# 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.................................................................................................................................. 19

3. Updating the Controller Firmware......................................................................................................... 24
   3.1. Updating the Controller Firmware.............................................................................................. 24

4. Installing the Drivers.............................................................................................................................. 25

5. Revision History.................................................................................................................................... 26

Microchip Information................................................................................................................................... 27
   The Microchip Website.......................................................................................................................... 27
   Product Change Notification Service.................................................................................................... 27
   Customer Support.................................................................................................................................... 27
   Microchip Devices Code Protection Feature......................................................................................... 27
   Legal Notice.......................................................................................................................................... 27
   Trademarks........................................................................................................................................... 28
   Quality Management System................................................................................................................ 29
   Worldwide Sales and Service................................................................................................................ 30
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><strong>Solutions Release</strong></td>
</tr>
<tr>
<td><strong>Package Release Date</strong></td>
</tr>
<tr>
<td><strong>Firmware Version</strong></td>
</tr>
<tr>
<td><strong>UEFI Version</strong></td>
</tr>
<tr>
<td><strong>Legacy BIOS</strong></td>
</tr>
<tr>
<td><strong>Driver Versions</strong></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><strong>Management Software</strong></td>
</tr>
<tr>
<td>(arcconf, maxView™, Event Monitor, BootUSB)</td>
</tr>
<tr>
<td><strong>PLDM</strong></td>
</tr>
</tbody>
</table>

**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 SmartHBA 2100/SmartRAID 3100 controller and SmartRAID 3100 and SmartRAID 3100 controller solutions 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>
<tr>
<td>SmartFWx100.fup</td>
<td>Programmable NOR Flash File Used for PLDM type 5 firmware flashing 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 1-7</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 1-7</td>
</tr>
</tbody>
</table>

**Driver Files**

**Table 1-4. Windows Storport Miniport SmartPQI Drivers**

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Binary</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2022, Server 2019 and Server 2016</td>
<td>SmartPqi.sys</td>
<td>x64</td>
</tr>
<tr>
<td>Windows 10 (version 21H2) and 11</td>
<td>SmartPqi.inf</td>
<td>x64</td>
</tr>
<tr>
<td></td>
<td>Smartpqi.cat</td>
<td>x64</td>
</tr>
</tbody>
</table>
### Table 1-5. Linux SmartPQI Drivers

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 9.1&lt;sup&gt;1&lt;/sup&gt;, 9.0&lt;sup&gt;2&lt;/sup&gt;, 8.7&lt;sup&gt;1&lt;/sup&gt;, 8.6, 8.5, 8.4, 7.9, 7.8</td>
<td>x64</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 12, SP5, SP4</td>
<td>x64</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 15 SP4, SP3, SP2</td>
<td>x64</td>
</tr>
<tr>
<td>Oracle Linux 7.9 UEK6U3</td>
<td>x64</td>
</tr>
<tr>
<td>Oracle Linux 9.0, 8.6 UEK7</td>
<td>x64</td>
</tr>
<tr>
<td>Ubuntu 22.04.1, 22.04, 21.04</td>
<td>x64</td>
</tr>
<tr>
<td>Ubuntu 20.04.5, 20.04.4, 20.04</td>
<td>x64</td>
</tr>
<tr>
<td>Ubuntu 18.04.5, 18.04.4, 18.04</td>
<td>x64</td>
</tr>
<tr>
<td>Ubuntu 16.04.5</td>
<td>x64</td>
</tr>
<tr>
<td>Debian 11.4, 10.12, 10.10</td>
<td>x64</td>
</tr>
<tr>
<td>Citrix xenServer 8.2.1, 8.1, 8.0</td>
<td>x64</td>
</tr>
<tr>
<td>Fedora 36 (inbox only)</td>
<td>x64</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeBSD 13.1, 12.3</td>
<td>x64</td>
</tr>
<tr>
<td>Solaris 11.4</td>
<td>x64</td>
</tr>
<tr>
<td>VMware 8.0, 7.0 U3/U2/U1</td>
<td>x64</td>
</tr>
</tbody>
</table>

### Host Management Software

#### Table 1-7. 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, Linux x64,</td>
<td>See the Arcconf download package for the OS-applicable</td>
</tr>
<tr>
<td></td>
<td>VMware 7.0 and above,</td>
<td>installation executable.</td>
</tr>
<tr>
<td></td>
<td>XenServer, FreeBSD x64,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris x86</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>Description</td>
<td>OS</td>
<td>Executable</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</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>VMware 7.0 and above</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linux x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XenServer</td>
<td></td>
</tr>
<tr>
<td>maxView™ vSphere Plugin</td>
<td>VMware 7.0 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.

