HBA 1100 Software/Firmware Release Notes

© 2023 Microchip Technology Inc. and its subsidiaries

Table of Contents

1. About This Release....3
   - 1.1. Release Identification....3
   - 1.2. Components and Documents Included in this Release....3
   - 1.3. Files Included in this Release....3
2. What's New?....6
   - 2.1. Features....6
   - 2.2. Fixes....6
   - 2.3. Limitations....13
3. Updating the Controller Firmware....17
   - 3.1. Updating the Controller Firmware....17
4. Installing the Drivers....19
5. Revision History....20

Microchip Information....21
- The Microchip Website....21
- Product Change Notification Service....21
- Customer Support....21
- Microchip Devices Code Protection Feature....21
- Legal Notice....21
- Trademarks....22
- Quality Management System....23
- Worldwide Sales and Service....24

© 2023 Microchip Technology Inc. and its subsidiaries

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	2.8.0
Package Release Date	December 15, 2023
Firmware Version	6.22[1, 2]
UEFI Version	2.8.3
Legacy BIOS	2.8.2
Driver Versions	Windows SmartPQI: • Windows Server 2016/2019/2022: 1010.74.0.1020 • Windows 10/11: 1010.74.0.1020 Linux SmartPQI: • RHEL 7/8/9: 2.1.24-046 • SLES 12/15: 2.1.24-046 • Ubuntu 18/20/22: 2.1.24-046 • Debian 10/11: 2.1.24-046 • Oracle Linux 7/8/9: 2.1.24-046 • Citrix XenServer 8: 2.1.24-046 • BC Linux 7.7: 2.1.24-046 • OpenEuler 20.03/22.03: 2.1.24-046 VMware SmartPQI: • VMware 7.0/8.0: 4530.0.104 FreeBSD SmartPQI: • FreeBSD 12/13: 4410.0.1005
arcconf/maxView™	4.14.00.26068
PLDM	6.25.9.0

Notes:

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

1.2 Components and Documents Included in this Release

Download the firmware, drivers, host management software, and supporting documentation for your 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:

© 2023 Microchip Technology Inc. and its subsidiaries

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 9.2[1], 9.1, 9.0[2], 8.8[1], 8.7, 8.6, 8.5, 7.9	x64
SuSE Linux Enterprise Server 12 SP5, SP4	x64
SuSE Linux Enterprise Server 15 SP5[1], SP4, SP3, SP2	x64
Oracle Linux 7.9 UEK6U3	x64
Oracle Linux 9.2[1], 9.1, 9.0, 8.8[1], 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	x64
Debian 11.6, 10.13	x64
Citrix xenServer 8.2.1, 8.1, 8.0	x64
Fedora 38 (inbox only)	x64

Notes:

1. New OS support—minimally tested drivers in this release. Fully supported drivers are expected in the next release
2. Support based off August 2022 RHEL 9.0 ISO refresh.

© 2023 Microchip Technology Inc. and its subsidiaries

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 SP1 LTS	X

Table 1-7. FreeBSD and VMware SmartPQI Drivers

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

Host Management Software

Table 1-8. Host Management Utilities

Description	OS	Executable
ARCCONF Command Line Utility	Windows® x64 Linux® x64 VMware 7.0 and above XenServer FreeBSD x64 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.

© 2023 Microchip Technology Inc. and its subsidiaries

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	
Remote Key Management		X	

2.2 Fixes

2.2.1 Firmware Fixes

2.2.1.1 Fixes and Enhancements for Firmware Release 6.22

This release includes the following fixes and enhancements:

- Added support for Remote Key Management of Managed SED.
- Added support for 256 bytes Key Management Service (KMS) key identifier.
- Added support for a redundant copy of controller settings data.
- Added support to improve flash interoperability with UBM backplanes.
- Fixed an issue where the controller firmware flashed event has random characters at the end of the event message.
  - Root Cause: When logging the event, a local variable that saves the active firmware image is used without being initialized. The variable is a two byte array. The first byte is used to save "A" or "B", firmware image version. The second byte is expected to be 0 and is used at the end of the event message. Since the array is not initialized, "A" or "B" is not null terminated causing random characters to appear at the end of the event message.
  - Fix: Initialize the local variable before using it.
  - Risk: Low
- Fixed an issue where taking the ownership of enterprise drive was failing on boot after panic shutdown.

