HBA 1100 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	2.9.0
Package Release Date	July 20, 2024
Firmware Version	7.11 B0[1]
UEFI Driver Version	2.14.4
Legacy BIOS	2.14.2
Driver Versions	Windows SmartPQI: • Windows Server 2019/2022: 1010.108.0.1015 • Windows 10/11: 1010.108.0.1015 Linux SmartPQI: • RHEL 7/8/9: 2.1.30-031 • SLES 12/15: 2.1.30-031 • Ubuntu 20/22/24: 2.1.30-031 • Debian 11/12: 2.1.30-031 • Oracle Linux 7/8/9: 2.1.30-031 • Citrix XenServer 8: 2.1.30-031 • BC Linux 7: 2.1.30-031 • OpenEuler 20/22: 2.1.30-031 VMware SmartPQI: • VMware 7.0/8.0: 4672.0.104 FreeBSD SmartPQI: • FreeBSD 13/14: 4540.0.1005
arcconf/maxView™	4.18.00.26842
PLDM	6.40.6.0

Note:

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".

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 and Server 2019 Windows 10 (version 22H2) and 11 (version 23H2)	SmartPqi.sys	x64
	SmartPqi.inf	x64
	smartpqi.cat	x64

Table 1-5. Linux SmartPQI Drivers for Arm

Drivers	Version
Red Hat Enterprise Linux 9.4, 8.10	Arm®
SuSE Linux Enterprise Server 12 SP5	Arm
SuSE Linux Enterprise Server 15 SP6[1], SP5, SP4	Arm
Ubuntu 24.04, 22.04.4, 20.04.5	Arm
BC Linux 7.7	Arm
OpenEuler 20.03 SP4 LTS, 22.03 SP3 LTS	Arm

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

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

Drivers	Version
Red Hat Enterprise Linux 9.4, 9.3, 8.10, 8.9, 8.8, 7.9	x86_64
SuSE Linux Enterprise Server 12, SP5	x86_64
SuSE Linux Enterprise Server 15 SP6[1], SP5, SP4	x86_64
Oracle Linux 7.9 UEK6U3	x86_64
Oracle Linux 9.4, 9.3, 8.9, 8.8 UEK7U2	x86_64
Ubuntu 24.04, 22.04.4, 22.04.3, 22.04	x86_64

.....continued	
Drivers	**Version**
Ubuntu 20.04.6, 20.04.5, 20.04	x86_64
Debian 12.5, 11.9	x86_64
Citrix xenServer 8.2.1	x86_64
Fedora 39 (inbox only)	x86_64
OpenEuler 20.03 SP4 LTS	x86_64
OpenEuler 22.03 SP3 LTS	x86_64
SLE-Micro 6.0, 5.5 (Inbox only)	x86_64

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

Table 1-7. FreeBSD and VMware SmartPQI Drivers

Drivers	Version
FreeBSD 14, 13.3	x64
VMware 8.0 U2/U1, 7.0 U3/U2	x64
VMware 8.0 U3 (Inbox only)[1]	x64

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

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 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 highlights major features supported by each Solutions Release.

Table 2-1. Feature Summary

Feature		Supported Release
Arcconf command to check Nand and NOR Flash type		2.9.0
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
4Kn, 512e and 512n Support		2.3.0
Legacy Boot Support		2.3.0
UEFI Driver, Boot Support		2.3.0

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 7.11

This release includes the following fixes and enhancements:

- Added RDE Drive Form Factor support for SAS/SATA.
- Added support for saving Managed SED master key and reset key in cipher text in controller NVRAM instead of clear text.
- Changed temperature polling period from 1 minute to 5 minutes for HBA mode drives that are in low power state.
- Added support for additional I/O stats in controller serial logs when a LUN reset occurred.
- Fixed an issue where foreign drives do not get imported when Managed SED change key is processed during system shutdown.
  - Root Cause:
    i. Admin rights are changed on the drive but datastore of the drive is not updated since the drive has failed the commands during system shutdown. During the subsequent boot, the drive is marked as foreign.

    ii. Some admin rights are changed and some are not since the drives have failed the commands during system shutdown. During the subsequent boot, the drives are marked as foreign.

