed locked SED is not exposed to the OS.
  - Root Cause: Incorrect failure reason kept failed drive from being exposed to OS.
  - Fix: For Managed SED conditions that needs to fail the drive, use new failure reason code to fail the drive so it will be exposed to the OS.

  - Risk: Low

- Fixed an issue on wrong state when taking ownership again on Microchip owned SED changes state to otherwise owned.
  - Root Cause: After the ownership is taken, ownership cannot be taken with MSID. After opening the session, authenticating session fails while attempting to take the ownership with MSID.
  - Fix: If the drive parameter indicates that the ownership is already taken, then do not attempt to take the ownership again and return success.
  - Risk: Low

- Fixed an issue where the controller shows password locked when firmware update occurs and Managed SED is never used.
  - Root Cause: Firmware runs a CRC check on the Managed SED NVRAM content and incorrectly reports that Managed SED is active because the default state of the NVRAM is all 0xFF values that generate a valid CRC result. The valid CRC result causes firmware to report password locked after the firmware update.
  - Fix: Firmware will run the CRC check and also read the Managed SED version information from the NVRAM content to ensure the NVRAM content is valid.
  - Risk: Low

- Fixed an issue where the drive fails during the drive firmware update.
  - Root Cause: After the drive firmware update, the host re-enquires about the drive parameters. The firmware will reset the existing drive parameters information and fill up the data again by re-enquiring about the drive. If there is a simultaneous firmware operation accessing drive parameters, it ends up with wrong values and fails. After a defined number of retries on firmware operation, the firmware fails the drive.
  - Fix: Avoid resetting the default drive parameter value fields for host drive parameter during re-inquiry.
  - Risk: Low

- Fixed an issue where an invalid persistent event tag ID is returned for reboot marker event.
  - Root Cause: Firmware fails to calculate the proper persistent event tag value for the reboot marker event.
  - Fix: Store the persistent event tag value in the persistent firmware metadata. On boot, the persistent event tag value is read from the persistent firmware metadata to resume the numbering from the previous boot.
  - Risk: Low

- Fixed an issue where a persistent event gave invalid data in the timestamp field.
  - Root Cause: During boot, firmware has not yet received the current time from the Real-Time Clock, which causes the persistent event log boot marker event to have invalid data in the timestamp field.
  - Fix: Reset the event structure to zero so it provides zeros instead of invalid data in the timestamp field.
  - Risk: Low

- Fixed an issue where the debug log was unable to capture persistent event logs.
  - Root Cause: The firmware moved the persistent event log pointer ahead of the logged events. Due to this, firmware fails to capture the logged events in the persistent event log memory.
  - Fix: Ensure the firmware never moves persistent event log pointer ahead of the logged events.
  - Risk: Low

- Added a workaround for a SATA spin-up hold issue observed when communicating with a Broadcom expander.
  - Root Cause: When a SATA drive behind a Broadcom expander is in spin-up hold, the expander does not set the logical link rate in SMP DISCOVER to SPINUP_HOLD, but rather sets the Attached SATA drive bit and sets the logical link rate to unknown. This causes logical drives to enter a Fail or Rebuild state, upon power cycle due to physical drives missing from initial discovery.
  - Fix: If an SMP discover response indicates attached SATA drive and an unknown logical link rate, firmware treats it as a spin-up hold case.
  - Risk: Low

- Fixed an issue where the VDM requests were not being serviced in a timely manner when the controller was under high load.
  - Root Cause: VDM handling thread was a very low priority and running on a CPU that already has high usage; as a result the VDM thread did not run in a timely manner due to higher priority threads.
  - Fix: Change the VDM thread to use a higher thread priority and move the thread to a CPU that had a lower usage.
  - Risk: Low

2.2.2 UEFI Fixes

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

2.2.2.1 Fixes and Enhancements for UEFI Driver 2.4.1/Legacy BIOS 2.4.3

This release includes the following UEFI fixes and enhancements:

- Added an HII option to configure Persistent Event Log Policy.
- Fixed an issue where the controller firmware updated with a wrong image returns success even if it is failing.
  - Root Cause: Error returned from internal command buffer is not mapped with the controller error status.
  - Fix: Propagate error infomation from the low-level command interface to the top.
  - Risk: Low
- Fixed an issue where Block I/O calls to multi-LUN devices fails if the multi-LUN configuration is changed.
  - Root Cause: Multi-LUN re-enumeration in HII caused clearing of the index data.
  - Fix: Do not re-enumerate multi-LUN devices in HII as it is not required.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.20-035

This release includes the following fixes and enhancements.

