Adaptec® SmartRAID 3200 and SmartHBA 2200 Installation and User Guide

Table of Contents

1. Regulatory Compliance Statements

Federal Communications Commission Radio Frequency Interference Statement

Attention: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. However, if this equipment does cause interference to radio or television equipment reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.
- Use a shielded and properly grounded I/O cable and power cable to ensure compliance of this unit to the specified limits of the rules.

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

UL Compliance Statement

From Microchip Adaptec products are tested and listed by Underwriters Laboratories, Inc. to UL 60950-1 /IEC 62368-1 Second Edition and IEC-60950-1/IEC 62368-1 Second Edition standards, file numbers E516387. Microchip Adaptec products are for use only with UL listed ITE.

Microchip Corporation	**Use only with the listed ITE:**
	SmartRAID Ultra 3258P-32i /e Single SmartRAID Ultra 3258P-16i /e Single SmartRAID 3258-16i /e Single SmartRAID 3254-16i /e Single SmartRAID Ultra 3254-16e /e Single SmartRAID 3254-16e /e Single SmartRAID 3254-8i /e Single SmartRAID 3252-8i /e Single SmartRAID 3204-8i /e Single SmartHBA 2200-16i Single

Tested to Comply
With FCC Standards

FOR HOME OR OFFICE USE

European Union Compliance Statement

This Information Technology Equipment has been tested and found to comply with EMC Directive 2014/30/EU, in accordance with:

- EN55032 (2014) Emissions:
  - Class B ITE radiated and conducted emissions
- EN 55035:2017 Immunity:
  - EN61000-4-2 (2009) Electrostatic discharge: ±4 kV contact, ±8 kV air
  - EN61000-4-3 (2010) Radiated immunity: 3V/m
  - EN61000-4-4 (2012) Electrical fast transients/burst: ±1 kV AC, ±0.5 kV I/O
  - EN61000-4-5 (2014) Surges: ±1 kV differential mode, ±2 kV common mode
  - EN61000-4-6 (2014) Conducted immunity: 3 Vrms
  - EN61000-4-11 (2004) Supply dips and variations: 30% and 100%
- EN 63000:2018 Technical Documentation:
  - For the assessment of electrical and electronic products with respect to the restriction of hazardous substances
- EC 62368-1:2014 (EU)
- IEC 60950-1:2005 (US)

In addition, all equipment requiring U.L. listing has been found to comply with EMC Directive 2014/35/EU, in accordance with EN 62368 with amendments A1, A2, A3, A4, A11, A12.

The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 – SI 2012 No. 3032.
Electromagnetic Compatibility Regulations 2016 – SI 2008 No. 1597.
The Electrical Equipment (Safety) Regulations 2016 – SI 2016 No. 1101.

Australian/New Zealand Compliance Statement

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to the Australian/New Zealand standard AS/NZS 3548 set out by the Spectrum Management Agency.

Canadian Compliance Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.
Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Japanese Compliance (Voluntary Control Council Initiative)

This equipment complies to class B Information Technology equipment based on VCCI (Voluntary Control Council for Interface). This equipment is designed for home use but it may causes radio frequency interference problem if used too near to a television or radio. Please handle it correctly per this documentation.

Korean Compliance (KCC) Statement

Microchip Adaptec® products are tested and certified by KCC:

Korean Compliance (KCC) Statement:

R-R-M5P-3258P-32i
The above certification covers the following series: SmartRAID Ultra 3258P-32i /e

Korean Compliance (KCC) Statement:

R-R-M5P-3254-16e
The above certification covers the following series:SmartRAID Ultra 3254-16e /e

Korean Compliance (KCC) Statement:

R-R-M5P-3258P-16i

The above certification covers the following series:

SmartRAID Ultra 3258P-16i/e
Korean Compliance (KCC) Statement:

R-R-M5P-3258-16i

The above certification covers the following series:

SmartRAID 3254-16i /e
SmartRAID 3254-8i /e
SmartRAID 3258-16i /e
Smart HBA 2200-16i
SmartRAID 3254-16e /e
SmartRAID 3252-8i /e
SmartRAID 3204-8i /e

B급 기기
(가정용 방송통신기자재)
Class B Equipment
(For Home Use Broadcasting & Communication Equipment)
이 기기는 가정용(B급) 전자파적합기기로서 주
로 가정에서 사용하는 것을 목적으로 하며, 모
든 지역에서 사용할 수 있습니다.

This equipment is home use (Class B) electromagnetic wave suitability equipment and to be used mainly at home and it can be used in all areas.

2. About This Guide

This Installation and User's Guide explains how to install and setup your SmartRAID 3200 or SmartHBA 2200 Series Host Bus Adapter, including driver installation, BIOS operations, troubleshooting tips, and instructions for flashing the adapter firmware.

These SmartRAID 3200 Series adapter models are described in this guide:

- Adaptec SmartRAID Ultra 3258P-32i /e
- Adaptec SmartRAID Ultra 3258P-16i /e
- Adaptec SmartRAID 3258-16i /e
- Adaptec SmartRAID 3254-16i /e
- Adaptec SmartRAID Ultra 3254-16e /e
- Adaptec SmartRAID 3254-16e /e Single
- Adaptec SmartRAID 3254-8i /e
- Adaptec SmartRAID 3252-8i /e
- Adaptec SmartRAID 3204-8i /e

These SmartHBA 2200 Series adapter models are described in this guide:

- Adaptec SmartHBA 2200-16i

2.1 What You Need to Know Before You Begin

This guide is written for data storage and IT professionals who are responsible for installing, configuring, and maintaining SmartHBA 2200/SmartRAID 3200 Series Host Bus Adapters in computers or servers in a "cloud" or data center environment. You should be familiar with computer hardware, operating system administration, data storage devices, and SAS and Serial ATA (SATA) technology.

If you are responsible for configuring the storage resources on the SmartRAID and SmartHBA adapters, you should be familiar with RAID technology and creating bootable volumes.

2.2 Terminology Used in this Guide

Many of the terms and concepts referred to in this guide are known to computer users by multiple names. This guide uses these terms:

- Host Bus Adapter or HBA (also known as controller, adapter, or I/O card)
- Disk drive (also known as hard disk, hard drive, or hard disk drive)
- Solid State Drive (also known as SSD or non-rotating storage media)
- Enclosure (also known as a storage enclosure, disk drive enclosure, or JBOD)

2.3 How to Find More Information

You can find more information about your SmartHBA 2200/SmartRAID 3200 Series Host Bus Adapter by referring to these documents, available for download at start.adaptec.com.

- *ARCCONF Command Line Utility User's Guide for Adaptec Smart Storage Controllers*—Describes how to use the ARCCONF utility to perform configuration and storage management tasks from an interactive command line. (*DS-60001685*)
- *SmartRAID 3200 Series and SmartHBA 2200 Series Host Bus Adapters Installation and User's Guide* (this manual)—Describes how to install SmartRAID 3200 and SmartHBA 2200 Series adapters in a computer or server, install drivers, and configure the adapter for initial use. (*DS-00004037A*)

- *Adaptec Flash Backup Module ASCM-35 and ASCM-40 Installation Instructions* (ESC-2170352)—Describes how to install the ASCM-35 and ASCM-40 Flash Backup module using the mounting plate method.

3. Kit Contents and System Requirements

This section lists the contents of your SmartHBA 2200/SmartRAID 3200 Series kit and the system requirements for successfully installing and using your adapter.

3.1 Kit Contents

SmartRAID 3200 Series kits:

- SmartRAID 3200 Series adapter
- Full-height ("FH") and Low-profile ("LP") brackets, with mounting screws
- ASCM-40F or ASCM-35F Supercap Module, including:
  - Supercap module extension cable
  - Full-height and Low-profile mounting plate, with mounting screws
  - Supercap mounting clip
  - Tie-wraps (nylon)

SmartHBA 2200 Series kits:

- SmartHBA 2200 Series adapter
- Full-height ("FH") and Low-profile ("LP") brackets, with mounting screws

Note: The latest firmware, drivers, utilities software, and documentation can be downloaded at storage.microsemi.com. For more information, see Downloading the Driver Package.

3.2 System Requirements

- PC-compatible computer with Intel Pentium, or equivalent, processor
- 4 GB of RAM minimum
- Available compatible PCIe slot (depending on your adapter model—see the descriptions in About Your Host Bus Adapter)
- One of these operating systems:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux
  - CentOS
  - SuSE Linux Enterprise Server
  - Ubuntu Linux
  - Debian Linux
  - Oracle Linux
  - Citrix Xenserver
  - Solaris
  - FreeBSD
  - VMware ESXi

  See the *Release Notes* for a complete list of supported OS versions.
- USB flash drive or CD burner, for creating driver disks and bootable media

4. About Your Host Bus Adapter

4.1 About Your SmartRAID 3200 Series Host Bus Adapter

This section provides an overview of the features of the SmartRAID 3200 Series adapter.

4.1.1 Standard Features

- Low profile, MD2 form factor on all boards with up to 16 ports, full-height, half-length form factor for 32 port variants
- 8-lane (x8) or 16-lane (x16 “ultra”) PCIe Gen4 host interface
- Internal SlimSAS (SFF-8654) and external mini-SAS HD connectors using SFF-9402 pinout to support U.2 and U.3)
- Secure Boot and Secure Debug
- maxCrypto CBE for SAS, SATA and NVMe devices
- Universal Backplane Management (UBM)
- Virtual Pin Port Management (VPP)
- SES (SAS expander-based backplanes), SGPIO (direct attached SAS/SATA backplanes)
- Dynamic adapter power management
- maxView tool suite support
- Support for 64 NVMe devices and up to 256 SAS/SATA and up to 64 LD/RAID arrays
- RAID 0, 1 Triple, 10 Triple, 5, 6, 50, 60
- RAID level migration and online capacity expansion
- Mixed mode and HBA mode support
- maxCache SSD caching (SmartRAID 325x only)
- Support for AMD x86 platform
- Zero Maintenance Cache Protection (ZMCP) integrated with all SmartRAID 325x products

Note: See the Product Brief for a complete list of supported features.

4.1.2 Mechanical Information

4.1.2.1 Board Dimensions

This table shows the board dimensions of the SmartRAID 3200 Series adapters, in inches.

Table 4-1. Full-Height (FH) Board Dimensions (32 port)

Dimension	Measure
Height	4.376
Length	6.60
PCB thickness	0.062
Max. component height, top side	Not to exceed 0.57 in.
Max. component height, bottom side	Not to exceed 0.105 in.

Table 4-2. Low-Profile (LP) Board Dimensions (16 port, 8 port)

Dimension	Measure
Height	2.731
Length	6.60
PCB thickness	0.062

.....continued	
Dimension	**Measure**
Max. component height, top side	Not to exceed 0.57 in.
Max. component height, bottom side	Not to exceed 0.105 in.

4.1.2.2 Heat Sink

SmartRAID 3200 Series adapters include a passive heat sink. The heat sink does not support an optional fan. The heat sink has a minimum of four push-pins located at its four corners to ensure an even distribution of force across the top of the ASIC. For airflow requirements, see 14.1. Environmental Specifications

4.1.3 Visual Indicators

LEDs on SmartRAID 3200 Series adapters provide a visual indication of the board hardware status and cache backup system. The LED locations vary, and may be on the front of the board or back of the board. The LED states are described in the following tables.

For LED locations, see the board images in 4.1.4. About the SmartRAID Ultra 3258P-32i /e Adapter, 4.1.7. About the SmartRAID Ultra 3258-16i /e, SmartRAID 3258-16i /e, and 3254-16i /e Adapters, and 4.1.8. About the SmartRAID 3254-8i /e, 3252-8i /e, and 3204-8i /e Adapters.

Table 4-3. SmartRAID 3200 Series Status LEDs

LED	Color	Meaning
DDR_LED1 (DS8)	Yellow	Cache backup error
DDR_LED2 (DS9)	Green	Dirty cache
DDR_LED3 (DS4)	Green	Charge status
HEARTBEAT (DS5)	Green	Heartbeat (blinks once per/second when firmware operating normally)
FAULT (DS7)	Yellow	Hardware Lockup/Fault: OFF = NORMAL OPERATION, ON = FAULT
CRYPTO (DS1)	Green	Cryptographic State: Off = NON-ENCRYPTING, On = ENCRYPTING
PAL_DEBUG (DS10)	Yellow (8i adapters) Red (16i adapters)	Debug LED control signal

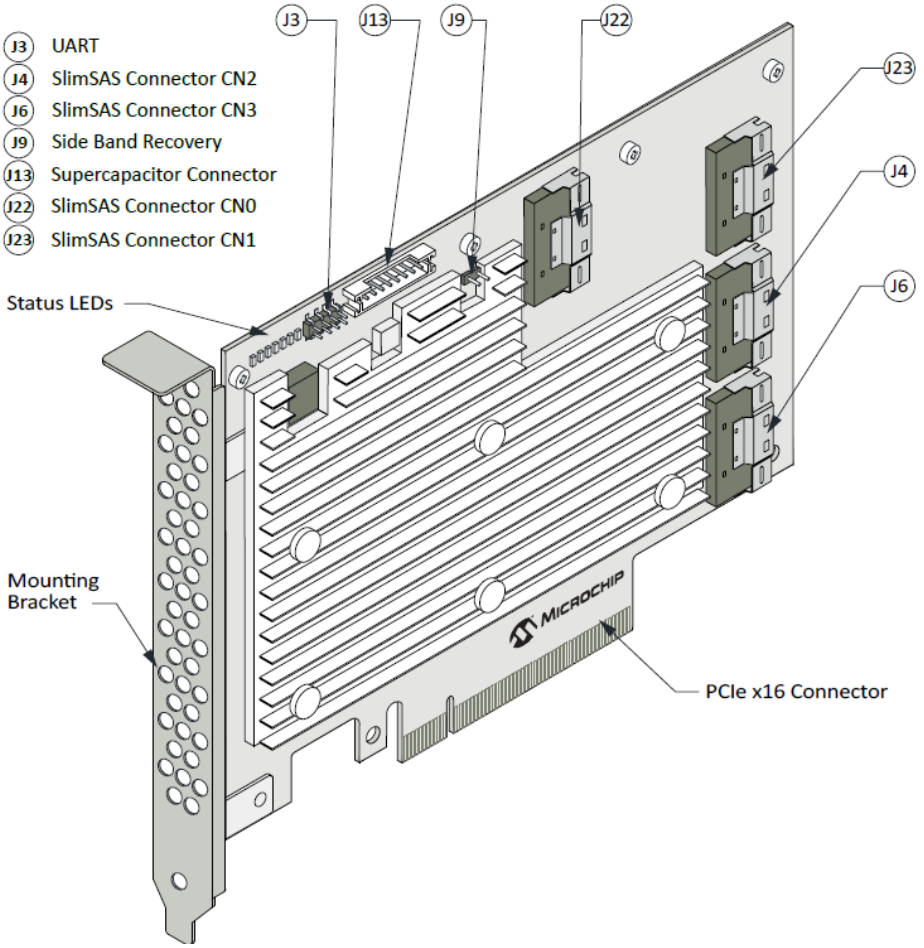
Table 4-4. SmartRAID 3200 Series DDR/FBWC LED States

Cache Status	DDR_LED1 (Yellow)	DDR_LED2 (Green)	DDR_LED3 (Green)	Meaning/Comments
Power-ON state	Off	1 Hz	1 Hz	Power-up
Not Charged	Off	Off	1 Hz	Backup power not ready
Battery Charged / not dirty	Off	Off	On	Backup power ready, no dirty cache
Battery Charged / dirty	Off	On	On	Backup power ready, dirty cache
No Battery	On	On	On	Cache error / Battery not connected
Over Temperature	1 Hz	On	Off	Over temperature
Backup in Progress	Off	1Hz	Off	Backup State
Backup in Flash	Off	On	1Hz	Backup State Cont. State
Backup Complete	Off	On	Off	Backup complete state
Charge Timeout	2 Hz	2 Hz	On	Battery charge timeout
General Error	On	On	On	Cache Error
Backup Incomplete	1 Hz	1 Hz	Off	Idle State & BDtF & brownout & bad volt
Backup/restore Error	On	On	Off	Backup complete state, restore error

4.1.4 About the SmartRAID Ultra 3258P-32i /e Adapter

The SmartRAID Ultra 3258P-32i /e Adapter is a tri-mode (SAS/SATA/NVMe) Host Bus Adapter with these features:

Figure 4-1. SmartRAID Ultra 3258P-32i /e Adapters

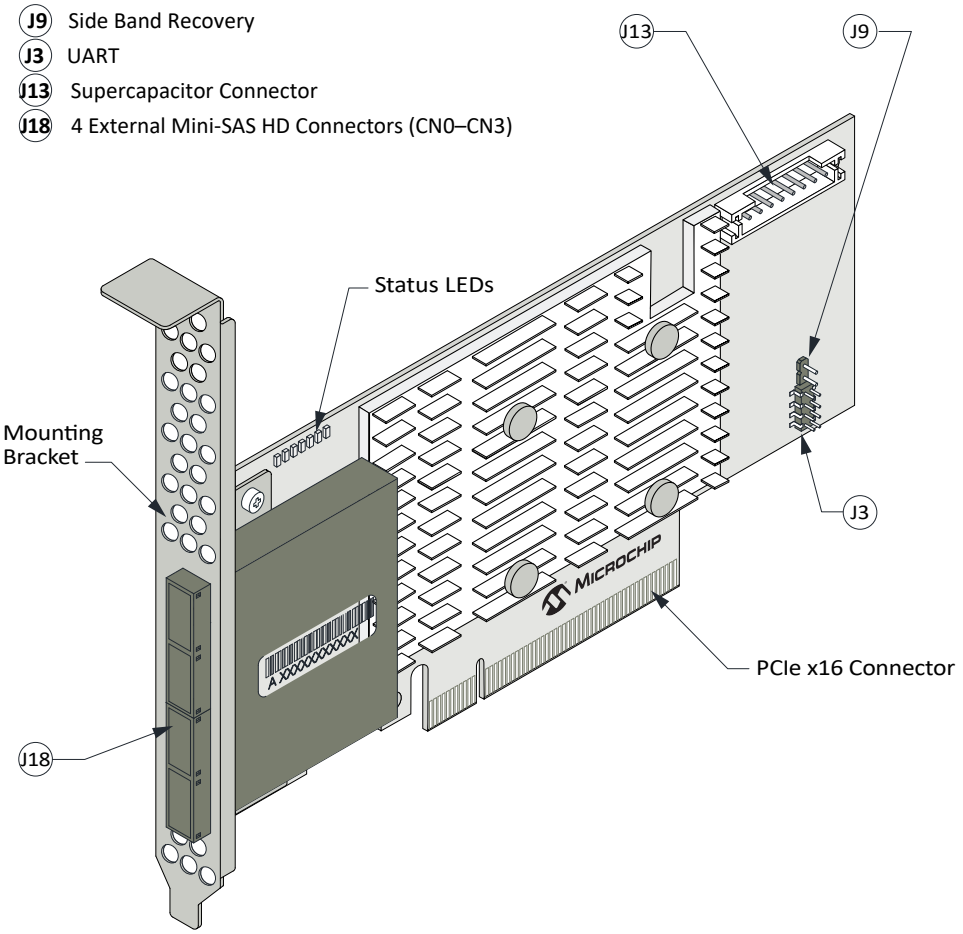


Form Factor	Full height PCI half length
Bus compatibility	PCIe 4.0
PCIe bus width	x16
Data transfer rate (SAS)	24 Gb/s per port
Phys (Unified Serial Ports)	32
Standard memory	8 GB DDR4, 32 MB SPI Flash
Connectors, internal	4x SlimSAS x8
Maximum number of disk drives	32 (SAS/SATA/NVMe)
Enclosure Support	UBM, VPP, SGPIO
Controller-Based Encryption	Yes
Thermal sensors	Processor temperature, Ambient temperature

4.1.5 About the SmartRAID Ultra 3254-16e /e Adapter

The SmartRAID Ultra 3254-16e /e Adapter is a tri-mode (SAS/SATA/NVMe) Host Bus Adapter with these features:

Figure 4-2. SmartRAID Ultra 3254-16e /e Adapters

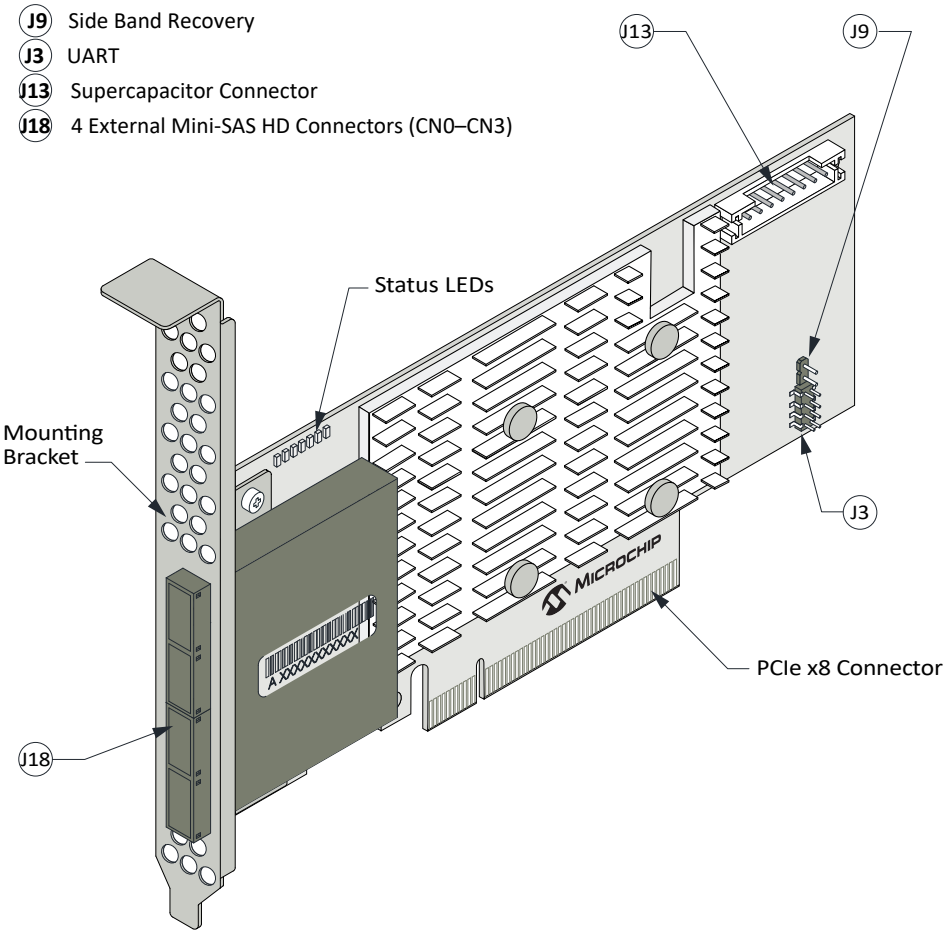


Form Factor	Full height PCI half length
Bus compatibility	PCIe 4.0
PCIe bus width	x16
Data transfer rate (SAS)	24 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	4 GB DDR4, 32 MB SPI Flash
Connectors, external	4x Mini-SAS HD
Maximum number of disk drives	16 (SAS/SATA/NVMe)
Enclosure Support	UBM, VPP, SGPIO
Controller-Based Encryption	Yes
Thermal sensors	Processor temperature, Ambient temperature

4.1.6 About the SmartRAID 3254-16e /e Adapter

The SmartRAID 3254-16e /e Adapter is a tri-mode (SAS/SATA/NVMe) Host Bus Adapter with these features:

Figure 4-3. SmartRAID 3254-16e /e Adapters

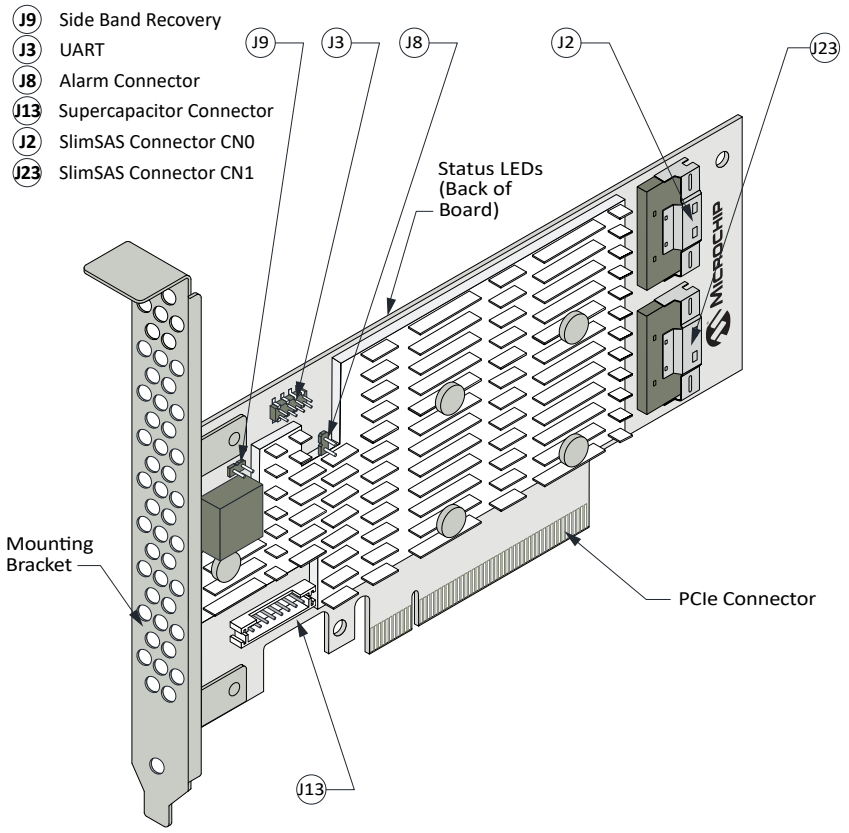


Form Factor	Full height PCI half length
Bus compatibility	PCIe 4.0
PCIe bus width	x8
Data transfer rate (SAS)	24 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	4 GB DDR4, 32 MB SPI Flash
Connectors, external	4x Mini-SAS HD
Maximum number of disk drives	16 (SAS/SATA/NVMe)
Enclosure Support	UBM, VPP, SGPIO
Controller-Based Encryption	Yes
Thermal sensors	Processor temperature, Ambient temperature

4.1.7 About the SmartRAID Ultra 3258-16i /e, SmartRAID 3258-16i /e, and 3254-16i /e Adapters

The SmartRAID Ultra 3258-16i /e, SmartRAID 3258-16i /e, and 3254-16i /e Adapters are tri-mode (SAS/SATA/NVMe) Host Bus Adapters with these features:

Figure 4-4. SmartRAID Ultra 3258-16i /e and SmartRAID 32xx-16i /e Adapters



Form Factor	Half height; half length
Bus compatibility	PCIe 4.0
PCIe bus width	SmartRAID Ultra 3258-16i /e: x16 SmartRAID 32xx-16i /e: x8
Data transfer rate (SAS)	24 Gb/s per port
PHYs (Unified Serial Ports)	16
Standard memory	4/8 GB DDR4 used in standard configuration, 32 MB SPI Flash
Connectors, internal	2x SlimSAS x8
Maximum number of disk drives	16 (SAS/SATA/NVMe)
Enclosure Support	UBM, VPP, SGPIO
Controller-Based Encryption	Yes
Thermal sensors	Processor temperature, Ambient temperature

4.1.8 About the SmartRAID 3254-8i /e, 3252-8i /e, and 3204-8i /e Adapters

The SmartRAID 3254-8i /e, 3252-8i /e, and 3204-8i /e Adapters are tri-mode (SAS/SATA/NVMe) Host Bus Adapters with these features:

Figure 4-5. SmartRAID 32xx-8i Adapters

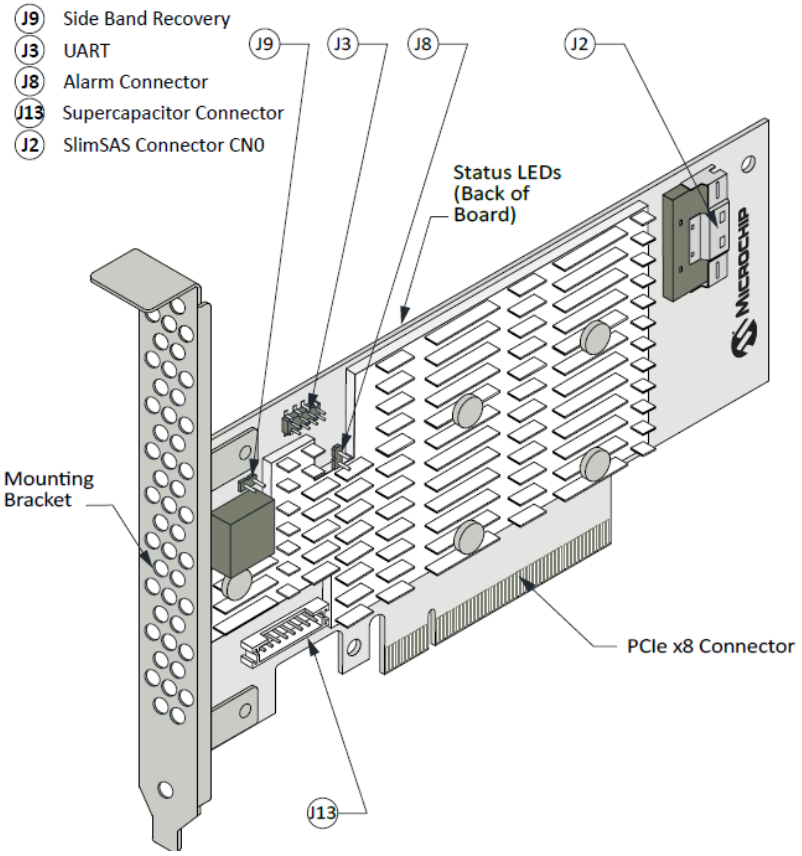


Table 4-5. SmartRAID 3254-8i /e, 3252-8i /e, and 3204-8i /e Adapters

Form Factor	Half height; half length
Bus compatibility	PCIe 4.0
PCIe bus width	x8
Data transfer rate (SAS)	24 Gb/s per port
PHYs (Unified Serial Ports)	8
Standard memory	2/4 GB DDR4, 32 MB SPI Flash
Connectors, internal	1x SlimSAS x8
Maximum number of disk drives	8 (SAS/SATA/NVMe)
Enclosure Support	UBM, VPP, SGPIO
Controller-Based Encryption	Yes
Thermal sensors	Processor temperature, Ambient temperature

4.2 About Your SmartHBA 2200 Series Host Bus Adapter

This section provides an overview of the features of the SmartHBA 2200 Series adapter.

4.2.1 Standard Features

- Low profile, MD2 form factor
- Fully tri-mode capable: 16 Gbps NVMe Gen 4, 24 Gbps SAS4 and 6 Gbps SATA
- 8-lane (x8) PCIe Gen 4 host interface
- Internal SlimSAS connector (using SFF-9402 pinout to support U.2 and U.3)
- Universal backplane management (UBM)
- Virtual Pin Port Management (VPP)
- SES (SAS expander-based backplanes), SGPIO (direct attached SAS/SATA backplanes)
- Secure Boot and Secure Debug
- Dynamic adapter power management
- arcconf/maxView support
- Support for 64 NVMe devices and up to 256 SAS/SATA devices
- Broad inbox OS coverage
- Comprehensive out-of-box driver support
- Multi-initiator support
- Support for AMD x86 platform

Note: See the Product Brief for a complete list of supported features.

4.2.2 Mechanical Information

4.2.2.1 Board Dimensions

See Table 4-2 for more information.

