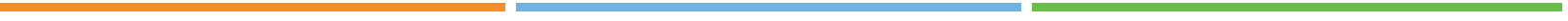


# Adaptec SmartRAID 3100 and SmartHBA 2100 Installation and User Guide



# Table of Contents

1. About This Guide.....	5
1.1. What You Need to Know Before You Begin.....	5
1.2. Terminology Used in this Guide.....	5
1.3. How to Find More Information.....	6
2. Kit Contents and System Requirements.....	7
2.1. Kit Contents.....	7
2.2. System Requirements.....	7
3. About Your SmartRAID 3100 Series Host Bus Adapter .....	8
3.1. Standard Features.....	8
3.2. Mechanical Information .....	8
3.3. Visual Indicators.....	8
3.4. About the Adaptec SmartRAID 3101-4i/3151-4i.....	10
3.5. About the Adaptec SmartRAID 3101E-4i.....	12
3.6. About the Adaptec SmartRAID 3102-8i/3152-8i/3154-8i.....	14
3.7. About the Adaptec SmartRAID 3102E-8i.....	16
3.8. About the Adaptec SmartRAID 3154-8e.....	18
3.9. About the Adaptec SmartRAID 3154-8i8e.....	20
3.10. About the Adaptec SmartRAID 3154-8i16e.....	22
3.11. About the Adaptec SmartRAID 3154-16i.....	24
3.12. About the Adaptec SmartRAID 3154-24i.....	26
3.13. About the SmartRAID 3162-8i/SmartRAID 3162-8i /e Adapter.....	28
4. About Your SmartHBA 2100 Series Host Bus Adapter .....	31
4.1. Standard Features.....	31
4.2. Mechanical Information .....	31
4.3. Visual Indicators.....	31
4.4. About the Adaptec SmartHBA 2100-4i4e.....	32
4.5. About the Adaptec SmartHBA 2100-8i.....	34
4.6. About the Adaptec SmartHBA 2100-8i8e.....	36
4.7. About the Adaptec SmartHBA 2100-16i.....	38
4.8. About the Adaptec SmartHBA 2100-24i.....	40
5. Installing the Controller and Disk Drives.....	43
5.1. Before You Begin.....	43
5.2. Selecting Disk Drives and Cables .....	43
5.3. Installing the Host Bus Adapter.....	43
6. Installing the Driver and an Operating System .....	51
6.1. Download the Driver Package.....	51
6.2. Creating a Driver Disk.....	51
6.3. Installing with Windows.....	51
6.4. Installing with Red Hat Linux .....	52
6.5. Installing with SuSE Linux Enterprise Server.....	52
6.6. Installing with Oracle Linux.....	53
6.7. Installing with Ubuntu Linux.....	53

6.8.	Installing with Debian Linux.....	53
6.9.	Installing with FreeBSD.....	54
6.10.	Installing with Citrix XenServer.....	55
6.11.	Installing with VMware.....	55
7.	Installing the Driver on an Existing Operating System.....	57
7.1.	Download the Driver Package.....	57
7.2.	Creating a Driver Disk.....	57
7.3.	Installing on Windows.....	57
7.4.	Installing on Red Hat.....	57
7.5.	Installing on SuSE Linux Enterprise Server.....	58
7.6.	Installing on Oracle Linux.....	58
7.7.	Installing on Ubuntu Linux.....	58
7.8.	Installing on Debian Linux.....	58
7.9.	Installing on FreeBSD.....	59
7.10.	Installing on Citrix XenServer.....	59
7.11.	Installing on VMware.....	60
8.	Managing SED.....	61
8.1.	Overview.....	61
8.2.	Supported Features .....	61
8.3.	Workflows .....	63
8.4.	Troubleshooting.....	68
9.	Solving Problems .....	70
9.1.	Troubleshooting Checklist.....	70
9.2.	Resetting the Adapter .....	70
10.	Using the Microchip SAS/SATA HII Configuration Utility.....	71
10.1.	Running the Microchip SAS/SATA Configuration Utility: UEFI/HII.....	71
10.2.	Controller Information.....	71
10.3.	Creating an Array.....	71
10.4.	Creating Arrays with RAID0.....	72
10.5.	Creating a maxCache Array.....	72
10.6.	Managing Arrays and Logical Drives.....	72
10.7.	Modifying SmartHBA 2100/SmartRAID 3100 Settings.....	76
10.8.	Recovering Cache Module.....	79
10.9.	Clearing the Controller Configuration.....	79
10.10.	Backup Power Source.....	79
10.11.	Managing Power Settings.....	79
10.12.	Out of Band Messaging Settings.....	80
10.13.	Using the Encryption Manager.....	81
10.14.	Configuring the Controller Port Mode.....	85
10.15.	Device Information.....	85
10.16.	Identifying a Disk Drive.....	85
10.17.	Erasing a Disk Drive.....	85
10.18.	Updating Drive Firmware.....	86
10.19.	Clearing Configuration Meta-data.....	86
10.20.	Setting the Bootable Device(s) for Legacy Boot Mode.....	86
10.21.	Updating the SmartHBA 2100/SmartRAID 3100 Firmware.....	87