  - Fix:
    i. During import, when unlock fails with the key provided by the user, use existing master key to unlock the drive.
    ii. During import, when change pin fails as authentication error with the old key provided by the user, attempt to authenticate with the new key provided by the user.
  - Risk: Low

- Fixed an issue where failed drive was reported as bay 255 in event logs.
  - Root Cause: Event was being logged before drive bay was discovered correctly.
  - Fix: Log event after drive bay is read properly.
  - Risk: Low
- Fixed possible lockup issue while hot plugging an enclosure from one connector port to another.
  - Root Cause: Deadlock scenario occurs where a command is frozen and is being sent to enclosure but another thread is waiting for this command to be sent.
  - Fix: Skip sending command to a frozen enclosure (when it is hot removed).
  - Risk: Medium
- Fixed an issue where server is taking more time to boot into OS and unable to perform any controller operation in presence of ATA Locked drive.
  - Root Cause: Server bootup was taking time when controllers are directly attached to a ATA Locked SATA drive. Controller firmware had an issue in dispatching the next queued command to the drive while processing Error D2H response from the drive and the same sequence is repeated for a long time that caused time out for one of the SCSI ATA passthrough requests. The "*Byte 0, bits 4: 0 of NCQ error log _info*" issue from the RLE response was not correct (that is, set to 0x80) even for all the NCQ tags 0-31 that received an error D2H response from the drive.
  - Fix: Modified firmware to send an errored SCSI response for those SCSI requests which are supposed to be aborted by the drive when it's in a ATA Locked drive. Preserve the failed Receive FPDMA Queued request at "`dev_ptr->failed_request`" before sending the RLE request to the drive as part of NCQ error handling. So that the SCSI check condition response will be sent for the failed request after the RLE command was getting processed successfully.
  - Risk: Low (Only with SATA Locked Drive)
- Fixed an issue where controller lockup with code=0x00001=No module.
  - Root Cause: When an Uncorrectable ECC occurred at a particular address with 64-bit address, its firmware handler reads higher address word from wrong location which resulted in fatal assert without proper lockup or recovery path.
  - Fix: Updated firmware to read the correct higher address word when processing the Uncorrectable ECC error to execute recovery or lockup handling rather than asserting when reading the wrong address.
    Risk: Low
- Fixed an issue where rediscovery is triggered after BME is enabled even if the channel is already discovered.
  - Root Cause: When BME is enabled for the first time, firmware requests MCTP rediscovery, even if it had already responded to any initial discovery messages.
  - Fix: Add option to ignore rediscovery requests for channels where discovery has already happened.

  - Risk: Low
- Fixed an issue where controller lockup with code=0x3D037=MSGU.
  - Root Cause: The controller internal RAM is only partially initialized for PCIE physical function 0 and virtual function 0. A read access to an uninitialized address may cause an ECC error and lead to a firmware lockup.
  - Fix: Initialize memory for the entire scratchpad areas and the ATU configuration table, including the unused physical function1, to initialize ECC for all addresses during MSGU PQI initialization sequence.
  - Risk: Low
- Fixed an issue where the device ready timeout is increased from 10s to 45s after reset.
  - Root Cause: Some large capacity SATA drives (4-8 TB) takes upto 30s to recover after a reset. Large capacity SATA drives would be marked as failed in some cases as they had not recovered in the 10s allowed by firmware before drive recovery.
  - Fix: Increased link reset time for SATA drives from 10s to 45s. The link reset time for SAS drives remains at 10s.
  - Risk: Medium
- Fixed an issue controller lockup with code=0x01ABD.
  - Root Cause: A SATA loss of signal condition causes a target reset. As a result SCSI-ATA-Translation requires that on ATA reset other than due to a TM function, the translation layer must terminate processing of all commands for each unit affected by the reset and establish a unit attention condition. Previously, if connection with a SATA drive was re-established during LOS recovery processing the firmware would not terminate processing of all commands.
  - Fix: Terminate processing of all commands on LOS recovery of SATA device.
  - 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 2.14.4/Legacy BIOS 2.14.2

This release includes the following UEFI fixes and enhancements:

- Added an enhancement to show drive write cache status as unknown when it is not configurable. The HII disk information will show the drive write cache status as unknown when it detects configuring write cache as not supported.
- Fixed an issue where the Managed SED Unlock Controller password in driver health form is not shown when lockout period is reset.
  - Root Cause: The unlock option in driver health menu for remote mode Managed SED controller password remains disabled even when the lockout timer is expired or reset.
  - Fix: Always show the unlock option if controller is waiting for password input. Error message will be shown after the attempt, if there is a password lockout period.
  - Risk: Low
- Fixed an issue where the driver health form shows the Managed SED controller locked message even after successful unlock.
  - Root Cause: Driver health form content is not updated if controller is unlocked successfully.
  - Fix: Refresh the driver health form with applicable messages after the controller unlock operation.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.30-031

This release includes the following fixes and enhancements.

