Table of Contents

1. About This Release.................................................................................................................................. 3
   1.1. Release Identification..................................................................................................................... 3
   1.2. Components and Documents Included in this Release................................................................. 4
   1.3. Files Included in this Release....................................................................................................... 4
2. What’s New?............................................................................................................................................. 7
   2.1. Features....................................................................................................................................... 7
   2.2. Fixes............................................................................................................................................. 7
   2.3. Limitations.................................................................................................................................. 12
3. Updating the Controller Firmware........................................................................................................ 16
   3.1. Updating the Controller Firmware.............................................................................................. 16
4. Installing the Drivers.............................................................................................................................. 17
5. Revision History.................................................................................................................................... 18
6. The Microchip Website........................................................................................................................... 19
7. Product Change Notification Service....................................................................................................... 19
8. Customer Support.................................................................................................................................. 19
9. Microchip Devices Code Protection Feature.......................................................................................... 19
10. Legal Notice...................................................................................................................................... 19
11. Trademarks......................................................................................................................................... 20
12. Quality Management System................................................................................................................ 21
13. Worldwide Sales and Service................................................................................................................ 22
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>
<thead>
<tr>
<th>Table 1-1. Release Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions Release</td>
</tr>
<tr>
<td>Package Release Date</td>
</tr>
<tr>
<td>Firmware Version</td>
</tr>
<tr>
<td>UEFI Version</td>
</tr>
<tr>
<td>Legacy BIOS</td>
</tr>
<tr>
<td>Driver Versions(^3)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Management Software</td>
</tr>
<tr>
<td>(arcconf, maxView(\textsuperscript{TM}), Event Monitor, BootUSB)</td>
</tr>
</tbody>
</table>

**Notes:**

1. Dowgrading 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 the firmware running on the board is older than 0.01 B594, existing data in the logical drives must be backed up if it needs to be used after the upgrade. After the upgrade from firmware prior to 0.01 B594, the logical drives will need to be recreated.

3. Only run the driver on firmware 0.01 build 500 or later.

4. Only Windows 11 Inbox driver is supported.
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Pre-Assembly Use</th>
<th>Post-Assembly Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartFWx100.bin</td>
<td>Programmable NOR Flash File Use to program NOR Flash for boards that are already running firmware.</td>
<td>—</td>
<td>x</td>
</tr>
</tbody>
</table>

Table 1-3. Firmware Programming Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arcconf romupdate</td>
<td>The command allows to upgrade/downgrade the firmware and BIOS image to the controller.</td>
<td>Refer to Table 1-8</td>
</tr>
<tr>
<td>maxView™ firmware upgrade wizard</td>
<td>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.</td>
<td>Refer to Table 1-8</td>
</tr>
</tbody>
</table>

Driver Files

Table 1-4. Windows Storport Miniport SmartPQI Drivers

<table>
<thead>
<tr>
<th>Package</th>
<th>Drivers</th>
<th>Binary</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Server 2022, Server 2019 and Server 2016 Windows 10</td>
<td>SmartPqi.sys</td>
<td>x64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SmartPqi.inf</td>
<td>x64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smartpqi.cat</td>
<td>x64</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Intel/AMD x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 8.4, 8.3, 8.2, 8.1, 7.9, 7.8, 7.7, 7.6</td>
<td>x64</td>
</tr>
<tr>
<td>CentOS 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7</td>
<td>x64</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 12¹, SP5, SP4, SP3²</td>
<td>x64</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 15 SP3, SP2, SP1¹</td>
<td>x64</td>
</tr>
</tbody>
</table>
Drivers | Intel/AMD x64
---|---
Oracle Linux 7.9, 7.8, UEK 6U1 | x64
Oracle Linux 8.4 UEK6 | x64
Oracle Linux 8.2 UEK6 | x64
Oracle Linux 8.3, 8.2 UEK6U1 | x64
Ubuntu 21.04 | x64
Ubuntu 20.04.2, 20.04.1, 20.04 | x64
Ubuntu 18.04.5, 18.04.4, 18.04 | x64
Ubuntu 16.04.5 | x64
Debian 10.10, 10.05 | x64
Debian 9.13 | x64
Citrix xenServer 8.2, 8.1, 8.0 | x64
Fedora 34 (inbox only) | x64

Notes:
1. To mitigate against the Spectre Variant 2 vulnerability, the RHEL 6.9, RHEL 7.4, RHEL 7.5 and SLES12 SP3 and higher drivers have been compiled to avoid the usage of indirect jumps. This method is known as "Retpoline".
2. SLES 12 SP3 cannot be installed on drives attached to the HBA 1100 controller in Cavium Thunder X2 systems due to a CPU and OS installation issue. This driver will support the HBA 1100 controller in Cavium Thunder X2 systems for non-boot drives. For Cavium Thunder X2 servers, if you choose to install SLES12 SP3, you have to install it on the system board’s SATA controller.
3. CentOS 7.4 requires the kernel to be updated to 4.11.0-44 or later.