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**

<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>Windows</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>VMware</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FreeBSD</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Solaris</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>OS certification</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>X</td>
<td></td>
</tr>
<tr>
<td>MCTP BMC Management</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SED Local Key Management</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configurable Big Block Cache Bypass</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Green Backup Support for SmartRAID</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4Kn Support in RAID</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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:
What's New?

- Added support for Managed SED adapter password.
- Added support for reporting consistency check metrics for host management tools.
- Added support for a new persistent event log policy that overwrites old events with the most recently occurred events.
- Fixed a performance drop issue on RAID 5 logical drives with 50/50 cache ratio on a 256K sequential read workload.
  - Root Cause: The performance impact for higher block sizes are due to read-ahead and caching. The problem occurs when there is a full cache-hit condition. For a full cache hit condition, the firmware is doing 512K of read-ahead. This helps for small block size requests, but not for large block size requests. Therefore, doing a smaller amount of read-ahead or no read-ahead helps large block requests.
  - Fix: Fixed by adjusting the read-ahead size based on the host request size. For host request size of 64K and smaller, the read-ahead size is 512K. For request size larger than 64K, the read-ahead size is 32K.
  - Risk: Low
- Fixed a parity inconsistency after RAID rebuild restarted with a new drive replacement.
  - Root Cause: Every 10 minutes during the rebuild process or when a graceful system shutdown occurs, firmware will save the rebuild progress information to RAID metadata. If a rebuilding drive is replaced with a new drive, the firmware will restart the rebuild from the beginning of the drive. If the system has an ungraceful shutdown within the first 10 minutes of restarting the rebuild, the rebuild will continue from the previously saved rebuild progress information in RAID metadata and run to completion, which will result in skipped blocks during the rebuild leaving incorrect data or parity in the rebuilt drive. When consistency check runs, it detects inconsistent parity on the skipped blocks and fixes them. The file system or the application can end up reading the incorrect data from those skipped blocks.
  - Fix: Firmware saves the Rebuild Progress Information in RAID metadata at the start of a rebuild.
  - Risk: Low
- Fixed an issue where incorrect drive location is listed in the POST message 1942, which list all the missing members per logical drive and their locations.
  - Root Cause: Upon Power On, a SGPIO backplane is dynamically configured. Therefore, the firmware maps each signal group's box index and bay in box based on the data-in bit stream. Only if there is a drive attached, then the firmware will set up the box index and bay in box of the corresponding drive structure.
  - Fix: When parsing the data, check for the "bay config" bit of each slot. If "bay config" bit is set, then set the box index and bay in box of the corresponding structure.
  - Risk: Low
- Fixed a lockup issue when importing a mixed type foreign replacement SED.
  - Root Cause: When a foreign SED is added as a replacement drive, firmware does not check the drive type. If the replacement SED is not the correct type, firmware does not fail it immediately, which causes errors when firmware tries to write RAID metadata. When a foreign replacement SED with RAID metadata is imported, a race condition occurs where RAID metadata is written to the drive before the drive is checked for RAID metadata, which results in a lockup.
  - Fix: When the mix type foreign replacement SED is detected, firmware will fail it.
  - Risk: Low
- Fixed an issue that foreign secured logical drive is exposed to the OS when controller does not have Managed SED enabled.
  - Root Cause: While checking if a logical drive must be in Locked state, firmware did not check if Managed SED is enabled or not.
  - Fix: Add a check for Managed SED enabled or not before returning state of a secured logical drive.
  - Risk: Low
- Fixed an issue where ownership of a replacement drive is taken when Managed SED is not enabled.
  - Root Cause: In a case where firmware tries to recover a RAID secured logical drive from a residual RAID physical disk, but Managed SED is disabled, firmware still tries to add RAID metadata to the drive and take ownership because it did not check if Managed SED is enabled or not before performing those operations.
Fix: Add a check for Managed SED enabled or not before taking ownership of SEDs for RAID physical drive members.
Risk: Low

Fixed an issue that Microchip owned SED can be a replacement for a non-secured logical drive.

Root Cause: When a Microchip owned SED is added as a replacement drive, it must fail SED Qualification, but current firmware does not fail it. Later, when Managed SED is enabled with the right master key, the Microchip owned SED is unlocked successfully, and becomes a normal replacement drive for the non-secured logical drive.
Fix: Firmware fails the Microchip owned SED when it is added as the replacement of a non-secured logical drive because it cannot pass the SED Qualification.
Risk: Low

Fixed an issue where SEDs in a Managed SED secured logical drive are allowed to revert to Original Factory State (OFS) using PSID/MPIN.