4.2.2.2 Heat Sink

SmartHBA 2200 Series adapters include a passive heat sink capable of bi-directional airflow. The heat sink does not support an optional fan. The heat sink has a minimum of four push-pins located at its four corners to ensure an even distribution of force across the top of the ASIC. For airflow requirements, see 14.1. Environmental Specifications

4.2.3 Visual Indicators

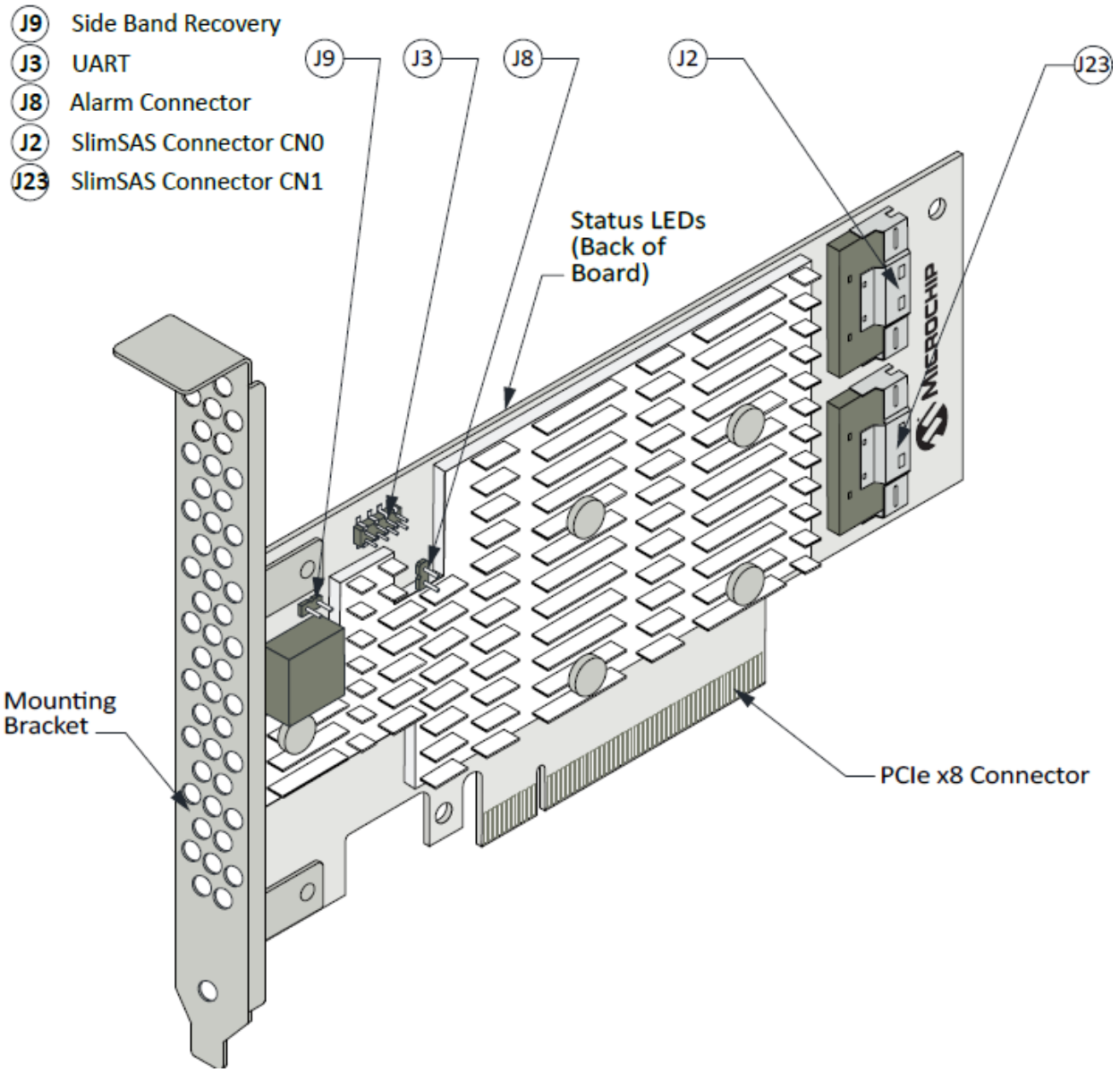
LEDs on the SmartHBA 2200 Series adapters provide a visual indication of the board hardware status. The LED are located on the back of the board. The LED states are described in section 4.1.3. Visual Indicators.

For LED locations, see the board images in 4.2.4. About the SmartHBA 2200-16i Adapter.

4.2.4 About the SmartHBA 2200-16i Adapter

The SmartHBA 2200-16i Adapter is a tri-mode (SAS/SATA/NVMe) Host Bus Adapter with these features:

Figure 4-6. SmartHBA 2200-16i Adapter



Form Factor	Half height; half length
Bus compatibility	PCIe 4.0
PCIe bus width	x8
Data transfer rate (SAS)	24 Gb/s per port
PHYs (Unified Serial Ports)	16
Standard memory	32 MB SPI Flash
Connectors, internal	2x SlimSAS x8
Maximum number of disk drives	16 (SAS/SATA)
Enclosure Support	UBM, VPP, SGPIO

Controller-Based Encryption	No
Thermal sensors	Processor temperature, Ambient temperature

5. Installing the Controller and Disk Drives

This section explains how to install your SmartHBA 2200/SmartRAID 3200 Series adapter in a computer cabinet or server and connect it to internal and external disk drives.

5.1 Before You Begin

- Read Safety Information.
- Familiarize yourself with your host bus adapter's physical features (for 3200 boards, see 4.1.1. Standard Features; for 2200 boards, see 4.2.1. Standard Features).
- Ensure that you have the right number of disk drives for your application (see 5.4. Selecting Disk Drives and Cables).

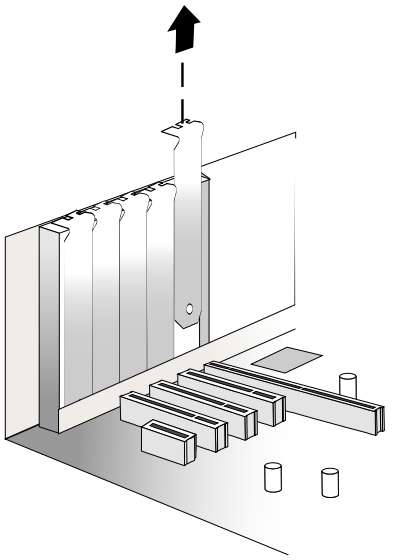
5.2 Installing the Host Bus Adapter

This section describes how to install your SmartHBA 2200/SmartRAID 3200 Series adapter in a computer cabinet or server and connect internal and external storage devices.

1. Turn off your computer and disconnect the power cord and any network cables. Open the cabinet, following the manufacturer's instructions.
2. Select an available PCIe expansion slot that's compatible with your adapter model and remove the slot cover, as shown in the figure below. (To check PCIe bus compatibility of your adapter, see 4. About Your Host Bus Adapter.)

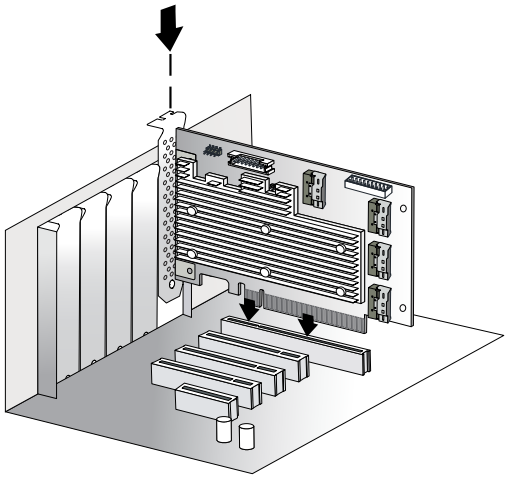
   Note: For SmartRAID 3200 Series adapters with an external supercapacitor module, select a slot for the adapter that's next to an *empty* slot in the backplane, ideally, a short.

   CAUTION Touch a grounded metal object before handling the adapter.

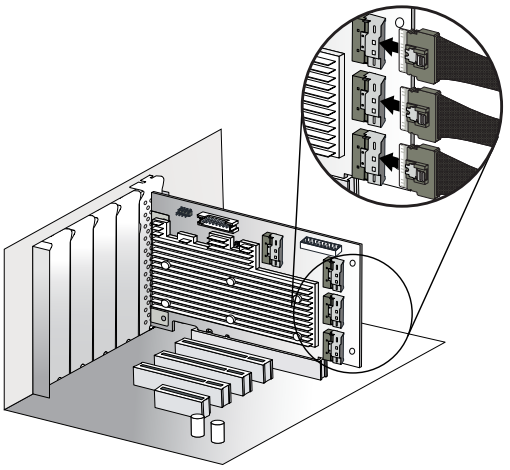


3. Insert the adapter into the expansion slot and press down gently but firmly until it clicks into place. When installed properly, the adapter should appear level with the expansion slot.

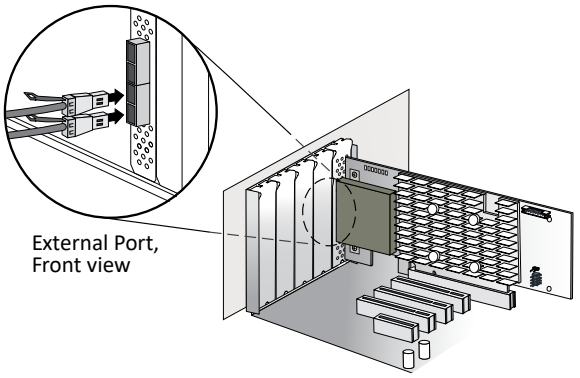
CAUTION Be sure to handle the adapter by its bracket or edges only. Apply pressure only on the edges when inserting the card into expansion slot.



4. Secure the bracket in the expansion slot, using the retention device (for instance, a screw or lever) supplied with your computer.
5. Connect cables between the adapter and internal or external disk drives or enclosures, as required:
   - For adapters with internal ports, connect SlimSAS cables between the adapter and internal disk drives or enclosures:



   - For adapters with external ports, connect miniSAS HD cables between the adapter and external disk drives or enclosures:



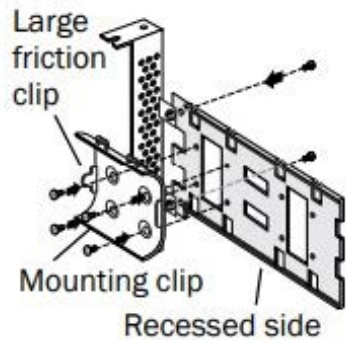
6. Close your computer cabinet, reconnect the power cord and network cables, then power up the system.

5.3 Installing Microchip Adaptec® Flash Backup Module ASCM-35F/ASCM-40F for SAS/SATA/NVMe SmartRAID Adapter

Note: If this is your initial install, please make sure to install the cap to the adapter first before installing the adapter in the system. If you are replacing the cap, power down your system and, while using the appropriate static protection, remove the adapter from your computer.

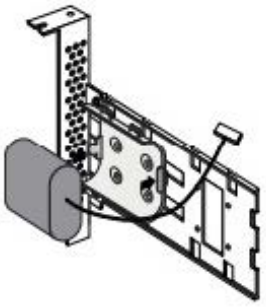
1. Using the appropriate static protection, remove the supercapacitor module from packaging.
2. Insert the supercapacitor module into the mounting clip. The supercapacitor module snaps securely into place between the large and small friction clips.
3. Insert the RAID adapter into a PCIe slot on the motherboard in the host computer.
4. Attach the bracket to the mounting plate, as shown in Figure 5-1. The bracket is installed on the front side of the mounting plate (the side with right-angle bends at the top and bottom), with the mounting screws inserted from the back. Be sure to attach the mounting plate to the bracket with the recessed side at the bottom.

Figure 5-1. Attaching the Bracket to the Mounting Plate



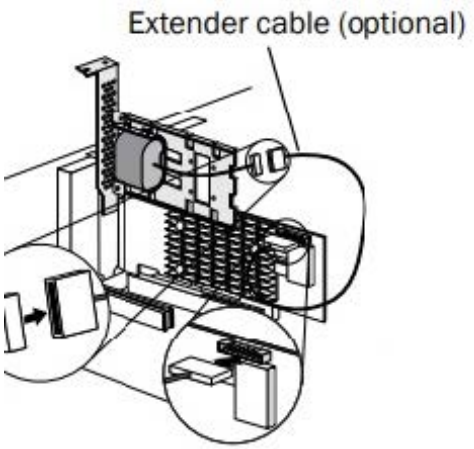
5. Choose a location for the mounting clip at the front or back of the mounting plate. Then, attach the mounting clip to the mounting plate with four (4) Phillips screws, as shown in Figure 5-1. The large friction clip should face the front of the mounting plate.
6. Insert the supercapacitor module into the mounting clip. The supercapacitor module snaps securely into place between the large and small friction clips, as shown in Figure 5-2. Be sure to orient the supercapacitor module such that the connecting cable faces the rear of the mounting plate.

Figure 5-2. Inserting the Supercapacitor Module into the Mounting Clp



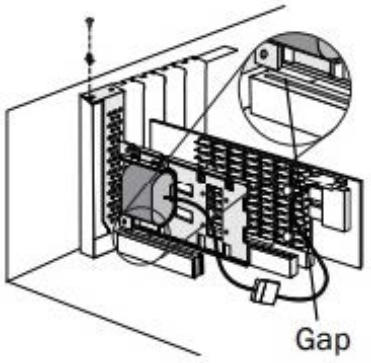
7. Attach the supercapacitor module to the adapter by inserting the connector into the socket on the adapter PCB, as shown in Figure 5-3.

Figure 5-3. Attaching the Supercapacitor Module to the Adapter



8. Install the mounting plate in the empty slot next to the adapter, as shown in Figure 5-4. After securing the mounting plate to the card cage, verify that the supercapacitor module and mounting plate sit above (and do not touch) the PCIe slot.

Figure 5-4. Installing the Mounting Plate in the Empty Slot



9. Restart your computer. The supercapacitor should reach full charge in 5-6 minutes.

Note: If you are installing the supercapacitor module for the first time, it may take up to 20 minutes to fully charge. When no supercapacitor is installed or the supercapacitor is not fully charged, the write cache is automatically disabled by default to prevent data loss.

5.4 Selecting Disk Drives and Cables

5.4.1 Disk Drives

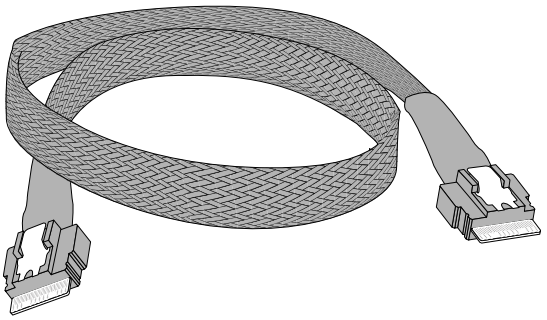
Your SmartHBA 2200/SmartRAID 3200 Series adapter supports SAS and SATA disk drives, Solid State Drives (SSDs), and SAS tape drives. For more information about compatible disk drives, refer to www.adaptec.com/compatibility.

5.4.2 Cables

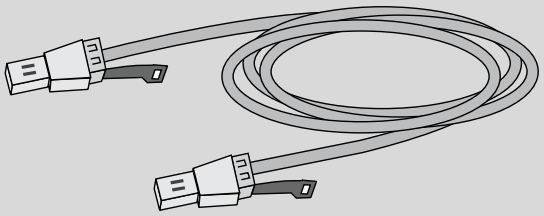
Depending on your application requirements, you can use any of the cables listed below (for typical applications; list not exhaustive). For more information about cabling options for your SmartHBA 2200/SmartRAID 3200 Series adapter, visit www.adaptec.com/cables

Note: We recommend using Microchip Adaptec cables only.

SlimSAS Cables



SlimSAS x8 : SlimSAS x8
SFF-8654 to SFF-8654



External Mini SAS HD to External Mini SAS HD
(SFF-8674 to SFF- 8674)

5.4.3 Using the Microchip HII BIOS Configuration Utility to Configure Controller Settings for Direct-Attached Devices

This section will be used to configure the port discovery protocol in the HII BIOS utility of the RAID/HBA controller through the system BIOS during server boot.

1. Configure direct-attached devices per NVMe protocol with required cabling and power connections.
2. Power on system and access System BIOS menu. Navigate to the Adaptec RAID/HBA Controller.
3. Navigate to Configure Controller Settings → Configure Port Discovery Protocol → Set Port Discovery Protocol.
4. Set Port CN# to be configured and change setting from "Auto Detect" to "Direct-Attached Cable," and submit changes.
5. Configure the number of targets for the direct-attached devices. Selection is equal to the number of connectors on the cable (i.e., 2, 4, or 8). Adaptec by Microchip proprietary cables are required. Submit Changes.
6. After submitting changes, this screen will indicate a successful configuration change. Save changes in the BIOS menu and restart.

5.5 Tri-Mode Connectivity Tips for Integration

Devices connected via enclosure/backplane

- Verify the correct cable type for the specific configuration is used.
  - Refer to the systems compatibility report (CR) for tested configuration settings.
    - https://adaptec.com/compatibility
  - Refer to the qualified cable description list for configurations not listed on systems CR.
    - https://adaptec.com/cables
- Verify the backplane is set to the correct mode.
  - Refer to the systems compatibility report (CR) for tested configuration settings.
    - https://adaptec.com/compatibility
- Refer to enclosure documentation for configurations not listed on systems CR.
- Verify the controller Backplane Mode setting is correct for the configuration
  - Available options:
    - View Current port Discovery Protocol
    - View Pending port Discovery Protocol
    - Set port Discovery Protocol
    - Reset port Discovery Protocol to default
  - Backplane Mode settings can be reviewed/changed in the UEFI BIOS utility, ARCCONF CLI utility, or maxView GUI
  - Available options are Auto-detect(default)/UBM/SGPIO/VPP
- This operation requires reboot.
- Additional guidelines
  - NVMe drives following U.3 pinout ***are*** compatible with enclosures intended for U.2 NVMe drives. NVMe drives following the U.2 pinout ***are not*** compatible with enclosures intended for use with NVMe U.3 drives.
  - Verify controller BIOS/firmware is at latest release
  - SlimSAS to Occulink is 1:1 connection to NVMe devices
- When configuring mixed devices in a single backplane, it is recommended to confirm configuration of NVMe devices before adding SAS/SATA devices
- If devices are not recognized
  - Verify all settings above
- If devices are not on NVMe/Systems CR, it's possible it is not compatible. Please select a tested device from list or contact Adaptec Apps Engineering at https://ask.adaptec.com

6. Installing the Driver and an Operating System

This chapter explains how to install the SmartPQI controller driver and an operating system on a bootable volume. It assumes that the SmartHBA 2200/SmartRAID 3200 is installed in a computer or server.