- Fixed an issue where during the processing of a TMF on a device, the driver is stuck while waiting for I/O to be drained from the driver's internal request queue.
  - Root Cause: During heavy I/O load, a data path request on a particular device is added to the driver's request list but encounters a conditional check where it needs more elements than are currently free in the inbound queue on a particular queue group. This request remains in the request list until the request submission function is triggered by the IRQ handler, but unfortunately no completions arrive on that queue group for a significantly long period of time. During the same time, a LUN reset is triggered on another device. While processing the TMF on the other device, attempts are made to fail I/Os queued on the device undergoing reset. However, I/Os queued on other devices are not failed due to the TMF condition check. Because of the stuck command in the request list and the failure to fail I/O on the other devices, the system experiences a LUN reset and system hang.
  - Fix: For devices which are not undergoing reset, return DID_REQUEUE and complete the requests that are stuck in the driver's internal request queue. This adds the request back to the mid-layer queue, ensuring that it is resubmitted after a short period without decrementing the retry count in the OS SCSI-mid-layer.
  - Risk: Low

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4540.0.1005

There are no known fixes for this release.

2.2.3.3 Fixes and Enhancements for Windows® Driver Build 1010.108.0.1015

There are no known fixes for this release.

2.2.3.4 Fixes and Enhancements for VMware Driver Build 4672.0.104

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 4.18.00.26842

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

- Added support to display the NAND and NOR Flash type as part of the controller properties in the Arcconf and the maxView.
- Fixed an issue where the arcconf was not displaying the "Task" command help for the HBA controller
  - Root Cause: Because of the HBA controller check for the arcconf help menu in the task command, "Task" was missing from the arcconf help menu for the HBA controller.
  - Fix: Changes added to display "Task" in the arcconf help menu for the HBA controller.
  - Risk: Low
- Fixed an issue where the maxView was displaying a cache error alert for a controller which doesn't support controller cache.
  - Root Cause: maxView didn't check the "FeatCacheSupport" feature bit before enabling show device alert for controllers that don't support controller cache and have logical devices.
  - Fix: Added a feature bit check "FeatCacheSupport" before generating the device alert for the controllers that don’t support the controller cache and have logical devices.
  - Risk: Low
- Fixed an issue where the maxView was not displaying the system name consistently across the reboot.

  - Root Cause: Usually, the Redfish server starts first, followed by the maxView webserver and subscribes to events with the configured hostname. This hostname will be added to maxView events. If the maxView web server starts before the Redfish server, maxView webserver tries to subscribe to events from the Redfish server using the loopback hostname 'localhost'. Here, the server is configured with the hostname 'localhost.localdomain', which will be used for event subscription under normal scenario when the Redfish server starts first, followed by the maxView webserver. If the maxView webserver starts first, it takes the loopback hostname 'localhost'. Due to this, two different hostnames are present in the events.
  - Fix: The code change has been made to always use the configured hostname for event subscription. The configured hostname will be used to subscribe to events if the Redfish server starts first. If the maxView web server starts first, it will attempt to subscribe to events using the configured hostname instead of 'localhost'. If, even after retrying for 20 seconds, it is not able to connect to the Redfish server using the configured hostname, then the maxView web server will attempt to establish a connection with the Redfish server using 'localhost'.
  - Risk: Low
- Fixed an issue where the maxView installer was setting the write permissions for the .txt files in the installation folder.
  - Root Cause: maxView installer was setting the write permissions for the .txt files in the installation folder.
  - Fix: Removed the write permissions for the .txt files in the installation folder and provided only the read-only permissions for these .txt files.
  - Risk: Low
- Fixed an issue where the maxView was not displaying a warning message when the Redfish server is connected through loopback network address.
  - Root Cause: maxView was not displaying a warning message when the Redfish server is connected through loopback network address.
  - Fix: Added a warning message tooltip on the IP Address attribute when Redfish server is connected through loopback network address
  - Risk: Low

2.2.4.2 Fixes and Enhancements for PLDM Release 6.40.6.0

This release includes the following fixes and enhancements:

- Added PLDM Type 6 support for Redfish Chassis for UBM Backplanes. This feature adds representation of UBM backplanes and their contained drives using Redfish resources and PDRs.
- Added PLDM Type 6 Redfish Resource:
  - UBM Chassis resource
    - It represents a single physical UBM backplane.
    - PLDM Type 6 RDE READ and HEAD operations are supported.
  - UBM Attached Drive resource
    - Will represented a single physical Drive attached to a UBM.
    - PLDM Type 6 RDE READ, UPDATE, UPDATE and HEAD operations are supported.
  - DriveCollection Resource
    - Will be the lone subordinate of a UBM Chassis resource.
    - Will publish properties as per the Redfish DriveCollection schema
    - PLDM Type 6 RDE READ and HEAD operations are supported
  - Absent Drive resource

    - Will represent a single drive bay of a UBM.
    - PLDM Type 6 RDE READ and HEAD operations are supported.
- PLDM Type 2 Command Changes:
  - GetPDR will now retrieve additional Drive and DriveCollection Redfish PDRs for each attached UBM.
  - Drive and DriveCollection Redfish PDRs will be static and will not generate PDR Change/Add/Modified alerts.
- Add Descriptor Type 0xFFFF for All Devices in Downstream Device ID Record PLDM Type 5 QueryDownstreamIdentifiers command response for downstream drives will now publish a Vendor Defined Descriptor which holds the ServiceLabel in the following format: `Slot=<Slot#>:Port=<Port#>:Box=<Box#>:Bay=<Bay#>`
- PLDM Type 6 Add Drive.FirmwareVersion support for RDE READs on Drive resources
  - RDE READ on a Drive resource will now publish FirmwareVersion property. The FirmwareVersion property will have the same value as the Revision property.
- Added PLDM Type 6 READ support for StorageController.Links.PCIeFunction. RDE READ on the StorageController resource will now publish the following properties:
  - Links.PCIeFunctions@odata.count
  - Links.PCIeFunctions@odata.id

  This property gets published as a deferred binding string of %PF0, where 0 is the PCIe Function of the controller.
- Updated permission flags on resources if operation cannot be performed. The PermissionFlags returned for an RDE operation have been brought into accordance with the PLDM Type 6 specification.
  - RDE READ and HEAD operations will return non-zero PermissionFlags in the response.
  - Operations failing with ERROR_NOT_ALLOWED will have a response with non-zero PermissionFlags.
  - All other operations and failures will result in PermissionFlags of 0x00 in the response.
- Added support for Drive.SlotCapableProtocols. This property will contain the drive protocols that are supported in the slot being read. It will now be published as part of the RDE READ response on all Drive resources, including those representing empty UBM bays. The following values are supported:
  - SAS
  - SATA
  - NVMe

  The Drive.SlotCapableProtocols property will be published as an array containing some or all of the above values depending on hardware specifications. If no protocols are supported, then an empty array will still be published.
- Added PLDM Type 6 READ Support for Drive.DriveFormFactor. RDE READ on a SAS/SATA Drive resource will now include the property DriveFormFactor in the response. The following values are supported:
  - Drive2_5
  - Drive3_5
  - M2

  For NVMe drives and all SAS and SATA drives with a form factor not listed above, the Drive.DriveFormFactor property will not be published.

- Added DriveMetrics support for all controllers, which allows reporting of some basic drive performance statistics information.
- Added PLDM Type 6 Redfish DriveMetrics Resource
  - Each DriveMetrics resource will be mapped to a single Drive resource.
  - PLDM Type 6 RDE READ and HEAD operations are supported.
- Updated RDE READ on Drive resources to add the Metrics property which will hold a link to the Drive's related DriveMetrics resource.
- PLDM Type 2 Command Changes
  - GetPDR will now retrieve additional DriveMetrics Redfish Resource PDRs for each Drive Resource.
    - DriveMetrics Redfish Resource PDRs will generate PDRRepoChange events and the PDRs will be added and deleted as drives are hot-plugged and hot-removed.
    - The GetSchemaURI and GetSchemaDictionary commands can fetch information related to the new DriveMetrics resource schema dictionary.
- Added support for StorageController.AssetTag to allow Redfish clients to assign an asset tag string to a StorageController resource which will persist across boot cycles.
- Added the RDE READ operation support for Drive resources which represent a Revertible (that is, shareable) spare drive.
- Fixed an issue where `NegotiateTransferParameters` command allows requester part size that is not a power of two.
  - Root Cause: While issuing NegotiateTransferParameters command with requester part size that is not a power of two, the command returns success instead of ERROR_INVALID_DATA. A code mistake caused only the first byte of the requester part size to be checked for power of two requirement.
  - Fix: Modified the code so that requester part size will be checked properly.
  - Risk: Low
- Fixed an issue where there are missing fields in `FileDescriptorPDR` for crash dump log.
  - Root Cause: The `FileDescriptorPDR` is missing the `SuperiorDirectoryFileIdentifier` and `FileMaximumFileDescriptorCount` fields.
  - Fix: Added the `SuperiorDirectoryFileIdentifier` and `FileMaximumFileDescriptorCount` fields to the crash dump log's `FileDescriptorPDR` to be in compliance with the PLDM Type 2 specification.
  - Risk: Low
- Fixed an issue where the `CacheSummary.Status.State` property in the `StorageController` resource is published as "Disabled" when the cache is not supported on the controller.
  - Root Cause: The case of the controller cache not being supported was not being directly handled when encoding the `StorageController` resource.
  - Fix: The `CacheSummary` health and state will be set to OK and absent, respectively, when the controller cache is not supported.
  - Risk: Low
- Fixed an issue where `OperationExecutionFlags` is incorrect in the `RDEOperationStatus` response for a completed operation.
  - Root Cause: When an operation status is completed, the `OperationExecutionFlags` should not have the `HaveResultPayload` or the `HaveCustomResponseParameters` bits set. A previous change that updated the response handler for the `RDEOperationStatus` command to properly set the `OperationExecutionFlags` bits based on the actual current