10.22. Creating a Support Archive.....	87
10.23. Resetting the Controller to Factory Defaults.....	87
11. Installing the SmartPQI Drivers from Source .....	88
11.1. Installation Instructions for Supported Linux OSes.....	88
11.2. Using the Installation DVD as the Repository.....	89
12. SmartRAID/SmartHBA Physical and Logical Device Support.....	91
13. Safety Information.....	92
13.1. Electrostatic Discharge (ESD).....	92
14. Technical Specifications.....	93
14.1. Environmental Specifications.....	93
14.2. DC Power Requirements.....	93
14.3. Current and Power Requirements .....	93
15. Revision History.....	95
Microchip Information.....	96
The Microchip Website.....	96
Product Change Notification Service.....	96
Customer Support.....	96
Microchip Devices Code Protection Feature.....	96
Legal Notice.....	96
Trademarks.....	97
Quality Management System.....	98
Worldwide Sales and Service.....	99

## 1. About This Guide

This Installation and User's Guide explains how to install and setup your Adaptec® SmartRAID 3100 or SmartHBA 2100 Series Host Bus Adapter, including driver installation, BIOS operations, troubleshooting tips, and instructions for flashing the adapter firmware.

These SmartRAID 3100 Series adapter models are described in this guide:

- Adaptec SmartRAID 3101-4i
- Adaptec SmartRAID 3101E-4i
- Adaptec SmartRAID 3151-4i
- Adaptec SmartRAID 3102-8i
- Adaptec SmartRAID 3102E-8i
- Adaptec SmartRAID 3152-8i
- Adaptec SmartRAID 3154-8i
- Adaptec SmartRAID 3154-8e
- Adaptec SmartRAID 3154-16i
- Adaptec SmartRAID 3154-24i
- Adaptec SmartRAID 3154-8i8e
- Adaptec SmartRAID 3154-8i16e
- Adaptec SmartRAID 3162-8i
- Adaptec SmartRAID 3162-8i /e

These SmartHBA 2100 Series adapter models are described in this guide:

- Adaptec SmartHBA 2100-8i
- Adaptec SmartHBA 2100-4i4e
- Adaptec SmartHBA 2100-8i8e
- Adaptec SmartHBA 2100-16i
- Adaptec SmartHBA 2100-24i

### 1.1 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 2100/SmartRAID 3100 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.

### 1.2 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)

## 1.3 How to Find More Information

You can find more information about your SmartHBA 2100/SmartRAID 3100 Series Host Bus Adapter by referring to these documents, available for download at [start.adaptec.com](http://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. (ESC-2161615)
- *Adaptec SmartRAID 3100 Series and SmartHBA 2100 Series Host Bus Adapters Installation and User's Guide* (this manual)—Describes how to install SmartRAID 3100 and SmartHBA 2100 Series adapters in a computer or server, install drivers, and configure the adapter for initial use. (ESC-2171547)
- *Adaptec Flash Backup Module ASCM-35 Installation Instructions*—Describes how to install the ASCM-35 Flash Backup module using the mounting plate method. (ESC-2170352)

## 2. Kit Contents and System Requirements

This section lists the contents of your SmartHBA 2100/SmartRAID 3100 Series kit and the system requirements for successfully installing and using your adapter.

### 2.1 Kit Contents

SmartRAID 3100 Series kits:

- SmartRAID 3100 Series adapter
- Full-height ("FH") and Low-profile ("LP") brackets, with mounting screws
- 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 2100 Series kits:

- SmartHBA 2100 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 [start.adaptec.com](http://start.adaptec.com). For more information, see 6.1. [Download the Driver Package](#).

### 2.2 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 3. [About Your SmartRAID 3100 Series Host Bus Adapter](#) or 4. [About Your SmartHBA 2100 Series 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
  - 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

### 3. About Your SmartRAID 3100 Series Host Bus Adapter

This section provides an overview of the features of the SmartRAID 3100 Series adapter.