Table 1-6. Linux SmartPQI Drivers for ARM

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Cavium ThunderX2 ARM x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 8.2, 8.1</td>
<td>X</td>
</tr>
<tr>
<td>CentOS 8.2, 8.0, 7.8</td>
<td>X</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 15 SP3, SP2, SP1</td>
<td>X</td>
</tr>
<tr>
<td>Ubuntu 20.04, 18.04.5, 18.04.4, 18.04.1, 18.04</td>
<td>X</td>
</tr>
<tr>
<td>BC Linux 7.6</td>
<td>X</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeBSD 13, 12.2, 11.4</td>
<td>x64</td>
</tr>
<tr>
<td>Solaris 11.4</td>
<td>x64</td>
</tr>
<tr>
<td>VMware 6.7 U3/U2, 6.5 U3/U2</td>
<td>x64</td>
</tr>
</tbody>
</table>
### Host Management Software

**Table 1-8. Host Management Utilities**

<table>
<thead>
<tr>
<th>Description</th>
<th>OS</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCCONF Command Line Utility</td>
<td>Windows x64</td>
<td>See the Arcconf download package for the OS-applicable installation executable.</td>
</tr>
<tr>
<td></td>
<td>Linux x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VMware 6.5 and above</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XenServer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FreeBSD x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris x86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linux ARM</td>
<td></td>
</tr>
<tr>
<td>ARCCONF for UEFI</td>
<td></td>
<td>Included as part of the firmware downloadable image.</td>
</tr>
<tr>
<td>maxView™ Storage Manager</td>
<td>Windows x64</td>
<td>See the maxView Storage Manager download package for the OS-applicable installation executable.</td>
</tr>
<tr>
<td></td>
<td>Linux x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VMware EXSi 6.5 and above</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XenServer</td>
<td></td>
</tr>
<tr>
<td>maxView™ vSphere Plugin</td>
<td>VMware 6.5 and above</td>
<td>See the VMware maxView Storage Manager download package for the OS-applicable installation executable.</td>
</tr>
<tr>
<td>Boot USB (offline or pre-boot) for ARCCONF and maxView Storage Manager</td>
<td>Linux x64</td>
<td>See the maxView BootUSB download package for the .iso file.</td>
</tr>
</tbody>
</table>
2. **What's New?**
   
   This section shows what’s new in this release.

   **Important:** Updated maxView to address log4j vulnerabilities.

2.1 **Features**

   The following table lists features supported for this release.

   **Table 2-1. Feature Summary**

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

2.2 **Fixes**

2.2.1 **Firmware Fixes**

2.2.1.1 **Fixes and Enhancements for Firmware Release 4.72 B0**

   This release includes the following fixes and enhancements:

   - Added additional debug information into controller crash dump log file.
   - Added driver and firmware handshake mechanism during the crash dump generation process (start and end of crash dump generation) to avoid any planned reboot/shutdown, thus ensuring the crash dump gets generated in these scenarios.
   - Added the NMI reason code into crash dump to differentiate various NMI scenarios that the driver can trigger.
   - Added support to configure default setting for the drive write cache.
   - Added support in PBSI to show maximum and negotiated link rate for physical drives.
   - Added support to avoid truncating PBSI I2C DSAP write message early based on the stop bit.
• Added support in PBSI to extend controller serial number size to 15 bytes.

• Fixed a problem where the physical drive firmware update does not succeed when initiated through Out-Of-Band (OOB) MCTP host transport.
  – Root Cause: Firmware was not setting the correct response to host for the SCSI pass through OUT direction commands.
  – Fix: To adjust the response buffer properly for these SCSI pass through commands.
  – Risk: Medium

• Fixed a problem where excess data is transferred for first and intermediate request packets for packetized OOB MCTP requests.
  – Root Cause: While responding to the assemble request packet, firmware is always sending a success acknowledgment packet with 308 bytes. Where 292 bytes are max_resp_length and 16 bytes are the MCTP header. For the first and intermediate acknowledgment packets the response data does not need to be provided.
  – Fix: For acknowledgment packets only send back the 16 byte header.
  – Risk: Low