© 2023 Microchip Technology Inc. and its subsidiaries

  - Root Cause: Changing a master key causes several SED authorities to also change to the new key. The SED flow requires an open session, perform an SED task, and an end session. During this flow, if the controller encounters a panic shutdown, but the SED drives do not encounter a power cycle, then the SED drives are left in the middle of the flow waiting for the session to end. When the controller restarts and attempts to start a new session to validate the datastore on the SED, a start session failure occurs.
  - Fix: Error recovery is added to retry the start session.
  - Risk: Low

- Fixed a issue where firmware Lockup is observed after hot removing an SES device while LUN reset to the device is in progress.
  - Root Cause: While processing host issued LUN reset to the device and if the device is hot removed, LUN reset task management is completed and cleared from the management list for the device. Lockup is observed when firmware attempts to clear LUN reset task management again for the removed device.
  - Fix: Before issuing reset to the device, if device does not exist and LUN reset task management is not present in the list, then the reset request is already cleared and so the firmware should not attempt to clear it again.
  - Risk: Low

- Fixed an issue for Managed SED in Local Key Management (LKM) mode where firmware allows to import the foreign SED while the adapter password is not received yet.
  - Root Cause: Firmware does not check for the received adapter password while processing the request to import a foreign SED. Firmware should fail the request if the adapter password is not provided as the master key is not available until the adapter password is provided. Without the master key, importing a foreign SED cannot be performed.
  - Fix: Firmware will check if the adapter password is not received then fail the request.
  - Risk: Low

- Fixed an issue where the I/O latency value is not as expected for NCQ priority SMR drives.
  - Root Cause: The RAID path did not have support for NCQ priority commands.
  - Fix: Added the support for priority bits in message derived from driver and propagate to lower layer firmware interface.
  - Risk: Low

- Fixed an issue that firmware fails to capture vendor specific expander logs.
  - Root Cause: This is caused by a code change that firmware relies on driver to provide data transaction direction. Linux SCSI layer is providing direction as data-out instead of data-in. This failed in CentOS 7.9 but passed in RHEL 9.1. This kind of incompatibility happened among various flavor of Linux if we depend on driver for data transaction direction.
  - Fix: For T10 supported commands like inquiry, firmware doesn't depend on the driver for data transfer direction. It sets it according to T10 specification. The fix is that now firmware sets data transfer direction as data-in for the read expander log only based on WDC OEM specification, and not relies on driver's input.
  - Risk: Low

- Fixed an issue where the slot number is shown as unknown for a failed physical drive present in SES supported enclosure.
  - Root Cause: The SCSI Enclosure Services (SES) supported enclosure will provide multiple additional status pages(0Ah), which consist of each physical drive's information such as the device type, WWN or SAS address, slot number and so on. This additional status page data will be compared against the controller-detected enclosure-specific data. On a successful

© 2023 Microchip Technology Inc. and its subsidiaries

comparison, the firmware will assign the slot number for the physical drive. For a failed physical drive, the WWN or SAS address comparison failed and resulted in firmware skipping the slot number assignment.

