SmartHBA 2100 and SmartRAID 3100 Software/Firmware Release Notes

Table of Contents

1. About This Release

The solution release described in this document includes firmware, OS drivers, tools, and host management software for the solutions from Microchip.

1.1 Release Identification

The firmware, software, and driver versions for this release are shown in the following table.

Table 1-1. Release Summary

Solutions Release	2.8.2
Package Release Date	November 07, 2023
Firmware Version	6.52[1, 2]
UEFI Driver Version	2.10.2
Legacy BIOS	2.10.2
Driver Versions	Windows SmartPQI: • Windows Server 2016/2019/2022: 1010.84.0.1012 • Windows 10/11: 1010.84.0.1012 Linux SmartPQI: • RHEL 7/8/9: 2.1.26-030 • SLES 12/15: 2.1.26-030 • Ubuntu 20/22: 2.1.26-030 • Debian 10/11/12: 2.1.26-030 • Oracle Linux 7/8/9: 2.1.26-030 • Citrix XenServer 8: 2.1.26-030 • BC Linux 7: 2.1.26-030 • OpenEuler 20/22: 2.1.26-030 VMware SmartPQI: • VMware 7.0/8.0: 4600.0.115 FreeBSD SmartPQI: • FreeBSD 12/13: 4460.0.1002
arcconf/maxView™	4.16.00.26273
PLDM	6.30.6.0

Notes:

1. Downgrading to 1.04 B0 or older builds from this release or prior 1.29 releases may cause the board to not boot or have supercap errors due to an incompatibility in SEEPROMs between this release and prior releases. See section “3. Updating the Controller Firmware”.
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 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

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

Table 1-3. Firmware Programming Tools

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

Driver Files

Table 1-4. Windows Storport Miniport SmartPQI Drivers

Drivers	Binary	Version
Server 2022, Server 2019 and Server 2016 Windows 10 and 11 (version 22H2)	SmartPqi.sys	x64
	SmartPqi.inf	x64
	smartpqi.cat	x64

Table 1-5. Linux SmartPQI Drivers for Arm

Drivers	Version
Red Hat Enterprise Linux 8.5, 8.4	Arm®
SuSE Linux Enterprise Server 12 SP5	Arm
SuSE Linux Enterprise Server 15 SP4, SP3, SP2	Arm
Ubuntu 22.04.3, 20.04.3	Arm
BC Linux 7.7	Arm
OpenEuler 20.03 SP3 LTS, 22.03 SP2 LTS	Arm

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

Drivers	Version
Red Hat Enterprise Linux 9.3[1], 9.2, 9.1, 9.0[2], 8.9[1], 8.8, 8.7, 8.6, 7.9	x86_64
SuSE Linux Enterprise Server 12, SP5	x86_64
SuSE Linux Enterprise Server 15 SP5, SP4, SP3	x86_64
Oracle Linux 7.9 UEK6U3	x86_64
Oracle Linux 9.2, 9.1, 8.8, 8.7 UEK7 U1	x86_64
Ubuntu 22.04.3, 22.04.2, 22.04	x86_64
Ubuntu 20.04.6, 20.04.5, 20.04	x86_64

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

Drivers	Version
Debian 12, 11.7, 10.13	x86_64
Citrix xenServer 8.2.1, 8.1	x86_64
Fedora 38 (inbox only)	x86_64
OpenEuler 20.03 SP3 LTS	x86_64
OpenEuler 22.03 SP2 LTS	x86_64

Notes:

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

Table 1-7. FreeBSD and VMware SmartPQI Drivers

Drivers	Version
FreeBSD 13.2, 12.4	x64
VMware 8.0 U2/U1, 7.0 U3/U2/U1	x64

Host Management Software

Table 1-8. Host Management Utilities

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

2. What's New?

This section shows what’s new in this release.

2.1 Features

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

Table 2-1. Feature Summary

Feature		Supported Release
Redfish Resource to Publish SuperCap Properties Support		2.8.2
Arcconf and Redfish Support in Secureboot ESXi Environment		2.8.2
Remote Key Management of Managed SED		2.8.0
Multi-Actuator Drive Support Enhancements		2.7.4
Managed SED Adapter Password Support		2.7.2
Managed SED Local Mode Support		2.7.0
Multi-Actuator Drive Support		2.7.0
Persistent Event Logging Support		2.6.2
Out of Band Interface Selection Support of MCTP or PBSI		2.5.2
MCTP BMC Management		2.4.8
SMR Drive Support	Enumeration, Unrestrected Command Flow-Through	2.3.0
	SATL Translation for HA/HM SMR Management	
	Identify all Drive Types	
Driver OS Certification Where Applicable		2.3.0
SNMP Management Software Support		2.3.0
Read Cache 100% upon Backup Power Source Failure		2.3.0
Configurable Big Block Cache Bypass		2.3.0
4Kn, 512e and 512n Support		2.3.0
Controller Based Encryption (CBE) Support*		2.3.0
Green Backup Support Included for SmartROC and SmartRAID		2.3.0
Survival Mode Power Management		2.3.0
Legacy Boot Support		2.3.0
UEFI Driver, Boot Support		2.3.0

Note: 3162-8i /e only.