#### 3.1 Standard Features

- Support for SAS and SATA Hard Disk Drives (HDD) and Solid State Drives (SSD)
- UEFI Driver, HII configuration utility
- Flash ROM for updates to firmware and BIOS
- Up to 24 ports, 12 Gb/s I/O
- SAS 3.0, PCIe 3.0
- Low-profile MD2 form factor
- Mini-SAS HD connectors
- Cache protection with supercapacitor module
- maxCrypto Controller-Based Encryption (CBE) (SmartRAID 3162-8i /e only)
- Support for disk drive enclosures with SES2 enclosure management hardware
- Thermal sensor, with logging capabilities
- GUI and CLI management utilities
- Support for RAID 0, 1, 5, 6, 10, 50, 60
- Universal asynchronous receiver/transmitter (UART) debug/diagnostic port

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

#### 3.2 Mechanical Information

##### 3.2.1 Board Dimensions

This table shows the board dimensions of the SmartRAID 3100 Series adapter, in inches.

**Table 3-1.** SmartRAID 3100 Series Board Dimensions

Dimension	Measure
Height	2.700"
Length	6.600"
PCB Thickness	0.062"
Max Component Height, Top Side	0.570"
Max Component Height, Bottom Side	0.105"

##### 3.2.2 Heat Sink

SmartRAID 3100 Series adapters include a passive heat sink. The heat sink does not support an optional fan. The heat sink has 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](#).

#### 3.3 Visual Indicators

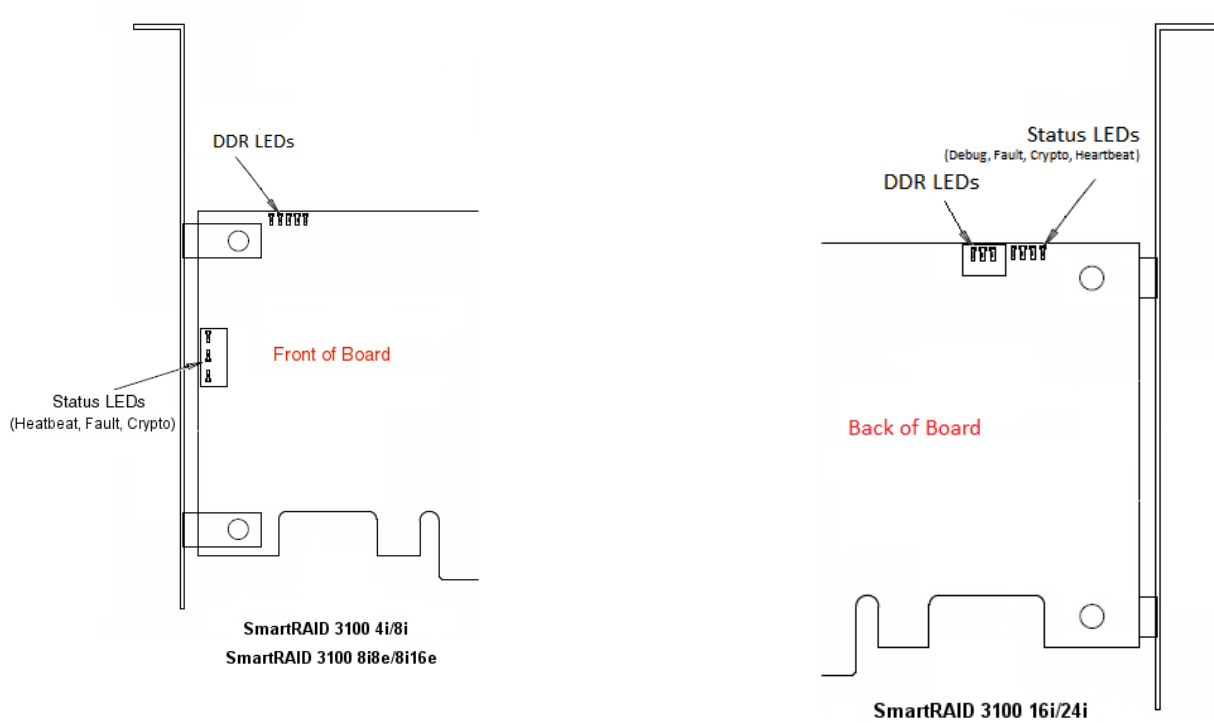
LEDs on SmartRAID 3100 Series adapters provide a visual indication of the board hardware status and cache backup system. The LED locations vary, and may be on the front of the board or back of



the board (see figures below), and include DDR LEDs (also referred to as Flash-Based Write Cache, or FBWC, LEDs) and status LEDs. The LED states are described in the following tables.