  - Fix: If the physical drive is detected by the controller and WWN or SAS address comparison failed, then compare the device slot number. If it matches, assign the slot number to the physical drive.
  - Risk: Low

- Fixed an issue where the LED blink for SES enclosure physical drives was incorrect after hot adding the SES enclosure.
  - Root Cause: When the SES expander cable is hot-plugged, firmware is prematurely setting up the SES index format as 0-based. This led to firmware skipping the use of Additional status page(0Ah) information for the physical drives present in the expander and using the 0-based indexing for the physical drives, causing the misalignment in the SES indices and incorrect LED to blink.
  - Fix: Set the SES index format only when the firmware finds the first present drive with an invalid slot number.
  - Risk: Low
- Fixed an issue where the foreign unconfigured SED is not exposed to the OS after import.
  - Root Cause: If any foreign unconfigured SED is connected to the controller, the controller firmware will fail to access the RAID metadata region of the SED, as it's locked. The controller firmware will not expose this foreign SED to OS until it gets unlocked to avoid any operations on the SED. While importing the foreign SED, firmware does not try to access the RAID metadata region and is not exposing the SED to the host.
  - Fix: Firmware will access the RAID metadata region of the SED while importing. If the read is successful, the firmware will expose the SED to the host.
  - Risk: Low
- Fixed an issue where MCTP over PCIe VDM is disabled while disabling VDM notification.
  - Root Cause: Initialization of MCTP over PCIe VDM and VDM discovery notification enable/disable settings are always handled together by the firmware. So whenever VDM discovery notification is disabled, MCTP over PCIe VDM is also gets disabled.
  - Fix: Initialization of MCTP over PCIe VDM and VDM discovery notification enable/disable operations will be handled independently in firmware.
  - Risk: Low
- Fixed an issue where Non-fast path commands stuck in SAT firmware pending queue.
  - Root Cause: In some cases, non-fast path commands such as INQUIRY can remain stuck in the firmware's SAT command pending queue, if the command cannot be sent out during NCQ traffic.
  - Fix: On completion of NCQ commands, add firmware to service the pending queue.
  - Risk: Medium
- Fixed an issue where OS fails to see controller due to long boot time due to locked SED timing out commands.
  - Root Cause: When an I/O times out, it takes a long time to recover that I/O. SED drive is timing out lots of I/Os so it takes too long to discover this drive. This failure does go away when the drive is unlocked.
  - Fix: Set a flag when a locked SED fails a command for I/O timeout and stop post spin-up operations. When drive is unlocked, check this flag and then do post spin-up operations.

© 2023 Microchip Technology Inc. and its subsidiaries

  - Risk: Medium
- Fixed an issue where local mode has Managed SED encryption enabled and tries to change the master key identifier without changing the master key, it does not successfully update the new master key identifier.
  - Root Cause: Logic was not saving the new master key/master key identifier values in the NVRAM.
  - Fix: Updated logic to make sure to check if master key/master key identifier has valid data, so it gets updated in NVRAM.
  - Risk: Low
- Fixed an issue where the firmware does not block the revert with PSID on a configured foreign SED.
  - Root Cause: Firmware must block the revert with PSID for a configured foreign SED.
  - Fix: Firmware blocks the revert with PSID on a configured foreign SED.
  - 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 2.8.3/Legacy BIOS 2.8.2

This release includes the following UEFI fixes and enhancements:

- Added Remote Key Management support for controller managed SED encryption. The remote key management server is utilized for encryption key generation and storage.
- Added controller password support for the remote mode controller managed SED encryption.
- Added multi actuator devices support for EFI SCSI pass thru protocol. The EFI SCSI pass thru protocol supports device enumeration and pass thru commands to multi actuator devices.
- Fixed an issue where PCIe slot information is not provided in the configuration tools.
  - Root Cause: UEFI driver does not get the PCIe slot information from EFI SMBIOS protocol.
  - Fix: Find PCIe slot number from the connected host root bridge configuration space if the slot information is not found in EFI SMBIOS protocol method.
  - Risk: Low

2.2.3 Driver Fixes

2.2.3.1 Fixes and Enhancements for Linux Driver Build 2.1.24-046

This release includes the following fixes and enhancements.

- Added support for ABORT handler in the driver in order to avoid I/O stalls across all devices attached to a controller when I/O requests time out.
- Added sysfs entry for NUMA node in /sys/block/sdX/device. NUMA node detail is added for each exposed device similar to NVMe devices.

2.2.3.2 Fixes and Enhancements for FreeBSD Driver Build 4410.0.1005

There are no known fixes for this release.