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 6.52

This release includes the following fixes and enhancements:

- Added support to save controller logs in host memory in the event of a system crash.
- Added support for remote managed SED rekey support.
- Added support for Configurable Spindown Spares policy.
- Added support for Solidigm B16A/B17A and Kioxia TH58TEGX NAND flash components. Adapters built with these NAND components require firmware release 6.52 or greater and firmware downgrade will be blocked to previous releases.

- Added support for permanent disablement of unused IOBAR support in PCIe configuration space.
- Fixed an issue where taking ownership of Enterprise or Opal SED was failing on boot after panic shutdown.
  - Root Cause: Changing a master key causes several SED authorities to also change to the new key. The SED flow requires an open session, perform an SED task, and an end session. During this flow, if the controller encounters a panic shutdown, but the SED drives do not encounter a power cycle, then the SED drives are left in the middle of the flow waiting for the session to end. When the controller restarts and attempts to start a new session to validate the datastore on the SED, a start session failure occurs.
  - Fix: Error recovery is added to perform a protocol stack reset and retry the start session.
  - Risk: Low
- Fixed the following three issues related to expander firmware upgrade:

  a. OS hang after OS command timeout during expander firmware upgrade.

  b. Firmware lockup due to heartbeat timeout during expander firmware upgrade.

  c. Firmware does not detect all the drives after expander firmware upgrade.

  - Root Cause: Following are the root cause for the preceding issues:

    i. If an OS command is routed to target device's internal firmware queue upon expander firmware upgrade, it is not going to be processed by the firmware during the expander firmware upgrade. All host commands should be blocked while expander firmware upgrade is under way, but this is not possible.

    ii. Expander firmware images can be large which can take almost three minutes to download to the expander. During the download a firmware thread is suspended and does not update the heartbeat counter. The lack of an updated heartbeat counter results in firmware triggering a lockup.

    iii. After expander is instructed to activate newly downloaded expander firmware, it may takes tens of seconds for the expander to reset. As a result, firmware may not detect all the devices.
  - Fix: Following are the fixes for the preceding issues:

    i. Upon device LUN reset, firmware aborts any command pending in the target device's internal firmware queue to resolve the OS hang.

    ii. When downloading expander firmware, update the heartbeat counter to resolve the firmware lockup.

    iii. Delay running device discovery so that all devices can be detected.
  - Risk: Low
- Fixed an issue where the controller firmware is not returning the correct queue depth back to the host driver for the RBOD device or storage array controller device. This can cause a degradation in the performance on these devices.
  - Root Cause: The firmware does not return the queue depth value for these RBOD/storage array controller devices back to the OS device driver.
  - Fix: The firmware will check for the request of reporting the queue depth for these devices then it will return the value back to OS device driver.
  - Risk: Low
- Fixed an issue that disk drives attached behind an enclosure are shown to have a duplicate bay number.
  - Root Cause: The SES additional status element page may contain a valid additional status element descriptor for an empty slot/bay with only a valid device slot number. This causes

firmware to assign an incorrect slot number to multiple drives which are in slots after the empty slot.

  - Fix: Firmware recognizes a valid additional status element descriptor for an empty slot/bay and skip over it during device discovery.
  - Risk: Low

- Fixed an issue that system hung upon device LUN reset due to I/O timeout on RBOD LUNs.
  - Root cause: Upon device LUN reset for a multi-LUN device, all requests pending at various firmware queues are flushed and if there is OS partition installed then OS may hang.
  - Fix: Do not flush requests pending at various firmware queues upon device LUN reset.
  - Risk: Low
- Fixed an issue where a SED drive state will be set to OFS instead of MCHP owned if Master key change process is interrupted due to panic shutdown.
  - Root Cause: During Master Key change process, several SED tasks are performed. If this process is interrupted due to panic shutdown, it can leave the drive in some intermediate state. On the next reboot, when firmware attempts to open a new session to validate the datastore, a session failure occurs. Power cycling the drive or a reset can clear this condition, or performing a "Protocol Stack Reset" can clear this condition.
  - Fix: Fixed by performing a "Protocol Stack Reset" if the SED drive is in locked state.
  - Risk: Low
- Fixed an issue of possible controller lockup while deleting a logical drive configuration on a controller.
  - Root Cause: There was a small timing hole while doing a check if cache needed to persist where a null pointer was hit.
  - Fix: Make sure to check for null pointer.
  - Risk: Low
- Fixed an issue where a spare drive failed to spin up.
  - Root Cause: The drive does spin up, but the controller gives up too soon. The controller was not expecting the 2:04:1A (Not Ready: Logical Unit Not Ready, Start Stop Unit Command In Progress) response.
  - Fix: Added support to handle the not ready error condition the drive was returning.
  - Risk: Low
- Fixed an issue where a maxCache logical drive is migrated from one controller to another and a maxCache pair failed error message could be seen at power-up.
  - Root Cause: Caching configuration parameters were not being copied over properly to the controller in a new server.
  - Fix: Make sure to properly copy caching configuration parameters when destination controller does not have caching enabled.
  - Risk: Low
- Fixed an issue where security enabled SED drives that are in expected qualification failed state are staying failed after deleting the logical drive.
  - Root Cause: When clearing the configuration, the failure state of the drive was persisting even though the clear configuration was successful.
  - Fix: Fixed firmware to clear the error condition if clear configuration is successful.
  - Risk: Low
- Fixed an issue where the rebuild is not starting on a degraded managed SED logical drive that has the first spare drive as foreign SED.