A compatible driver is available inbox for many operating systems. If you are installing an OS version that already has a compatible driver, install the OS normally using the available OS media or image, then update the driver later using the procedures in 7. Installing the Driver on an Existing Operating System

Note: For information about building the SmartPQI drivers from source, see 11. Installing the SmartPQI Drivers from Source .

6.1 Download the Driver Package

Complete these steps to download the drivers for your operating system(s):

1. Open a browser window, then type start.adaptec.com in the address bar.
2. Enter your product or adapter model number, then select SmartHBA 2200/SmartRAID 3200.
3. Select your operating system version, for instance, Microsoft Windows Server 2019 or Red Hat Enterprise Linux 7; then select the appropriate driver from the list.
4. Download the controller driver package (zip file archive).
5. When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (\windows 2019, \rhel7, and so on).

   Notes:

   - For OSs that provide an inbox smartpqi driver with support for Microchip Smart Storage Controllers, it is not necessary to create a driver disk from the downloaded driver files. Refer to the instructions for each OS for specific driver disk requirements.
   - See the *Release Notes* for a complete list of available driver files.

6.2 Installing with Windows

Note: Use the following procedure for all supported Windows versions. You will need your Windows Installation DVD (or equivalent virtual media/iso image) to complete this task.

To install the controller SmartPQI driver while installing Windows:

1. Insert the Windows installation DVD, then restart the computer.
2. Follow the on-screen instructions to begin the Windows installation.
3. When prompted to specify a location for Windows, select **Load Driver**.
4. Insert the USB driver disk, browse to the driver location, then click **Ok**.
5. When prompted to select the driver to install, click **Next**.
6. Follow the on-screen instructions to complete the installation.

6.3 Installing with Red Hat Linux

To install the controller SmartPQI driver while installing Red Hat Linux, follow the steps in the sections below.

RHEL7 Update 6 Installation and Above

To install the RHEL7 driver with a Linux system:

1. Install the Linux system using the inbox smartpqi driver.
2. After the installation completes, install the latest smartpqi driver rpm by using the following command (where #.#.#-### is the build number):

```
rpm –ivh kmod-smartpqi-#.#.#-###.rhel7u9.x86_64.rpm
```

RHEL7 Installation with Secure Boot

To install the RHEL driver with a Linux system with secure boot enabled:

Note: For more information about installing RHEL with secure boot, refer to the RedHat online resources for "Signing Kernel Modules for Secure Boot".

1. Install the Linux system using the inbox smartpqi driver in secure boot mode.
2. Enroll the Microchip public key for secure boot:
   a. Import public key:
      ```
      mokutil --import smart_driver_key_pub.der
      ```
   b. Reboot system.
   c. During boot, perform MOK key enrollment to accept the new key.
3. After the installation completes, install the signed driver rpm using the following command (where #.#.#-### is the build number):
   ```
   rpm –ivh kmod-smartpqi-#.#.#-###.<rhel_version>.x86_64.rpm
   ```
4. Reboot.

6.4 Installing with SuSE Linux Enterprise Server

To install the controller SmartPQI driver while installing SuSE Linux, follow the steps in the sections below.

Installing with SLES 12 SP3 and Above

Follow these steps to install the driver while installing SLES 12 SP5:

1. Install the Linux system using the inbox smartpqi driver.
2. After the installation completes, install the latest smartpqi driver rpm by using the following command (where #.#.#-### is the build number and the SLES version is formatted as follows: sles12sp5):
   ```
   rpm -ivh smartpqi-ueficert-#.#.#-###.<sles_version>.x86_64.rpm

   rpm -ivh smartpqi-kmp-default-#.#.#-###.<sles_version>.x86_64.rpm
   ```
3. For SLES15 installations that will be using the Xen Hypervisor, run the following command after installing the driver rpm. This will ensure the updated driver is used for Xen.
   ```
   /sbin/update-bootloader --refresh
   ```

SLES 12 Installation with Secure Boot

To install the SLES driver with a Linux system with secure boot enabled:

1. Install the Linux system using the inbox smartpqi driver in secure boot mode.
2. Enroll the Microchip public key for secure boot.
   a. Install the ueficert package:
      ```
      rpm -ivh smartpqi-ueficert-#.#.#-###.<sles_version>.x86_64.rpm
      ```
   b. Import public key:
      ```
      mokutil --import /etc/uefi/certs/17A8B2BE.crt
      ```
   c. Reboot.
   d. During boot, perform MOK key enrollment to accept the new key.

3. Install Microchip signed driver rpm package:

```
rpm -ivh smartpqi-kmp-default-#.#.#-###.<sles_version>.x86_64.rpm
```

4. Reboot.

6.5 Installing with Oracle Linux

To install the controller SmartPQI driver while installing Oracle Linux, follow the steps in the sections below.

Installing with Oracle Linux 7.6 and Above

Follow these steps to install the driver while installing Oracle Linux 7.6:

1. Install the Linux system using the inbox smartpqi driver.
2. After the installation completes, install the latest smartpqi driver rpm for the kernel you intend to run (where #.#.#-### is the build number and the Oracle Linux version is formatted as follows: ol7u9):

```
Base Kernel: rpm –ivh kmod-smartpqi-#.#.#-###.<ol_version>.x86_64.rpm

UEK Kernel: rpm –ivh kmod-smartpqi-uek-#.#.#-###.<ol_version>.x86_64.rpm
```

6.6 Installing with Ubuntu Linux

To install the controller SmartPQI driver while installing Ubuntu Linux:

Note: The following instructions apply to Ubuntu Server 18.04 LTS and above only.

1. Install the Linux system using the inbox smartpqi driver.
2. Install the smartpqi DKMS package (`smartpqi-dkms_#.#.#-###_all.deb`) by using the following commands (where #.#.#-### is the build number):

   Note: The smartpqi DKMS package rebuilds the smartpqi driver automatically whenever the kernel on the system is updated. This ensures that you have a smartpqi driver to support the new kernel.

```
apt-get update
apt-get –f install build-essential dkms
dpkg -i smartpqi-dkms_#.#.#-###_all.deb
```

6.7 Installing with Debian Linux

To install the controller SmartPQI driver while installing Debian Linux 9.13 and above:

1. Install the Linux system using the inbox smartpqi driver.
2. Reboot the system.
3. Install the smartpqi DKMS package (`smartpqi-dkms_#.#.#-###_all.deb`) by using the following commands (where #.#.#-### is the build number):

   Note: The smartpqi DKMS package rebuilds and activates the smartpqi driver automatically any time the kernel on the system is updated. This insures you have a smartpqi driver to support the new kernel.

```
apt-get install build-essential dkms
dpkg -i smartpqi-dkms_#.#.#-###_all.deb
```

6.8 Installing with FreeBSD

To install the controller SmartPQI driver while installing FreeBSD:

1. Copy the driver module (smartpqi.ko) to a USB drive.

   Disk partition the USB key, using gpart on a unix system.

For example:

```
# gpart create -s GPT da1
# gpart add -t freebsd-ufs da1
# newfs /dev/da1p1
# mount /dev/da1p1 /mnt
# cp smartpqi.ko /mnt
```

2. Insert the USB driver disk.
3. Insert the FreeBSD Installation disk into the CD/DVD drive and boot from it.
4. From the FreeBSD boot menu, press Escape to launch the boot loader prompt.
5. Perform the following steps at the boot loader prompt:
   a. Check all the present modules by executing following command.

      ```
      # lsmod
      ```

      Expected Output: It will show all the present modules.
   b. Unload the kernel module by executing the following command:

      ```
      # unload
      ```

   c. Check whether the kernel is unloaded or not by executing the following command:

      ```
      # lsmod
      ```

      Expected Output: It will show all the present modules.
   d. Check whether the USB drive is detected or not by executing the following command:

      ```
      # lsdev
      ```

      Expected Output:
      part 0: ..... (removable)
      part 1: ..... (removable)
      part 2: ..... (removable)
   e. Load the kernel by executing the following command:

      ```
      # load /boot/kernel/kernel
      ```

   f. Load the driver module by executing the following command:

      ```
      # load part< USB key location >:smartpqi.ko
      ```

      For example: `# load part2:smartpqi.ko`
   g. Continue the Installation procedure by typing the following command and pressing **Enter**.

      ```
      # boot
      ```

   h. After completing the kernel installation and before rebooting the system, add the driver to the new system. Choose "YES" when it prompts the following message for the manual configuration.

      "The installation is now finished. Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications?
   i. Use the following commands to complete the manual configuration:
      i. Mount the USB key by using the following command:

         ```
         # mount /dev/da1p1 /media
         ```

ii. Copy the driver to the boot directory by using the following command:

```
# cp /media/smartpqi.ko /boot/modules/smartpqi.ko
```

iii. Ensure that the boot loader loads by using the following command:

```
# vi /boot/loader.conf
```

iv. Add the following line:

```
smartpqi_load="YES"
# reboot
```

6. If the system halts at `# mountroot>`, check for the boot partition using the following command:

```
# mountroot> ?
```

Note: The boot partition is primarily present in P2, so use the following command:

```
# mountroot> ufs:/dev/<da0p2>
```

6.9 Installing with Citrix XenServer

Note: For Hypervisor 8.2 or later, install Hypervisor on the system using the driver included in the release. Then update driver as necessary using the latest driver release from the Citrix support site.

Note: For XenServer 7.6 and above, a USB key is supported for the driver update ISO. On a Linux system, use the dd command to write the SmartPQI driver ISO image to the USB key. You will need the XenServer installation DVD (or equivalent virtual media/iso image) to complete this task. You must have administrator privilege to install the driver image.

To install the controller SmartPQI driver while installing Citrix XenServer:

1. On the machine where you want to install the OS and SmartPQI driver, insert the XenServer installation DVD, then restart your computer.
2. When prompted to add a driver, insert the driver USB key, press `F9`, then select **local media**.

   Note: Leave the driver USB key inserted throughout the installation.
3. Verify the SmartPQI driver and "**use**".
4. Continue the XenServer installation, following the on-screen instructions.
5. Remove the driver USB key, then reboot your computer.

6.10 Installing with VMware

Note: You will need a writable CD or USB flash drive to complete this task. You must have administrator privileges to create the driver disk and install the driver image.

To install the controller SmartPQI driver with VMware ESXi, you must create a custom boot image using the VMware Image Builder tool. This tool automates the process of customizing the ESXi install-ISO and runs as a script under Microsoft PowerShell.

To install the SmartPQI controller driver while installing VMware:

1. Use VMware's ESXi image builder process to build a boot/install image that includes the desired driver. Instructions for this process can be found at docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-62B15826-B529-4519-B57A-98DFD0CC5522.html?hWord=N4IghgNiBcIJIFswHMCmACAQgVwJYQBNUAnEAXyA.
2. On the VMware ESXi machine, insert the custom boot CD/USB, then restart your computer.
3. Follow the on-screen instructions to begin the VMware installation.
4. Complete the VMware installation, following the on-screen instructions.

5. Remove the custom boot CD or USB drive, then reboot your computer.

7. Installing the Driver on an Existing Operating System

This chapter explains how to install the SmartPQI controller driver on an existing operating system. It assumes that the SmartHBA 2200/SmartRAID 3200 is installed in a computer or server and the OS is already installed.

Notes:

- To install the driver while you're installing an operating system, see Installing the Driver and an Operating System.
- For information about building the SmartPQI drivers from source, see 11. Installing the SmartPQI Drivers from Source .

7.1 Download the Driver Package

Complete these steps to download the drivers for your operating system(s):

1. Open a browser window, then type start.adaptec.com in the address bar.
2. Enter your product or adapter model number, then select SmartHBA 2200/SmartRAID 3200.
3. Select your operating system version, for instance, Microsoft Windows Server 2019 or Red Hat Enterprise Linux 7; then select the appropriate driver from the list.
4. Download the controller driver package (zip file archive).
5. When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (\windows 2019, \rhel7, and so on).

   Notes:

   - For OSs that provide an inbox smartpqi driver with support for Microchip Smart Storage Controllers, it is not necessary to create a driver disk from the downloaded driver files. Refer to the instructions for each OS for specific driver disk requirements.
   - See the *Release Notes* for a complete list of available driver files.

7.2 Installing on Windows

Note: The following instructions apply to all supported Windows operating systems.

To install the controller SmartPQI driver on Windows:

1. Start or restart Windows.
2. In the Control Panel, launch the Device Manager, right-click your Smart Storage Controller, then select **Update Driver Software**.
3. Insert the driver disk, then select **Browse my computer for driver software**.
4. Browse to the driver disk location, then click **Next**.
5. Select the driver from the list, then click **Next**.
6. When the installation is complete, remove the driver disk and restart your computer.

7.3 Installing on Red Hat

To install the controller SmartPQI driver on Red Hat Linux, follow the steps in the sections below.

Installing on RHEL7 Update 6 and Above

To install the RHEL7 driver on a Linux system:

1. Install the latest smartpqi driver rpm by using the following command (where #.#.#-### is the build number and the RHEL version is formatted as follows: rhel7u9):

   ```
   rpm –ivh kmod-smartpqi-#.#.#-###.<rhel_version>.x86_64.rpm
   ```

2. Reboot the system.

7.4 Installing on SuSE Linux Enterprise Server

To install the controller SmartPQI driver on SLES, follow the steps below.

Installing on SLES 12 SP3 and Above

Follow these steps to install the driver on SLES 12 SP5:

1. Install the latest smartpqi driver rpm by using the following command (where #.#.#-### is the build number and the SLES version is formatted as follows: sles12sp5):

```
rpm -ivh smartpqi-ueficert-#.#.#-###.<sles_version>.x86_64.rpm
rpm -ivh smartpqi-kmp-default-#.#.#-###.<sles_version>.x86_64.rpm
```

2. For SLES15 installations that will be using the Xen Hypervisor, run the following command after installing the driver rpm. This will ensure the updated driver is used for Xen.

```
/sbin/update-bootloader --refresh
```

3. Reboot the system.

7.5 Installing on Oracle Linux

To install the controller SmartPQI driver on Oracle Linux, follow the steps below.

Installing on Oracle Linux 7.6 and Above

To install the SmartPQI driver on an Oracle Linux system:

1. Install the latest smartpqi package using the following commands (where #.#.#-### is the build number and the Oracle Linux version is formatted as follows: ol7u9):

```
Base Kernel: rpm –ivh kmod-smartpqi-#.#.#-###.<ol_version>.x86_64.rpm
UEK Kernel: rpm –ivh kmod-smartpqi-uek-#.#.#-###.<ol_version>.x86_64.rpm
UEK6ol7 Kernel: rpm –ivh kmod-smartpqi-uek6ol7-#.#.#-###.x86_64.rpm
UEK6ol8 Kernel: rpm –ivh kmod-smartpqi-uek6ol8-#.#.#-###.x86_64.rpm
```

7.6 Installing on Ubuntu Linux

Notes:

1. For driver installation on Ubuntu Linux, you may need to create the root account and password.
2. The SmartPQI driver is available as inbox for Ubuntu 18.04 and above.

To install the controller SmartPQI driver on Ubuntu:

1. Login to the system using the root user credentials.
2. Update the Ubuntu package index by using the following command:

```
sudo apt-get update
```

3. Load the Ubuntu unpacking tools:

```
sudo apt-get –f install build-essential dkms
```

4. Install the latest SmartPQI DKMS DEB driver package by using the following command (where #.#.#-### is the build number):

```
dpkg -i smartpqi-dkms_#.#.#-###_all.deb
```

7.7 Installing on Debian Linux

To install the controller SmartPQI driver on Debian 9.13 and above:

1. Login to the system as root, or sudo to root.

2. Install the supporting package for the SmartPQI DKMS deb package:

```
apt-get update
apt-get install build-essential dkms
```

3. Install the SmartPQI DKMS DEB driver package using the following command (where #.#.#-### is the build number):

```
dpkg -i smartpqi-dkms_#.#.#-###_all.deb
```

4. Reboot system.

7.8 Installing on FreeBSD

To install the controller SmartPQI driver on FreeBSD:

1. Check whether the driver package is installed or not.

```
# pkg info | grep smartpqi
```

2. Install the SmartPQI package by using the following command:
   For FreeBSD 11:

```
# pkg add smartpqi-amd64.txz
```

   For FreeBSD 12 and 13:

```
# pkg add smartpqi-amd.pkg
```

   Note: Upgrade the package if it already exists, using the following command.
   For FreeBSD 11:

```
# pkg upgrade smartpqi-amd64.txz
```

   For FreeBSD 12 and 13:

```
# pkg upgrade smartpqi-amd.pkg
```

3. Restart the system.

```
# reboot
```

7.9 Installing on Citrix XenServer

Note: For Hypervisor 8.2 or later, if Hypervisor was installed on the system using the driver included in the release, then update the driver as necessary using the latest driver release from the Citrix support site.