- Switched to using “block-mq” tags instead of linear searching.
- Fixed an issue where the maximum LUN number supported by SmartPQI is not set correctly.
  - Root Cause: When multi-actuator support was added to SmartPQI, the maximum number of LUNs supported by SmartPQI was supposed to be changed from unlimited to 256, but the setting was inadvertently left at unlimited.
  - Fix: The maximum LUN number supported by SmartPQI is now set correctly to 256.
  - Risk: Low
- Fixed an issue where Linux performance drops when large CPU affinity is used.
  - Root Cause: The driver was using a single hint variable in the function that gets a free I/O request element from the I/O request pool that was causing contention when it was utilized by a large number of threads.
  - Fix: Eliminate the initial contention by removing the hint and instead assign each CPU its own starting point within the request element array based on its CPU number.
  - Risk: Low
- Fixed an issue to update hardware queue mapping when “block-mq” is not enabled or supported.
  - Root Cause: No mapping for CPUs exceeding the maximum queue group count.
  - Fix: Updated the mapping algorithm to provide a valid mapping for all CPUs.
  - Risk: Low
- Fixed an issue where “block-mq” and managed interrupts support are not enabled by default for 5.x Linux kernels.
  - Root Cause: The appropriate definitions are not enabled in the build files.
  - Fix: Enable the appropriate flags for 5.x Linux kernels.
  - Risk: Low
- Fixed a problem where the driver does not issue flush cache to physical drives during PCIe hot remove.

  - Root Cause: During controller PCIe graceful hot remove, the driver does not send commands to the drives to flush the cache.
  - Fix: Add Graceful Removal state check in remove path to allow flush cache to be issued to the physical drives.
  - Risk: Low
- In some situations, the presence of a multi-actuator drive could cause no drives to be listed for a controller, during OS installation. The driver can also hit an unrecoverable Call trace during rmmod.
  - Root Cause: The `pqi_slave_destroy` routine is called multiple times for a multi-LUN device that causes a Call trace.
  - Fix: Remove device only upon the last `pqi_slave_destroy` call.
  - Risk: Low

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4330.0.1038

There are no known fixes for this release.

2.2.3.3 Fixes and Enhancements for Solaris Driver Build 11.4120.0.1005

There are no known fixes for this release.

2.2.3.4 Fixes and Enhancements for Windows Driver Build 1010.52.0.1012

- Fixed an issue where I/O errors are observed in a multipath configuration when cable is unplugged/plugged.
  - Root Cause: The SmartPQI driver returns I/O with the following SRB status and SCSI check conditions, which leads the Disk/MPIO driver to report disk errors on multipath configuration.

```
SrbStatus = SRB_STATUS_ERROR
    ScsiStatus= Check Condition
    SenseKey  = 0x05 Illegal Request
    ASC&ASCQ  = 26:00 Invalid Field In Parameter List or
                25:00 Logical Unit Not Supported
```

  - Fix: The SmartPQI driver processes the I/O with SCSI error `Sense Key: Illegal Request` on multipath physical devices and then needs to return `SrbStatus=SRB_STATUS_NO_DEVICE` instead of `SrbStatus=SRB_STATUS_ERROR` allowing the MPIO driver to perform I/O failover.
  - Risk: Medium
- Fixed an issue where the default driver setting does not properly set the drive queue depth. This issue was observed in physical drives and logical drives after a hot-plug event.
  - Root Cause: The SmartPQI driver added multi-LUN drive support and code was added that set all the LUNs off a specified target. Driver was passing wrong Bus, TargetId, LUN address to Storport API set queue depth.
  - Fix: Pass the correct (Bus, TargetId, LUN) address for the device.
  - Risk: Low
- Fixed an issue where the SmartPQI driver is not loading with VM's.
  - Root Cause: On a VM Server 2016 with Discrete Device Assignment (DDA) due to a February security update the PCI command register bit PCI_ENABLE_MEMORY_SPACE (0x0002) does not get explicitly set when the underlying bus driver is VPCI(that is, in a VM). This caused the SmartPQI driver not to load due to the driver checking for the bit to be set.
  - Fix: Removed checking the PCI command register bit PCI_ENABLE_MEMORY_SPACE (0x0002) so the driver will load. The underlying bus driver already guarantees that access to the device MMIO registers is enabled.
  - Risk: Low
- Fixed an issue where the Diskpart utility shows one disk's SAN policy is offline after updating the device driver.
  - Root Cause: The device driver assigns a new SCSI Target ID to the last disk of the SES/SEP group that causes Partition Manager to detect it as a new device and set it offline.
  - Fix: The driver assigns the same SCSI Target ID for all devices within the SES/SEP group.
  - Risk: Low