  - Root Cause: When the firmware tries to activate the available spare drive for the degraded managed SED logical drive, it will choose the first available spare drive without checking the foreign SED status. But during spare activation, the firmware will check foreign SED status and will not activate the spare if it is a foreign SED.
  - Fix: Added foreign SED status check in firmware while selecting the spare drive for activation.
  - Risk: Low
- Fixed an issue where the controller is giving the second oldest event as the oldest event.
  - Root Cause: The controller can store a maximum of 128 events. Once it reaches the maximum limit, a new event will replace the oldest event. While doing so, firmware incremented the event pointer twice in different places.
  - Fix: Removed the second increment operation on the event pointer during a rollover.
  - Risk: Low
- Fixed an issue where the rebuild is not starting on the foreign SED after changing the controller master key to the foreign drive key.
  - Root Cause: When the controller-managed SED master key is changed to match the foreign drive key, firmware tries to import the foreign SED and unlock it. During this rekey process, firmware used the old master key to unlock foreign SED and failed to unlock and manage the foreign SED.
  - Fix: Added a check in firmware to decide which master key to use for unlocking the foreign SED among the reset key and old master key.
  - Risk: Low
- Fixed an issue where a transforming fault-tolerant managed SED logical drive is marked FAILED after hotplugging a foreign SED and rebooting the system.
  - Root Cause: During bootup, if there is a locked SED in the managed SED logical drive, the logical drive will be marked as SED_LOCKED. Later, firmware will check whether the locked SED is a foreign drive and fail the drive to remove the SED_LOCKED state on the logical drive. But firmware failed to update the controller metadata of the foreign SED. Due to this, the transformation is not able to resume after the reboot, and the logical drive is moved to the FAILED state.
  - Fix: Update controller metadata while the firmware is failing the foreign SED to unlock the managed SED logical drive.
  - Risk: Low
- Fixed an issue where the controller allowed importing a foreign SED in a degraded logical drive which has a different drive type.
  - Root cause: During the bootup, the firmware will check and qualify the newly detected replacement drives to get listed in the logical drive. The firmware will fail the replaced physical drive if it is of a different drive type compared to the existing physical drives in the logical drive. The firmware failed to do this check on a foreign SED and allowed the import of the foreign SED of different drive type to the managed SED logical drive.
  - Fix: Added a drive type check for foreign SED in the firmware bootup path.
  - Risk: Low
- Fixed an issue where Predictive Spare Rebuild (PSR) is not starting on the managed SED logical drive after replacing the foreign SED spare drive with a controller owned drive.
  - Root cause: If PSR is enabled, the firmware will try to activate the spare drive when it observes a predictive failed data drive. But if the spare drive is a foreign SED, it will not be activated. When this foreign SED spare drive is replaced with a controller-owned SED, the firmware does not have any check to activate the spare on predictive failed SED.

- Fix: While the firmware handles the hot insertion of a drive, it will check the need for the spare activation.
- Risk: Low

- Fixed an issue where Predictive Spare Rebuild (PSR) is not starting on the RAID 0 logical drive, if it is the first logical drive in the array followed by multiple fault-tolerant logical drives.
  - Root Cause: When a spare drive is assigned to the array, where the RAID 0 logical drive is the first logical drive in the array followed by multiple fault-tolerant logical drives, the spare will be assigned to all fault-tolerant logical drives, except the RAID 0 logical drives in the array by the host management tools in a sequence. If one of the data drives in the array is moved to the predictive failed state, the user can enable PSR to activate rebuilds of the predictive failed drive using the spare drive. When PSR is enabled, the firmware will start the PSR immediately on all the logical drives in the array, which have predictive failed drives and assigned spare drives. As the spare drive was not yet assigned to the RAID 0 logical drive by the host management tool, the PSR did not occur. The host management tool will assign a spare drive to RAID 0 logical drives with a delay after enabling the PSR, and the RAID0 logical drive will never get a chance to go through PSR.
  - Fix: While the firmware handles the configuration update for a logical drive, it will check the need for the spare activation and rebuild.
  - Risk: Low
- Fixed an issue to allow MCTP re-discovery on the first Bus Master Enable (BME) set only.
  - Root Cause: The firmware triggers an MCTP re-discovery on every BME set. On some systems, the server becomes confused and thinks the controller does not have an EID. This means the host cannot send MCTP messages to the controller.
  - Fix: Only allow for a MCTP re-discovery on the first BME set only and not subsequent BME set calls.
  - 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 2.10.2/Legacy BIOS 2.10.2