Note: To copy the driver RPM file to XenServer, you must have access to a remote copy utility, such as WinSCP, putty, or Linux scp. You must have root privilege to install the driver.

To install the controller SmartPQI driver on Citrix XenServer (where #.#.#-### is the build number and the Citrix XenServer version is formatted as follows: xen7.6):

1. Using a remote copy utility, copy the driver RPM file to a local directory on XenServer. This example uses Linux scp to copy the driver to /tmp/smartpqi:
   `scp citrix-smartpqi-#.#.#-###.<xen_version>.rpm root@<xen-server-ip>:/tmp/smartpqi`
2. Install the driver module rpm:
   `rpm -ivh /tmp/smartpqi/citrix-smartpqi-#.#.#-###.<xen_version>.rpm`
3. Reboot your computer.

7.10 Installing on VMware

Note: The instructions in this section must be executed on the ESXi server's command line. To access the command line:

1. Enable ESXi system console login. At ESXi system console, press **F2** and log in as root.
2. Select “Troubleshooting Options” and press **ENTER**.
3. Select “Enable ESXi shell”.
4. Select "Enable SSH".
5. Press **ESC** to exit from the menus back to the ESXi splash screen.
6. Press **ALT + F1** to open the ESXi shell login screen.
7. Log in as root.

To install the controller SmartPQI driver on VMware:

1. Using a remote copy utility, such as Linux `scp`, copy the downloaded driver VIB package onto the ESXi server’s tmp directory using the following command (where xxxxxxx is the version/build number):
   For ESXi 7.0:

   ```
   # scp smartpqi-70.xxxx.0.xxx-1OEM.700.0.0xxxxxxx.x86_64.vib root@<esxi_server_address>:/tmp
   ```

   For ESXi 8.0:

   ```
   # scp smartpqi-80.xxxx.0.xxx-1OEM.800.0.0xxxxxxx.x86_64.vib root@<esxi_server_address>:/tmp
   ```

2. On the ESXi server console, install the driver package (.vib file).
   For ESXi 7.0:

   ```
   # esxcli software vib install -v file:/tmp/
   smartpqi-70.xxxx.0.xxx-1OEM.700.0.0xxxxxxx.x86_64 –maintenance-mode
   ```

   For ESXi 8.0:

   ```
   # esxcli software vib install -v file:/tmp/
   smartpqi-80.xxxx.0.xxx-1OEM.800.0.0xxxxxxx.x86_64 –maintenance-mode
   ```

3. Restart the system.

   ```
   # reboot
   ```

4. After rebooting the system, check whether the driver package is installed. Compare the driver vib version shown by the command below with the version that was installed, to make sure they are the same.

   ```
   # esxcli software vib list | grep smartpqi
   ```

5. Restore system console security settings:
   a. At ESXi system console, press **F2** and log in as root.
   b. Select “Troubleshooting Options” and press **ENTER**.
   c. Select “Disable ESXi shell”.
   d. Select "Disable SSH".
   e. Press **ESC** to exit back to the ESXi splash screen.

8. Managing SED

8.1 Overview

8.1.1 Introduction

A Self-Encrypting Drive (SED) encrypts data through disk-based encryption with a Media Encryption Key (MEK). The MEK is known only to the SED and cannot be recovered through forensic analysis. Smart controllers enable the use of SEDs as logical drives or physical drives.

The controller is responsible for managing and delivering the credentials required by the SED for enabling the disk-based encryption. SAS, SATA, and NVME drives that are compliant to the Opal 2.0 and Enterprise 1.01 industry standards are supported.

This section describes the functionality provided by the managed SED features.

This table lists the terms used in this section.

Table 8-1. Terminology

Term	Definition
Credential	A value (password, key, or PIN) that grants access privilege
Encrypted	A value that is obfuscated with an algorithm
PIN	A value (up to 32 bytes) used as a credential on a SED
Key	A value input to a hash function used to create a PIN
Locking range	An LBA range of a SED that may have unique credentials
Identifier	The "name" component of a name—values pair as in Key Identifier: Key
RAID set	A drive or group of drives that contain one or more RAID volumes
Secured	A SED managed by the smart controller. The SED PIN is required to access user data.
Unsecured	A SED that is not managed by the smart controller
Password	This refers to the controller password. The controller password is not related to the SED PIN or the adapter master key
OFS	Original Factory State. This is the state of a newly manufactured SED. No security attributes or locking ranges are configured.
LKM	Local Key Management
RKM	Remote Key Management
UEFI	Unified Extensible Firmware Interface
HII	Human Interface Infrastructure
KMS	Key Management Service

8.2 Supported Features

The features described in the following sections are part of the managed SED feature set. Users can configure the managed SED feature settings through the UEFI HII and ARCCONF or maxView OS-based tools.

8.2.1 Supported SED Types

Adapters support attaching SAS, SATA, and NVMe SED (depending on the controller used) that are compliant with the following industry standards:

- TCG Storage Security Subsystem Class: Enterprise Standard version 1.01
- TCG Storage Security Subsystem Class: Opal standard version 2.01

8.2.2 Logical and Physical Drives

Adapters support using SEDs for logical and physical drives with the disk-based encryption feature enabled. Encryption-enabled drives are referred to as secured drives. The controller delivers the credentials to the SEDs and unlocks them. SEDs can also be used for logical and physical drives without the disk-based encryption feature turned on (like a non-SED device) and is referred to as non-secured drives.

Secured SED drives can also be used as boot drives or MaxCache logical drives. Adaptec Controllers also support coexistence of both secured and non-secured drives.

If a secure logical drive is used as a boot device in local key management mode and the controller password is enabled, the controller password must be entered from the HII utility every time the OS is booted.

Note: Mixing of different SED drive types (Opal and Enterprise) in a logical drive or maxCache array is not supported.

8.2.3 Local and Remote Key Management

The controller is responsible for delivering the credentials (PIN) to the SEDs. When the controller is managing SEDs, a Master Key is created during the initial setup. The Master Key is required to secure the SEDs and unlock the user data on managed SEDs.

Local Key Management

The Master Key is stored locally in the controller NVRAM. Optionally, a Master Key Identifier can also be entered at the time of Master Key creation.

Remote Key Management

The Master Key is generated and stored by key management server external to the controller. The controller will communicate with the server to retrieve the Master Key.

8.2.4 Controller Password

The controller password is an optional setting while configuring controller managed SED encryption.

Local Key Management

The controller password is intended to provide an extra level of security for local SED management and guards against theft of the server, adapter, and the SEDs. The adapter will not unlock any SED until the controller password input is provided in the configuration utility.

Remote Key Management

Controller password in remote key management mode serves as a backup option to unlock controller and encrypted devices in the case when the key management server becomes unavailable. Controller password option is only provided in HII utility. If controller password is configured, an encrypted version of the Remote Master Key is stored in the controller NVRAM. If the controller is not able to connect to the remote key server, the controller password can be used to retrieve and decrypt the Remote Master key from controller NVRAM.

8.2.5 Changing the Master Key in Local Key Management Mode

Updating the Master Key is a controller wide operation that applies to all secured SED drives.

8.2.6 Reverting to OFS

Controller management tools can revert a secured SED to the OFS. Secured logical drives must be deleted before returning to OFS, which also destroys all the data on the logical drive.

If the credential of the secured SED is unavailable, reverting to the OFS requires the 32-byte PSID from the drive's label to perform the revert operation.

8.2.7 Importing a Foreign Secured SED

A foreign SED is defined as a secured physical or logical drive that was previously attached to an Adaptec controller with a different credential than what is stored in the new Adaptec controller. The controller can detect that the drive was moved from a different controller and can import the drive to the new controller when the original credentials are entered. In remote key management mode, foreign controller managed SED devices whose Master key belongs to same key management server are automatically imported during boot.

Note: The controller cannot import secured SED volumes from non-Adaptec controllers.

8.2.8 Controller Factory Reset

Factory Reset deletes all secrets, keys, passwords, and identifiers on the controller and places the controller's encryption configuration in a factory new state. It does not modify the drives.

8.3 Workflows

8.3.1 Rules to Enable SED Management

These are the rules for enabling SED management:

- All SEDs in a secure logical drive must be the same SSC type (Enterprise, Opal, and so on).
- When creating a new secure logical drive, all SEDs must either be in OFS or owned by the controller.
- Unsecured drives must be in OK state before they can be secured.
- For Local Key Management—If controller password is enabled, ensure it is entered before performing any drive removal/re-insertion operations while the controller is powered on. Otherwise, the newly added SED will be in the Locked state without the credentials and will not transition the logical drive to the correct state such as Rebuild or Transformation.
- Once a secure volume is created using the SED management feature, down revving the firmware to a version that does not have support for SED management feature will render the secure volume inaccessible.
- Remote key management mode is provided for selection only if the system environment supports remote key management services and complies to the requirements of controller. Enabling remote key management mode requires reboot to complete the operation.

8.3.2 Securing an SED in Local Key Management Mode

Use the following steps to secure the SED:

1. Connect the supported SED to the controller.
2. Enable SED management from HII, ARCCONF, or maxView. The tools will generate a Master Key with an option to override with a custom Master Key. Optionally, the Master Key Identifier and the controller password can be provided.
3. Establish the controller's ownership of the SED by selecting OFS SEDs to be secured by the controller.

Upon subsequent power-on, the user must enter the controller password (if the controller password is enabled) to unlock the SED drives.

8.3.3 Securing an SED in Remote Key Management Mode

Use the following steps to secure the SED:

1. Connect the supported SED to the controller.
2. Refer to system vendor documentation to establish connection between system and remote key management server.

3. Enable SED management from HII, ARCCONF, or maxView™. Choose the key management mode as remote. Master key generated by the key management server will be used for encryption. Controller password can be provided optionally in HII. System reboot is required to complete operations in remote key management mode.
4. Establish the controller's ownership of the SED by selecting OFS SEDs to be secured by the controller.

8.3.4 Setting Up SED Management with UEFI HII

SED management can be enabled from the controller management tools such as UEFI HII, ARCCONF CLI, or maxView GUI. The following sections describe how to set up SED management with the UEFI HII configuration utility. Refer to the ARCCONF or maxView user guides for details about using those tools.

8.3.4.1 Enabling Controller-Managed SED Encryption

Use the following steps to enable controller-managed SED excryption:

1. Boot to system BIOS setup utility and select the controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Key Management Mode** as **Local** or **Remote**, then select **Set/Change Managed SED Settings**.
4. Select **Configure Managed SED**.
5. If configuring Local Key Management Mode, enter appropriate input to **Master Key Identifier** and **Master Key** fields.
   Note: Write down the Master Key Identifier and Master Key and keep in a safe location. If it gets lost or forgotten, the only recovery option is to revert SEDs with PSID, which will result in data loss.
   - **Master Key Identifier** is a hint to the master key used for encryption. The master key Identifier must be 1 to 32 characters long for Local Key Management mode, using only ASCII characters. A default identifier is provided which can be updated by entering the input.
   - **Master Key** is used by the key manager for encryption. A valid key must be 8 to 32 characters long with ASCII characters only and contain a combination of alphanumeric characters including, at least one upper-case character, at least one lower-case character, at least one numeric character, and one non-alphanumeric character (such as '#' or '$').
   - Record the Master Key. A method does not exist for recovering or displaying the Master Key once the value is set. Failure to provide the Master Key may result in encrypted data being inaccessible.
6. Controller Password is an optional setting. If setting controller password is required, then provide input in the **Set/Change Controller Password** field and select **Enabled** for the **Controller Password** field.
   - If **Controller Password** is set in Local Key Management mode, all the encrypted devices will be offline at startup. The user must enter the controller password to bring the encrypted devices online. A valid password must be 8 to 32 characters long with ASCII characters only.
   - If **Controller Password** is set along with remote key management mode and on any of the subsequent reboot if controller detects that the key management server is unavailable, then an unlock option will be provided in the UEFI HII menu. Controller can only unlock encrypted devices if the key management server is made available or by entering a valid controller password.
7. Select **Submit Changes**

8.3.4.2 Changing the Master Key in Local Key Management Mode

Changing the Master Key results in generating a new credential for all the attached SEDs. The user may change the Master Key by supplying the current Master Key, the new Master Key and a new Master Key Identifier. It is strongly recommended to change the Master Key Identifier when changing the Master Key. If a new Master Key Identifier is not provided, the old identifier is retained.

Use the following steps to change the Master Key:

1. Boot to system BIOS setup utility and select the controller to enter the HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Set/Change Managed SED Settings**.
4. Select **Configure Managed SED**.
5. Enter new **Master Key Identifier** and new **Master Key** into fields.
6. Select **Submit Changes.**
7. Enter old Master Key to authenticate the operation.
8. Select **Submit Changes.**

8.3.4.3 Changing Controller Password

Use the following steps to change the controller password:

1. A valid controller password must be 8 to 32 characters long with ASCII characters. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Set/Change Managed SED Settings**.
4. Select **Configure Managed SED**.
5. Enter input for **Set/Change Controller Password** and select **Enabled** for **Controller Password** field.
6. Select **Submit Changes.**
7. Local key management mode requires additional authentication using Master key, enter current Master Key to authenticate the operation.
8. Select **Submit Changes**.

8.3.4.4 Unlocking Controller

When Controller Password is set in local key management mode, data on the encrypted devices will be offline during system boot. The controller password must be entered to unlock the controller and bring the encrypted devices online. After three wrong attempts, the controller password will be locked out for some time. If controller password is set along with remote key management mode and on any of the subsequent reboot if controller detects that the key management server is unavailable, then unlock option is provided in the UEFI HII menu. Controller can only unlock encrypted devices if the key management server is made available or a valid controller password is entered.

1. Boot to system BIOS setup utility and select the controller to enter theHII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Unlock Controller**.
4. Enter controller password, then select **Submit**.

Note: In local key management mode, it is recommended to supply the password, before performing any operations such as removing or adding the drives. Without the password, the controller will not be able to unlock the drive to perform the RAID operations such as rebuild, background parity initialization, and consistency check operations.

8.3.5 RAID Logical Drive Operations

The following sections provide the set of operations that are applicable only for the RAID logical drives.

8.3.5.1 Creating Secure RAID Logical Drives

SED management can be enabled on RAID logical drives at the time of creation using SEDs that are in OFS or owned by the controller.

1. Boot to system BIOS setup utility and select controller to enter the HII configuration utility.
2. From the main menu, select **Array Configuration**, then select **Create Array**.
3. Select SED drives which you want to include in the array, then select **Proceed to next Form**.
4. Select **SED Encryption** as **Enabled**.
   - When SED Encryption is enabled, all the logical drives in the array will be encrypted using SED disk-based encryption. The array's physical drive will be owned by the controller. There is no operation to convert back.
5. Select **RAID Level**, then select **Proceed to next Form**.
6. Configure remaining array settings.
7. Select **Submit Changes**.

8.3.5.2 Assigning Hot Spares to Secure Logical Drives

Generally, SEDs used as spares inherit the current security of the RAID set it is activated for.

Only SEDs of the same SSC type (Enterprise, Opal, etc.) may be added to a secure logical drive. Adding a SED to a managed SED logical drive will automatically secure the SED.

A non-SED or Otherwise Owned SED cannot be added to a secure logical drive. Only secure (Adaptec-owned) or OFS SEDs can be added to secure logical drives.

8.3.5.3 Importing foreign SED

A foreign SED is defined as an Adaptec owned SED with a credential that is different from its connected adapter. This can happen when:

- The SED was migrated from a different adapter. This is the most common case.
- The SED was previously owned by the connected adapter but was removed for a period. During the removed period, the connected adapter Master Key was changed.

The adapter will check for foreign SEDs during discovery or hot plug events and will provide a status that foreign SEDs were found. The user may select configured/unconfigured foreign SEDs and supply the Master Key of the foreign SEDs to import them.

Note: Importing a secure RAID set with an active background operation such as rebuild or transformation may require an additional reboot after import to restart the pending operation.

8.3.5.4 Deleting Secure RAID Logical Drives

When the last logical drive on a secure RAID array is deleted, the adapter will execute a Revert on each SED in the RAID array and return the SEDs to OFS.

Delete volume may be executed on foreign-secure volumes. The RAID metadata and DataStore will be deleted but the locking ranges cannot be deleted without the SED PIN. The SEDs will become unconfigured, Otherwise Owned SEDs and must be reverted with PSID before re-use.

When the adapter is in RAID mode, revert with PSID must be done through Adaptec user tools such as HII, ARCCONF, or maxView.