2.2.3.3 Fixes and Enhancements for Windows® Driver Build 1010.74.0.1020

- Added registry value "LunResetBehavior" feature. Setting this registry value changes the SRB_FUNCTION_RESET_LOGICAL_UNIT behavior. The new LUN reset behavior is to return the SRB status after the internal TMF LUN reset command completes. If the TMF does not complete, the driver will let it hang until timeout. The new behavior for the TMF LUN reset timeout is set to what the SRB timeout passes into the miniport. HW_RESET_BUS hardware callback routine will pause the controller I/O for up to 25 seconds while checking to see if controller completes all I/O

© 2023 Microchip Technology Inc. and its subsidiaries

within 18 seconds. If I/O is still not completed then the callback hardware bus reset will be failed. If the driver does not detect any outstanding I/O after 18 seconds, then the hardware bus reset callback will be marked as successful.
Note: The new reset LUN behavior will only occur if the registry value "LunResetBehavior" is present and set to 1.

- Fixed an issue where the random drives in the system were going offline after a hot plug and reboot.
  - Root Cause: Incorrect logic in traversing the report_physical_lun response while hot adding drives to the system. In the drive hotplug handling path, the driver was using an incorrect size while traversing the list of physical devices without checking the firmware feature support.
  - Fix: Added logic to check the firmware feature set to determine the size of the RPL entry while traversing the RPL response.
  - Risk: Low
- Fixed an issue where an incorrect tag table is assigned for PQI queue groups.
  - Root Cause: The incorrect tag table assignment for the PQI queue groups when there are more than eight NUMA nodes present in the system. The driver was skipping the creation of IOBypass queues associated with certain queue groups because of the invalid tag table assignment.
  - Fix: Resolved issues with the invalid tag table assignment when there are more than eight NUMA nodes present within the system.
  - Risk: Medium

2.2.3.4 Fixes and Enhancements for VMware Driver Build 4530.0.104

This release includes the following fixes and enhancements:

- Fixed an issue when PSOD occurs while attempting to access memory which had already been released.
  - Root Cause: PSOD happened when one CPU released a device and freed memory. Simultaneously, another CPU was attempting to free the same memory triggered by a hot-plug timeout.
  - Fix: Modifications made to avoid the double-freeing of the device memory.
  - Risk: Medium
- Fixed an issue where PSOD is observed during array creation and deletion.
  - Root Cause: The PSOD error occurred as a result of a NULL de-reference within a function. This issue arises when a report logical LUN fails and an external RAID device is connected, leading to a NULL de-reference.
  - Fix: Added changes to avoid the NULL de-reference.
  - Risk: Low
- Fixed an issue where the Hotswappped HBA drives are detected after 20 minutes or when a manual rescan is done.
  - Root Cause: When a new device is hotswapped with an old device on the same slot, both the new and the old device will have the same `scsi3addr`. Due to this, the new device will be assigned the marked for removal flag status, resulting in not being added to the new device list during device discovery.
  - Fix: The device marked for removal flag status will only be set if `scsi3addr`, model number, and serial number of both devices are equal. If `scsi3addr` is the same but serial or model number are different, the drive will be detected as new and will be added to the new device list.
  - Risk: Low

© 2023 Microchip Technology Inc. and its subsidiaries

2.2.4 Management Software Fixes

2.2.4.1 Fixes and Enhancements for Arcconf/maxView Build 4.14.00.26068

Microchip strongly recommends the maxView users to update to the latest version of the tools to avoid a security vulnerability that has since been resolved.