Root Cause: Firmware incorrectly allows PSID/MPIN operations to return SEDs to the Original Factory State when SEDs are part of a Managed SED secured logical drive. This can lead to some unexpected behaviors/errrors when accessing the Managed SED secured logical drive after the SEDs are reverted.
Fix: Firmware disallows SEDs in a Managed SED secured logical drive to be reverted to OFS using PSID/MPIN.
Risk: Low

Fixed a potential data loss scenario caused by downgrading from firmware that supports Managed SED to firmware that does not support Managed SED.

Root Cause: Logical drives secured using Managed SED capabilities can be susceptible to a potential data loss if the firmware on the controller is downgraded to release 5.00 or earlier because those releases do not support Managed SED capabilities. If a warm reboot occurs after a firmware downgrade, the SED drives might be left unlocked which will allow modification of the existing logical drive configuration or data. Any time a cold reboot occurs, it locks SEDs and the data on the logical drive or HBA drive becomes inaccessible.
Fix: If Local Key Management is enabled, added additional checks to block firmware downgrade from firmware supporting Managed SED to firmware not supporting Managed SED. If downgrading to firmware release 5.00 or earlier, managed SED must be disabled.
Risk: Low

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 when panic shutdown occurs while delete logical drive or clear configuration is in progress causing drive failures on next reboot.

Root Cause: When a panic shutdown occurs while delete logical drive or clear configuration is occurring, on reboot the deleted logical drive reappears and some drives are failed with various failure reason codes. When RAID metadata is cleared on the drive, it also deletes the RAID metadata range and then restores the ownership. This process can take several seconds per drive. When a panic shutdown occurs, some drives are left with RAID metadata cleared and some with RAID metadata along with RAID metadata band and ownership not removed. On next boot, this creates various behaviors on start-up like previous logical drive reappears because there is at least one drive that has valid RAID metadata and few drives in failed states.
Fix: When RAID metadata is cleared on the drive, do not delete RAID metadata locking range and restore to OFS. Let the clear RAID metadata complete on all the drives and then delete RAID metadata locking range and restore to OFS for those drives (done by all the callers of clear RAID metadata). This way RAID metadata is cleared on the drives before Managed SED related activities (delete RAID metadata locking range and revert the master key) occurs which takes a few seconds per drive.
Risk: Low
What's New?

- 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 firmware allows the non-secured maxCache logical drive to be associated with the secured primary logical drive.
  - Root Cause: When firmware is associating a maxCache logical drive to its primary logical drive, firmware does not check if both logical drives have the same security type.
  - Fix: Added a logical drive security check so that firmware only associates a maxCache logical drive to a primary logical drive if the security type is the same.
  - 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 OS possibly places logical drives containing multiple predictive failed physical drives offline.
  - Root Cause: When a logical drive has multiple predictive failed drives, firmware disables the predictive failed drive avoidance policy. This can cause I/O latency issues. After all but one of the predictive drives are replaced and the logical drive rebuilds completed, the I/O latency issue may remain and result in the OS marking the logical drive offline.
  - Fix: Ensure updating the predictive failed drive avoidance policy status after every logical drive state update.
  - Risk: Low

- Fixed controller lockup during clear configuration after maxCache logical drive is moved from SmartRAID to SmartHBA controller.
  - Root Cause: When a maxCache logical drive is moved from the SmartRAID controller to the SmartHBA controller, the maxCache logical drive state changes to UNSUPPORTED, as maxCache is not supported by the SmartHBA controller. When the clear controller configuration operation is issued, the firmware tries to clear the maxCache resources information and results in a controller lockup.
  - Fix: The firmware checks the cache configuration status before clearing respective resources.
  - 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 a transforming logical drive fails when the controller is abruptly rebooted after logical drive deletion.

  - Root Cause: If an array has multiple logical drives and if the host deletes any logical drive that is not the last in the array, then transformation is queued for all the logical drives physically located after the deleted logical drive. Each transformation request suspends the current transformation, updates the RAID metadata, saves it in logical drives, and update the transformation progress status. So when one such transformation request is received from the host, the firmware suspended the transformation and then updates saved the RAID metadata into logical drives, and before updating the transformation progress status, the system is abruptly rebooted. This causes the logical drives' metadata and transformation progress status to be out of sync. Due to this reason, the logical drive moves to a FAILED state.
  - Fix: Add an extra variable in the RAID metadata to store the current transformation progress information and use it to invalidate the transformation progress data due to an abrupt reboot.
  - Risk: Medium

• Fixed an issue where the RAID metadata is present after clear configuration and a reboot.

  - Root Cause: When predictive spare rebuild is completed on a logical drive, firmware fails the predictive failed drive. But firmware did not clear the RAID metadata present in the failed drive during clear configuration. During the next boot, the firmware found valid RAID metadata in the predictive failed drive and loads the RAID metadata causing the logical drive to come up again.
  - Fix: Firmware will spin up the failed drive during clear configuration and clear the RAID metadata.
  - 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 controller moved to an Abnormal Volume State mode after a graceful reboot with SED logical drives.