8.3.5.5 Adding SEDs Through Transformation

SEDs may be added to non-SED or passive SED logical drives. The SED will be checked for the presence of locking ranges and if there are any locking ranges present, the SED will not be allowed to be added to the volume.

Only SEDs of the same SSC type (Enterprise, Opal, etc.) may be added to a secure volume. Adding a SED to a managed SED logical drive will automatically secure the SED.

A non-SED or Otherwise Owned SED cannot be added to a secure logical drive. Only secure (Adaptec-owned) or OFS SEDs can be added to secure logical drives.

8.3.6 HBA Physical Drive Operations

This section details physical drive operations for HBAs.

8.3.6.1 Taking Ownership of SED

Use the following steps to take ownership of the SED:

1. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Take SED Ownership**.
4. Select devices that you want the controller to manage their SED encryption settings.
5. Select **Submit Changes**.

8.3.6.2 Revert

Revert destroys all user data, returns the SED to OFS and deletes any controller related data present in the drives.

The adapter has two versions of the Revert operation available: Microchip Revert and Revert with PSID.

8.3.6.3 Adaptec Revert

Adaptec Revert is performed on secure unconfigured SED owned by the Adaptec controller.

1. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Revert Managed SED to Original Factory State**.
4. Select the devices that you want to revert.
5. Select **Submit Changes**.

8.3.6.4 Revert with PSID

Revert with PSID can return any SED to OFS. It should not be used on the Adaptec controller-managed SEDs unless they are foreign and the SED Key is lost.

1. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Disk Utilities**.
3. Select the SED drive to revert using PSID.
4. Select option **Revert to Original Factory State using PSID**.
5. **Enter PSID** of the drive.
6. Select **Submit Changes.**

8.3.6.5 Importing Foreign SED

Use the following steps to import foreign SEDs:

1. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Import Foreign SED**.
4. Select the devices that you want to import.
5. **Enter Foreign SED Master Key**. For importing the devices configured on foreign remote key management. The hexadecimal key value can be provided as input after retrieving it from the key management server.
6. Select **Submit Changes**.

Note: In remote key management mode, foreign controller managed SED devices whose Master key belongs to same key management server are automatically imported during boot.

8.3.7 Disabling SED Management

Disabling SED management results in the loss of data. Prior to disabling the SED management, all the secure logical drives must be deleted. Once disabled, all secure physical drives are reverted to OFS. Any secure foreign physical drives will transition to Otherwise Owned state.

1. Boot to system BIOS setup utility and select controller to enter HII configuration utility.
2. From the main menu, select **Configure Controller Settings** > **Self-Encryption Drive (SED) Based Encryption Setup**.
3. Select **Key Management Mode** as **Disabled**, then select **Set/Change Managed SED Settings.**
4. Select **Submit Changes**.

8.3.8 Factory Reset

Factory Reset will delete all the SED management–related information (Master Key, Controller Password, etc.) from the controller and restore the controller to the factory state. SED management must be disabled as described in Section 8.3.7. Disabling SED Management prior to resetting the controller to factory settings.

8.4 Troubleshooting

8.4.1 Lost Controller Password in Local Key Management Mode

When the Controller Password feature is enabled and the password is forgotten, the Controller Password feature can be disabled by changing the SED management configuration. Configuration changes require the user to enter the Master Key, which was generated at the time of SED enablement (see 8.3.4.1. Enabling Controller-Managed SED Encryption for details).

8.4.2 Moving SEDs to a Different Controller While Key Change Is in Progress

Moving a SED to another server or adapter while a key change is in progress should only occur if there is a server or controller failure. If the server or controller is still running, then wait until the key change is completed before the move occurs.

The controller can detect that the moved SEDs are foreign, and it was undergoing a key change.

This is a case of a Foreign Import (section 8.3.5.3. Importing foreign SED) and an interrupted key change scenario. The general handling is to follow the Foreign Import process; however, in this case, the user must provide both the old and new Master Keys.

The management tools support retrieving both the Key Identifier and the Reset Key Identifier from the foreign SED. After both the old and new foreign keys are provided, the controller completes the key change that was in progress prior to the move and then execute the additional key change to import the foreign SEDs.

8.4.3 Moving SEDs to a New Controller when the Server Is Powered Off with Controller Password Enabled

The following use cases describe the process for moving SEDs to a new controller when the server is powered off with the controller password enabled.

Case 1: If the moved SEDs are MCHP-owned, but do not have any logical volumes on it, the SEDs will be discovered as foreign SEDs and will be in the Data Locked state. Once adapter password is provided, the foreign SEDs will be in locked state. The SEDs are not visible to the host. After the user imports the foreign SEDs, they will be unlocked, Microchip-owned. Now they are exposed to the host. See 8.3.6.5. Importing Foreign SED.

Case 2: If the moved SEDs are MCHP-owned, and have secured logical volumes on it, the volume will be in data locked before adapter password is provided. Once adapter password is given, the secured logical volumes become locked. After user imports all the foreign SEDs, the secured volumes will be in OK state.

Note: This applies to Local Key Management only.

8.4.4 Failure in Enabling Remote Key Management Mode SED Encryption/Unlocking SED

In remote key management mode if controller is unable to retrieve the key due to key communication errors then the SED encryption will remain disabled and existing encrypted devices will become offline.

Ensure the system supports key management service, configured correctly and complies with controller requirements. Check Controller Information menu on key management server status, fix any connection issues.

Ensure PCIe UEFI option rom execution is in enabled state.

If controller password is set and the controller report key communication error with KMS then the controller can be unlocked by providing controller password input in HII.

9. Solving Problems

This section provides basic troubleshooting information and solutions for solving problems with your SmartHBA 2200/SmartRAID 3200 Series Host Bus Adapter.

9.1 Troubleshooting Checklist

If you encounter difficulties installing or using your SmartHBA 2200/SmartRAID 3200 Series Host Bus Adapter, check these items first:

- With your computer powered off, check the connections to each disk drive, power supply, enclosure, and so on.
- Try disconnecting and reconnecting disk drives from the adapter.
- Check that your adapter is installed in a compatible PCIe expansion slot. To verify the bus compatibility of your adapter, see 4. About Your Host Bus Adapter.
- Ensure that your adapter is firmly seated and secured in the PCIe expansion slot.
- If your adapter is not detected during system boot, try installing it in a different compatible expansion slot. (See Installing the Host Bus Adapter for instructions.)
- Did the driver install correctly? It may need to be reloaded after a reboot or kernel update; see 6. Installing the Driver and an Operating System.
- Check the Release Notes for compatibility issues and known problems.

If you are still unable to resolve a problem, contact Microchip Support.

9.2 Resetting the Adapter

You may need to reset your SmartHBA 2200/SmartRAID 3200 if it becomes inoperable or if a firmware upgrade is unsuccessful. SmartHBA 2200/SmartRAID 3200 adapters support a reset protocol called Side Band Recovery. For information about Side Band Recovery, contact your support representative. To locate the Side Band Recovery jumper on your adapter, see the board illustrations in 4. About Your Host Bus Adapter.

10. Using the Microchip SAS/SATA HII Configuration Utility

The Microchip SAS/SATA Configuration Utility (MSCU) is a BIOS-based utility that you can use to manage your SmartHBA 2200/SmartRAID 3200 adapters and the devices attached to them. It comprises a set of tools for creating and managing arrays, viewing and modifying adapter properties, viewing disk drive properties, flashing the HBA firmware, and managing disk drives and spares.

10.1 Running the Microchip SAS/SATA Configuration Utility: UEFI/HII

On servers that support the Unified Extensible Firmware Interface, or UEFI (version 2.10 or higher), the BIOS-level configuration options are presented with a UEFI/HII interface (Human Interaction Infrastructure). UEFI/HII provides an architecture-independent mechanism for initializing add-in cards, like the SmartHBA 2200/SmartRAID 3200, and rendering contents.

In the UEFI/HII interface, the server's standard BIOS provides access to the SmartHBA 2200/SmartRAID 3200 configuration options. How you access the BIOS varies, depending on the server manufacturer, but typically it's started by simply pressing `DEL`. Once you enter setup, navigate to the menu where forms of third-party vendors are displayed. The menu location depends on server manufacturer. Select your controller from the list. Menus are categorized for Controller Settings, Array Configuration, Disk Utilities, and Administration.

Menu-based instructions for completing tasks appear on-screen. Menus can be navigated using the arrows, `ENTER`, `ESC`, and other keys on your keyboard or using mouse, depending on browser capability.

This appendix provides instructions for navigating and completing tasks with the UEFI/HII interface.

10.2 Controller Information

The Controller Information menu provides details about the controller, including the Board Id, firmware revision number, operating mode, UEFI driver version, encryption support, and World Wide Name. It also provides a configuration summary. To view the SmartHBA 2200/SmartRAID 3200 information, start the Microchip SAS/SATA Configuration Utility and select **Controller Information** from the main menu.

10.3 Creating an Array

Use the Array Configuration option to create new arrays. You can select drives, specify the RAID level and encryption options (if supported by your controller), and configure array settings, including stripe size and logical drive size.

To create an array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Create Array.**
4. Select each drive you want to include in the array: use the arrow keys to select a drive, press `Enter`, then `Proceed`.

   Note: Be sure not to mix drive types! Select SATA drives or SAS drives only.
5. Select **Proceed to next Form**, then press `Enter`.
6. (*For controllers with maxCrypto Controller-Based Encryption only*) Select encryption options for the array: encrypted volume or plaintext volume (not encrypted).

   Note: You will be prompted for your account credentials (Admin or User) if you are not logged into the Encryption Manager; see 10.11.1. Encryption Manager Full Setup.

7. Select the RAID level.
8. Select **Proceed to next Form**.
9. Configure array settings: select the stripe size (from 16KiB to 1024KiB, depending on the number of disks and RAID level), logical drive size (default=all available space), the unit of measure (GiB, TiB, MiB), SSD Over Provisioning Optimization (enable or disable over provisioning on solid state drives in the array, if applicable), and caching (utilizing the controller's cache memory).
10. Select **Submit Changes**.

10.4 Creating a maxCache Array

Note: This option is available only in the UEFI/HII interface.

Use this option to create a maxCache array. The maxCache array supports read and redundant write caching, using a reserved logical device comprised of SSDs only. You can select drives, specify the RAID level, and configure array settings, such as the logical drive size and cache Write policy.

Note: When using maxCache in conjunction with an encrypted primary logical drive, the maxCache volume will also be encrypted automatically.

To create a maxCache array:

1. From the main menu, select **Array Configuration**, then select **Create maxCache Array.**
2. Select each drive you want to include in the array: use the arrow keys to select a drive, press `Enter`, then select **Proceed to next Form**.
3. Select the RAID level, then select **Proceed to next Form**.
4. Configure array settings: select the Cache Line size (64KiB or 256KiB), logical drive size (default=all available space), unit of measure (GiB, TiB, MiB), and cache Write Policy (write-back, write-through).
5. Select **Submit Changes**.
6. Select the data logical drive associated with the maxCache device (16 GB minimum).

10.5 Managing Arrays and Logical Drives

Use the Array Configuration option to manage arrays and logical drives. You can view logical drive properties, create and delete logical drives and spares, and delete logical drives and arrays.

10.5.1 Viewing Logical Drive Properties

To view logical drive properties:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**
2. Use the arrow keys the select an array, press `Enter`, then select **List Logical Drives.**
3. Use the arrow keys to select a logical drive, press `Enter`, then select **Logical Drive Details**.

10.5.2 Creating Logical Drives

Use the Create Logical Drive option to create new logical drives. This option creates a logical drive from the free space on the selected array.

To create a logical drive:

1. From the main menu, select **Array Configuration**, then select **Create Logical Drive.**
2. Select each drive you want to include in the array: use the space bar to the select a drive, then press `Enter`.

   Note: Be sure not to mix drive types! Select SATA drives or SAS drives only.
3. Select **Proceed to next Form**, then press `Enter`.

4. Select the RAID level, then select **Proceed to next Form**.
5. Configure array settings: select the stripe size (from 16KiB to 1024KiB, depending on the number of disks and RAID level), logical drive size (default=all available space), the unit of measure (GiB, TiB, MiB), SSD Over Provisioning Optimization (enable or disable over provisioning on solid state drives in the array, if applicable), and caching (utilizing the controller's cache memory).
6. Select **Submit Changes**.

10.5.3 Enabling IO Bypass

Use this option to enable IO Bypass acceleration for logical drives comprised of SSDs only.

To adjust the IO Bypass settings:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys to the select an array, press `Enter`, then select **IO Bypass Settings.**
3. From the pop-up menu, select **Enabled** or **Disabled**, then press `Enter`.
4. Select **Submit Changes**.

10.5.4 Editing Logical Drive Properties

Use this option to edit logical drive properties, including acceleration method and logical drive label.

To edit logical drive properties:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys to select an array, press `Enter`, then select **List Logical Drives.**
3. Use the arrow keys to select a logical drive, press `Enter`, then select **Edit Logical Drive**.
4. Select **Acceleration Method**, then select one of these options from the pop-up menu:
   - IO Bypass (for logical drives comprised of SSDs)
   - Controller Cache
   - None (to disable acceleration)
5. Select **Logical Drive Label**, then type the new label.
6. Select **Submit Changes**.

10.5.5 Deleting a Logical Drive

Note: Use this procedure to delete an individual logical drive. To delete all logical drives on an array, see 10.5.9. Deleting an Array.

To delete a logical drive:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys the select an array, press `Enter`, then select **List Logical Drives.**
3. Use the arrow keys to select a logical drive, press `Enter`, then select **Delete LD**.

   Note: Be sure to delete logical drives from the bottom of the list and move up. If you delete a logical drive from the middle of the list, the remaining logical drives move to the Transformation state. During that time, you cannot delete any other logical drives until they all move to the Optimal state.

10.5.6 Assigning Spares

A spare is a disk drive that automatically replaces a failed drive in a logical drive. A spare drive must meet the following criteria:

- It must be an unassigned drive or a spare for another array.

- It must be the same type as existing drives in the array (for example, SATA or SAS).
- The drive capacity must be greater than or equal to the smallest drive in the array.

To assign a spare to an array:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys the select an array, press `Enter`, then select **Manage Spare Drives.**
3. Select the spare activation type:
   - **Assign Dedicated Spare**: activate spare when drive fails
   - **Assign Auto Replace Spare**: activate spare when drive reports a predictive failure (SMART) status
   - **Change Spare type to Dedicated**: change assigned spare type from AutoReplace to Dedicated
   - **Change Spare type to AutoReplace**: change assigned spare type from Dedicated to AutoReplace
4. Use the arrow keys to select the drive to assign as a spare.

   Note: Only drives that meet the above criteria are displayed.

10.5.7 Deleting a Spare Drive

To delete a spare drive:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys the select an array, then press `Enter`.
3. Select **Manage Spare Drives**, then select **Delete**.
4. If the array has more than one assigned spare, use the arrow keys to select a spare from the list, then press `Enter`.

10.5.8 Identifying the Drives in an Array

Use this option to identify and locate the physical drives in an array by turning on their Identification LED.

To identify the physical drives in an array:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays.**
2. Use the arrow keys to select an array, then press `Enter`.
3. Select **Identify Device**.
4. Enter a value into **Identification Duration (seconds).** This value determines how long the LED on the device will remain on.
5. Select **Identify by Drive Configuration type**, then select one of these options from the pop-up menu:
   - Data Drive(s) only
   - Spare Drive(s) only
   - All Physical Drives (default)
6. Select **Start**, then press `Enter`.
7. To turn off the Identification LED(s), press `Esc` to return to the previous menu, then select **Stop**.

10.5.9 Deleting an Array

Note: Use this procedure to delete all logical drives on an array, and the array itself. To delete an individual logical drive, see 10.5.5. Deleting a Logical Drive.

To delete an array:

1. From the main menu, select **Array Configuration**, then select **Manage Array LD.**
2. Use the arrow keys the select an array, press `Enter`, then select **Delete Array.**

10.5.10 Add Drives

Table 10-1. Add Drives

Option	Definition
Expand array	Expands the array by adding data drives.
Add drive to existing parity group	Adds an equal number of drives to each parity group in an array.
Add entire parity group	Add drives by adding entire parity groups to array.
Auto expand	Based on the parity group, it will auto expand.

10.5.11 Remove Drives

Table 10-2. Remove Drives

Option	Definition
Shrink array	Shrinks the array by removing the current data drives from array.
Remove drive from existing parity group	Removes an equal number of drives to each parity group from array.
Remove entire parity group	Removes drives by removing entire parity groups from array.
Auto shrink	Based on the parity group, it will auto shrink.

10.5.12 Move Drives

Use this option to replace one or more drives in the array with drives of the same type.

