HBA 1100 Software/Firmware Release Notes

Table of Contents

1. About This Release

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

1.1 Release Identification

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

Table 1-1. Release Summary

Solutions Release	2.7.4
Package Release Date	March 17, 2023
Firmware Version	5.91[1,2]
UEFI Version	2.6.2
Legacy BIOS	2.6.2
Driver Versions	Windows SmartPQI: • Windows 2016/2019/2022: 1010.64.0.1037 • Windows 10/11: 1010.64.0.1037 Linux SmartPQI: • RHEL 7/8/9: 2.1.22-040 • SLES 12/15: 2.1.22-040 • Ubuntu 16/18/20/22: 2.1.22-040 • Debian 10/11: 2.1.22-040 • Oracle Linux 7/8/9: 2.1.22-040 • Citrix XenServer 8: 2.1.22-040 VMware SmartPQI: • VMware 7.0/8.0: 4440.0.124 FreeBSD/Solaris SmartPQI: • FreeBSD 12/13: 4390.0.1010 • Solaris 11: 11.4120.0.1005
Management Software (arcconf, maxView™, Event Monitor, BootUSB)	4.11.00.25823
PLDM	6.20.8.0

Notes:

1. Downgrading to 1.04 B0 or older builds from this release or prior 1.29 releases may cause the board to not boot or have supercap errors due to an incompatibility in SEEPROMs between this release and prior releases. Refer to the section "3. Updating the Controller Firmware" to downgrade an existing board.
2. If Managed SED is enabled, do not downgrade firmware to version 5.00 or earlier because they do not support Managed SED capabilities. Disable Managed SED if downgrading to firmware versions 5.00 or earlier.

1.2 Components and Documents Included in this Release

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

1.3 Files Included in this Release

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

Firmware Files

Table 1-2. Firmware Files

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

Table 1-3. Firmware Programming Tools

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

Driver Files

Table 1-4. Windows Storport Miniport SmartPQI Drivers

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

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

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

.....continued	
Drivers	**Intel/AMD x64**
SuSE Linux Enterprise Server 12 SP5, SP4	x64
SuSE Linux Enterprise Server 15 SP4, SP3, SP2	x64
Oracle Linux 7.9 UEK6U3	x64
Oracle Linux 9.1, 9.0, 8.7, 8.6 UEK7	x64
Ubuntu 22.04.2, 22.04.1, 22.04	x64
Ubuntu 20.04.5, 20.04.4, 20.04	x64
Ubuntu 18.04.5, 18.04.4, 18.04	x64
Ubuntu 16.04.5	x64
Debian 11.5, 10.13	x64
Citrix xenServer 8.2.1, 8.1, 8.0	x64
Fedora 37 (inbox only)	x64

Notes:

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

Table 1-6. Linux SmartPQI Drivers for Arm

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

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

Drivers	Version
FreeBSD 13.1, 12.4	x64
Solaris 11.4	x64
VMware 8.0, 7.0 U3/U2/U1	x64

Host Management Software

Table 1-8. Host Management Utilities

Description	OS	Executable
ARCCONF Command Line Utility	Windows x64 Linux x64 VMware 7.0 and above XenServer FreeBSD x64 Solaris x86 Linux ARM	See the Arcconf download package for the OS-applicable installation executable.
ARCCONF for UEFI	—	Included as part of the firmware downloadable image.
maxView™ Storage Manager	Windows x64 VMware 7.0 and above Linux x64 XenServer	See the maxView Storage Manager download package for the OS-applicable installation executable.
maxView™ vSphere Plugin	VMware 7.0 and above	See the VMware maxView Storage Manager download package for the OS-applicable installation executable.
Boot USB (offline or pre-boot) for ARCCONF and maxView Storage Manager	Linux x64	See the maxView BootUSB download package for the .iso file.

2. What's New?

This section shows what's new in this release.

2.1 Features

The following table lists features supported for this release. Features to be supported in future releases or supported in current release are designated as "X".