2.2.3.5 Fixes and Enhancements for VMware Driver Build 4380.0.108

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 4.09.00.25611

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

- Added ESXi 8.0 support for maxView and arcconf.
- Added a display property in arcconf GETCONFIG and GETVERSION command ouput to display the SEEPROM version.
- Added support in arcconf to update the PSOC expander firmware.
- Added an option in maxView and arcconf to configure the Persistent Event Log Policy.
- Added following UI enhancements in maxView:
  - Added an option to switch the ribbon between classic and simplified view. The simplified view displays only the applicable operations in the ribbon.
  - Added a new **Inventory** tab in maxView enterprise node to display and export the configurations in a CSV format.
  - Added a new **Properties** tab in maxView physical device node and moved few properties from **Summary** tab for better user experience.
  - Consolidated all the resources related properties from other tabs to **Resources** tab in physical device and logical device node.
- Fixed an issue where UEFI arcconf was not allowing the user to enable the erase completed drive.
  - Root Cause: Operation to enable erased drive was not available in UEFI arcconf due to a wrong feature bit check.
  - Fix: Feature bit check is corrected to allow enabling erased drive operation in UEFI arcconf.
  - Risk: Low
- Fixed an issue where UEFI arcconf displayed unreadable text for reported location in GETCONFIG command output.
  - Root Cause: Invalid format specifier was used for reported location string in display.
  - Fix: Added changes to use the valid format specifier to display the reported location in UEFI arcconf GETCONFIG command output.
  - Risk: Low
- Fixed an issue where maxView was not allowing to select the ‘Number of Targets’ drop-down for backplane discovery protocol.
  - Root Cause: The empty list was returned for “Number of Targets” that resulted in non-selectable drop-down during backplane discovery protocol change in maxView.
  - Fix: The overwritten empty list is removed and returned with valid values for “Number of Targets”. Now, the “Number of Targets” drop-down is selectable and valid values are listed in maxView.
  - Risk: Low
- Fixed an issue in maxView where **Management Protocol** drop-down was not relevant after depreciation of CIM protocol in ESXi 7.x and above.
  - Root Cause: **Management Protocol** drop-down was added in maxView when both CIM and redfish were supported. CIM is no longer supported by maxView. So, the **Management Protocol** is not applicable anymore.
  - Fix: Removed **Management Protocol** and added **Operating System** drop-down in **Add System** dialog with options **Windows/Linux**, **ESXi 7.x**, and **ESXi 8.x**.
  - Risk: Low
- Fixed an issue in maxView where the connector level mode change was allowed when the controller was waiting for the adapter password whereas the same operation was blocked at the controller level.
  - Root Cause: The Connector Level mode change was allowed from maxView when the controller was waiting for the adapter password. When the controller was waiting for password the Connector mode change should be blocked from controller and individual connector level.

  - Fix: The Connector mode change is blocked from maxView when the controller is waiting for adapter password. maxView blocks this operation from both Controller and Connector level.
  - Risk: Low
- Fixed an issue in maxView where the Revert to OFS operation was not working when the PSID of SED drive was entered in lowercase.
  - Root Cause: maxView was not allowing next step when PSID was in lowercase during Revert to OFS operation. There was a check in maxView to allow only uppercase PSID.
  - Fix: The check for validating PSID in maxView is modified to accept both uppercase and lowercase PSID for Revert to OFS operation.
  - Risk: Low

2.2.4.2 Fixes and Enhancements for PLDM Release 6.15.13.0

This release includes the following fixes and enhancements:

- Redfish GET on a drive resource in PLDM will now support Multi-Actuator (MA) drives. There will be a single drive resource per MA drive with CapacityInBytes being equal to the total capacities of all the LUNs. The Identifiers include the **DurableName** and **DurableNameFormat** of each LUN. All other properties are the same.
- In addition to the existing NumericSensor PDR published for the hard drive temperature sensor, a new set of NumericSensor PDRs with entityInstanceNumber = 2 has been added to provide temperature readings for individual drives.
- The Type 5 commands QueryDownstreamDevices, QueryDownstreamIdentifiers, and GetDownstreamFirmwareParameters now provide information for enclosure SEPs connected to the controller. The following descriptors will be reported for the enclosure SEPs using the QueryDownstreamIdentifiers command:
  - SCSI Vendor ID
  - SCSI Product ID
  - Vendor-defined descriptor containing the SEP location in “Slot=<slot>:Port=<port>:Box=<box>” format.
- Redfish POST requests to perform the Drive.Actions.#SecureErase ACTION will now be rejected with the extended error message ResourceInUse if the targeted Drive is a SED that is not in the original factory state (OFS).
- Removed the Status.Health property from Redfish GET responses for the Storage resource.
- Fixed an issue where an unnecessary DriveOK alert was sent when importing a foreign SED.
  - Root Cause: The logic for the drive alerts code was checking for DriveOfflineCleared conditions in the same If condition for the DriveOK alert.
  - Fix: Fixed the drive alert generation logic to remove the unnecessary DriveOfflineCleared check.
  - Risk: Low
- Fixed an issue where a Type 5 GetStatus command following an ActivateFirmware command might return the wrong ReasonCode.
  - Root Cause: ReasonCode field was not set correctly when the firmware device proxy processes the ActivateFirmware command resulting in an incorrect value.
  - Fix: Firmware device proxy now correctly sets the ReasonCode field in the GetStatus response to “1—ActivateFirmware command was received” after the update agent sends an ActivateFirmware command for a downstream device (drive).
  - Risk: Low
- Fixed an issue where the ControllerPasswordEntered Redfish alert was sent with an incorrect messageId.
  - Root Cause: The ControllerPasswordEntered Redfish alert changed to ControllerPasswordAccepted in the released version of the DMTF StorageDevice registry v1.1.
  - Fix: Changed the ControllerPasswordEntered Redfish alert to ControllerPasswordAccepted.
  - Risk: Low
- Fixed an issue where the Links.Storage property was not published with the drive resource.
  - Root Cause: Links.Storage was not included in the drive resource schema dictionary, and no implementation was present to publish that property with the drive resource.

  - Fix: Updated the schema dictionaries to include Links.Storage in the drive resource and added the property to the drive resource Redfish GET response.
  - Risk: Low
- Fixed an issue where a drive's ServiceLabel is sometimes erroneously published with a leading zero on its Port number.
  - Root Cause: Current logic was formatting the port in the ServiceLabel as “%02u” which results in the leading 0 when the port is a single digit number.
  - Fix: Corrected the logic to make the formatting of the port in the ServiceLabel dynamic based on the string length of the port name.
  - Risk: Low
- Fixed an issue where GetDownstreamFirmwareParameters returned incorrect ComponentActivationMethods and CapabilitiesDuringUpdate values.
  - Root Cause: A bit indicating support for drive firmware updates was not being set.
  - Fix: Firmware updates for downstream devices have been enabled for UBM and drive devices. Since UBM firmware updates are not allowed on some controllers, a check has been put into place to verify if the UBM firmware updates are allowed when attempting to update the device.
  - Risk: Low
- Fixed an issue where Redfish alerts generated early in the boot sequence were not being received by the Server Management controller.
  - Root Cause: Publishing Redfish events required event support to be negotiated using NegotiateRedfishParameters. This negotiation was being done after the initial polling for controller events, so those initial Redfish events were not sent to the management controller.
  - Fix: Removed the requirement for event support negotiation as a prerequisite for passing Redfish events.
  - Risk: Medium
- Fixed an issue where the ControllerPreviousError alert was sent with an incorrect messageId and severity.
  - Root Cause: The internal table of alert definitions includes MessageId and Severity information for this alert that is not compliant with the DMTF alert registry.
  - Fix: Updated the alert definitions to include correct MessageId and Severity information.
  - 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)
  - No Storage Manager support

2.3.2 Firmware Limitations

2.3.2.1 Limitations for Firmware Release 5.61 B0

This release includes the following firmware limitations:

- Persistent Event Logs(PEL) will be cleared if,
  - Upgrading to the firmware version 5.61 B0.
  - Downgrading from the firmware version 5.61 B0.