• Fixed a controller 0x1E30 lockup problem when the drive topology is hot removed and added back into the controller in a loop.
  – Root Cause: When handling the device hotplug, firmware disables the interrupts and tries to update the seven segment display by allocating a logical request. After updating it through the SES diagnostic pages, and then freeing the logical request, firmware tries to wake up tasks waiting on this logical request while the interrupts are disabled, thus resulting in the lockup.
  – Fix: Added necessary code to enable and disable interrupts while freeing up the logical request.
  – Risk: Medium

• Fixed an issue where SED HBA drive security status is not updated in the PLDM layer.
  – Root Cause: When SED HBA drive's status changes, firmware does not notify the PLDM layer.
  – Fix: Notify PLDM layer when the SED drive status changes.
  – Risk: Low

• Fixed an issue where the Fault LED is not turned ON when firmware fails a bad HBA drive connected to an expander during device discovery or hot-plug.
  – Root Cause: When firmware fails a HBA drive during device discovery or hot-plug, it does not set the “select” bit to 1 in the SES control page to turn on the Fault LED. The issue is that firmware still sees this failed HBA drive is exposed to host so firmware does not control the drive LED and the host must control the drive LED. This leads to the firmware not setting the “select” bit to 1 in the SES control page for the failed HBA drive when firmware is performing the LED update operation.
  – Fix: Firmware sets the “select” bit to 1 in SES control page for the failed HBA drive which is not exposed to host and turns ON the drive's Fault LED correctly.
  – Risk: Low

• Fixed an issue where SATA HDD enterprise SEDs fail during SED qualification if initiated immediately after drive reset.
  – Root Cause: As part of SED qualification discovery, firmware issues StartSession by sending SECURITY PROTOCOL OUT commands. Immediately after drive reset if the SED qualification is run, StartSession fails due to protocol error and commands to the drive are aborted with sense key set to ILLEGAL REQUEST and sense code CMD_SEQ_ERROR. In this case, firmware immediately fails the drive with reason code 0x4D (SED protocol command failure) after failing to StartSession without retrying.
  – Fix: Firmware will retry the StartSession procedure after encountering this error.
  – Risk: Low

• Fixed SGPIO backplane configuration issue.
- Root Cause: For SGPIO backplanes that are dynamically configured during boot the drive bay mapping may not match what is reported by the backplane.
- Fix: Configure the SGPIO backplane based on the configuration information retrieved from the backplane.
- Risk: Low

- Added support to return NCQ Priority Information for SATA drive information to host.
- Fixed an issue where the enclosure fails to receive SES control from the controller when drives are partially populated.
  - Root Cause: Zero-based and one-based numbering detection algorithm fails because the unpopulated bays are skipped during the scan.
  - Fix: Scan all bays, do not skip.
  - Risk: Low

- Fixed an issue where the controller sends SES control commands to wrong bay number after enclosure power cycle.
  - Root Cause: The SES indexes are off by one index when a zero-based format enclosure is detected.
  - Fix: Do not adjust slot numbers with +1, when setting the expander attached drive identification.
  - Risk: Low

- Fixed an issue where diskname is not showing for drives after deletion of logical drive and RAID metadata present on the SEDs.
  - Root Cause: Firmware is unable to read the RAID metadata on boot if SED is locked.
  - Fix: Firmware will no longer look for locked to unlocked state transition. It will check if current status is unlocked, then it will read the RAID metadata and update drive flags allowing RAID metadata to be cleared.
  - Risk: Low

- Fixed an issue where the sanitize support flag of an OPAL SED is set to not support if Update Security State (0x1F) command is received right after this OPAL SED reverted to factory default or Original Factory State (OFS) and before the firmware can update the status change for this OPAL SED.
  - Root Cause: The logic in Update Security State command updates the state (for example, lock, unlocked, locking enabled, etc.) of a SED but it does not update the sanitize support flag for a SED. The firmware does update both SED's state and sanitize support flag. For OPAL SED, the firmware relies on the state of OPAL SED to carry out the update of the SED's sanitize support flag. If the state of a OPAL SED is not in the "locking enabled" state, the sanitize support flag is not updated. In this case, the Update Security State command is executed before the firmware so the OPAL SED state is updated. It will not be in "locking enabled" state after it is reverted to OFS. As a result, the sanitize support flag is not updated when firmware runs the check/update.
  - Fix: In the function that processes Update Security State command, check if an OPAL SED is in the "locking enabled" state then skip updating the status of this OPAL SED. The OPAL SED status will be updated by firmware so the sanitize support modes also get updated accordingly.
  - Risk: Low