This release includes the following UEFI fixes and enhancements:

- Added support to the Controller Information menu to display controller CPLD and SEEPROM versions
- Added support in the logical drive members information menu to show transient drive information for transforming logical drives.
- Added a configuration option to change Spindown Spares Policy that indicates if controller will spindown inactive spares to a state of lower power consumption.
- Added support for additional data and content consistency for Save Support Archive operation, so the output will match with the output of other tools.
- Added HII menu option to perform rekey operation for Remote mode controller managed SED encryption.
- Added new options to the controller firmware update menu to select Active and Backup ROM region for firmware updates as well as to toggle the controller active ROM image.
- Added new HII menu under Disk Utilities to enumerate UBM backplanes along with the option to update backplane firmware.
- Fixed an issue with the unreadable characters for some HII menu help strings.
  - Root Cause: Incorrect translation of string from English to Chinese language.
  - Fix: Updated unicode string file with correct translated string for Chinese language.

  - Risk: Low
- Fixed an issue where the System HII browser freezes after entering Controller information menu when there is a lockup on the controller.
  - Root Cause: Command transactions were not getting timed due to incorrect counter usage.
  - Fix: Added appropriate timer event to track the command time out and to detect controller firmware readiness.
  - Risk: Low
- Fixed an issue where UEFI Self Certification Tests for Block I/O protocol fails.
  - Root Cause: UEFI driver fails to handle the SCSI response sense data that includes unit attention status returned with a non-standard descriptor format.
  - Fix: Updated error handling for SCSI unit attention response with non-standard sense data descriptor format.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.26-030

This release includes the following fixes and enhancements.

- Fixed an OS crash issue that happens while creating/deleting a logical drive or adding/removing physical drives.
  - Root Cause: The driver is rescanning a device which does not exist. There was a problem where a device rescan operation is failing because the device pointer being used is not valid. This results in a NULL pointer de-reference issue and causes an OS crash.
  - Fix: Multiple conditions will be evaluated before notifying the OS to do a rescan. Driver will skip re-scanning the device if any one of the following conditions are met:
    - Device was not added to the OS scsi mid-layer yet or the device was removed.
    - Devices which are marked for removal or in the process of removal.
  - Risk: Low
- Fixed an issue to eliminate race condition while rescanning a logical drive. Under very rare conditions, after a logical drive size expansion the OS still sees the size of the original logical drive.
  - Root Cause: The rescan flag in the driver is used to signal the need for a logical drive rescan. A race condition occurs in the driver which leads to one thread overwriting the flag inadvertently. As a result, the driver is not notifying the OS scsi mid-layer to rescan the logical drive.
  - Fix: Acquire spinlock and set the rescan flag.
  - Risk: Low

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4460.0.1002

This release includes the following fix:

- Fixed an issue where under certain I/O conditions a program doing large block disk reads can cause a controller to crash.
  - Root Cause: The SCSI read request and destination address in the DMA descriptor is incorrect, causing the DMA engine in the controller to assert.
  - Fix: Change the alignment for creating `bus_dma_tags` in the driver from PAGE_SIZE (4k) to 1, which allows the controller to manage its own address range for DMA transactions.
  - Risk: Medium

2.2.3.3 Fixes and Enhancements for Windows® Driver Build 1010.84.0.1012

This release includes the following fixes and enhancements.

- Added support for the DMA V3 kernel API, which simplifies the management of scatter/gather lists and reduces the need for driver intervention during complex DMA transfers.
- Added support for the driver to use StorPortMaskMsixInterrupt() API to enable and disable interrupts when the driver is running on Server 2022 (Version 21H1) and later. The driver will continue to use the legacy method on older versions of the OS where the API is not supported.
- Fixed the I/O errors that were observed inconsistently for MPIO enabled physical drives. The I/O errors reported for multipath during cable plug/unplug.
  - Root Cause: The MPIO driver detects a device error instead of path failure when Read Capacity, Test Unit Ready, or Inquiry command failed with "`SCSI status = Check Condition with Sense Key = Illegal Request (KCQ=5:26:00)`" and "`SRB status = SRB_STATUS_ERROR`".
  - Fix: The SmartPQI driver returns "`SRB status = SRB_STATUS_NO_DEVICE`" for "`Sense Key = Illegal Request (KCQ=5:26:00)`" to indicate that one of the paths has failed.
  - Risk: Low

2.2.3.4 Fixes and Enhancements for VMware Driver Build 4600.0.115

There are no known fixes for this release.