Table 2-1. Feature Summary

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

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 5.91

This release includes the following fixes and enhancements:

- Added support for a Dual-Actuator drive to return LUN specific information such as Unique WWID and Unique ID.
- Added support to ensure only Microchip-owned SED can be sanitized.
- Disabled the Minimum Power mode.
- Added support for improving secure erase time for disks supporting the WRITE SAME command.
- Added support for switching persistent event log policy without clearing the existing event logs.
- Added support for cascaded expander to uniquely identify the attached enclosure and physical devices.
- Fixed an issue where PLDM event consumer was missing events from the previous boot.
  - Root Cause: PLDM event consumer was initialized before events were put into buffer.
  - Fix: PLDM event consumer is initialized after events are placed in buffer.
  - Risk: Low

- Fixed an issue where the required reason for controller reboot is not getting updated for the sanitize policy change.
  - Root Cause: When the sanitize policy is changed, the firmware updates the NVRAM content of the controller with the new sanitize policy. On the next boot, the firmware uses the NVRAM content to update the current sanitize policy. However, firmware is not updating the reboot required reason for this sanitize policy change.
  - Fix: Firmware will update reboot required reason when the sanitize policy is changed.
  - Risk: Low
- Fixed an issue where the controller reports sanitizing complete on a hot-removed and hot-plugged back in HDD that happens while sanitize is being performed.
  - Root Cause: There was a race condition where the sanitize status was cleared when a hot plug was detected.
  - Fix: Mark status of the hot plug device and do not resume sanitize if that status is set.
  - Risk: Low
- Fixed an issue of the Managed SED adapter password internal lockout wait timeout being reset on system reboot.
  - Root Cause: When a user is in Locked Out state, a message instructs user to either wait for 15 minutes or reboot the system. On reboot, firmware was resetting timer to 15 minutes.
  - Fix: Clear the countdown timer upon reboot to allow the user to enter the adapter password..
  - Risk: Low
- Fixed an issue where firmware is processing additional unlock adapter password request even if the controller is already unlocked.
  - Root Cause: When handling the unlock adapter password request from the host, firmware does not check if the controller is already unlocked or not. However, firmware still processes the request while the controller is unlocked.
  - Fix: During the unlock adapter password request handling, firmware will check if the adapter password is already unlocked and complete the request with an error status.
  - Risk: Low
- Fixed an issue of power surge when too many SATA drives are spinning up simultaneously.
  - Root Cause: During boot, multiple SATA drives were spun up almost simultaneously during RAID metadata read; causing power surge.
  - Fix: Instead of Test Unit Ready command, use the ATA passthrough command with the Check Power mode command to check the power condition to determine whether to spin up the drive or not.
  - Risk: Low
- Fixed an issue where the failed SED drive is found during drive spin-up.
  - Root Cause: During discovery, a locked SED drive was in Idle Power state, and when trying to spin up, it failed with access denied because the drive was locked.
  - Fix: Do not fail the locked SED drive so there is a chance to unlock it after device discovery has completed.
  - Risk: Low
- Fixed an issue where the datastore is updated, when SED is moved to “Otherwise Owned”.
  - Root Cause: When SED is being tagged as “Otherwise Owned”, the datastore of the SED is being updated.
  - Fix: If SED is tagged as “Otherwise Owned”, it must not have its datastore updated.
  - Risk: Low
- Fixed an issue where a hot-added Managed SED is reported to the host before it is fully ready.
  - Root Cause: Firmware is reporting a hot-added Managed SED to the host before the process of unlocking the drive is complete.
  - Fix: Firmware will report the Managed SED to the host when the drive is completely ready.