- Fixed an issue where the firmware reports to host as OFA supported and capable for all non-OFA binaries.
  - Root Cause: While updating OFA feature flags, firmware is not checking OFA header for OFA feature enabled flag before updating the feature bits.
  - Fix: OFA capable and OFA supported feature bits should be set to true only if OFA header feature enabled flag is set to “true” indicating the OFA feature is enabled in the firmware image.
  - Risk: Low

- Fixed an issue where a replacement cable attached after an external cable was discovered with error is not discovered correctly.
  - Root Cause: The error status of the prior cable was not being cleared prior to the new cable being discovered. This resulted in a persistent "failed" state for the new cable.
  - Fix: Ensure prior cable information is cleared before processing the hot-add discovery for a new cable in that location.
2.2.2 UEFI Fixes

Note: Microsoft signed and secure boot is supported.

2.2.2.1 Fixes and Enhancements for UEFI Driver 1.3.15.2/Legacy BIOS 1.3.15.2

This release includes the following legacy BIOS fixes and enhancements:

- Fixed an issue where junk characters are displayed in the BMC settings page.
  - Root Cause: The background initialization code for the menu was missing.
  - Fix: Added required background initialization code.
  - Risk: Low

- Fixed an issue where bootup freezes with Insyde Legacy BIOS on AMD ROME platform.
  - Root Cause: The Legacy Option ROM was not checking if the Keyboard buffer was empty before reading and writing to ports 60h and 64h.
  - Fix: Check if the Keyboard buffer is clear before reading and writing to ports 60h and 64h. If not, clear the buffer by reading the data from Port 60h.
  - Risk: Medium

This release includes the following UEFI fixes and enhancements:

- Updated driver name from MSCC/Microsemi to Microchip Technology Inc.
- Added new option under controller settings “Unchanged” for Configured Physical Drive Write Cache state. This setting ensures Physical Drive Write Cache state will not change for configured drives.
- Fixed an issue where HII and health messages display incorrect translation for Chinese and Japanese strings.
  - Root Cause: Incorrect translation for few HII options and driver health messages.
  - Fix: Corrected language translations for Unicode strings.
  - Risk: Low

- Fixed an issue where UEFI arconf CLI freezes when save support archive operation is performed.
  - Root Cause: Memory is corrupted when user does not enter any file system and performs save support archive operation. The current directory remains NULL.
  - Fix: Do not access current file system and provide error message when user has not selected a valid file system.
  - Risk: Low

- Fixed an issue where the Version field of Firmware Management Protocol is not populated with 32 bit version.
  - Root Cause: The Version field of Firmware Management Protocol is not populated with 32 bit version instead it is assigned with a truncated long version.
  - Fix: The Version field of Firmware Management Protocol is assigned with 32 bit version format.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.14-035

This release includes the following fixes and enhancements.

- Fixed an issue of driver spin down when system transitions to the Suspend (S3) state in certain systems.
  - Root Cause: In certain system (based on PCI IDs), when the OS transitions the system into the Suspend (S3) state, the flush cache command indicates a system RESTART instead of SUSPEND. This avoids drive spin-down.
– **Fix**: Avoid drive spin-down when system transitions to the Suspend state.
– **Risk**: Medium

- **Added enable SATA NCQ priority support to** `sysfs`. The driver needed device attribute `sas_ncq_prio_enable` for I/O utility to enable SATA NCQ priority support and to recognize I/O priority in SCSI command and pass priority information to controller firmware. This device attribute works only when device has NCQ priority support and the controller firmware can handle I/O with NCQ priority attribute.

- **Fixed an issue where during kdump OS is dropping into a shell if the controller is in Locked-up state.**
  - **Root Cause**: Driver issues SIS soft reset to restore the controller to SIS mode when OS boots into kdump mode. If the controller is in Locked-up state, the SIS soft reset does not work. Since the controller lockup code has not been cleared, the driver considers firmware is no longer up and running. In this case, the driver returns an error code to OS and kdump fails. After kdump failure, some OS distributions do not reboot cleanly which leads to the OS dropping into a recovery shell.
  - **Fix**: During kdump, driver will reboot the system if the controller is in Locked-up state.
  - **Risk**: Low

- **Fixed an issue where when one of the path fails during I/O and IOBypass path gets disabled for a multipath device, the I/O is again retried in the RAID path. These requests were submitted to non-existent devices in the RAID path and firmware responded to those requests with Illegal request and 'Invalid field in parameter list' sense data.**
  - **Root Cause**: Even when the device path has gone, the driver continued submitting requests in RAID path and they are returned from firmware as illegal requests.
  - **Fix**: When one of the paths is removed in dual domain, return DID_NO_CONNECT to SCSI mid-layer of the OS. The DID_NO_CONNECT return helps multipath to stop issuing Test Unit Ready and other media access commands before failing the path. Failing the path quickly helps routing I/O to the opposite path faster.
  - **Risk**: Low