2.2.4 Management Software Fixes

2.2.4.1 Fixes and Enhancements for Arcconf/maxView™ Build 4.16.00.26273

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

- Microchip strongly recommends the maxView users to update to the latest version of the tools to avoid a security vulnerability that has since been resolved.
- Added support in Arcconf and maxView to configure the "Spindown spares policy".
- Added support to install and run Arcconf and redfish server in the secureboot ESXi environment.
- Added support in Arcconf and maxView to prevent the firmware rollback when the given controller firmware update contains a hardware security update and the controller write cache is enabled.
- Enhanced the UEFI Arcconf `savesupportarchive` command to capture the support logs in the same format as host Arcconf.
- Fixed an issue where Arcconf create command help was missing the SSDIOBYPASS option.
  - Root Cause: SSDIOBYPASS option was not added in Arcconf help when the user executes create command.
  - Fix: Implemented changes to add SSDIOBYPASS option in Arcconf help when the user executes create command.
  - Risk: Low
- Fixed an issue where invalid drive temperature was displayed in maxView for dedicated spare drive.
  - Root Cause: The temperature data was collected using a signed character variable resulting the variable to hold incorrect data for high temperature values.
  - Fix: Replaced the signed character variable with unsigned character variable to collect temperature and display invalid temperatures as “Not available” from Arcconf/maxView.
  - Risk: Low
- Fixed an issue where `arcconf SLOTCONFIG` command was not displaying the UBM backplane attached drives.

  - Root Cause: Slot mapping for the drive connected to the UBM backplane was missing in Arcconf. This resulted in not displaying the UBM backplane attached drives.
  - Fix: Implemented changes to list the slots of the UBM backplane for the `arcconf SLOTCONFIG` command.
  - Risk: Low
- Fixed an issue where `savesupportarchive` captures empty crash dump file when the crash dump buffer size was zero from firmware.
  - Root Cause: An empty crash dump file was created while executing `savesupportarchive` when crash dump buffer size was zero from firmware.
  - Fix: Implemented changes only to generate crash dump file when available in firmware using `savesupportarchive` command.
  - Risk: Low
- Fixed an issue where maxView was creating logical device with reduced size when creating maxCache with 256 KB cache line size.
  - Root Cause: The size was calculated with default cache line size (64 KB) instead of user specified cache line size (256 KB) which resulted in reduced size of logical device.
  - Fix: Implemented the changes to calculate size with user specified cache line size (256 KB).
  - Risk: Low
- Fixed an issue where UBM backplanes were enumerated incorrectly in Arcconf and maxView.
  - Root Cause: Arcconf and maxView were displaying UBM controllers as UBM backplane devices which resulted in incorrect enumeration of UBM backplanes.
  - Fix: Added changes in the Arcconf to display one UBM backplane with multiple UBM controllers under it. Added the changes in the maxView to display one UBM backplane in the Enterprise Tree View and display only the required information along with UBM controller ID in the Backplane Summary tab.
  - Risk: Low
- Fixed an issue where maxView Desktop application was displaying the warning messages in the startup dialog.
  - Root Cause: When maxView Desktop application is launched, the warning messages which were part of initialization process were displayed.
  - Fix: Suppressed the warning messages which were part of initialization process and added a similar information for all the Operating systems as "*maxView Storage Manager is initializing and will launch once initialization is complete*".
  - Risk: Low
- Fixed an issue where maxView was sending email notification twice per event.
  - Root Cause: When email is configured with port 587, the SMTP server sent the email and returned the error as '*AUTH LOGIN failed (535 Authentication failed. Restarting authentication process.)*' and another email was sent through fallback mechanisms because of SMTP error 535.
  - Fix: Blocked sending an email through fallback mechanism when SMTP server returns the error as '*AUTH LOGIN failed (535 Authentication failed. Restarting authentication process.)*'.
  - Risk: Low
- Fixed an issue in maxView firmware upgrade wizard where maxView was displaying two options '*Flash Active ROM*' and '*Flash Active and Backup ROM*' for the controller that doesn't support flashing active ROM.

  - Root Cause: maxView displays two options '*Flash Active ROM*' and '*Flash Active and Backup ROM*' for controllers in firmware upgrade wizard where the controller supports flashing only backup ROM.
  - Fix: The maxView firmware upgrade wizard displays only "*Flash on Backup ROM*" option for those controllers.
  - Risk: Low
- Fixed an issue in maxView where maxCache Statistics tab was missing.
  - Root Cause: The Advanced Statistics code clean-up caused the maxCache statistics tab not to be displayed in the maxView.
  - Fix: Added the logic to display the cache statistics tab for maxCache logical device and update the data.
  - Risk: Low
- Fixed an issue where the RAID 50/60 legs (parity group) migration operation was displaying success message, but the legs were not migrated to the valid user specified value.
  - Root Cause: The user specified legs (parity group) value was not passed as an argument to the migrate logical device SDK API which resulted in the operation returning success, but the parity groups were not migrated.
  - Fix: Added the changes to input the user specified legs count as an argument to the migrate logical device SDK API for migrating the RAID 50/60 logs.
  - Risk: Medium