  - Risk: Low

- Fixed an issue where on reboot after panic shutdown, Ownership or Revert of the drive is unsuccessful.
  - Root Cause: When “Take Ownership” occurs, several administrative pins are changed from MSID to the new master pin (key). Similarly, when “Revert to OFS (Original Factory State)” occurs, several administrative pins are changed from existing master pin to default MSID.
  - Fix:
    - When Take Ownership or Revert is occurring on the drive, track the start and complete steps of the Ownership or Revert process. On boot, if the tracking information is valid, then revert the drive using the master key.
    - For enterprise drive, during Revert for the change of master pin, if the session authentication fails with STATUS NOT AUTHORIZED, then retry using the other pin (MSID).
  - Risk: Low

- Fixed a controller lock-up issue caused by a Loss of Sync (LOS) during sequential write traffic.
  - Root Cause: The controller SAS hardware state machines are stuck due to the LOS during sequential write traffic.
  - Fix: Issue Reset of the controller SAS hardware.
  - Risk: Low

- Fixed an incorrect treatment of the SMP Discover response with the ATTACHED SATA DEVICE set and ATTACHED SAS DEVICE TYPE bits set to 0.
  - Root Cause: SATA drive is not discovered immediately because the expander did not respond to its X_RDY after a PHY reset sequence. Therefore, the drive delayed the sending of the Device to Host Frame Information Structure (FIS) to the expander. During this window of time, the firmware sends an SMP Discover and the response has the ATTACHED SATA DEVICE bit set but the ATTACHED SAS DEVICE TYPE bits are set to 0. The firmware treats this combination of bits as “no device”.
  - Fix: Treat the SMP discover response with ATTACHED SATA DEVICE bit is set and ATTACHED SAS DEVICE TYPE bits set to 0 as spin up hold.
  - Risk: Low

2.2.2 UEFI Fixes

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

2.2.2.1 Fixes and Enhancements for UEFI Driver 2.6.2/Legacy BIOS 2.6.2

This release includes the following UEFI fixes and enhancements:

- Added HII option, Configure Controller UEFI Driver Health Reporting in the Configure Controller Settings menu to enable or disable reporting controller configuration errors and information using driver health protocol.
- Added an HII option to unset, temporarily suspend and resume controller password options for controller based encryption settings
- The Device Information menu under Disk Utilities is enhanced with multi-LUN information such as WWID and size of multi-LUN devices.
- Added a new HII menu, Configuration, under Configure Controller Settings that permits setting the PCIe maximum read request size and also shows current values of PCIe Max Read Request Size and Max Payload Size.
- Enhanced the temperature sensor location information display under controller information menu to show as location strings.
- Fixed an issue where the **Import Foreign Local Key** option for Managed SED encryption setting appears even when no foreign devices are present.
  - Root Cause: Eligibility check for foreign import was missing when the controller is in Locked state.
  - Fix: Added an appropriate eligibility check for foreign import when the controller is in Locked state.
  - Risk: Low
- Fixed an issue where system freezes during boot after enabling IOMMU remapping.

  - Root Cause: UEFI driver communication queues and interfaces were using the DMA-mapped address instead of the host address.
  - Fix: Changed the UEFI driver communication queues to use the host allocated and mapped address.
  - Risk: Medium
- Fixed an issue where an incorrect value is set for the VDM Discovery option under out of band settings menu.
  - Root Cause: The VDM Discovery option under out of band settings menu was considering incorrect values for enable and disable options.
  - Fix: Corrected the values per controller's expectations for the VDM Discovery option.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.22-040

This release includes the following fixes and enhancements.

- Fixed an issue of sending a command to physical devices during device discovery.
  - Root Cause: The smartPQI driver was sending a SCSI TEST UNIT READY command to physical devices during device discovery. The driver's device discovery thread hung if a physical device failed to complete this command.
  - Fix: The driver no longer sends a SCSI TEST UNIT READY command to physical devices during device discovery. It uses a different method to detect sanitize/erase in progress.
  - Risk: Low
- Fixed an issue where the OS crashes on aarch64 servers using the out-of-box driver during driver initialization.
  - Root Cause: The driver attempts to communicate with the controller firmware using a `writew()` kernel call to a byte aligned address. This works on x86_64 servers but fails on aarch64 systems.
  - Fix: Change the `writew()` to two `writeb()` calls.
  - Risk: Medium
- Fixed an issue where the OS crashes when a drive is hot removed during I/O stress test.
  - Root Cause: An I/O request pointer can be invalid if the block layer provides incorrect multi-queue host tag. This can lead to invalid I/O request pointer deference.
  - Fix: Validate the block layer provided host tag and handle the I/O request pointer properly if an invalid host tag is received.
  - Risk: Low
- Fixed an issue with the driver not mapping full length of PCI BAR 0.
  - Root Cause: The driver is only mapping the controller registers up to and including the PQI standard registers.
  - Fix: Update the length to include the full size of PCI BAR.
  - Risk: Low