- **Fixed an issue where the controller spins down drives during a warm boot on Linux.**
  - **Root Cause**: The Linux SmartPQI driver has a callback function that the OS calls when the system is being shut down or being rebooted. This callback function calls the Flush Cache command. The command has a parameter that allows the driver to indicate to the firmware the reason for the flush cache (shutdown, hibernate, suspend, or restart). The OS callback function does not indicate to the driver whether it is being called for shutdown or warm boot, so the driver indicates to the firmware that the reason for the flush cache is a system shutdown. The firmware always spins down drives in this case.
  - **Fix**: The SmartPQI driver uses a Linux kernel global variable to distinguish between a system shutdown and a warm boot and sets the Flush Cache command parameter accordingly.
  - **Risk**: Low

- **Fixed an issue where duplicate device nodes for Ultrium tape drive and medium changer are being created.**
  - **Root Cause**: The Ultrium tape drive is a multi-LUN SCSI target. It presents a LUN for the tape drive and a second LUN for the medium changer. The controller firmware lists both LUNs in the report logical LUNS results, so the SmartPQI driver exposes both devices to the OS. Then the OS does its normal device discovery through the SCSI REPORT LUNS command, which causes it to re-discover both devices a second time, resulting in duplicate device nodes.
  - **Fix**: When the OS re-discovers the two LUNs for the tape drive and medium changer, the driver recognizes that they have already been reported and blocks the OS from adding them a second time.
  - **Risk**: Low

### 2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4170.0.1014

This release includes the following enhancements and fixes:

- **Fixed an issue where debug log messages were flooding the kernel logs.**
  - **Root cause**: There are a lot of DBG_INFO prints which are logged by SmartPQI and one DBG_ERR print causing log contention which should not be considered an error.
  - **Fix**: Disable the DBG_INFO prints from logging and change DBG_ERR to DBG_INFO for a message not considered an error.
2.2.3.3 **Fixes and Enhancements for Solaris Driver Build 4120.0.1005**
There are no known fixes for this release.

2.2.3.4 **Fixes and Enhancements for Windows Build 1010.12.0.1007**
There are no known fixes for this release.

2.2.3.5 **Fixes and Enhancements for VMware Driver Build 4230.0.103**
This release includes the following enhancements and fixes:

- Fixed an issue where possibility of a null device pointer needs to be prevented in one of the functions where it waits for the outstanding commands to get completed.
  - **Root Cause:** Device may have been removed.
  - **Fix:** Check for a null device pointer before starting the wait loop.
  - **Risk:** Low
- Fixed an issue where a failed lookup results in an array out of bounds condition.
  - **Root Cause:** A device lookup function returns INVALID_ELEM (0xffff) when device is not found, but calling function does not check for error, and unconditionally uses lookup’s return as index into the device list.
  - **Fix:** Print message and do not continue device addition or deletion if lookup function returns INVALID_ELEM.
  - **Risk:** Low

2.2.4 **Management Software Fixes**

2.2.4.1 **Fixes and Enhancements for Arcconf/maxView Build B24713**
This release includes the following fixes and enhancements for arcconf/maxView:

- Upgraded the log4j version in maxView and vSphere plugin to 2.16.0, which has the fix for CVE-2021-44228 and CVE-2021-45046 vulnerabilities.

2.3 **Limitations**

2.3.1 **Firmware Limitations**

2.3.1.1 **Limitations for Firmware Release 4.72 B0**
This release includes the following firmware limitations:

- 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, a reboot is known to fix such instances.
  
  **Note:**
  This issue was mostly seen when using Linux OS.

2.3.1.2 **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 volume operations.
– Description: Refer to entry “Fixed an issue where firmware may become unresponsive while attempting to flash firmware or execute other RAID logical volume 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.