2.2.4.2 Fixes and Enhancements for PLDM Release 6.30.6.0

This release includes the following fixes and enhancements:

- Added support for the RDE ACTION #Storage.ResetToDefaults to clear event logs and crash dumps stored on the controller in addition to its previous functionality. Logs and crash dumps will be deleted regardless of the requested ResetType.
- Added support for the PLDM Type 6 long-running task for certain RDE operations. When a new RDE operation request is received that is anticipated to exceed the 6 second timeout limit, the PLDM Type 6 state machine will transition to the TASK_RUNNING state. When in this state, the BMC can send the `RDEOperationStatus` command to query for task completion or failure. Additionally, a `RedfishTaskExecuted` event will be sent to any event listeners when the task is completed. Long-running tasks will only be supported if the BMC negotiates for Task support using the `NegotiateRedfishParameters` command. The following RDE operations will be executed through the long-running task:
  - RDE DELETE for a Volume resource which is not the last created on a given array.
  - RDE DELETE for the last remaining Volume on an array which has SED encryption enabled.
  - RDE ACTION for `#Storage.ResetToDefaults` when `ResetType = ResetAll` when encrypted Volumes are present.
  - RDE ACTION for `#Storage.ResetToDefaults` when a crash dump is present on the controller.
- The AutoVolumeCreate property is now published in RDE READ responses for the Storage resource. This property will have a value of "NonRAID" on controllers which support the HBA Volume feature. Additionally, the schema version of the Storage resource was updated to v1.15.0 to incorporate this new property in the dictionary.
- The following properties are now published in RDE READ responses for the StorageController resource:
  - Links.Batteries
  - Links.Batteries@odata.count

- Added support for the Battery Redfish resource to publish properties describing a supercap backup power source connected to the controller. The addition of this resource includes parent resources BatteryCollection, PowerSubsystem, and Chassis. The following schema versions are supported for these resources:
  - Chassis - v1.22.0
  - PowerSubsystem - v1.1.0
  - BatteryCollection - unversioned
  - Battery - v1.2.0
- Added support for Storage.Status.HealthRollup and StorageController.Health to publish a value of "Critical" in RDE READ responses when dirty cache flush failures occur during POST.
- Fixed an issue where WriteCacheProtected alert is sometimes not generated after clearing a cache temporarily disabled condition. After experiencing a condition that results in a WriteCacheTemporarilyDegraded event being generated, no corresponding WriteCacheProtected event is sent after rectifying the condition.
  - Root Cause: A previous fix to suppress WriteCacheProtected events at boot time inadvertently prevented the event from ever being sent.
  - Fix: Revised the condition for generating WriteCacheProtected events to more narrowly define the specific sequence of conditions that denote a good cache status just after boot time.
  - Risk: Low
- Fixed an issue where `StorageController.CacheSummary.Status.Health` has "OK" value instead of "Warning" when the cache is in a temporarily degraded state.
  - Root Cause: The logic to determine the cache health was incorrectly trying to consider the state of a backup power source in cases where such backup power sources are not required.
  - Fix: Corrected the logic related to the check of the backup power source state.
  - Risk: Low
- Fixed an issue where the response to a `GetDownstreamFirmwareParameters` command did not return "DC power cycle" as a supported component activation method for drives or expander SEPs.
  - Root Cause: Only the "AC power cycle" and "System reboot" `ComponentActivationMethods` bits were tagged as valid activation methods for drives and expander SEPs.
  - Fix: Modified the `ComponentActivationMethods` field for drives and expander SEPs to include setting the "DC power cycle" bit as a supported activation method.
  - Risk: Low

2.3 Limitations

2.3.1 General Limitations

This release includes the following general limitation:

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

2.3.2 Firmware Limitations

2.3.2.1 Limitations for Firmware Release 6.52

This release includes the following firmware limitations:

- Persistent Event Logs (PEL) are getting cleared when:
  - Upgrading from firmware releases prior to 5.61 to 5.61 or later firmware releases.
  - Downgrading from firmware releases 5.61 or later to firmware releases prior to 5.61.
- Firmware downgrade 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 rebooting after the firmware update is pending or the flashed new firmware version is older than 5.32 B0.
  - Workaround: Reboot the system
- Logical drive is not detected when 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, or, the 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.
- Power cycle to the enclosure may be needed if connected server goes through abnormal shutdown under following condition: SED operation on OPAL drives like taking ownership, reverting the ownership, or changing the master key where firmware internally performs open session, performs SED management, and ends session gets interrupted due to abnormal shutdown on the server. This condition causes firmware to restart on reboot while drives are left off in the middle of performing SED task and so drives needs to be power cycled also.
  - Workaround:
    - Allow the change master key operation to complete before shutting down the server.
    - If SEDs are in an external enclosure, power cycle the external enclosure and SEDs before powering up the server with the controller.
- Firmware downgrade from firmware version 6.22 B0 to any older firmware version is blocked if Managed SED is enabled.
  - Workaround: Disable Managed SED and try firmware downgrade.
- Managed SED cannot be enabled on the controller, where reboot is pending after firmware downgrade from firmware version 6.22 B0 to any older firmware version.
  - Workaround: Reboot the controller and enable the Managed SED.
- The host may encounter a BSOD when executing clear configuration with a large number of encrypted logical drives.
  - Workaround:
    - Delete the logical drives one by one.
    - Reboot the system.