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4390.0.1010

- Fixed an issue where a wrong LUN is reset when LUN RESET TMF is issued.
  - Root Cause: While issuing LUN RESET TMF to the second LUN of the Dual-Actuator drive, the first LUN is also reset. In the current code, LUN address and LUN number fields are not updated in `tmf req struture` for multi-LUN devices.
  - Fix: Added changes in IOBypass/RAID TMF structures to send `tmf request` for multi-LUN devices.
  - Risk: Low
- Fixed an issue where the partition information for all LUNs of a multi-actuator drive is reported to be the same after hot-removal and hot-reinsertion of the drive.
  - Root Cause: For a multi-actuator drive, the partition information for LUN1 is reported with the information from LUN0 after a hot-removal and hot-reinsertion of the drive. After hot-reinserting a Multi-Actuator drive, I/O to LUNs is submitted using the RAID path. However, commands sent to Multi-Actuator drives through the RAID path are not handled correctly.

  - Fix: Added support to send commands to Multi-Actuator drives through the RAID path when needed.
  - Risk: Medium

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 1010.64.0.1037

- Fixed an issue where the Dual-Actuator device is inaccessible after receiving a Report LUN command with an allocation length less than eight.
  - Root Cause: The driver failed to verify whether the allocation length of the Report LUN command was less than eight and updated an invalid LUN number for the Dual-Actuator device.
  - Fix: The driver will not update the LUN number for the Dual-Actuator device when the allocation length of the Report LUN command is less than eight.
  - Risk: Low
- Fixed an issue where BSOD SYSTEM_THREAD_EXCEPTION_NOT_HANDLED is observed in systems containing a significantly large number of CPUs with BIOS setting (Sub-NUMA) SNC4 enabled.
  - Root Cause: The BIOS SNC4 (sub NUMA cluster) switch changes the max CPU group value returned by the OS that exceeds the driver's max group count and causes a buffer overrun. The buffer overrun results in the driver accessing out of range memory triggering a SYSTEM_THREAD_EXCEPTION_NOT_HANDLED BSOD.
  - Fix: Dynamically get the max CPU group value from the OS to avoid the buffer overrun.
  - Risk: Low

2.2.3.5 Fixes and Enhancements for VMware Driver Build 4440.0.124

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 4.11.00.25823

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

- Added the Desktop maxView Web Application support where the maxView process starts when the user opens the maxView GUI and the process stops when the user closes the maxView GUI.
- Added support for PCIe Maximum Read Request Size (MRRS) configuration.
- Added Multi-Actuator drive support where maxView and arcconf displays the additional LUN details.
- Added the user configurable option to prevent halting boot process on UEFI driver health.
- Deprecated support Minimum Power mode.
- Fixed an issue where Arcconf was displaying the “Physical Block Size” as “Unknown” for the 16 KB physical block size drives
  - Root Cause: The 16 KB physical block size was not included in the macro and the display string which caused Arcconf to display the string as Unknown.
  - Fix: Added changes to include the 16 KB physical block size in the macro and the display string.
  - Risk: Low
- Fixed an issue where maxView was failing to upgrade or downgrade the expander firmware.
  - Root Cause: maxView was not passing the Expander Upgrade mode which caused the operation to fail.
  - Fix: Added changes to update the User Provided Mode property while passing the expander firmware upgrade parameters.
  - Risk: Low

2.2.4.2 Fixes and Enhancements for PLDM Release 6.20.8.0

This release includes the following fixes and enhancements:

- Updated the Redfish resource and annotation schema dictionaries to their latest version available in the DMTF 2022.2 schema bundle. The updated schema dictionary versions are as follows:
  - Annotations: v1.1.1 → v1.2.0

  - Drive: v1.14.0 → v1.15.0
  - Event: v1.7.0 → 1.7.1
  - Port: v1.6.0 → 1.7.0
  - StorageController: v1.5.0 → v1.6.0
  - Storage: v1.12.0 → v1.13.0
  - Volume: v1.6.2 → v1.8.0
- Added the following Redfish annotation to the Drive resource:
  - @Redfish.WriteableProperties - LocationIndicatorActive and/or WriteCacheEnabled will conditionally be added to this annotation array depending on support and validation conditions.
- The SensorId field in the GetPDR response for the individual drive temperature NumericSensor PDRs will now be set to the drive's Redfish resourceId.
- Added support for updating the SEP firmware through PLDM Type 5 commands.
  Note: Self-contained activation of the SEP firmware updates is not currently supported with this release.
- Fixed an issue where an UpdateComponent request for a drive will still be accepted with an invalid ComponentImageSize.
  - Symptom: When sending an UpdateComponent request with a ComponentImageSize larger than the specified allowed maximum for a drive, the response's ComponentCompatibilityResponse value is that the component can be updated when it cannot be updated.
  - Root Cause: No check in UpdateComponent for when a component image size is too large for a physical drive. The maximum component image size allowed for a drive is 16 MiB.
  - Fix: Added a component image size check for a physical drive in UpdateComponent.
  - Risk: Low
- Fixed an issue where DurableName associated with each LUN on a Multi-Actuator drive is published with incorrect values.
  - Symptom: Identifiers.DurableName for each LUN on a Multi-Actuator drive resource is the same.
  - Root Cause: The API which fetches DurableName for Multi-Actuator drives was working incorrectly.
  - Fix: Fixed the API that fetches DurableName for Multi-Actuator drives.
  - Risk: Low
- Fixed an issue where an incorrect extended error message was sent when attempting a SecureErase ACTION on a SED that is not in its OFS.
  - Symptom: Attempting the Drive.#SecureErase ACTION on a SED that is not in OFS will fail with the extended error message ActionNotSupported instead of the expected ResourceInUse.
  - Root Cause: A change in firmware behavior to strip support for the drive sanitize patterns from non-OFS SEDs' IDPD response caused a preemption of the non-OFS check in the SecureErase request validation code.
  - Fix: Added a check of SED status when no sanitize erase patterns are supported by the drive to help determine the most appropriate extended error to send.
  - Risk: Low
- Fixed an issue where the updateTime field in the GetPDRRepositoryInfo command response was not being updated correctly.
  - Symptom: The update time fields in the GetPDRRepoInfo response are empty.
  - Root Cause: The update time was not maintained by PLDM.
  - Fix: Added code to track the update time as well as fill in the update time fields in the response.
  - Risk: Low
- Fixed an issue where duplicate entries for an expander were seen in the Type 5 downstream device inventory.
  - Symptom: The value for the ‘Box’ portion of the ServiceLabel identifier for a Storage Enclosure Processor (SEP) is being reported incorrectly.
  - Root cause: The APIs that were being used to determine SEP location were designed primarily for use with drives instead of SEPs.
  - Fix: Modified the construction of the ServiceLabel identifier to use the appropriate APIs to fetch the Port and Box segments.