- If panic shutdown or power loss occurs when clear configuration or delete logical drive operations are in progress with Managed SED logical drives, on the subsequent system power-up, the SEDs need to be manually returned to the OFS state with the Master Key or PSID method.
  - Workaround: Let the clear configuration/delete logical drive on secure logical drive complete before shutting down the power.
- After three failed attempts to unlock the adapter password, the lockout timer for 15 minutes starts. If the system is rebooted during this lockout period, the internal lockout timer gets reset back to 15 minutes instead of continuing with the countdown before the reboot.
  - Workaround: Wait for password lockout timer countdown to complete before attempting to unlock the adapter or rebooting.
- A firmware update causes the UART log buffer (Serial Output Buffer) to be reinitialized, since the DDR gets reinitialized.
  - Workaround: None
- SATA drives attached to a non-Microchip expander may get into a failed state when upgrading the controller firmware from previous releases to this release due to the expander not clearing STP affiliation.
  - Workaround: Power cycle the expanders to clear the STP affiliation.
- A rare corner-case scenario where controller may hang during expander firmware update on multi-level expander/SEP device topology along with I/Os.
  - Workaround: After the enclosure firmware update, avoid enclosure Reset. It is recommended to download the new firmware and perform manual power cycle. This issue is intermittent and can cause a hang that requires a system reboot.
    Note: This issue was mostly seen when using Linux OS.

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 2.4.1/Legacy BIOS Build 2.4.3

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 Limitations for Linux Driver Build 2.1.20-035

This release has the following Linux limitation:

- This release includes the following limitation when doing a driver injection (DUD) install. On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, SLES15SP3, OpenEuler 22.03LTS), the DUD install will hang if an attached drive (either HBA mode or logical drive) has Write Cache enabled.
  - Workaround: There are two workarounds for this issue:
    - Make sure the Write Cache is disabled for any attached drive.
    - For RHEL7.9/8.2/8.3 and OpenEuler 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. Reported on RHEL 8.5, 8.6,9.0 and 9.1.
  - Workaround: There are two workarounds for this issue:
    - Load OS from USB device instead of virtual media.
    - Load OS from virtual media but initiation ISO verification (media test) during install followed by ESC to cancel media test.
- 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 is expected in the mid-October UEK7 release, version number still pending.
  Note: This does not affect Oracle 8 UEK 7.
  - Workaround: Install the rpm using `--nodeps` when dependency failures occur.
    - 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, install the SmartPQI rpm using the `--nodeps`.
- On AMD/RHEL 7.9 systems, the system might panic due to a bug in the IOMMU module. For details, see https://lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/
  - Workaround: Disable the IOMMU setting option in BIOS.
- Depending on hardware configurations, the SmartPQI expose_ld_first parameter may not always work consistently.
  - Workaround: None
- 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: There is a workaround for this issue which 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 XenServer 8.1 LTS, Ubuntu 18.04.5 LTS), only one multi-actuator drive LUN is displayed in the OS installation menu.
  - Workaround: Inject/Load the OOB driver during OS installation. Go to console mode (Ctrl+Alt+F2), issue the command “rmmod smartpqi” followed by “modprobe smartpqi”. Exit console mode (Ctrl+Alt+F1) and proceed to the Primary disk selection screen in the GUI.
- On some distributions (including RHEL 9.0/Oracle Linux 9.0), users are unable to inject the OOB driver (DUD) during installation 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 1010.52.0.1012

This release includes the following limitation:

- In certain circumstances, the installation may fail on Windows Server 2016 and Windows 2012 R2 after selecting drives.
  - Workaround: Follow these steps to ensure drives are clean and all partitions are removed before beginning a new installation:
    a. Hit Shift + F10 to open command prompt
    b. Type `Diskpart`
    c. Type `List Disk`
    d. Select the disk you want to clean. For example, to select Disk 0 type `select disk 0`.
    e. Type `Clean`
- BSOD observed on Windows Server 2019 while loading OOB driver if BIOS setting SNC4 is enabled.
  - Workround: Change the BIOS setting to SNC2.

2.3.4.3 Limitations for FreeBSD Driver Build 4330.0.1038

There are no known limitations for this release.

2.3.4.4 Limitations for Solaris Driver Build 11.4120.0.1005

There are no known limitations for this release.

2.3.4.5 Limitations for VMware Driver Build 4380.0.108

This release includes the following limitations:

- A controller lockup might occur when using VMDirectPath on an single processor AMD system. Lockup has only been seen with in a Linux Guest VM.
  - Workaround: None

2.3.5 Management Software Limitations

2.3.5.1 Limitations for Arcconf/maxView Build 4.09.00.25611

There are no known limitations for this release.

2.3.5.2 Limitations for PLDM Release 6.15.13.0

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.

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 2.3.2.2. 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
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

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 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, 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.

ISBN: 978-1-6683-1607-8

Quality Management System

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

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			