2.3.2.2 Limitations for Firmware Release 1.32 Build 0

- Firmware release 1.32b0 may become unresponsive while attempting to flash firmware or execute other RAID logical drive operations.
  - Description: Refer to entry "Fixed an issue where firmware may become unresponsive while attempting to flash firmware or execute other RAID logical drive operations" in the Firmware fixes section.
  - A fix for this issue is available in the 1.60 B0 firmware release. If a firmware flash failure is occurring, try the following workarounds:

- Workaround: If there are no target devices (expanders or drives) attached to the controller, attach a target device to the controller and try the host management operation again.
- Workaround: If the system is operating using UEFI, the HII tool can be used to flash the firmware to this release as outlined in the *Microchip SmartIOC 2100/SmartROC 3100 Installation and User's Guide (ESC-2170577),* appendix entry “Updating the SmartIOC 2100/ SmartROC 3100 Controller Firmware”.
- Workaround: If there are target devices attached to the controller and this issue occurs or none of the workarounds can be used, contact Microchip Support.

2.3.3 UEFI Limitations

2.3.3.1 Limitations for UEFI Build 2.10.2/Legacy BIOS Build 2.10.2

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 Limitations for Linux Driver Build 2.1.26-030

This release includes the following limitations:

- On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, SLES15SP3, OpenEuler 20.03LTS, and 22.03LTS including SP releases), the driver injection (DUD) install will hang if an attached drive (either HBA mode or Logical Volume) has Write Cache enabled.
  - Workaround: There are two workarounds for this issue:
    - Ensure that the Write Cache is disabled for any attached drive.
    - For RHEL7.9/8.2/8.3 and OpenEuler 20.03LTS, 22.03LTS, add `rd.driver.blacklist=smartpqi` to the grub entry along with `inst.dd`.
- RHEL driver injection (DUD) install where OS ISO is mounted as virtual media on BMC based servers (non-ILO). Installer will hang after driver injection. It is reported on RHEL 8.5, 8.6, 9.0, and 9.1.
  - Workaround:
    - Load the OS from USB device instead of virtual media.
    - Load the OS from virtual media but initiate ISO verification (media test) during the installation followed by ESC to cancel the media test.
    - Edit grub to include the boot argument "`nompath`". Replace "`inst.dd`" with "`nompath inst.dd`" for DUD install.
- Oracle 9 UEK 7 kernel causes SmartPQI rpm dependency failures. This is an issue with how the kernel package was created by Oracle. Correct UEK7 kernel for Oracle 9, which is expected in the mid-October UEK7 release, version number is still pending.
  Note: This does not affect Oracle 8 UEK 7.
  - Workaround: Install the rpm using "`--nodeps`" when dependency failures occur.
    - Update:
      For SmartPQI driver versions > 2.1.20-020 and UEK7 kernels >= 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm will install normally.

      For UEK7 kernels < 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm needs to be installed using the "`--nodeps`".
- On AMD systems, the system might crash or hang due to a bug in the IOMMU module. For details, see lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/.
  - Workaround: Disable the IOMMU setting option in BIOS.
- Depending on hardware configurations, the SmartPQI `expose_ld_first` parameter may not always work consistently.

  - Workaround: None
- On some distributions (including RHEL 9.0/Oracle Linux 9.0), you are unable to inject the OOB driver (DUD) during install when a multi-actuator drive is attached.
  - Workaround: Install using the inbox driver, complete OS installation, then install the OOB driver.

2.3.4.2 Limitations for Windows Driver Build 1010.84.0.1012

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. Controller cache flushing will continue and complete while the system is in the BSOD state. 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.
- A system crash may occur when hibernating a system installed on a Dual Actuator drive.
  - Workaround:
    - Avoid hibernating the system while running heavy I/Os to multiple Dual Actuator drives.
    - Stop running the I/Os to the drives and then hibernate the system.
    - Reboot the server to recover the system.

2.3.4.3 Limitations for FreeBSD Driver Build 4460.0.1002

This release contains the following limitations:

- Customized kernels built with the INVARIANTS flag are not currently supported.