  - Root Cause: When an internal-cache-based transformation is in-progress on the SED logical drive, the controller went through a graceful reboot. On the next boot, the SED logical drive is in the LOCKED state, and transformation is not resumed on it. But internal cache for transformation is allocated and firmware treats this memory as a dirty cache after a graceful reboot and moves the controller to Abnormal Volume State mode.
  - Fix: Do not resume the transformation or allocate any resources for transformation on SED-locked logical drives.
  - Risk: Low

• Fixed an issue where the maxCache data was lost during a graceful reboot with SED logical drives.

  - Root Cause: The firmware tried reading the data from maxCache during the boot and this operation fails, as SED logical drive is in the LOCKED state. When the data read operation on maxCache fails, the firmware will reset maxCache configuration and update the host about the maxCache data loss.
  - Fix: Avoid reading/writing the data from/to maxCache when the SED logical drive is in the LOCKED state.
What's New?

- Risk: Low
- Fixed an issue where the controller locked up while resuming transformation after a cold boot.
  - Root Cause: If a transformation running with the internal-cache method was interrupted due to abrupt power loss, and the backup power source is removed on the next boot, the transformation method switches from the internal-cache to a disk-based method. The firmware copies the data from the internal cache to disk and during this process an uninitialized variable was used that triggered a firmware lockup.
  - Fix: Firmware will initialize the variable before utilizing it.
  - Risk: Low
- Fixed an issue where the logical drive failed during the heal array transformation.
  - Root Cause: When firmware receives heal array operation on a logical drive with an active spare, the transformation begins. During this transformation, if a previously failed disk is replaced, firmware incorrectly releases the active spare before completing the transformation and moves the logical drive to FAILED state.
  - Fix: Avoid releasing an active spare disk during the heal array transformation. After the transformation is completed, it gets released to the respective spare pool.
  - Risk: Medium
- Fixed an issue where rebuild does not start on an array with the spare disk.
  - Root Cause: When firmware receives heal array operation on a logical drive with an active spare, the transformation begins. Once the transformation is completed, firmware failed to release the active spare from the old configuration. Due to this, the spare disk is in a Used state, and firmware is unable to utilize this spare disk for rebuild operation on the new configuration.
  - Fix: When a transformation is completed, firmware must release the spare disks associated with the old configuration.
  - Risk: Medium
- 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
- Fixed a possible lockup that could happen during bootup on a logical drive that was undergoing transformation and reboot happens during transformation, and then a drive fails while battery/super capacitor finishes charging.
  - Root Cause: Logical drive gets into Abnormal state. As part of this process, a call was made to restart transformation, but another thread process had marked transformation already running, so this resulted in lockup.
  - Fix: Made fix to suspend transformation when putting logical drive into Abnormal state.
  - 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

• Fixed an issue where creating RAID 60 on 24 SATA SSDs resulted in controller lockup.
  – Root Cause: A system with 24 SATA SSDs running Rapid Parity Initialization (RPI) may encounter a 0x1ABD lockup due to firmware processing the RPI IOs and not processing completions for other IOs in a timely manner. The unprocessed completions can then cause firmware to encounter I/O timeouts and may trigger a 0x1ABD lockup.
  – Fix: Firmware will process I/O completions in a timely manner to avoid the I/O timeouts and 0x1ABD lockup.
  – Risk: Medium

2.2.2 UEFI Fixes

Note: Microsoft signed and secure boot is supported.

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

This release includes the following UEFI fixes and enhancements:

• Added an HII option to configure Persistent Event Log Policy.
• Added an HII field to show Consistency Check status for each logical drive.
• Fixed an issue where system freezes when 64 failed logical drive are present.
  – Root Cause: While framing driver health message with error code 0x1946, the length of message copied is more than the allocated amount causing the system to access invalid memory.
  – Fix: Allocate and copy the message as per the content of dynamic message.
  – Risk: Low
• Fixed an issue driver health message with error code 0x1943 is not shown when expected.
  – Root Cause: Controller reporting unsupported status is not considered when encrypted devices are connected to an unsupported controller.
  – Fix: Trigger 0x1943 error message when controller reports unsupported configuration.
  – Risk: Low
• Fixed an issue where OS on a logical drive does not boot when an intermediate logical drive within the array is deleted.
  – Root Cause: Block I/O calls fail due to incorrect internal indexing to route the I/O when logical drive numbering is not linear.
  – Fix: Corrected logical drive indexing to consider the actual logical drive number.
  – Risk: Low
• Fixed an issue where no logical drive information is shown when Managed SED controller password is set.
  – Root Cause: Software blocks any editable configuration APIs when controller password is enabled.
  – Fix: Change to direct APIs instead of editable configuration APIs for populating logical drive information.
  – Risk: Low
• 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 information 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.
What's New?