state of the operation exposed that `OperationExecutionFlags` bits were not properly being reported.
  - Fix: Unset the `HaveResultPayload` and `HaveCustomResponseParameters` bits in `OperationExecutionFlags` for completed RDE operations.
  - Risk: Low
- Fixed an issue where the controller serial log contains repeated prints related to an error with handling a `GetSchemaDictionary` request.
  - Root Cause: The request was being sent to fetch the registry schema class dictionary for various Redfish resources, but this dictionary is not supported. The response completion code is erroneously being set to ERROR_INVALID_DATA instead of ERROR_UNSUPPORTED as directed in the PLDM Type 6 specification.
  - Fix: Modified the `GetSchemaDictionary` and `GetSchemaURI` command handler functions to return ERROR_UNSUPPORTED if the registry schema class is passed in the request.
  - Risk: Low
- Fixed an issue where a `GetSensorReading` request with the `rearmEventState` option set for the version state sensor did not move the version state sensor presentState or previousState to normal.
  - Root Cause: The `rearmEventState` option was not being accounted for when a controller flash was detected.
  - Fix: If a controller flash is detected, the `rearmEventState` option will be considered when processing a `GetSensorReading` request.
  - Risk: Low
- Fixed an issue where on certain controllers, `GetSensorReading` on a `NumericSensor` of EntityType DEVICE_FILE returns an error completion code of INVALID_SENSOR_ID.
  - Root Cause: The logic that validates the requested `SensorId` from the `GetSensorReading` request was incorrectly returning that the `SensorId` is not valid on controllers that do not support individual drive temperature numeric sensors.
  - Fix: Corrected the logic to validate the requested `SensorId` regardless of whether or not the controllers support individual drive numeric sensors.
  - Risk: Low
- Fixed an issue when RDE UPDATE on a SED HBA volume resource to take ownership of the SED or to revert a SED fails.
  - Root Cause: Controller firmware requires more than 6 seconds to take ownership or revert a SED. The time needed by controller firmware is more than PLDM's allowed response time and hence the RDE UPDATE operation fails.
  - Fix: The following changes have been made:
    - RDE UPDATE on a SED HBA volume resource will now be performed by a long running task.
    - If the MC has not negotiated TASK support by using RDENegotiateRedfishParameters command, RDE UPDATE on a SED HBA volume will return a completion code of ERROR_NOT_ALLOWED.
  - Risk: Medium
- Fixed an issue where the StorageController.Status.State property would not be 'Updating' when controller firmware had been flashed and was pending activation.
  - Root Cause: When encoding the StorageController.Status.State property, no check was made for the presence of controller firmware pending activation.

  - Fix: The presence of controller firmware pending activation is now considered when encoding StorageController.Status.State. The StorageController.Status.State property will be 'Updating' if pending controller firmware is present.
  - 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 7.11

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 from firmware version 7.11 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.

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 2.14.4/Legacy BIOS Build 2.14.2

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 Limitations for Linux Driver Build 2.1.30-031

This release includes the following limitations:

- SL-Micro 6.0 fails to boot after installation on 4Kn drives.
  - Workaround: This is a SUSE issue and only workaround is to use non-4Kn drives.
- 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.
- 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 1010.108.0.1015

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 the 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`
- 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 4540.0.1005

This release contains the following limitations:

- FreeBSD 13.2 and later OS installations will fail with the out of box driver.
  - Workaround: Install with inbox driver then update to latest.