2.3.4.4 Limitations for VMware Driver Build 4600.0.115

This release includes the following limitation:

- 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, 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 Arcconf/maxView Build 4.16.00.26273

This release includes the following limitations:

- Windows SNMP service is not working after installing maxView. In some versions of Windows operating system when Adaptec SNMP subagent is installed, SNMP service does not respond due to the registry configuration which blocks TCP IN/OUT bound traffic to the SNMP subagents even when the firewall is disabled.
  - Workaround: Follow the below steps to enable the TCP IN/OUT bound traffic to the SNMP subagents:

    i. Login to the system as Administrator and open Registry by issuing regedit in the command prompt.

    ii. Navigate to `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Static\System]`.

    iii. Find the “Name” string that starts with “SNMP-3” and “SNMP-4”.

iv. Change the “Action=Block” to “Action=Allow” of those entries.

v. Restart the “Windows Firewall” service.

vi. Restart the “SNMP Service” service.

2.3.5.2 Limitations for PLDM Release 6.30.6.0

There are no known limitations for this release.

2.3.6 Hardware Limitations

This release includes the following hardware limitations:

- Two Wire Interface (TWI) address conflicts can cause system DDR memory to not be discovered.
  - Description: The 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

Note: SmartRAID3102e-81, SmartRAID 3101e-4i, and all SmartRAID 3200, SmartHBA 2200, and HBA 1200 adapters do not have the FRU SEEPROM so are not affected by this hardware limitation.

3. Updating the Controller Firmware

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

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

3.1 Updating the Controller Firmware

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

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* (DS00004439, 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.

Revision	Date	Description
L	11/2023	SR 2.8.2 Production Release
K	10/2023	SR 2.8.0 Patch Release with maxView™ version B26068
J	10/2023	SR 2.7.0 Patch Release with maxView version B25339
H	07/2023	SR 2.8.0 Production Release
G	03/2023	SR 2.7.4 Production Release
F	11/2022	SR 2.7.2 Production Release
E	08/2022	SR 2.7.0 Production Release
D	03/2022	VMware driver version updated from 4250.0.120 to 4252.0.103
C	02/2022	SR 2.6.6 Production Release
B	12/2021	SR 2.6.4.1 Patch Release with maxView version B24713. Updated Fixes and Enhancements for maxView Storage Manager/ARCCONF section for log4j vulnerabilities.
A	11/2021	SR 2.6.4 Production Release with firmware version 4.72 B0 (Previously ESC-2161026)
29	04/2021	SR 2.6.2 with firmware version 4.11 B0
28	04/2021	SR 2.6.1.1 with VMware driver version 4054.2.118.
27	03/2021	SR 2.6.1 with VMware driver version 4054.1.103.
26	02/2021	SR 2.6 Production Release
25	10/2020	SR 2.5.4 Production Release
24	08/2020	SR 2.5.2.2 Production Release with Firmware 3.00
23	03/2020	SR 2.5.2 Production Release with Firmware 2.93
22	03/2020	SR 2.5 Production Release with Firmware 2.66
21	02/2020	SR 2.5.2 Production Release
20	10/2019	SR 2.5 Production Release
19	09/2019	Updated for SR 2.4.8.1 (fw v2.31 Build 0)
18	08/2019	Updated for SR 2.4.8
17	01/2019	SR2.4 Production Release
16	06/2018	SR2.3 Production Release
15	06/2018	Updated for RC Release
14	10/2017	Update supported OSs
13	10/2017	First Production Release
1-12	06/2016 to 07/2017	Pre-Production Release.

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, 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, TimeCesium, TimeHub, TimePictra, TimeProvider, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, Power MOS IV, Power MOS 7, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, Turing, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-6683-3400-3

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Quality Management System

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

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Australia - Sydney
Tel: 61-2-9868-6733

China - Beijing
Tel: 86-10-8569-7000

China - Chengdu
Tel: 86-28-8665-5511

China - Chongqing
Tel: 86-23-8980-9588

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115

China - Hong Kong SAR
Tel: 852-2943-5100

China - Nanjing
Tel: 86-25-8473-2460

China - Qingdao
Tel: 86-532-8502-7355

China - Shanghai
Tel: 86-21-3326-8000

China - Shenyang
Tel: 86-24-2334-2829

China - Shenzhen
Tel: 86-755-8864-2200

China - Suzhou
Tel: 86-186-6233-1526

China - Wuhan
Tel: 86-27-5980-5300

China - Xian
Tel: 86-29-8833-7252

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444

India - New Delhi
Tel: 91-11-4160-8631

India - Pune
Tel: 91-20-4121-0141

Japan - Osaka
Tel: 81-6-6152-7160

Japan - Tokyo
Tel: 81-3-6880- 3770

Korea - Daegu
Tel: 82-53-744-4301

Korea - Seoul
Tel: 82-2-554-7200

Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

Malaysia - Penang
Tel: 60-4-227-8870

Philippines - Manila
Tel: 63-2-634-9065

Singapore
Tel: 65-6334-8870

Taiwan - Hsin Chu
Tel: 886-3-577-8366

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600

Thailand - Bangkok
Tel: 66-2-694-1351

Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4485-5910
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-72400

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra'anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-72884388

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820