- 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 where "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 an issue 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.

```plaintext
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.
What's New?

- 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
This release includes the following enhancements and fixes:
- Fixed an issue of PSOD when deleting logical drive.
  - Root Cause: Driver maintains a linked list of removed devices protected by a lock. A timer function iterates through the list and frees those devices whose timeout has expired. In the timer function, the lock is released for a short interval to notify the OS about device removal and acquired back. During this time, the device that was in removal stage came back. Consequently, the driver removes this entry from the list. The timer function was trying to free this entry from list which was already freed.
  - Fix: Check for the device removal state before freeing the device entry.
  - Risk: Low

- Fixed an issue where firmware lockup was observed.
  - Root Cause: For a RAID logical drive with IOBypass enabled, the driver frames CDB based on the SCSI command. This may result in translating a SCSI READ(16) to a READ(10) based on the LBA and transfer size and set the command length to 10 bytes. If the IOBypass I/O fails, the driver will retry the same command via RAID path. The driver was supposed to use the original CDB sent by the OS SCSI layer, but the driver does not reset the command length back to the original command length of 16 bytes. This may result in a partial copy of the SCSI CDB with incorrect CDB transfer length. Firmware frames the SGL based on CDB transfer length that results in SGLs that do not match with the data transfer size, and that triggers a firmware lockup.
  - Fix: Reset the SCSI command length when retrying a IOBypass I/O down the RAID path.
  - Risk: Medium

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 output 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 support in maxView and arcconf to configure remote Key Management Server (KMS) based CBE (Controller Based Encryption).
• Added properties in maxView and arcconf to display the logical device consistency check runtime metrics.
• 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.
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 the VolumeCapabilities resource will now include the annotation Name@Redfish.OptionalOnCreate. Additionally, the Redfish GET response for a Volume resource shows both the DisplayName and Name properties published with the same value, that is, the volume label. Either of DisplayName or Name can be used to set a volume label at create time using Redfish POST or modify the label using Redfish PATCH.**

- **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.**

- **Sending a Redfish PATCH request to update the WriteCacheEnabled property of a Drive resource is now supported for drives configured as a Volume’s data drive.**

- **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 Redfish PATCH to set Volume.IOPerfModeEnabled to true silently disabled caching for other volumes on the same array.**
  - **Root Cause:** The code was combining the check for other volume cache policies with another check that could cause a different error. This caused the check to let the requests through.
  - **Fix:** Made the two checks independent of each other and now fail such calls with the appropriate error information.
  - **Risk:** Low

- **Fixed an issue where not all permitted values were published for the VolumeCapabilities WriteCachePolicy@Redfish.AllowableValues.**
  - **Root Cause:** The condition for publishing allowable WriteCachePolicy values was not accounting for cases where controller caching is supported but not configured.
  - **Fix:** Added a check for the controller cache not being configured when determining the WriteCachePolicy@Redfish.AllowableValues values to publish.
  - **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 VolumeCapabilities resource can be published with incorrect values for WriteCachePolicy@Redfish.AllowableValues when the controller's battery is charging.
  – Root Cause: In cases where the backup power source is charging, the cache goes into a temporarily degraded state. In such case, the VolumeCapabilities READ response uses the logic intended for unconfigured cache to determine the WriteCachePolicy allowable values.
  – Fix: Modified the VolumeCapabilities READ response generation code to determine the allowable values for WriteCachePolicy using configured cache rules when the cache is temporarily disabled.