2.2.4.2 Fixes and Enhancements for Arcconf/maxView™ Build 4.14.00.26064

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

- Added remote Key management service (KMS) support for the managed SED.
- Added support to display the CPLD revision and Platform image revision in Arcconf and maxView.
- Added UBM controller firmware upgrade support in Arcconf and maxView.
- Added SPDM Certificate Storage and Management support.
- Fixed an issue where phantom enclosures are displayed under every connector when there was a VPP backplane in the configuration.
  - Root Cause: maxView/Arcconf was discovering invalid enclosure object per connector when there is a VPP backplane in the configuration.
  - Fix: Implemented changes to skip adding the invalid enclosure objects without a SEP device to the configuration.
  - Risk: Low
- Fixed an issue where invalid enclosure slot count was displayed in maxView.
  - Root Cause: maxView was displaying invalid connector IDs for an enclosure where enclosure has multiple expanders in it, resulting in wrong slot count.
  - Fix: Implemented changes to add the proper connector ID for the enclosure with multiple expanders.
  - Risk: Low
- Fixed an issue where GETSMARTSTATS command is failing in Arcconf.
  - Root Cause: The Arcconf command resolver could not find the associated GETSMARTSTATS command resulting in a failure to execute the command.
  - Fix: Implemented changes to load the GETSMARTSTATS command in Arcconf.
  - Risk: Low
- Fixed an issue where auto discovery function in maxView is not working in a specific configuration.
  - Root Cause: The firewall setting was blocking SSDP packets which were used for auto discovery functionality. This resulted in maxView not discovering the specific windows machines during auto discovery.
  - Fix: Added firewall inbound rule for the maxView redfish server port. Also, a discover button in auto discovery dialog to refresh the auto discovered servers in maxView.
  - Risk: Low

2.2.4.3 Fixes and Enhancements for PLDM Release 6.25.9.0

This release includes the following fixes and enhancements:

- Added support for self-contained activation of storage enclosure firmware flashed using Type 5 downstream device firmware update.
- Changed the Availability state set of the controller composite state sensor to require a rearm in order to transition from a state of Starting to Enabled.
- Changed the Version state set of the controller composite state sensor to reflect changes in firmware version in downstream devices in addition to the controller.

© 2023 Microchip Technology Inc. and its subsidiaries

- Updated the Storage resource to use the v1.14.0 schema and added RDE READ support for the following properties:
  - EncryptionMode
  - LocalEncryptionMode
- All drives connected to the controller which are not configured as a data or spare drive for a RAID Volume resource will now have an associated Volume resource, informally referred to as an HBA Volume or JBOD Volume, with RAIDType of "None" automatically created by the controller.
  - These Volumes will have Redfish URIs and PLDM Type 5 resource IDs listed in the Volume PDR published using a GetPDR request for that PDR handle.
  - Configuration changes such as creation and deletion of RAID Volumes and unconfigured drive removal or insertion will result in `pldmPDRRepositoryChgEvent` events being sent to any active event listeners.
  - RDE READ for an unconfigured drive resource will have a Links.Volumes entry for its associated HBA Volume resource.
  - RDE READ for the StorageController resource will have the value of "None" added to its SupportedRAIDTypes value array.
  - RDE READ for the VolumeCollection resource will have entries for HBA Volumes in its Members property array, and Members@odata.count will add these Volume resources to its count value.
- Fixed an issue where PLDM Type 5 downstream device firmware update fails on Microchip (SXP 24G SAS-4 Expander) SEPs.
  - Symptom: PLDM Type 5 GetFirmwareData fails on SXP 24G SAS-4 Expanders.
  - Root Cause: PLDM uses 16K buffer chunks; whereas, SXP 24G SAS-4 Expanders will only accept 4K buffers.
  - Fix: For expander SEPs, break the 16K buffer into 4K chunks for flashing.
  - Risk: Low
- Fixed an issue of inappropriate returning Allow equal to POST on Storage and Drive to advertise the actions.
  - Symptom: Redfish clients observe the POST value being returned in the Allow header for Redfish requests for Drive and Storage resources when only GET and HEAD should be returned.
  - Root Cause: The implementation of RDE ACTION operations for these resources erroneously included a change to set the CREATE bit in the `PermissionFlags` bitfield in RDE command responses.
  - Fix: Reverted the setting of the `PermissionFlags` CREATE bit for these resources when ACTION operation support has been negotiated.
  - Risk: Low.
- Fixed an issue when the energy pack is not required, `StorageController[CacheSummary][Status][Health]` shall be OK.
  - Symptom: Users would receive cache and battery alerts on systems where an energy pack is not applicable. Redfish `StorageController[CacheSummary][Status][Health]` would show statuses other than OK when an energy pack was not applicable and there were no ECC errors.
  - Root Cause: Incorrect assumptions on what hardware setups are available to users.
  - Fix: Added checks for read cache percentage and NBWC to determine if a backup power source is applicable. Cache and battery alerts are filtered if a backup power source is not