2.3.2 UEFI Limitations

2.3.2.1 Limitations for UEFI Build 1.3.15.2/Legacy BIOS Build 1.3.15.2
There are no known limitations for this release.

2.3.3 Driver Limitations

2.3.3.1 Limitations for Linux Driver Build 2.1.14-035
This release has the following Linux limitations:
  • When doing a driver injection (DUD) install. On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, and SLES15SP3), the DUD install hangs if a drive in HBA mode has the Drive Write Cache enabled.
    – Workaround: There are two workarounds for this issue:
      • Ensure the Drive Write Cache is disabled for any drive in HBA mode.
      • For RHEL7.9, RHEL8.2, and RHEL8.3, add rd.driver.blacklist=smartpqi to the grub entry along with inst.dd.
  • Due to a change in the SCSI mid-layer, some Linux distributions may take a long time to come up if the system is rebooted while a hard disk(s) is being sanitized. This has currently been observed with inbox smartPQI drivers on RHEL 7.9, RHEL8.3, and SLES 15SP2.
    – Workaround: Do not reboot the system while a hard disk(s) is being sanitized or update to the SmartPQI 2.1.12-055 or later driver release.
  • On AMD/RHEL 7.9 systems, the system might panic due to an issue in the IOMMU module. For more information, see lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/
    – Workaround: Disable the IOMMU setting option in BIOS.
  • On AMD/UEK6 systems, the system might hang during kdump if IOMMU is enabled.
    – Workaround: Disable IOMMU setting option in BIOS.
  • The smartpqi.expose_ld_first parameter does not work correctly consistently.
    – Workaround: None
  • Hibernating Linux system using pm-hibernate command causes system to hang.
    – 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: Extend the udev(systemd) timeout during a kdump operation. Use the following to increase the timeout for udev(systemd):

```
vi /etc/sysconfig/kdump
add udev.event-timeout=300 to KDUMP_COMMANDLINE_APPEND
systemctl restart kdump
systemctl status kdump
```

2.3.3.2 Limitations for Windows Driver Build 1010.12.0.1007
There are no known limitations for this release.
2.3.3 Limitations for FreeBSD Driver Build 4170.0.1014
This release includes the following FreeBSD driver limitations:
  • Under heavy I/O with transfer size more than 128k, controller may go offline. This happens in FreeBSD 13.
    – Workaround: Reduce the I/O transfer size of the application to less than 128k.

2.3.4 Limitations for Solaris Driver Build 4120.0.1005
There are no known limitations for this release.

2.3.5 Limitations for VMware Driver Build 4230.0.103
There are no known limitations for this release.

2.3.4 Management Software Limitations

2.3.4.1 Limitations for Arcconf/maxView Build B24713
This release includes the following Arcconf/maxView limitations:
  • Advanced statistics will not be available in maxView.arcconf.
  • ADU report in support archive will not be available in zip format. The relevant logs are captured under Controller_X_Debug_Log.txt.
  • SSD report in support archive will not be available.
  • OS partition information is not available in FreeBSD and Solaris OS in maxView/arcconf.
  • Remote arcconf (CIM client) is not supported for ESXi 7.x and onwards.
  • Due to data type mismatch between maxView and redfish server, eccRecoveredReadErrors and serviceHours properties in the drive error counter tab will not be reflecting the current value.
    – Workaround: User needs to use arcconf CLI GETCONFIG command to refer the current value for these error counter properties.
  • In ESXi 7.x, maxView GUI may not update the latest configuration automatically when the operations are performed through the ESXi host arcconf.
    – Workaround: User needs to refresh the configuration using the refresh link provided in the top right corner in the maxView GUI before performing any operations.
  • When user tries to access the maxView main.xhtml page directly when the previous session was still active, user may end up with a warning page mentioning “XML Parsing Error: no root element found”.
    – Workaround: User needs to use the login page to get authenticated and create a new session to access the main.xhtml page.
  • When the SED drive is in Locked state, the hard drive level refresh SED security status operation is not available in the maxView GUI.
    – Workaround: Use the controller level refresh SED security status operation or use arcconf command to refresh the SED security status.

2.3.5 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.