10.6 Modifying SmartHBA 2200/SmartRAID 3200 Controller Settings

To modify the SmartHBA 2200/SmartRAID 3200 settings, start the Microchip SAS/SATA Configuration Utility, select **Configure Controller Settings** from the main menu, then select **Modify Controller Settings**, **Modify Cache Settings**, or **Advanced Controller Settings**. You can set the options in the table below.

Option	Description
Modify Controller Settings	
Transformation Priority	Sets the priority for array expansion: • Low: normal system operations take priority over array expansion • Medium: normal system operations and array expansion get equal priority • High: expansion takes precedence over all other system operations
Rebuild Priority	Sets the priority for rebuilding a failed logical drive: • Low: normal system operations take priority over rebuilds • Medium: normal system operations and rebuilds get equal priority • Medium High: rebuilds get higher priority than normal system operations • High: rebuilds take precedence over all other system operations
Surface Scan Analysis Priority	Determines the time, in seconds, that a controller must be inactive before a surface scan analysis is started on the physical drives connected to it. The scanning process checks physical drives for bad sectors and, in fault-tolerant logical drives, such as RAID 5, it also verifies the consistency of parity data. Delay value ranges from 1-30 seconds. Set the value to "0" to disable the feature. Set the value at "31" to maintain high priority.

.....continued

Option	Description
Current Parallel Surface Scan Count	Sets the surface scan count for the controller. Set the value to "1" to disable the feature. **⚠ CAUTION** Disabling Surface Scan Analysis is not recommended as it will prevent the controller from proactively finding and correcting disk surface errors, which may lead to data loss.
Unconfigured Physical Drive Write Cache	Enables and disables physical drive write cache for unconfigured drives on the controller.
HBA Physical Drive Write Cache State	Enables and disables physical drive write cache for HBA drives on the controller.
Configured Physical Drive Write Cache State	Enables and disables physical drive write cache for configured drives on the controller.
Modify Spare Activation Mode	
Spare Activation Mode	Sets the spare activation mode to activate on failure or predictive failure activation. The failure spare activation mode, activates the spare assigned for the Logical Drive when a member of the Logical drive fails. In Predictive Spare activation mode, activation is done when a drive reports a predictive failure.
Configure Controller Port Mode	
Connector Mode (CN0:CN3	Configures the controller connectors to different operating modes: • HBA: exposes physical drives to the operating system • RAID: exposes only RAID volumes to the operating system • Mixed: exposes RAID volumes and physical drives to the operating system
Modify Cache Settings	
No Battery Write Cache	Allows write caching to be enabled when a battery/supercapacitor is not present or fully charged. This setting affects all logical drives on the controller. **⚠ CAUTION** Enabling write caching on a cache module without a fully charged battery/ supercapacitor may cause data loss in the event of a power failure.
Cache Ratio (Read)	Sets the ratio of controller cache memory used for read-ahead cache versus write cache. Cache ratio values range from 0–100, in increments of 5.
Write Cache Bypass Threshold	All writes larger than the specified value will bypass the write cache and be written directly to the disk for non-parity RAID volumes. A smaller value allows the controller to reserve write caching to I/Os smaller than the threshold.
Advanced Controller Settings (*RAID mode or Mixed mode only*)**:**	
Degraded Mode Performance Optimization	For degraded RAID 5 logical drives, enabling this setting directs the controller to attempt to improve performance of large read requests by buffering physical drive requests. Disabling this setting forces the controller to read from the same drives multiple times.
Physical Drive Request Elevator Sort	Sets the behavior of the drive's write Elevator sort algorithm, a scheduling optimization that prioritizes I/O requests such that disk arm and head motion continues in the same direction. Enabling the elevator sort improves seek times and disabling the elevator sort improves throughput.
Alternate Inconsistent Repair Policy	Sets the surface analysis inconsistency repair policy for RAID 5 when the controller detects that the parity information does not match the data on the drives. Disabling the repair policy directs the controller to update the parity information, leaving the data untouched. Enabling the repair policy directs the controller to update the data on the drives based on the parity information.
Max Drive Request Queue Depth	Sets the queue depth for the controller. Valid values are Automatic, 2, 4, 8, 16, and 32.
Monitor and Performance Analysis Delay	Sets the Monitor and Performance Analysis delay for the controller, in minutes. Set the value to zero to disable Monitor and Performance Analysis. Default is 60 minutes.

.....continued

Option	Description
HDD Flexible Latency Optimization	Enables flexible latency optimization for HDDs. When FLS is enabled, the controller detects high-latency I/O requests and applies a cutoff, or threshold, value, after which it suspends elevator sorting and services the request right away. Valid values are: • Disable (default). • Low • Middle(100 ms) • High • Very high(30 ms) • Very high(10 ms)
Configure Port Discovery Protocol	This menu provides options to configure the protocols used by the controller to discover the ports. A discovery protocol is the signal group/PHY mode protocol used to discover what's attached. Options are Auto-detect/UBM/SGPIO/VPP This operation requires reboot. Provide options to: • View Current port Discovery Protocol • View Pending port Discovery Protocol • Set port Discovery Protocol • Reset port Discovery Protocol to default
Modify Expander Minimum Scan Duration	This menu provides option to configure minimum scan duration for expanders. Entered value should be in seconds.

10.7 Clearing the Controller Configuration

Clearing the controller configuration destroys the controller meta-data, including partition information.

CAUTION When you clear the controller configuration, all data on the attached media (SSD/HDD) will no longer be accessible and cannot be recovered. Be sure you no longer need the data on the controller before proceeding!

To clear the controller configuration:

1. From the main menu, select **Configure Controller Settings**, then select **Clear Configuration**.
2. Select **Delete All Array Configurations** or **Delete Configuration Metadata on All Physical Drives.**
3. Select **Submit Changes**.

10.8 Backup Power Source

Use the Backup Power Source option to check the status of the cache system's backup power supply, if applicable. From the main menu, select **Configure Controller Settings**, then select **Backup Power Source**.

10.9 Managing Power Settings

Use the Manage Power Settings option to configure the controller's power modes. There are three available power modes. You can also enable Survival mode.

- **Maximum Performance** (default): All settings are selected based on maximum performance. Power savings options that affect performance are disabled.
- **Balanced**: You can use this setting to save power with minimal effects on performance. For large queue depths, this setting affects throughput by 10% or less. At lower queue depths or infrequent I/O, impacts on performance may be greater. This command is typically useful in

environments using only hard drives, and is not recommended when using SSDs. Settings are based on the user configuration, such as the number or types of drives, the RAID level, storage topology, and so forth. Significant changes to the configuration may require a reboot for optimal setting selection. If a reboot is required to change settings, UEFI HII prompts for a reboot to reflect requested settings.

- **Survival Mode**: Allows the controller to throttle back dynamic power settings to their minimums when the temperature exceeds the threshold. Enabling Survival Mode allows the server to continue running in more situations, but may affect performance.

To change the power settings for a controller:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Controller Configuration**.
4. Select **Manage Power Settings**, then select **Power Mode**.
5. Press **Tab** to select the power mode.
6. Select **Survival Mode**, then press `Tab` to select Enabled or Disabled.
7. Select **Submit Changes**.

10.10 Out of Band Messaging Settings

Use this option to configure the Out of Band Messaging Interface to PBSI, MCTP, or Disable.

Note: This option is supported in the UEFI/HII interface only.

To change the Out of Band Messaging settings for a controller:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**.
4. Select **Out of Band Messaging Settings**.
5. Select **OOB Interface** and press `Enter`.
6. From the pop-up menu, select **PBSI**, **MCTP**, or **Disable OOB interface**.
7. To configure Out of Band Messaging for PBSI, set these parameters:

PBSI Parameters	Description
SMBus Slave Address	Sets the SMBus (System Management Bus) slave address of the controller to a valid hexadecimal address value.
SMBus Clock Speed	Sets the SMBus clock speed: • Feature Disabled (Default) • SMBus clock speed 100 kHz • SMBus clock speed 400 kHz
SMBus Clock Stretching	Sets the SMBus Clock Stretching mode: • Enable: Enables SMBus clock stretching • Disable: Disables SMBus clock stretching

8. To configure Out of Band Messaging for MCTP, set these parameters:

MCTP Parameters	Description
SMBus Slave Address	Sets the SMBus (System Management Bus) slave address of the controller to a valid hexadecimal address value. (For valid range, refer to the Management Component Transport Protocol (MCTP) SMBus/I2C Transport Binding Specification document.)
SMBus Device Type	Sets the SMBus Device Type:

MCTP Parameters	Description
	• Default • Fixed • ARP (Address Resolution Protocol)
SMBus Physical Channel	Sets the SMBus Channel mode: • Enable: Enables SMBus channel • Disable: Disables SMBus channel
Use Static EIDs during Initialization	Sets the Static End Point Identifier (EID) mode: • Enable: Enables Static EID • Disable: Disables Static EID
VDM Discovery Notify	Sets the Vendor Defined Message (VDM) discovery notification mode: • Enable: Enables VDM discovery notification • Disable: Disables VDM discovery notification

9. Select **Submit Changes**.

10.11 Using the Encryption Manager

Notes:

1. This option is available only in the UEFI/HII interface; UEFI version 2.4A or higher, recommended.
2. This option is available only for controllers that support maxCrypto Controller-Based Encryption. See 4.1. About Your SmartRAID 3200 Series Host Bus Adapter for more information.

The Encryption Manager allows you to configure the controller-based encryption options on your Smart Storage controller. The Encryption Manager supports two roles for managing encryption services:

- A Crypto Officer (Admin) role that can perform all encryption operations
- A User role with reduced privileges

Once you configure the Encryption Manager, you can encrypt arrays and logical drives, and create storage spaces with mixed encrypted and plaintext volumes. For more information about creating and managing encrypted volumes, see 10.3. Creating an Array.

10.11.1 Encryption Manager Full Setup

Use the Full Setup option to configure the Encryption Manager for initial use. This option allows you to set the master encryption key, configure the Crypto Officer account, and enable other basic encryption settings. It also allows you to accept the Encryption Manager Terms of Use.

To configure the Encryption Manager:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **Full setup**.
5. Using the arrow keys and Enter key, configure basic encryption settings:
   a) In the Encryption Mode field, select one of these options:
      - **Enable and Allow future...** to enable encryption and allow plaintext logical devices to be created in addition to encrypted logical devices.
      - **Enable and Disallow future...** to enable encryption and allow only encrypted logical devices to be created.

- **Disable** to disable the Encryption Manager. If encryption is disabled, all encrypted logical drives are set to offline and the data becomes inaccessible; newly created logical drives will not be encrypted. (They will be created as plaintext logical drives.)

b) In the Enter new password field, enter the Crypto Officer password: press `Enter`, type the password in the pop-up window, then press `Enter` to submit.

The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (#,!,@,...).

c) In the Master Key field, enter the master encryption key: press `Enter`, type the key in the pop-up window, then press `Enter` to submit.

The Master Key is a 10-32 character string, comprising all printable ASCII characters.

⚠ CAUTION Be sure to record the master key and store in a safe place. Once set, the Master Key cannot be displayed or recovered, only reset. Failure to provide the Master Key may result in encrypted data being irretrievable.

6. Select **Proceed to Next Form**.
   The Terms of Use form opens.
7. Select **Accept** to accept the Terms and Conditions.
8. Select **Submit Changes**.

10.11.2 Modifying the Encryption Manager Configuration

Use this option to modify the Encryption Manager configuration, including the master encryption key and other basic encryption settings, and the Crypto Officer and User account settings.

Note: This option is available only after you complete the Encryption Manager Full setup; see 10.11.1. Encryption Manager Full Setup.

To modify the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **Crypto Officer Settings**.
5. Using the arrow keys and Enter key, modify basic encryption settings, as needed (encryption enable/disable, master encryption key, allow/disallow future plaintext volumes).
6. In the Firmware Update field, select **Unlock** to allow controller firmware upgrades. Select **Lock** to block (prevent) firmware upgrades.
7. Using the arrow keys and Enter key, configure the Crypto Officer and User account settings:
   a) Change the Crypto Officer password, as needed: press `Enter`, type the password in the pop-up window, then press `Enter` to submit.
   b) Enter the Password Recovery Question for a forgotten password: press `Enter`, type the recovery question in the pop-up window, then press `Enter` to submit.
   The recovery question is 16-255 characters, comprising all printable ASCII characters.
   c) In the Password Recovery Answer field, enter the answer to the recovery question.
   The recovery answer is 16-64 characters and is case sensitive, comprising all printable ASCII characters.
   Note: Password recovery is available only for the Crypto Officer account.

d) In the User Password field, enter the User account password: press `Enter`, type the password in the pop-up window, then press `Enter` to submit.

8. Select **Proceed to Next Form**.
   The Terms of Use form opens.
9. Select **Accept** to accept the Terms and Conditions.
10. Select **Submit Changes**.

10.11.3 Modifying User Account Settings

Use this option to modify User account settings, including the account password and firmware upgrade options.

Note: This option is available only after you complete the Encryption Manager Full setup; see .

To modify the User Account Settings:

1. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
2. Select **Manage Encryption Settings**, then select **User Settings**.
3. Modify the User account password, as needed: press `Enter`; when the pop-up window opens, type the password, then press `Enter` to submit.

   The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (#,!,@,...).
4. In the Firmware Update field, select **Unlock** to allow the controller firmware to be upgraded. Select **Lock** to prevent the controller firmware from being upgraded.
5. Select **Proceed to Next Form**.
6. Select **Submit Changes**.

10.11.4 Resetting a Forgotten Password

Use this option to reset the Crypto Officer password by answering the recovery question.

Note: Password recovery is available only for the Crypto Officer account.

To reset a forgotten password:

1. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
2. Select **Manage Encryption Settings**, then select **Forgot Crypto Officer Password**.
3. Enter the answer to the password recovery question;
4. Enter the Crypto Officer's new password: press `Enter`; when the pop-up window opens, type the password, then press `Enter` to submit..
5. Select **Submit Changes**.

10.11.5 Clearing the Encryption Manager Configuration

Clearing the Encryption Manager configuration resets all keys, passwords, and users, including the Crypto Officer account and User account, and places the Encryption Manager in the factory-new state. If encrypted volumes are still configured, this option is only available in the Microchip SAS/SATA Configuration Utility or by running the GUI/CLI tools in offline mode.

Note: Clearing the configuration does not affect the encrypted logical drives in your storage space. However, to continue accessing or managing encrypted volumes, you must reconfigure the basic encryption settings in the Encryption Manager; see 10.11.1. Encryption Manager Full Setup.

To clear the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Clear Configuration**.
5. If your storage space includes encrypted volumes, enter the Encryption Master Key.
   The Master Key is a 10-32 character string, comprising all printable ASCII characters.
6. Select **Submit Changes**.

10.11.6 Re-Keying a Logical Drive

Use this option to re-key a logical drive for added security. The logical drive key is used with the master key to encrypt the device.

To re-key a logical drive:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
2. Select an array, then select **List Logical Drives**.
3. Select an encrypted logical drive, then select **Volume key rekey**.
4. Select your account type: Crypto Officer or User.
5. Select **Submit Changes**.

10.11.7 Converting Plaintext Data to Encrypted Data

Use this option to convert plaintext data to encrypted data. You can choose to preserve or discard the existing data during conversion.

To convert plaintext data:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
2. Select an array, then select **List Logical Drives**.
3. Select a plaintext logical drive, then select **Convert Plaintext Data to Encrypted Data**.
4. Select your account type: Crypto Officer or User.
5. In the Convert Plaintext Data to Encrypted Data field, select discard existing data or preserve existing data during conversion.
6. Select **Submit Changes**.

10.11.8 Erasing an Encrypted Logical Drive

Use this option to securely erase existing data on an encrypted logical drive. Secure erase completely destroys the data on the logical drive; the data is completely and irretrievably eradicated.

To erase an encrypted logical drive:

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
2. Select an array, then select **List Logical Drives**.
3. Select an encrypted logical drive, then select **Secure erase**.
4. Select your account type: Crypto Officer or User.
5. Select **Submit Changes**.

10.11.9 Importing a Foreign Master Key

When an encrypted logical drive is moved to another controller, the master key used to encrypt the logical drive is needed to decrypt it. Use the Import Foreign Local Key option to import the master key so that the logical drive data can be accessed and managed on the new controller.

Note: This option is available only if an encrypted logical device with a missing key is detected in the configuration.

To import a foreign master key:

1. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
2. Select **Import Foreign Local Key**.
3. Enter the master key used to encrypt the logical drive.
   The Master Key is a 10-32 character string, comprising all printable ASCII characters.
4. Enter the Crypto Officer password: press `Enter`; when the pop-up window opens, type the password, then `Enter`.
5. Select **Submit Changes**.

10.12 Configuring the Controller Port Mode

You can set entire controller port mode or set independent port mode to:

- HBA: exposes physical drives to the operating system
- RAID: exposes only RAID volumes to the operating system and reserves all physical drives for array creation
- Mixed: exposes RAID volumes and unconfigured physical drives to the operating system
- Independent: Allows to set above options independently for each connector of the controller.