  - Risk: Low
- Fixed an issue where a DriveOffline Redfish alert is not sent when a Drive resource begins a sanitize operation.
  - Symptom: When a Drive resource is in the Predictive Failure state and the drive is undergoing a sanitize operation, a DrivePredictiveFailure alert is generated, but a DriveOffline alert is not generated.
  - Root Cause: When the drive is sanitizing, the logic to push a DriveOffline alert was not hit if the Drive resource is also in a Predictive Failure state.
  - Fix: Corrected the logic such that a DrivePredictiveFailure alert will be generated along with DriveOffline alert with a severity of OK.
    This fix also adds the following changes:
    - DrivePredictiveFailureCleared alert will now be generated along with a DriveOfflineCleared alert.
    - DriveOK alert will be now be generated along with DriveOffline alert with a severity of OK when the Drive's health changes from something other than OK to OK.
  - Risk: Medium
- Fixed an issue where incorrect CapabilitiesDuringUpdate flags were set for UBM PICs which do not support firmware updates.
  - Symptom: PLDM type 5 GetDownstreamFirmwareParameters command returns CapabilitiesDuringUpdate with CAN_BE_UPDATED bit set for UBM backplane PICs which cannot be updated.
  - Root Cause: There was no logic to check if the UBM PIC firmware can be updated or not when sending the response for the GetDownstreamFirmwareParameters command.
  - Fix: Added logic to return ComponentActivationMethods and CapabilitiesDuringUpdate to be ZERO when the UBM firmware PIC cannot be updated.
  - Risk: Low
- Fixed an issue where an unflashable SMP PSOC device was appearing in the Type 5 downstream device inventory.
  - Symptom: QueryDownstreamIdentifiers and the other associated Type 5 downstream device inventory commands erroneously return a device for the enclosure SEP with the device number 380 when this device number is reserved for an unflashable SMP PSOC.
  - Root Cause: The enclosure SEP enumeration did not have appropriate logic in place to filter out devices that were not of a type other than SEP.
  - Fix: Revised the SEP enumeration to not return device numbers that point to devices other than enclosure SEPs.
  - Risk: Low
- Fixed an issue where hot-removed SEPs could prevent other remaining SEPs from being included in the Type 5 downstream device inventory.
  - Symptom: The SEP inventory returned by the Type 5 downstream device inventory commands did not agree with the SEP count returned by the controller firmware.
  - Root Cause: Hot-removed SEPs persist in the controller firmware response as a zeroed slot. When this occurred at the beginning of the array in the firmware response, enumeration of any other SEP device numbers in the array was prevented.
  - Fix: Added logic to ignore zeroed entries in the firmware response when enumerating SEPs. This allows subsequent non-zero entries to be returned by the enumeration API.
  - Risk: Low
- Fixed an issue where a controller firmware update through PLDM fails if the final requested image segment is smaller than the spec-defined minimum transfer size.
  - Symptom: When updating controller firmware through PLDM Type 5, certain firmware images fail the image size validation check performed when the Type 5 State Machine is in the VERIFY state.
  - Root Cause: The RequestFirmwareData command used to download the firmware image data from the Update Agent has a minimum transfer size of 32 bytes. If the last transfer request needs less than this amount of image data, a padded transfer is requested so that 32 bytes of image + padding is received. In cases where this condition is met, an error in the calculation of the size of the last image transfer to the controller's collect buffer caused more data to be sent to the buffer than expected.
  - Fix: Corrected the calculation of the final collect buffer transfer size to correctly omit the final transfer padding.

- 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 5.91

This release includes the following firmware limitations:

- Receive Diagnostic command sent through out-of-band MCTP observes a fatal error for the Supported Diagnostic page and the Configuration Diagnostic page.
  - Workaround: None
- A reboot during a controller firmware update through PLDM can make the controller go offline.
  - Workaround:
    - Controller firmware flashing through other tools like Arcconf
    - Do not perform a reboot during the controller firmware flashing process through the PLDM path
- A firmware update causes the UART log buffer (Serial Output Buffer) to be reinitialized, since the DDR gets reinitialized.
  - Workaround: None
- Persistent Event Logs (PEL) will be cleared if,
  - 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.