© 2023 Microchip Technology Inc. and its subsidiaries

applicable. Redfish `StorageController[CacheSummary][Status][Health]` will be OK if a backup power source is not applicable and there are no ECC errors.
  - Risk: Medium
- Fixed an issue for possible memory leak in RDE GET on a Drive resource.
  - Symptom: An RDE Get operation will have a memory leak if one of the Binary Encoded JSON (BEJ) encoding calls fails while encoding the Identifiers section of the response.
  - Root Cause: The macros used to perform the BEJ encoding perform an early return after logging the error. In the case of the Identifiers section there is a buffer that is allocated before the encoding starts which needs to be freed once the encoding completes. The early return skips the code that performs the free.
  - Fix: New macros were created that set a flag rather than return early. The flag is used to skip down to the free call early. After the free, if the flag is set the code performs the return.
  - Risk: Low
- Fixed an issue where PLDM Type 2 GetPDRRepositoryInfo returns incorrect RepositorySize when no physical drives are present.
  - Symptom: Mismatch in the PDR Repository size and number of records for a PLDM terminus when a user queries the PLDM Type 2 GetPDRRepositoryInfo command for a configuration with zero drives.
  - Root Cause: A Drive Action PDR is still present in the repository despite there not being any drives present on the device.
  - Fix: Deleting Drive Action PDR when all drives are removed if Action is negotiated. Re-adding Drive Action PDR when the first drive gets added if Action is negotiated.
  - Risk: Low

2.3 Limitations

2.3.1 General Limitations

This release includes the following general limitation:

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

2.3.2 Firmware Limitations

2.3.2.1 Limitations for Firmware Release 6.22

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.
- Power cycle to the enclosure may be needed if connected server goes through abnormal shutdown under following condition: SED operation on OPAL drives like taking ownership, reverting the ownership, or changing the master key where firmware internally performs open session, performs SED management, and ends session gets interrupted due to abnormal shutdown on the server. This condition causes firmware to restart on reboot while drives are left off in the middle of performing SED task and so drives needs to be power cycled also.

© 2023 Microchip Technology Inc. and its subsidiaries

  - Workaround:
    - Allow the change master key operation to complete before shutting down the server.
    - If SEDs are in an external enclosure, power cycle the external enclosure and SEDs before powering up the server with the controller.
- Firmware downgrade from firmware version 6.22 B0 to any older firmware version is blocked if Managed SED is enabled.
  - Workaround: Disable Managed SED and try firmware downgrade.
- Managed SED can't 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 2.8.3/Legacy BIOS Build 2.8.2

There are no known limitations for this release.

2.3.4 Driver Limitations

2.3.4.1 Limitations for Linux Driver Build 2.1.24-046

This release includes the following limitations:

- On some distributions (RHEL7.9, RHEL8.2, RHEL8.3, SLES15SP2, SLES15SP3, OpenEuler 20.03LTS, and 22.03LTS including SP releases), the 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.