  – 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 the StorageController's CacheSummary.Status property is published with a value of StandbyOffline instead of UnavailableOffline when the backup power source cable is not connected to the controller at boot.
  – Root Cause: No specific check for a missing backup power source was included when determining the StorageController's CacheSummary property values.
  – Fix: Modified the StorageController RDE GET handler to publish CacheSummary.Status with a value of UnavailableOffline in the cited case.
  – Risk: Low

• Fixed an issue where the StorageController's Status.Health property is published with a value of Warning instead of OK when the backup power source cable is not connected to the controller at boot.
  – Root cause: No specific check for a missing backup power source was included when determining the StorageController's Status.Health property values.
  – Fix: Modified the StorageController RDE GET handler to publish Status.Health with a value of Ok in the cited case.
  – 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 a Volume create request is erroneously accepted when the request payload contains a WriteCachePolicy value conflicting with the existing cache configuration.
  – Root Cause: Volume create request payload validation was missing a check for requests for active write caching when the controller’s cache ratio setting was set to 100% reads.
  – Fix: Added a validation check to reject such requests with a messageId of PropertyValueIncorrect.
  – Risk: Low
• 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
• Fixed an issue where the BatteryCharging alert was sent with an incorrect severity on certain controllers.
  – Root Cause: The BatteryCharging alert was hard-coded to only be sent with a Severity of Warning.
  – Fix: Modified the BatteryCharging event logic to send a Severity of OK for certain controllers.
  – 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.
• Converting a non-secured logical drive to Managed SED secured logical drive is not supported in this release. Attempting to perform the conversion will fail in the application with an error message, “An unknown error occurred during the operation.”
  – Workaround: None
• 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.

• If panic shutdown or power loss occurs while creating secure volume, depending on when the create process is interrupted, user might or might not see the new volume being created on reboot. If volume is not created successfully, then new volume needs to be deleted. If there is any SED left in the otherwise owned state, user will have to revert the drive to original factory state (OFS) using PSID manually.
  – Workaround: If the volume is not created successfully, delete the new volume after reboot and SEDs in otherwise owned state can be reverted to OFS using PSID.

• If panic shutdown or power loss occurs while a secure volume is undergoing transformation, depending on when the transformation process is interrupted, user might or might not see the new volume being created. If volume is not created successfully then new volume needs to be deleted and If there is any SED that is in the otherwise owned state, user will have to revert the drive to original factory state (OFS) using PSID manually.
  – Workaround: If the volume is not created successfully, delete the new volume after reboot and SEDs in otherwise owned state can be reverted to OFS using PSID.

• 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.

• Deleting a secure SED logical drive using firmware that does not support the SED Local Key Management (LKM) feature can cause the physical drive status to be incorrect when moved back to firmware that supports SED Local Key Management.
  – Workaround: Delete the secure SED logical drive prior to downgrading to firmware 5.00 or earlier.

• 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.

• Controller cache will not be converted into 100% read cache, if any backup power source cable error, charge or charge timeout error occurs when expansion or transformation task is active.
  – Workaround: None

• Firmware downgrade is blocked if disk-based transformation is in-progress.
  – Workaround: Wait for the transformation to complete and retry the firmware downgrade.

• Transformation is blocked if,
  • Reboot after the firmware update is pending.
  • Flashed new firmware version is older than 5.32 B0.
    – Workaround: Reboot the system.

• Logical drive is not detected if,
  • Disk-based transformation is in-progress during logical drive movement to a different controller and the different controller has a firmware version older than 5.32 B0.