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 2.3.1.2. 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 (DS00004281A, 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.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>12/2021</td>
<td>SR 2.6.4.1 Patch Release with maxView™ version B24713. Updated Fixes and Enhancements for maxView Storage Manager/ARCCONF section for log4j vulnerabilities.</td>
</tr>
<tr>
<td>A</td>
<td>11/2021</td>
<td>SR 2.6.4 with VMware driver version 4230.0.103 (previously ESC-2162192)</td>
</tr>
<tr>
<td>22</td>
<td>08/2021</td>
<td>SR 2.6.2 with VMware driver version 4150.0.119</td>
</tr>
<tr>
<td>21</td>
<td>04/2021</td>
<td>SR 2.6.1.1 with VMware driver version 4054.2.118</td>
</tr>
<tr>
<td>20</td>
<td>03/2021</td>
<td>SR 2.6.1 with VMware driver version 4054.1.103</td>
</tr>
<tr>
<td>19</td>
<td>02/2021</td>
<td>SR 2.6 Production Release</td>
</tr>
<tr>
<td>18</td>
<td>10/2020</td>
<td>SR 2.5.4 Production Release</td>
</tr>
<tr>
<td>17</td>
<td>08/2020</td>
<td>SR 2.5.2.2 Production Release with Firmware 3.00</td>
</tr>
<tr>
<td>16</td>
<td>02/2020</td>
<td>Update for SR 2.5.2</td>
</tr>
<tr>
<td>15</td>
<td>10/2019</td>
<td>Update for SR 2.5</td>
</tr>
<tr>
<td>14</td>
<td>08/2019</td>
<td>Update for SR 2.4.8 Release</td>
</tr>
<tr>
<td>13</td>
<td>03/2019</td>
<td>Update for SR 2.4.4 Release</td>
</tr>
<tr>
<td>12</td>
<td>01/2019</td>
<td>SR2.4 Production Release</td>
</tr>
<tr>
<td>11</td>
<td>10/2018</td>
<td>SR2.3 firmware update with Cavium/ARM support and Ubuntu driver.</td>
</tr>
<tr>
<td>10</td>
<td>06/2018</td>
<td>SR2.3 Production Release</td>
</tr>
<tr>
<td>8</td>
<td>10/2017</td>
<td>Update supported OSs</td>
</tr>
<tr>
<td>8</td>
<td>10/2017</td>
<td>First Production Release</td>
</tr>
<tr>
<td>1-7</td>
<td>10/2016 to 07/2017</td>
<td>Pre-Production Release.</td>
</tr>
</tbody>
</table>
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.
Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.
<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>ASIA/PACIFIC</th>
<th>ASIA/PACIFIC</th>
<th>EUROPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Office</td>
<td>2355 West Chandler Blvd. Chandler, AZ 85224-6199</td>
<td>Tel: 61-2-9868-6733</td>
<td>Tel: 43-7242-2244-39</td>
</tr>
<tr>
<td>Chandler, AZ</td>
<td>China - Beijing</td>
<td>Tel: 86-10-8569-7000</td>
<td>Fax: 43-7242-2244-393</td>
</tr>
<tr>
<td>Tel: 480-792-7200</td>
<td>China - Chengdu</td>
<td>Tel: 86-28-8665-5511</td>
<td>Denmark - Copenhagen</td>
</tr>
<tr>
<td>Fax: 480-792-7277</td>
<td>China - Chongqing</td>
<td>Tel: 86-23-8980-9588</td>
<td>Tel: 45-4485-5910</td>
</tr>
<tr>
<td>Technical Support:</td>
<td>China - Dongguan</td>
<td>Tel: 86-769-8702-9880</td>
<td>Fax: 45-4485-2829</td>
</tr>
<tr>
<td><a href="http://www.microchip.com/support">www.microchip.com/support</a></td>
<td>China - Guangzhou</td>
<td>Tel: 86-20-8755-8029</td>
<td>Finland - Espoo</td>
</tr>
<tr>
<td>Web Address:</td>
<td>China - Hangzhou</td>
<td>Tel: 86-671-8792-8115</td>
<td>Tel: 358-9-4520-820</td>
</tr>
<tr>
<td><a href="http://www.microchip.com">www.microchip.com</a></td>
<td>China - Hong Kong SAR</td>
<td>Tel: 852-2943-5100</td>
<td>France - Paris</td>
</tr>
<tr>
<td></td>
<td>China - Nanjing</td>
<td>Tel: 86-25-8473-2460</td>
<td>Tel: 33-1-69-53-63-20</td>
</tr>
<tr>
<td></td>
<td>China - Qingdao</td>
<td>Tel: 86-532-8502-7355</td>
<td>Fax: 33-1-69-30-90-79</td>
</tr>
<tr>
<td></td>
<td>China - Shanghai</td>