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 2.6.2/Legacy BIOS Build 2.6.2

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 Limitations for Linux Driver Build 2.1.22-040

This release has the following Linux limitation:

- This release includes the following limitation when doing a driver injection (DUD) install. On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, SLES15SP3, OpenEuler 22.03LTS), the DUD install will hang if an attached drive (either HBA mode or logical drive) has Write Cache enabled.
  - Workaround: There are two workarounds for this issue:
    - Make sure the Write Cache is disabled for any attached drive.
    - For RHEL7.9/8.2/8.3 and OpenEuler 22.03LTS, add `rd.driver.blacklist=smartpqi` to the grub entry along with inst.dd.
- RHEL driver injection (DUD) install where OS ISO is mounted as virtual media on BMC based servers (non-ILO). Installer will hang after driver injection. Reported on RHEL 8.5, 8.6,9.0 and 9.1.
  - Workaround: There are two workarounds for this issue:
    - Load OS from USB device instead of virtual media.
    - Load OS from virtual media but initiation ISO verification (media test) during install followed by ESC to cancel media test.
- Oracle 9 UEK 7 kernel causes SmartPQI rpm dependency failures. This is an issue with how the kernel package was created by Oracle. Correct UEK7 kernel for Oracle 9 is expected in the mid-October UEK7 release, version number still pending.
  Note: This does not affect Oracle 8 UEK 7.
  - Workaround: Install the rpm using `--nodeps` when dependency failures occur.
    - For SmartPQI driver versions > 2.1.20-020 and UEK7 kernels >= 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm will install normally.
    - For UEK7 kernels < 5.15.0-3.60.2.el9uek.x86_64, install the SmartPQI rpm using the `--nodeps`.
- On AMD/RHEL 7.9 systems, the system might panic due to a bug in the IOMMU module. For details, see https://lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/
  - Workaround: Disable the IOMMU setting option in BIOS.
- 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), user is 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 1010.64.0.1037

This release includes the following limitation:

- In certain circumstances, the installation may fail on Windows Server 2016 and Windows 2012 R2 after selecting drives.

- Workaround: Follow these steps to ensure drives are clean and all partitions are removed before beginning a new installation:
  a. Hit Shift + F10 to open command prompt
  b. Type `Diskpart`
  c. Type `List Disk`
  d. Select the disk you want to clean. For example, to select Disk 0 type `select disk 0`.
  e. Type `Clean`

2.3.4.3 Limitations for FreeBSD Driver Build 4390.0.1010

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 4440.0.124

This release includes the following limitations:

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

2.3.5 Management Software Limitations

2.3.5.1 Limitations for Arcconf/maxView Build 4.11.00.25823

There are no known limitations for this release.

2.3.5.2 Limitations for PLDM Release 6.20.8.0

There are no known limitations for this release.

2.3.6 Hardware Limitations

This release includes the following hardware limitations:

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

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

3. Updating the Controller Firmware

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

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

3.1 Updating the Controller Firmware

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

Note:

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

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

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

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

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

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

1. **Mandatory:** Flash the target with the provided “SmartFWx100.bin" image with arcconf/maxView software.
   – If the arcconf/maxView software becomes unresponsive or hangs then power cycle the system to recover and refer to firmware limitation section 2.3.2.2. Limitations for Firmware Release 1.32 Build 0.
2. **Mandatory:** If flashing completes, use the OS shutdown/restart operation to gracefully reboot the system to complete the firmware update process.

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

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

1. **Mandatory:** Flash the controller with the provided “SmartFWx100_ v1.29_b314.bin" image with arcconf/maxView software.
2. **Mandatory:** Reboot the system to refresh all components**.**
3. **Mandatory**: Flash the target with the provided " SmartFWx100.bin" image with arcconf/maxView software.
4. **Mandatory**: Use the OS shutdown/restart operation to gracefully reboot the system to complete the firmware update process.

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

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

4. Installing the Drivers

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

5. Revision History

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

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

Microchip Information

The Microchip Website

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

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

Product Change Notification Service

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

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

Customer Support

Users of Microchip products can receive assistance through several channels:

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

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

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

Microchip Devices Code Protection Feature

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

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

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded

by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

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

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

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

Trademarks

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

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

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

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

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

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

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

ISBN: 978-1-6683-2135-5

Quality Management System

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

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 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	**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	**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	**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