  • Firmware downgrade occurred while internal-cache based transformation was in progress, but the Backup Power Source failed before firmware activation.
  – Workaround: Move the logical drive to a controller with firmware version 5.32 B0 or later.

• PBSI shows dedicated hotspare type when auto replace hotspare is configured.
What's New?

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".

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 RHEL 7.9/8.2/8.3 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 initiate 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:

• The Windows driver issues an internal flush cache command for flushing the controller cache to the drives before changing the power state of the system (during shutdown/reboot/hibernate). Due to many factors, example of speed of drives, size of cache, type of data in cache, and so on. The time taken by the controller to flush the cached data can exceed the operating system specified timeout values. A system crash can be expected in those scenarios. In general, it is advised not to do heavy write operations on logical drives composed of slow drives while initiating a system shutdown in Windows 10 environments.

• 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.
    – Workaround: 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

• If the controller SED Encryption feature is “On” and locked, Datastores created from secured logical drives on the controller are not automatically mounted even after unlocking the controller, they are not visible through the ESXi hypervisor client.
• Workaround: Use the command `vmkfstool -V` or `esxcli storage filesystem rescan`. Alternatively, you can also use the `Rescan` option from the `Devices` tab in the Hypervisor’s Storage section. Any of these options solve the issue by forcing a rescan, causing the datastore to mount.

2.3.5 Management Software Limitations

2.3.5.1 Limitations for ArcconfimaxView 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

This release includes the following PLDM limitations:

- **Action** `Storage.ResetToDefault` with a ResetType of ‘ResetAll’ is not supported when the controller has logical drives that are encrypted.
  - Workaround: None

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 SmartRAID 3100 and SmartHBA 2100 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.

Notes:
1. If the running firmware is older than 1.98 and a transformation is in progress, complete the transformation before proceeding with the following steps to upgrade the firmware.
2. 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 Adaptec controller 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® SmartRAID 3100 Series and SmartHBA 2100 Series Host Bus Adapters Installation and User's Guide (DS00004439C, previously ESC-2171547)" 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>F</td>
<td>11/2022</td>
<td>SR 2.7.2 Production Release</td>
</tr>
<tr>
<td>E</td>
<td>08/2022</td>
<td>SR 2.7.0 Production Release</td>
</tr>
<tr>
<td>D</td>
<td>03/2022</td>
<td>VMware driver version updated from 4250.0.120 to 4252.0.103</td>
</tr>
<tr>
<td>C</td>
<td>02/2022</td>
<td>SR 2.6.6 Production Release</td>
</tr>
<tr>
<td>B</td>
<td>12/2021</td>
<td>SR 2.6.4.1 Patch Release with maxView™ version B24713.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Fixes and Enhancements for maxView Storage Manager/ARCCONF section</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for log4j vulnerabilities.</td>
</tr>
<tr>
<td>A</td>
<td>11/2021</td>
<td>SR 2.6.4 Production Release with firmware version 4.72 B0 (Previously ESC-2161026)</td>
</tr>
<tr>
<td>29</td>
<td>04/2021</td>
<td>SR 2.6.2 with firmware version 4.11 B0</td>
</tr>
<tr>
<td>28</td>
<td>04/2021</td>
<td>SR 2.6.1.1 with VMware driver version 4054.2.118.</td>
</tr>
<tr>
<td>27</td>
<td>03/2021</td>
<td>SR 2.6.1 with VMware driver version 4054.1.103.</td>
</tr>
<tr>
<td>26</td>
<td>02/2021</td>
<td>SR 2.6 Production Release</td>
</tr>
<tr>
<td>25</td>
<td>10/2020</td>
<td>SR 2.5.4 Production Release</td>
</tr>
<tr>
<td>24</td>
<td>08/2020</td>
<td>SR 2.5.2.2 Production Release with Firmware 3.00</td>
</tr>
<tr>
<td>23</td>
<td>03/2020</td>
<td>SR 2.5.2 Production Release with Firmware 2.93</td>
</tr>
<tr>
<td>22</td>
<td>03/2020</td>
<td>SR 2.5 Production Release with Firmware 2.66</td>
</tr>
<tr>
<td>21</td>
<td>02/2020</td>
<td>SR 2.5.2 Production Release</td>
</tr>
<tr>
<td>20</td>
<td>10/2019</td>
<td>SR 2.5 Production Release</td>
</tr>
<tr>
<td>19</td>
<td>09/2019</td>
<td>Updated for SR 2.4.8.1 (fw v2.31 Build 0)</td>
</tr>
<tr>
<td>18</td>
<td>08/2019</td>
<td>Updated for SR 2.4.8</td>
</tr>
<tr>
<td>17</td>
<td>01/2019</td>
<td>SR2.4 Production Release</td>
</tr>
<tr>
<td>16</td>