2.3.4.4 Limitations for VMware Driver Build 4672.0.104

There are no known limitations for this release.

2.3.5 Management Software Limitations

2.3.5.1 Limitations for Arcconf/maxView Build 4.18.00.26842

There are no known limitations for this release.

2.3.5.2 Limitations for PLDM Release 6.40.6.0

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 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.
- When downgrading firmware, there may be cases when newer hardware is not supported by an older version of firmware. In these cases, attempting to downgrade firmware will be prevented (fail). It is recommended to regularly qualify newer firmware versions, to ensure that newer hardware is supported in your system(s).

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
N	07/2024	SR 2.9.0 Production Release.
M	03/2024	SR 2.8.4 Production Release.
L	12/2023	SR 2.8.0 Patch Release with maxView version B26068
K	11/2023	SR 2.7.0 Patch Release with maxView version B25339
J	11/2023	SR 2.8.2 Production Release
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 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, 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.

ISBN: 978-1-6683-4975-5

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	**Australia - Sydney** Tel: 61-2-9868-6733	**India - Bangalore** Tel: 91-80-3090-4444	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393
Atlanta Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455	**China - Beijing** Tel: 86-10-8569-7000	**India - New Delhi** Tel: 91-11-4160-8631	**Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829
Austin, TX Tel: 512-257-3370	**China - Chengdu** Tel: 86-28-8665-5511	**India - Pune** Tel: 91-20-4121-0141	**Finland - Espoo** Tel: 358-9-4520-820
Boston Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088	**China - Chongqing** Tel: 86-23-8980-9588	**Japan - Osaka** Tel: 81-6-6152-7160	**France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79
Chicago Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075	**China - Dongguan** Tel: 86-769-8702-9880	**Japan - Tokyo** Tel: 81-3-6880- 3770	**Germany - Garching** Tel: 49-8931-9700
Dallas Addison, TX Tel: 972-818-7423 Fax: 972-818-2924	**China - Guangzhou** Tel: 86-20-8755-8029	**Korea - Daegu** Tel: 82-53-744-4301	**Germany - Haan** Tel: 49-2129-3766400
Detroit Novi, MI Tel: 248-848-4000	**China - Hangzhou** Tel: 86-571-8792-8115	**Korea - Seoul** Tel: 82-2-554-7200	**Germany - Heilbronn** Tel: 49-7131-72400
Houston, TX Tel: 281-894-5983	**China - Hong Kong SAR** Tel: 852-2943-5100	**Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906	**Germany - Karlsruhe** Tel: 49-721-625370
Indianapolis Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380	**China - Nanjing** Tel: 86-25-8473-2460	**Malaysia - Penang** Tel: 60-4-227-8870	**Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44
Los Angeles Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800	**China - Qingdao** Tel: 86-532-8502-7355	**Philippines - Manila** Tel: 63-2-634-9065	**Germany - Rosenheim** Tel: 49-8031-354-560
Raleigh, NC Tel: 919-844-7510	**China - Shanghai** Tel: 86-21-3326-8000	**Singapore** Tel: 65-6334-8870	**Israel - Hod Hasharon** Tel: 972-9-775-5100
New York, NY Tel: 631-435-6000	**China - Shenyang** Tel: 86-24-2334-2829	**Taiwan - Hsin Chu** Tel: 886-3-577-8366	**Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781
San Jose, CA Tel: 408-735-9110 Tel: 408-436-4270	**China - Shenzhen** Tel: 86-755-8864-2200	**Taiwan - Kaohsiung** Tel: 886-7-213-7830	**Italy - Padova** Tel: 39-049-7625286
Canada - Toronto Tel: 905-695-1980 Fax: 905-695-2078	**China - Suzhou** Tel: 86-186-6233-1526	**Taiwan - Taipei** Tel: 886-2-2508-8600	**Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340
	China - Wuhan Tel: 86-27-5980-5300	**Thailand - Bangkok** Tel: 66-2-694-1351	**Norway - Trondheim** Tel: 47-72884388
	China - Xian Tel: 86-29-8833-7252	**Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Poland - Warsaw** Tel: 48-22-3325737
	China - Xiamen Tel: 86-592-2388138		**Romania - Bucharest** Tel: 40-21-407-87-50
	China - Zhuhai Tel: 86-756-3210040		**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