Notes:

1. Changing the port mode from Mixed or HBA to RAID mode removes access to physical drives from the operating system.
2. HBA mode is not available if a port is already configured with logical drives.

To configure the port mode for a controller:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Configure Controller Port Mode**.
4. Select the controller port mode (HBA, RAID, Mixed).
5. Select **Submit Changes**.

10.13 Device Information

The Device Information menu provides details about the device, such as the Model, Serial Number, and Device Type. To view the device information, start the Microchip Configuration Utility, select your controller, then press `Enter`. From the main menu, select **Disk Utilities**, select the disk drive, then press `Enter`.

10.14 Identifying a Disk Drive

You can use the disk utilities to physically locate and identify a disk drive by turning on its Identification LED.

To identify a disk drive:

1. From the main menu, select **Disk Utilities**.
2. Select the disk drive you want to locate, then press `ENTER`.
3. Select **Identify Device**, then enter a value into **Identification Duration (seconds)**. This value determines how long the LED on the device will remain on.

4. Select **Start**, then press `Enter`.
5. To turn off the Identification LED, press `ESC` to return to the previous menu, select **Stop** and press `Enter`.

10.15 Erasing a Disk Drive

You can use the disk utilities to erase existing data on any unassigned disk drive. The erase operation destroys the data by writing random patterns across the drive; it does not just write zeros.

To erase a disk drive:

1. From the main menu, select **Disk Utilities**.
2. Select the disk drive you want to erase, then press `Enter`.
3. Select **Erase Disk,** then select **Continue**.

10.16 Updating Drive Firmware

You can use the disk utilities to flash a hard drive with new firmware.

To update drive firmware:

1. Copy the firmware binary file to a USB flash drive, then connect the USB drive to the machine. Alternatively, copy the firmware binary to a known location on your machine.
2. From the main menu, select **Disk Utilities**, then select **Update Drive Firmware**.
3. Select a disk drive, then enter the firmware update mode:

Option	Description
Mode 5	Download and Activate
Mode 7	Download in Multiple Transfers
Mode E	Download in Multiple Transfers but Do Not Activate
Mode E+F (HBA Mode only)	Download in Multiple Transfers and Activate

4. Enter the Transfer Size, in 512 byte-increments. The default transfer size is 32768 (32K) bytes. The maximum transfer size is 262144 (256K) bytes.

   Note: Transfer Size is not applicable for Mode 5.
5. Select **Proceed.**
6. Select the storage device where the firmware binary file is located (the USB drive, for instance), navigate the folder hierarchy, then select the firmware binary file.

   The firmware is sent to the hard drive.
7. When the update is complete, reboot the server.

10.17 Clearing Configuration Meta-data

You can use the disk utilities to clear the controller configuration meta-data from any drive that is not part of an array.

Note: This option is enabled only if the selected drive contains controller configuration meta-data. A drive may contain configuration meta-data even if it is not part of an array.

To clear the configuration meta-data from a drive:

1. From the main menu, select **Disk Utilities**.
2. Select a disk drive with configuration meta-data, then press `Enter`.
3. Select **Clear Configuration Metadata,** then select **Continue**.

10.18 Setting the Bootable Device(s) for Legacy Boot Mode

Note: This option is applicable only for Legacy Boot Mode.

This option sets the primary and secondary physical boot device(s) for Legacy Boot Mode. The secondary boot device acts as a failover to the primary boot device.

To set the physical boot device(s) for a controller:

1. From the menu, select **Set Bootable Device(s) for Legacy Boot Mode**, then select **Select Bootable Physical Drive**.
2. To set the default bootable device, select a physical drive from the list, then select **Set as Primary Bootable Device**.
3. To set the secondary bootable device, select a physical drive from the list, then select **Set as Secondary Bootable Device**.

Note: To clear previously set boot devices, select **Clear Bootable Device(s)**.

10.19 Updating the SmartHBA 2200 Firmware

To update the SmartHBA 2200 firmware:

1. Copy the firmware binary file (.bin) to a USB flash drive, then connect the USB drive to the machine. Alternatively, copy the firmware binary to a known location on your machine.
2. From the main menu, select **Administration**, then select **Flash Controller Firmware**.
3. Select **Continue with flashing Firmware.**
4. Select the storage device where the firmware binary file is located (the USB drive, for instance), navigate the folder hierarchy, then select the firmware binary file.

   The firmware is sent to the controller.
5. When the update is complete, reboot the server.

10.20 Creating a Support Archive

Use this option to save configuration and status information to help Customer Support diagnose a problem with your system. Saved information includes device logs, drive logs, event logs, error logs, controller logs, and statistics.

To create a support archive:

1. From the main menu, select **Administration**, then select **Save Support Archive**.
2. Select the device where the support archive information will be gathered and stored, then press `Enter`.

   The system gathers the logs and statistics for the device and displays the path where the information is saved.
3. Press any key to complete the operation and exit.

10.21 Resetting the Controller to Factory Defaults

⚠ CAUTION Use extreme caution when resetting the controller to factory defaults. This operation clears configured arrays, controller configuration metadata on the drives, license keys, and encryption configuration, causing all existing data and configuration settings to be irretrievably lost.

Use this option to reset the SmartHBA 2200 to factory default settings.

To reset the controller:

1. From the main menu, select **Administration**.
2. Select **Reset controller settings to factory defaults**.

3. Select **Submit Changes**.

10.22 Extracting Controller Debug Token

Note: For advanced users. Contact Microchip support for more information.

This option allows user to save the controller debug token to a selected storage device.

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (See 10.1. Running the Microchip SAS/SATA Configuration Utility: UEFI/HII.
2. Select your controller, then press ENTER.
3. Start the Microchip HII Configuration Utility, navigate to the Device Settings menu, then select your controller.
4. From the main menu, select **Administration**.
5. Select **Extract Debug Token**.
6. Select **Storage Media**.
7. Select **Submit Changes**.

11. Installing the SmartPQI Drivers from Source

This section explains how to build and install the SmartPQI drivers from source code for the supported Linux OSes, including how to install the packages using the installation DVD as the repository.

11.1 Installation Instructions for Supported Linux OSes

This section explains how to install the driver from source for the following Linux OSes:

- RHEL OS images
- SuSE OS images

Use the following command to determine the type of OS installed on a Linux system:

```
# lsb_release -a
```

Note: The following instructions assume you are installing the packages from the RHEL or SuSE repositories; if not, refer to 11.2. Using the Installation DVD as the Repository.

To install the SmartPQI driver from source:

1. Build the driver from the source using the following command:`$ sudo su`
   Note: You must have administrator privileges to perform the installation steps.
2. Install the following driver dependency packages and reboot the system if necessary:
   RHEL: `# yum install kernel kernel-devel kernel-headers gcc`
   SLES: `# zypper install kernel-devel kernel-syms gcc make`
3. Extract the driver source code from the `source tar.bz2` file by using the following command:`# tar –jxvf smartpqi-1.1.2-125.tar.bz2`
4. Compile the `smartpqi.ko` file by using the following command:

   ```
   # cd smartpqi-1.1.2
   # make -f Makefile.alt
   ```

   Note: After the compilation you will get a smartpqi.ko driver file, which is the driver module.
5. Use the following command to backup the existing inbox driver:

   ```
   # mv /lib/modules/`uname -r`/kernel/drivers/scsi/smartpqi/smartpqi.ko \
   /lib/modules/`uname -r`/kernel/drivers/scsi/smartpqi/smartpqi.ko.org
   ```
6. Copy the smartpqi.ko driver file to the destination by using the following command:`# cp ./smartpqi.ko /lib/modules/`uname -r`/kernel/drivers/scsi/smartpqi`
7. Use the following command to rebuild initramfs/initrd process with the newly installed smartpqi driver:`# dracut -v -f --add-drivers smartpqi`
   Note:
   - The dracut command places the newly installed `smartpqi.ko` driver modules into the initramfs/initrd file to include them in the Linux kernel.
8. Reboot the system to load the new initramfs/initrd, which will contain the newly installed `smartpqi.ko` driver.

11.2 Using the Installation DVD as the Repository

Follow the instructions in this section to install the packages required to compile the driver modules using the OS installation DVD as the repository. In these procedures, the DVD is used as the package repository.

Installing Packages on a RHEL-based OS

The following steps install the packages required to compile the driver modules from source on a RHEL-based OS.

1. Execute the following command to become a super user to edit and make changes to various system files:

   ```
   $ sudo -i
   ```

   Note: Super user rights are required to edit and make changes in various system files.
2. Get the name of the installation DVD entry in `/dev` directory. The DVD is visible as `/dev/srX`. Use the following command to list all the scsi devices on the system.

   ```
   # lsscsi
   ```
3. Once the DVD name is confirmed, create a location to mount the DVD, for example:

   ```
   # mkdir /media/iso
   ```
4. Add the following line to `/etc/fstab` to create the DVD entry:

   ```
   /dev/srX /media/iso udf,iso9660 noauto,user,ro 0 0
   ```
5. Use the following command to mount the DVD:

   ```
   # mount /dev/srX
   ```
6. Create a `dvd.repo` to use the packages from the mounted DVD location:

   ```
   [dvd]
          name=Red Hat Enterprise Linux Installation DVD
          baseurl=file:///media/iso
          enabled=1
   ```
7. Import the GPG keys for YUM to authenticate the RPM packages in the DVD:

   ```
   # rpm --import /media/iso/RPM-GPG*
   ```
8. Run the following commands to enable the DVD repository:

   ```
   # yum repolist
   # yum install
   ```

Installing Packages on a SuSE-based OS

The following steps install the packages required to compile the driver modules from source on a SuSE-based OS.

1. Execute the following command to become a super user:

   ```
   $ sudo su
   ```

   Note: Super user rights are required to edit and make changes in various system files.
2. Get the name of the installation DVD entry in `/dev` directory. The DVD is visible as `/dev/srX`. Use the following command to list all the scsi devices on the system.

   ```
   # lsscsi
   ```
3. Once the DVD name is confirmed, create a location to save the DVD image, for example:

   ```
   # mkdir /var/iso
   ```
4. Create an ISO image from the installation disk. Once the DVD image is saved, zypper uses the ISO as an installation service and install the packages from it by using the following command:

   ```
   # dd if=/dev/srX of=/var/iso/sles.iso
   ```
5. Once the installation disk is saved as an ISO image, set it as an installation service by using the following command:

   ```
   # zypper sa “iso:/?iso=/var/iso/sles.iso” “SLES xy spz”
   ```

   Where, xy z is the SLES distribution ID eg 10 sp1.
6. Run the following command after adding the ISO image as an installation service:

```
# zypper sl
```

12. SmartRAID/SmartHBA Physical and Logical Device Support

Table 12-1. SmartRAID/SmartHBA Physical and Logical Device Support

Item	SmartRAID Adapters	SmartHBA Adapters	Description
Max single/dual devices supported	256	256	# of physical SAS/SATA devices supported. Includes SEP devices, expanders. Results into 238 storage devices supported
Max # of RAID arrays supported	64	64	Maximum number of RAID arrays supported / exposed to host OS
Max # of logical drives/single cached volumes (single drive R0)	64	64	Maximum number of logical drives (single or RAID) exposed to host / OS
Multi-LUN	Y	Y	Support for LUNs per SCSI ID available (for RBODs, tape libraries)
# of LUNs supported per SCSI ID	256	256	# of SCSI LUNs supported per SCSI ID (other than RAID LUNs)
RAID 0: max. devices per volume, RAID 1: 2 devices per volume or 3 devices with no plus hot spare, RAID 10: max. devices per volume	128 drives per volume max.	128 drives max.	Supported drive count in striping and mirroring RAID arrays and the combination of both (RAID10)
RAID 5: max devices per volume	128	128	Supported drive count in a RAID5
RAID 50, 6, 60 max. devices per volume	128	N/A	Supported drive count in the named RAID arrays
maxCache 4.0 logical caching volumes	32	N/A	Maximum 32 logical drives can be accelerated by maxCache. 32 LDs used for acceleration.
# of spare drives supported	32	32	Number per Array/number per adapter

13. Safety Information

To ensure your personal safety and the safety of your equipment:

- Keep your work area and the computer clean and clear of debris.
- Before opening the system cabinet, unplug the power cord.

13.1 Electrostatic Discharge (ESD)

⚠ CAUTION ESD can damage electronic components when they are improperly handled, and can result in total or intermittent failures. Always follow ESD-prevention procedures when removing and replacing components.

To prevent ESD damage:

- Use an ESD wrist or ankle strap and ensure that it makes skin contact. Connect the equipment end of the strap to an unpainted metal surface on the chassis.
- Avoid touching the adapter against your clothing. The wrist strap protects components from ESD on the body only.
- Handle the adapter by its bracket or edges only. Avoid touching the printed circuit board or the connectors.
- Put the adapter down only on an antistatic surface such as the bag supplied in your kit.
- If you are returning the adapter to Microchip Product Support, put it back in its antistatic bag immediately.

If a wrist strap is not available, ground yourself by touching the metal chassis before handling the adapter or any other part of the computer.

14. Technical Specifications

14.1 Environmental Specifications

Note: SmartHBA 2200/SmartRAID 3200 Series adapters require adequate airflow to operate reliably. Forced airflow is **required**. See the Recommended Airflow table below for more information.

Ambient temperature with forced airflow	0 °C to 55 ° C
Relative humidity	20% to 80%, non-condensing
Altitude	Up to 3,000 meters

Note: Ambient temperature is measured 1” from the HBA processor.

Table 14-1. Recommended Airflow

Controller	Recommended Airflow/Linear Feet per Minute (LFM)
Adaptec SmartHBA 2200-16i	250 LFM
Adaptec SmartRAID 3204-8i /e	250 LFM
Adaptec SmartRAID 3252-8i /e	250 LFM
Adaptec SmartRAID 3254-8i /e	250LFM
Adaptec SmartRAID 3254-16i /e	250 LFM
Adaptec SmartRAID 3258-16i /e	250 LFM
Adaptec SmartRAID Ultra 3254-16e /e	330 LFM
Adaptec SmartRAID 3254-16e /e	250 LFM
Adaptec SmartRAID Ultra 3258P-16i /e	300 LFM
Adaptec SmartRAID Ultra 3258P-32i /e	300 LFM

14.2 DC Power Requirements

Bus Type	Description	Requirements
PCIe	DC voltage	3.3 V ± 9%, 12 V ± 8%, 3.3 V ± 9% (auxiliary power from PCIe slot)

14.3 Current and Power Requirements

Adapter Model	Typical Power	Typical Current
Adaptec SmartHBA 2200-16i	19.6 W	0.15 A at 3.3 VDC; 1.52 A at 12 VDC
Adaptec SmartRAID 3204-8i /e	17.8 W	0.09 A at 3.3 VDC; 1.46 A at 12 VDC
Adaptec SmartRAID 3252-8i /e	17.8 W	0.09 A at 3.3 VDC; 1.46 A at 12 VDC
Adaptec SmartRAID 3254-8i /e	17.8 W	0.09 A at 3.3 VDC; 1.46 A at 12 VDC
Adaptec SmartRAID 3254-16i /e	21.3 W	0.09 A at 3.3 VDC; 1.75 A at 12 VDC
Adaptec SmartRAID 3254-16e /e	21.3 W	0.09 A at 3.3 VDC; 1.75 A at 12 VDC
Adaptec SmartRAID 3258-16i /e	21.3 W	0.09 A at 3.3 VDC; 1.75 A at 12 VDC
Adaptec SmartRAID Ultra 3254-16e /e	26.5 W	0.15 A at 3.3 VDC; 2.17 A at 12 VDC
Adaptec SmartRAID Ultra 3258P-16i /e	30 W	0.15 A at 3.3 VDC; 2.46 A at 12 VDC
Adaptec SmartRAID Ultra 3258P-32i /e	35 W	0.15 A at 3.3 VDC; 2.88 A at 12 VDC

Note: Smart adapters with a x16 PCIe interface require a x16 PCIe expansion slot that can supply 75 watts of power.

15. Revision History

Table 15-1. Revision History

Revision	Date	Description
G	07/2024	Updated for SR 3.4.0 release.
F	02/2024	Updated for SR 3.3.4 release. Added " /e" designation to select boards.
E	06/2023	Updated for SR 3.3.0 release.
D	03/2023	Updated for SR 3.2.4 release. Added Managed SED section.
C	06/2022	Updated for SR 3.1.8 release.
B	07/2021	Updated for SR 3.1.4 release.
A	06/2021	Document created.

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 devices:

- 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 and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- 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. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized

access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication is provided for the sole purpose of designing with and using Microchip products. Information regarding device applications and the like 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.

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.

ISBN: 978-1-6683-4921-2

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	**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			