<td>06/2018</td>
<td>SR2.3 Production Release</td>
</tr>
<tr>
<td>15</td>
<td>06/2018</td>
<td>Updated for RC Release</td>
</tr>
<tr>
<td>14</td>
<td>10/2017</td>
<td>Update supported OSs</td>
</tr>
<tr>
<td>13</td>
<td>10/2017</td>
<td>First Production Release</td>
</tr>
<tr>
<td>1-12</td>
<td>06/2016 to 07/2017</td>
<td>Pre-Production Release.</td>
</tr>
</tbody>
</table>
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, maxXtus, 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.


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 and its subsidiaries. All Rights Reserved.

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.
## Worldwide Sales and Service

<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>ASIA/PACIFIC</th>
<th>ASIA/PACIFIC</th>
<th>EUROPE</th>
</tr>
</thead>
</table>
| **Corporate Office**<br>2355 West Chandler Blvd.<br>Chandler, AZ 85224-6199<br>Tel: 480-792-7200<br>Fax: 480-792-7277<br>Technical Support: [www.microchip.com/support](http://www.microchip.com/support)<br>Web Address: [www.microchip.com](http://www.microchip.com)<br>**Atlanta**<br>Duluth, GA<br>Tel: 678-957-9614<br>Fax: 678-957-1455<br>**Austin, TX**<br>Tel: 512-257-3370<br>**Boston**<br>Westborough, MA<br>Tel: 774-760-0087<br>Fax: 774-760-0088<br>**Chicago**<br>Itasca, IL<br>Tel: 630-285-0071<br>Fax: 630-285-0075<br>**Dallas**<br>Addison, TX<br>Tel: 972-818-7423<br>Fax: 972-818-2924<br>**Detriot**<br>Novi, MI<br>Tel: 248-848-4000<br>**Houston, TX**<br>Tel: 281-894-5983<br>**Indianapolis**<br>Noblesville, IN<br>Tel: 317-773-8323<br>Fax: 317-773-5453<br>Tel: 317-536-2380<br>**Los Angeles**<br>Mission Viejo, CA<br>Tel: 949-462-9523<br>Fax: 949-462-9608<br>Tel: 951-273-7800<br>**Raleigh, NC**<br>Tel: 919-844-7510<br>**New York, NY**<br>Tel: 631-435-6000<br>**San Jose, CA**<br>Tel: 408-735-9110<br>Tel: 408-436-4270<br>**Canada - Toronto**<br>Tel: 905-695-1980<br>Fax: 905-695-2078<br>| **Australia - Sydney**<br>Tel: 61-2-9868-6733<br>**China - Beijing**<br>Tel: 86-10-8569-7000<br>**China - Chengdu**<br>Tel: 86-28-8665-5511<br>**China - Chongqing**<br>Tel: 86-23-8980-9588<br>**China - Dongguan**<br>Tel: 86-769-8702-9880<br>**China - Guangzhou**<br>Tel: 86-20-8755-8029<br>**China - Hangzhou**<br>Tel: 86-571-8792-8115<br>**China - Hong Kong SAR**<br>Tel: 852-2943-5100<br>**China - Nanjing**<br>Tel: 86-25-8473-2460<br>**China - Qingdao**<br>Tel: 86-532-8502-7355<br>**China - Shanghai**<br>Tel: 86-21-3326-8000<br>**China - Shenyang**<br>Tel: 86-24-2334-2829<br>**China - Shenzhen**<br>Tel: 86-755-8864-2200<br>**China - Suzhou**<br>Tel: 86-186-6233-1526<br>**China - Wuhan**<br>Tel: 86-27-5980-5300<br>**China - Xian**<br>Tel: 86-29-8833-7252<br>**China - Xiamen**<br>Tel: 86-952-2388138<br>**China - Zhuhai**<br>Tel: 86-756-3210040<br>| **India - Bangalore**<br>Tel: 91-80-3090-4444<br>**India - New Delhi**<br>Tel: 91-11-4160-8631<br>**India - Pune**<br>Tel: 91-20-4121-0141<br>**Japan - Osaka**<br>Tel: 81-6-6152-7160<br>**Japan - Tokyo**<br>Tel: 81-3-6880-3770<br>**Korea - Daegu**<br>Tel: 82-53-744-4301<br>**Korea - Seoul**<br>Tel: 82-2-554-7200<br>**Malaysia - Kuala Lumpur**<br>Tel: 60-3-7651-7906<br>**Malaysia - Penang**<br>Tel: 60-4-227-8870<br>**Philippines - Manila**<br>Tel: 63-2-634-9065<br>**Singapore**<br>Tel: 65-6334-8870<br>**Taiwan - Hsin Chu**<br>Tel: 886-3-577-8366<br>**Taiwan - Kaohsiung**<br>Tel: 886-7-213-7830<br>**Taiwan - Taipei**<br>Tel: 886-2-2508-8600<br>**Thailand - Bangkok**<br>Tel: 66-2-694-1351<br>**Vietnam - Ho Chi Minh**<br>Tel: 84-28-5448-2100<br>| **Austria - Wels**<br>Tel: 43-7242-2244-39<br>Fax: 43-7242-2244-393<br>**Denmark - Copenhagen**<br>Tel: 45-4485-5910<br>Fax: 45-4485-2829<br>**Finland - Espoo**<br>Tel: 358-9-4520-820<br>**France - Paris**<br>Tel: 33-1-69-53-63-20<br>Fax: 33-1-69-30-90-79<br>**Germany - Garching**<br>Tel: 49-8931-9700<br>**Germany - Haan**<br>Tel: 49-2129-376400<br>**Germany - Heilbronn**<br>Tel: 49-7131-72400<br>**Germany - Karlsruhe**<br>Tel: 49-721-625370<br>**Germany - Munich**<br>Tel: 49-89-627-144-0<br>Fax: 49-89-627-144-44<br>**Germany - Rosenheim**<br>Tel: 49-8031-354-560<br>**Israel - Ra’anana**<br>Tel: 972-9-744-7705<br>**Italy - Milan**<br>Tel: 39-0331-742611<br>Fax: 39-0331-466781<br>**Italy - Padova**<br>Tel: 39-049-7625286<br>**Netherlands - Drunen**<br>Tel: 31-416-690399<br>Fax: 31-416-690340<br>**Norway - Trondheim**<br>Tel: 47-72864388<br>**Poland - Warsaw**<br>Tel: 48-22-3325737<br>**Romania - Bucharest**<br>Tel: 40-21-407-87-50<br>**Spain - Madrid**<br>Tel: 34-91-708-08-90<br>Fax: 34-91-708-08-91<br>**Sweden - Gothenberg**<br>Tel: 46-3-708-60-40<br>**Sweden - Stockholm**<br>Tel: 46-8-5090-4654<br>**UK - Wokingham**<br>Tel: 44-118-921-5800<br>Fax: 44-118-921-5820