© 2023 Microchip Technology Inc. and its subsidiaries

    - Load the OS from virtual media but initiate ISO verification (media test) during the installation followed by ESC to cancel the media test.
    - Edit grub to include the boot argument "`nompath`". Replace "`inst.dd`" with "`nompath inst.dd`" for DUD install.
- Oracle 9 UEK 7 kernel causes SmartPQI rpm dependency failures. This is an issue with how the kernel package was created by Oracle. Correct UEK7 kernel for Oracle 9, which is expected in the mid-October UEK7 release, version number is still pending.
  Note: This does not affect Oracle 8 UEK 7.
  - Workaround: Install the rpm using "`--nodeps`" when dependency failures occur.
    - Update:
      For SmartPQI driver versions > 2.1.20-020 and UEK7 kernels >= 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm will install normally.
      For UEK7 kernels < 5.15.0-3.60.2.el9uek.x86_64, the SmartPQI rpm needs to be installed using the "`--nodeps`".
- On AMD systems, the system might crash or hang due to a bug in the IOMMU module. For details, see lore.kernel.org/linux-iommu/20191018093830.GA26328@suse.de/t/.
  - Workaround: Disable the IOMMU setting option in BIOS.
- Depending on hardware configurations, the SmartPQI `expose_ld_first` parameter may not always work consistently.
  - Workaround: None
- When multiple controllers are in a system, udev(systemd) can timeout during `kdump/kexec` resulting in an incomplete kdump operation. The indication of the timeout is the following console log entry: "`scsi_hostX: error handler thread failed to spawn, error = -4`".
  - Workaround: Extend the udev(systemd) timeout during a kdump operation. Perform the following steps to increase the timeout for udev(systemd):

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

2.3.4.2 Limitations for Windows Driver Build 1010.74.0.1020

There are no known limitations for this release.

2.3.4.3 Limitations for FreeBSD Driver Build 4410.0.1005

There are no known limitations for this release.

2.3.4.4 Limitations for VMware Driver Build 4530.0.104

This release includes the following limitation:

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

2.3.5 Management Software Limitations

2.3.5.1 Limitations for Arcconf/maxView Build 4.14.00.26064

This release includes the following limitations:

- Import foreign drive operation will fail to import the foreign drive when the remote master key is in ASCII format and the length is less than 32 characters.

© 2023 Microchip Technology Inc. and its subsidiaries

- Workaround: To import the foreign drive with an ASCII format master key which has less than 32 characters length, convert the master key from ASCII format to HEX format and input the HEX value.

2.3.5.2 Limitations for PLDM Release 6.25.9.0

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

© 2023 Microchip Technology Inc. and its subsidiaries

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.

© 2023 Microchip Technology Inc. and its subsidiaries

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.

© 2023 Microchip Technology Inc. and its subsidiaries

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.

© 2023 Microchip Technology Inc. and its subsidiaries

5. Revision History

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

Revision	Date	Description
L	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.

© 2023 Microchip Technology Inc. and its subsidiaries

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

© 2023 Microchip Technology Inc. and its subsidiaries

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.