<td>Tel: 86-21-3326-8000</td>
<td>Germany - Garching</td>
</tr>
<tr>
<td></td>
<td>China - Shenyang</td>
<td>Tel: 86-24-2334-2829</td>
<td>Tel: 49-8931-9700</td>
</tr>
<tr>
<td></td>
<td>China - Shenzhen</td>
<td>Tel: 86-755-8864-2200</td>
<td>Germany - Haan</td>
</tr>
<tr>
<td></td>
<td>China - Suzhou</td>
<td>Tel: 86-186-6233-1526</td>
<td>Tel: 49-2129-3766400</td>
</tr>
<tr>
<td></td>
<td>China - Wuhan</td>
<td>Tel: 86-27-5980-5300</td>
<td>Germany - Heilbronn</td>
</tr>
<tr>
<td></td>
<td>China - Xian</td>
<td>Tel: 86-29-8833-7252</td>
<td>Tel: 49-7131-72400</td>
</tr>
<tr>
<td></td>
<td>China - Xi'an</td>
<td>Tel: 86-592-2388138</td>
<td>Germany - Karlsruhe</td>
</tr>
<tr>
<td></td>
<td>China - Zhumai</td>
<td>Tel: 86-756-3210040</td>
<td>Tel: 49-721-625370</td>
</tr>
<tr>
<td></td>
<td>China - Zhuhai</td>
<td>Tel: 86-755-8864-2200</td>
<td>Germany - Munich</td>
</tr>
<tr>
<td></td>
<td>Tel: 43-7242-2244-39</td>
<td>Tel: 86-25-8473-2460</td>
<td>Tel: 49-89-627-142-4</td>
</tr>
<tr>
<td></td>
<td>Fax: 43-7242-2244-393</td>
<td>Tel: 86-532-8502-7355</td>
<td>Fax: 49-89-627-142-44</td>
</tr>
<tr>
<td></td>
<td>Tel: 45-4485-5910</td>
<td>Tel: 86-755-8864-2200</td>
<td>Germany - Rosenheim</td>
</tr>
<tr>
<td></td>
<td>Fax: 45-4485-2829</td>
<td>Tel: 86-20-3-577-8366</td>
<td>Tel: 49-8031-354-560</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-21-3326-8000</td>
<td>Tel: 86-7-213-7830</td>
<td>Israel - Ra’anana</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-24-2334-2829</td>
<td>Tel: 86-2-694-1351</td>
<td>Tel: 972-9-744-7705</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-755-8864-2200</td>
<td>Tel: 84-28-5448-2100</td>
<td>Italy - Milan</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-186-6233-1526</td>
<td>Tel: 39-0331-742611</td>
<td>Tel: 39-0331-466781</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-27-5980-5300</td>
<td>Tel: 972-9-744-7705</td>
<td>Italy - Padova</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-29-8833-7252</td>
<td>Tel: 39-049-7625286</td>
<td>Netherlands - Drunen</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-592-2388138</td>
<td>Tel: 31-416-690399</td>
<td>Fax: 31-416-690340</td>
</tr>
<tr>
<td></td>
<td>Tel: 86-756-3210040</td>
<td>Tel: 44-118-921-5800</td>
<td>Norway - Trondheim</td>
</tr>
<tr>
<td></td>
<td>Tel: 49-8031-354-560</td>
<td>Tel: 44-118-921-5800</td>
<td>Tel: 47-72864388</td>
</tr>
<tr>
<td></td>
<td>Tel: 39-0331-742611</td>
<td>Tel: 44-118-921-5800</td>
<td>Poland - Warsaw</td>
</tr>
<tr>
<td></td>
<td>Tel: 972-9-744-7705</td>
<td>Tel: 44-118-921-5800</td>
<td>Romania - Bucharest</td>
</tr>
<tr>
<td></td>
<td>Tel: 39-0331-466781</td>
<td>Tel: 40-21-407-87-50</td>
<td>Spain - Madrid</td>
</tr>
<tr>
<td></td>
<td>Tel: 972-9-744-7705</td>
<td>Tel: 34-91-708-08-90</td>
<td>Fax: 34-91-708-08-91</td>
</tr>
<tr>
<td></td>
<td>Tel: 39-0331-742611</td>
<td>Tel: 46-31-704-60-40</td>
<td>Sweden - Gothenberg</td>
</tr>
<tr>
<td></td>
<td>Tel: 972-9-744-7705</td>
<td>Tel: 46-8-5090-4654</td>
<td>Tel: 46-31-704-60-40</td>
</tr>
<tr>
<td></td>
<td>Tel: 39-0331-466781</td>
<td>Tel: 46-8-5090-4654</td>
<td>Sweden - Stockholm</td>
</tr>
<tr>
<td></td>
<td>Tel: 972-9-744-7705</td>
<td>Tel: 46-8-5090-4654</td>
<td>UK - Wokingham</td>
</tr>
<tr>
<td></td>
<td>Tel: 44-118-921-5800</td>
<td>Tel: 44-118-921-5800</td>
<td>Tel: 44-118-921-5800</td>
</tr>
<tr>
<td></td>
<td>Fax: 44-118-921-5820</td>
<td>Fax: 44-118-921-5820</td>
<td>Fax: 44-118-921-5820</td>
</tr>
</tbody>
</table>