© 2023 Microchip Technology Inc. and its subsidiaries

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-3569-7

Quality Management System

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

© 2023 Microchip Technology Inc. and its subsidiaries

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office	**Australia - Sydney**	**India - Bangalore**	**Austria - Wels**
2355 West Chandler Blvd.	Tel: 61-2-9868-6733	Tel: 91-80-3090-4444	Tel: 43-7242-2244-39
Chandler, AZ 85224-6199	**China - Beijing**	**India - New Delhi**	Fax: 43-7242-2244-393
Tel: 480-792-7200	Tel: 86-10-8569-7000	Tel: 91-11-4160-8631	**Denmark - Copenhagen**
Fax: 480-792-7277	**China - Chengdu**	**India - Pune**	Tel: 45-4485-5910
Technical Support:	Tel: 86-28-8665-5511	Tel: 91-20-4121-0141	Fax: 45-4485-2829
www.microchip.com/support	**China - Chongqing**	**Japan - Osaka**	**Finland - Espoo**
Web Address:	Tel: 86-23-8980-9588	Tel: 81-6-6152-7160	Tel: 358-9-4520-820
www.microchip.com	**China - Dongguan**	**Japan - Tokyo**	**France - Paris**
Atlanta	Tel: 86-769-8702-9880	Tel: 81-3-6880- 3770	Tel: 33-1-69-53-63-20
Duluth, GA	**China - Guangzhou**	**Korea - Daegu**	Fax: 33-1-69-30-90-79
Tel: 678-957-9614	Tel: 86-20-8755-8029	Tel: 82-53-744-4301	**Germany - Garching**
Fax: 678-957-1455	**China - Hangzhou**	**Korea - Seoul**	Tel: 49-8931-9700
Austin, TX	Tel: 86-571-8792-8115	Tel: 82-2-554-7200	**Germany - Haan**
Tel: 512-257-3370	**China - Hong Kong SAR**	**Malaysia - Kuala Lumpur**	Tel: 49-2129-3766400
Boston	Tel: 852-2943-5100	Tel: 60-3-7651-7906	**Germany - Heilbronn**
Westborough, MA	**China - Nanjing**	**Malaysia - Penang**	Tel: 49-7131-72400
Tel: 774-760-0087	Tel: 86-25-8473-2460	Tel: 60-4-227-8870	**Germany - Karlsruhe**
Fax: 774-760-0088	**China - Qingdao**	**Philippines - Manila**	Tel: 49-721-625370
Chicago	Tel: 86-532-8502-7355	Tel: 63-2-634-9065	**Germany - Munich**
Itasca, IL	**China - Shanghai**	**Singapore**	Tel: 49-89-627-144-0
Tel: 630-285-0071	Tel: 86-21-3326-8000	Tel: 65-6334-8870	Fax: 49-89-627-144-44
Fax: 630-285-0075	**China - Shenyang**	**Taiwan - Hsin Chu**	**Germany - Rosenheim**
Dallas	Tel: 86-24-2334-2829	Tel: 886-3-577-8366	Tel: 49-8031-354-560
Addison, TX	**China - Shenzhen**	**Taiwan - Kaohsiung**	**Israel - Ra'anana**
Tel: 972-818-7423	Tel: 86-755-8864-2200	Tel: 886-7-213-7830	Tel: 972-9-744-7705
Fax: 972-818-2924	**China - Suzhou**	**Taiwan - Taipei**	**Italy - Milan**
Detroit	Tel: 86-186-6233-1526	Tel: 886-2-2508-8600	Tel: 39-0331-742611
Novi, MI	**China - Wuhan**	**Thailand - Bangkok**	Fax: 39-0331-466781
Tel: 248-848-4000	Tel: 86-27-5980-5300	Tel: 66-2-694-1351	**Italy - Padova**
Houston, TX	**China - Xian**	**Vietnam - Ho Chi Minh**	Tel: 39-049-7625286
Tel: 281-894-5983	Tel: 86-29-8833-7252	Tel: 84-28-5448-2100	**Netherlands - Drunen**
Indianapolis	**China - Xiamen**		Tel: 31-416-690399
Noblesville, IN	Tel: 86-592-2388138		Fax: 31-416-690340
Tel: 317-773-8323	**China - Zhuhai**		**Norway - Trondheim**
Fax: 317-773-5453	Tel: 86-756-3210040		Tel: 47-72884388
Tel: 317-536-2380			**Poland - Warsaw**
Los Angeles			Tel: 48-22-3325737
Mission Viejo, CA			**Romania - Bucharest**
Tel: 949-462-9523			Tel: 40-21-407-87-50
Fax: 949-462-9608			**Spain - Madrid**
Tel: 951-273-7800			Tel: 34-91-708-08-90
Raleigh, NC			Fax: 34-91-708-08-91
Tel: 919-844-7510			**Sweden - Gothenberg**
New York, NY			Tel: 46-31-704-60-40
Tel: 631-435-6000			**Sweden - Stockholm**
San Jose, CA			Tel: 46-8-5090-4654
Tel: 408-735-9110			**UK - Wokingham**
Tel: 408-436-4270			Tel: 44-118-921-5800
Canada - Toronto			Fax: 44-118-921-5820
Tel: 905-695-1980			
Fax: 905-695-2078			

© 2023 Microchip Technology Inc. and its subsidiaries