Front panel brackets on SmartRAID 3100-4i/8i controllers have three holes for the Heartbeat LED, Fault LED, and Crypto LED.

**Figure 3-1.** SmartRAID 3100 Series LED Locations



**Table 3-2.** SmartRAID 3100 Series Status LEDs

LED	Color	Meaning
DDR_LED1	Yellow	Cache backup error
DDR_LED2	Green	Dirty cache
DDR_LED3	Green	Charge status
HEARTBEAT	Green	Heartbeat (blinks once per/second when firmware operating normally)
FAULT	Yellow	Hardware Lockup/Fault
CRYPTO	Green	Cryptographic State: Off = NON-ENCRYPTING, On = ENCRYPTING
AVS_ENB	Green	The controller is operating normally if this LED is on or off: On = Adaptive Voltage Scaling (AVS) Enabled, Off = Adaptive Voltage Scaling (AVS) Disabled <b>Note:</b> Not supported on SmartRAID 3100-16i and SmartRAID 3100-24i adapters.
PAL_DEBUG	Yellow (8i/8e adapters) Red (16i/24i adapters)	Debug LED control signal

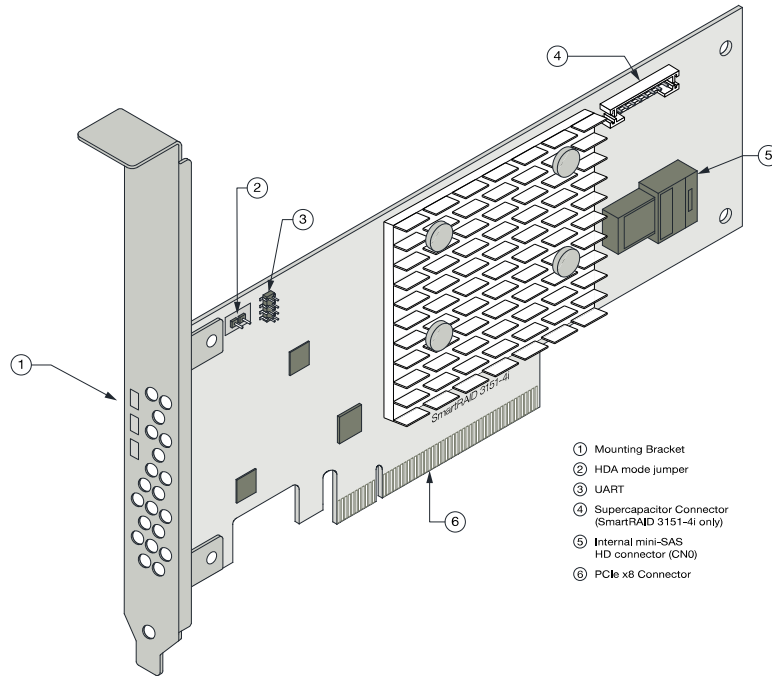
**Table 3-3.** SmartRAID 3100 Series DDR/FBWC LED States

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

### 3.4 About the Adaptec SmartRAID 3101-4i/3151-4i

The Adaptec SmartRAID 3101-4i/3151-4i is a SAS Host Bus Adapter with these features:

Figure 3-2. Adaptec SmartRAID 31x1-4i

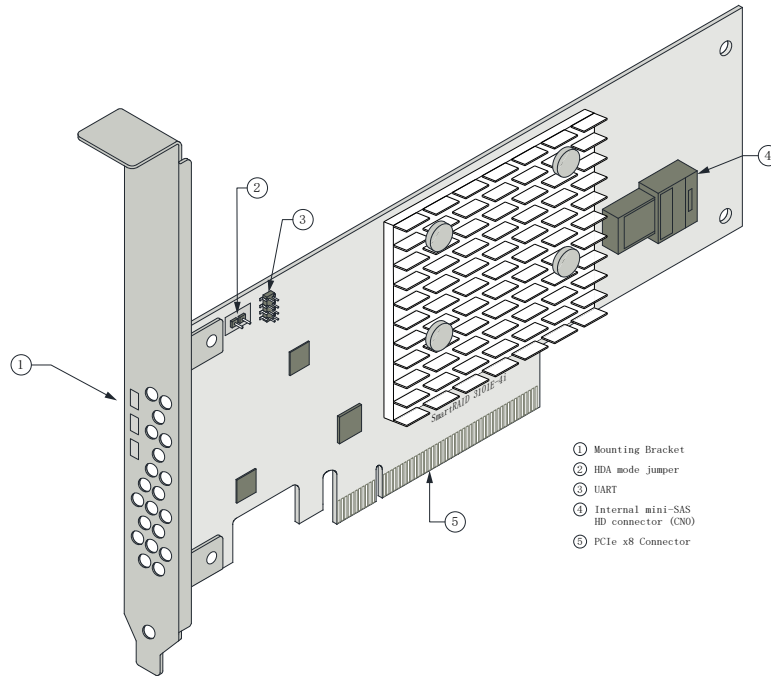


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	4
Standard memory	32 MB Boot Flash, 256 Kb SEEPROM, 1Mb MRAM
Cache	1 GB
Connectors, internal	1 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	4 direct-attached (or up to 238 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Encryption	No
Thermal sensor	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature
Cache Protection/Backup	<b>SmartRAID 3101-4i:</b> No (non-upgradeable) <b>SmartRAID 3151-4i:</b> Integrated ASCM-35F backup module with external supercapacitor

### 3.5 About the Adaptec SmartRAID 3101E-4i

The Adaptec SmartRAID 3101E-4i is a SAS Host Bus Adapter with these features:

Figure 3-3. Adaptec SmartRAID 3101E-4i

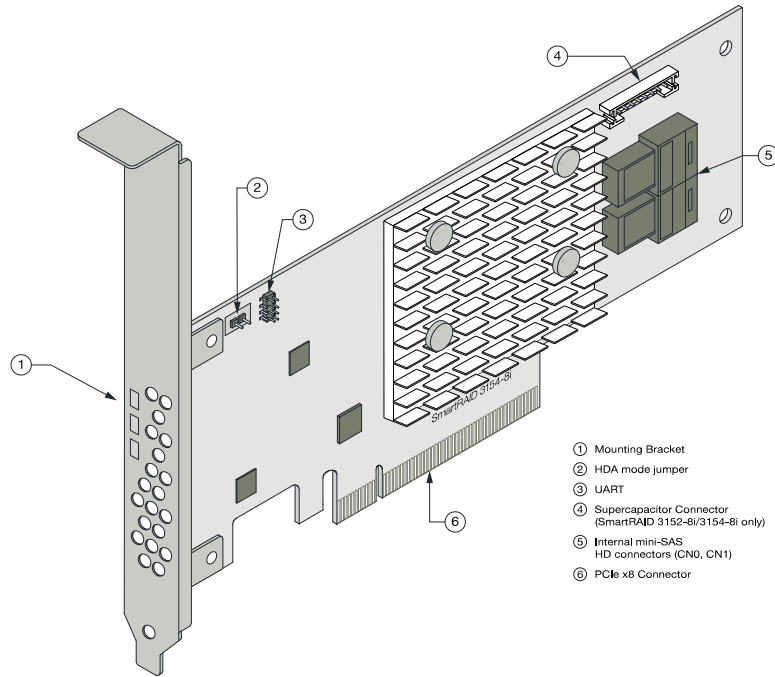


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	4
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1Mb MRAM
Cache	1 GB
Connectors, internal	1 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	4 direct-attached
Enclosure Support	SES2, SES3, IBPI and SGPIO
Expander Support	No (no drives of any type detected if connected via expander)
Encryption	No
Thermal sensor	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature
Cache Protection/Backup	No (non-upgradeable)

### 3.6 About the Adaptec SmartRAID 3102-8i/3152-8i/3154-8i

The Adaptec SmartRAID 3102-8i/3152-8i/3154-8i is a SAS Host Bus Adapter with these features:

Figure 3-4. Adaptec SmartRAID 31xx-8i



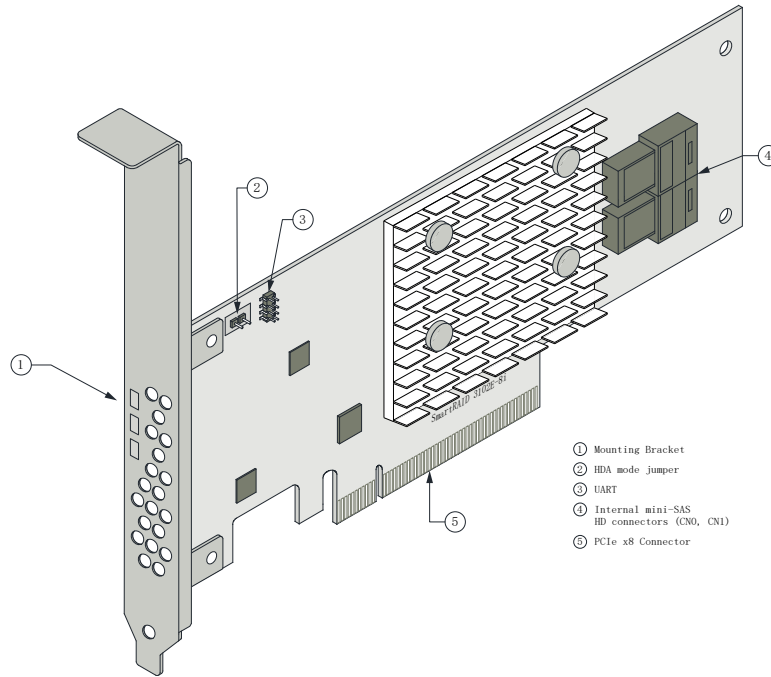
Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb SEEPROM, 1Mb MRAM
Cache	<b>SmartRAID 3102-8i/3152-8i:</b> 2 GB <b>SmartRAID 3154-8i:</b> 4 GB
Connectors, internal	2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	8 direct-attached (or up to 246 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Encryption	No
Thermal sensor	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature
Cache Protection/Backup	<b>SmartRAID 3102-8i:</b> No (non-upgradeable) <b>SmartRAID 3152-8i/3154-8i:</b> Integrated ASCM-35F backup module with external supercapacitor

### 3.7 About the Adaptec SmartRAID 3102E-8i

The Adaptec SmartRAID 3102E-8i is a SAS Host Bus Adapter with these features:



Figure 3-5. Adaptec SmartRAID 3102E-8i

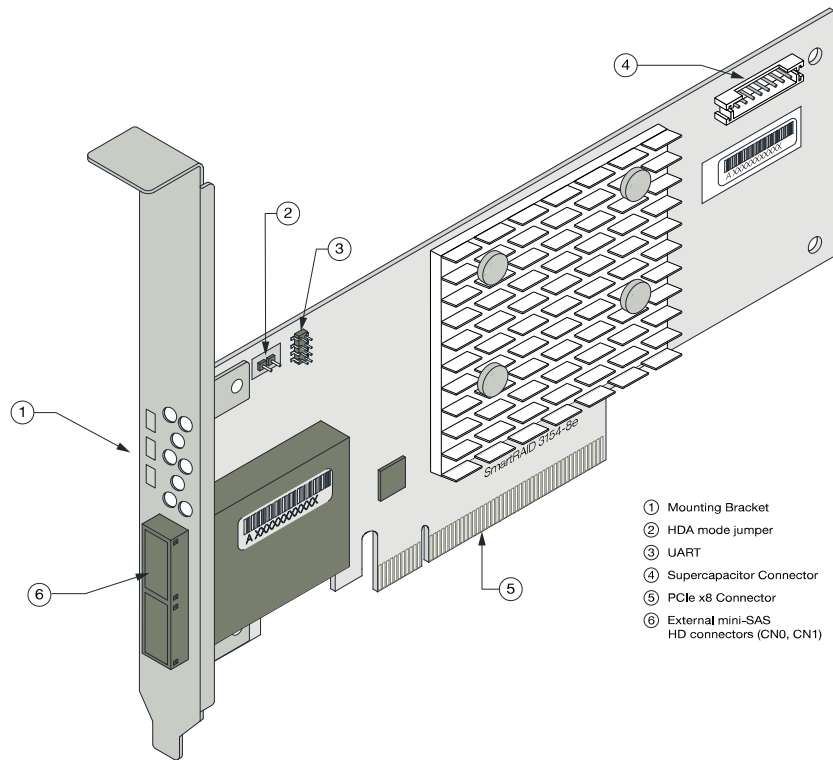


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb SEEPROM, 1Mb MRAM
Cache	2 GB
Connectors, internal	2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	8 direct-attached
Enclosure support	SES2, SES3, IBPI and SGPIO
Expander support	No (no drives of any type detected if connected via expander)
Encryption	No
Thermal sensor	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature
Cache Protection/Backup	No (non-upgradeable)

### 3.8 About the Adaptec SmartRAID 3154-8e

The Adaptec SmartRAID 3154-8e is a SAS Host Bus Adapter with these features:

Figure 3-6. Adaptec SmartRAID 3154-8e

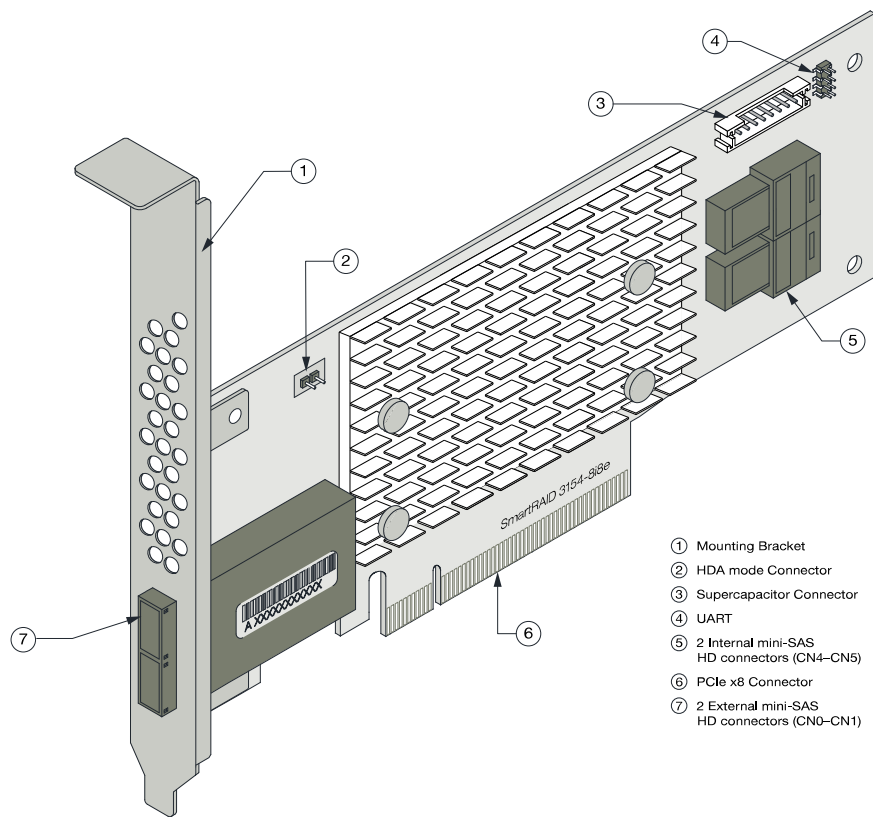


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1 Mb MRAM
Cache	4 GB
Connectors, external	2 mini-SAS HD x4 (SFF-8644)
Maximum number of disk drives	8 direct-attached (or up to 254 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Encryption	No
Thermal sensor	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature
Cache Protection/Backup	Integrated ASCM-35F backup module with external supercapacitor

### 3.9 About the Adaptec SmartRAID 3154-8i8e

The Adaptec SmartRAID 3154-8i8e is a SAS Host Bus Adapter with these features:

Figure 3-7. Adaptec SmartRAID 3154-8i8e

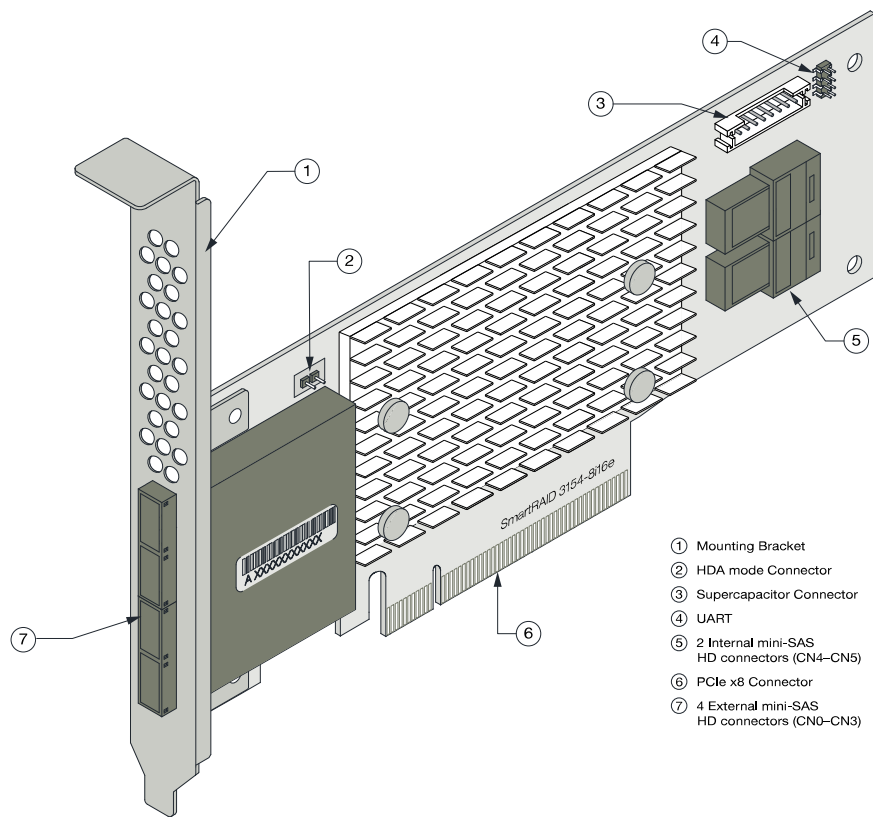


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 128 Kb EEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	2 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum number of disk drives	16 direct-attached (or up to 246 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Thermal sensor	Processor temperature, Ambient temperature
Cache Protection/Backup	Integrated ASCM-35F backup module with external supercapacitor

### 3.10 About the Adaptec SmartRAID 3154-8i16e

The Adaptec SmartRAID 3154-8i16e is a SAS Host Bus Adapter with these features:

Figure 3-8. Adaptec SmartRAID 3154-8i16e



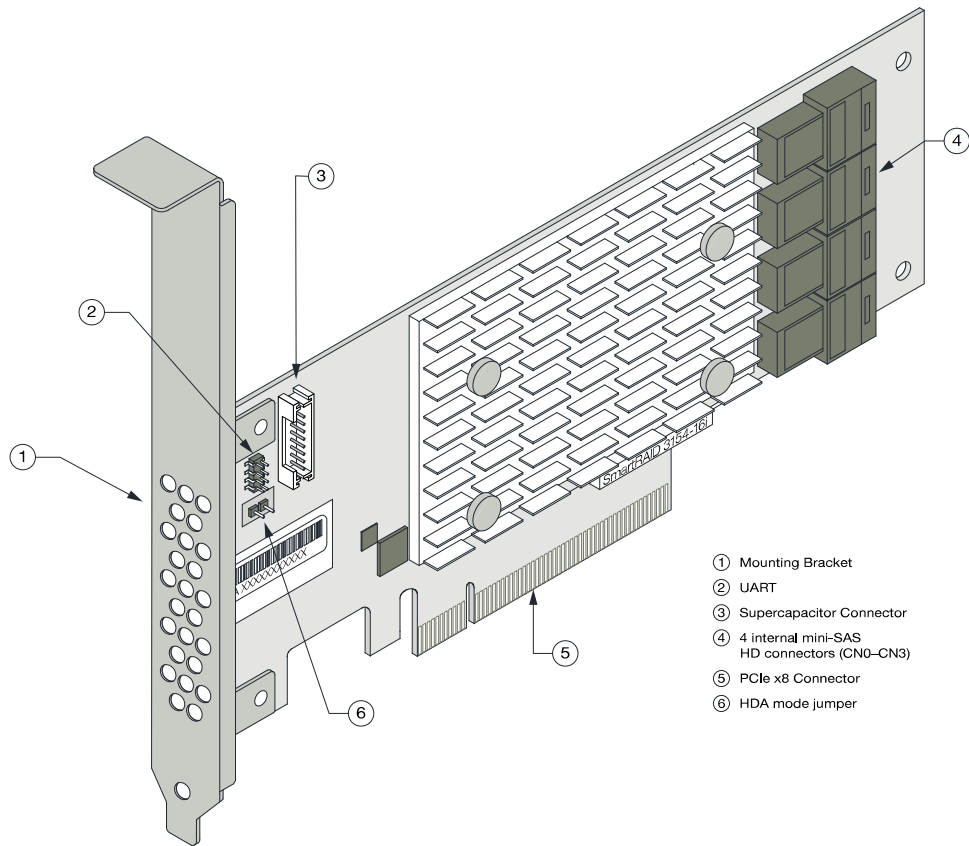
Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	24
Standard memory	32 MB boot flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	4 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum number of disk drives	24 direct-attached (or up to 246 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Thermal sensor	Processor temperature, Ambient temperature
Cache Protection/Backup	Integrated ASCM-35F backup module with external supercapacitor

### 3.11 About the Adaptec SmartRAID 3154-16i

The Adaptec SmartRAID 3154-16i is a SAS Host Bus Adapter with these features:



Figure 3-9. Adaptec SmartRAID 3154-16i



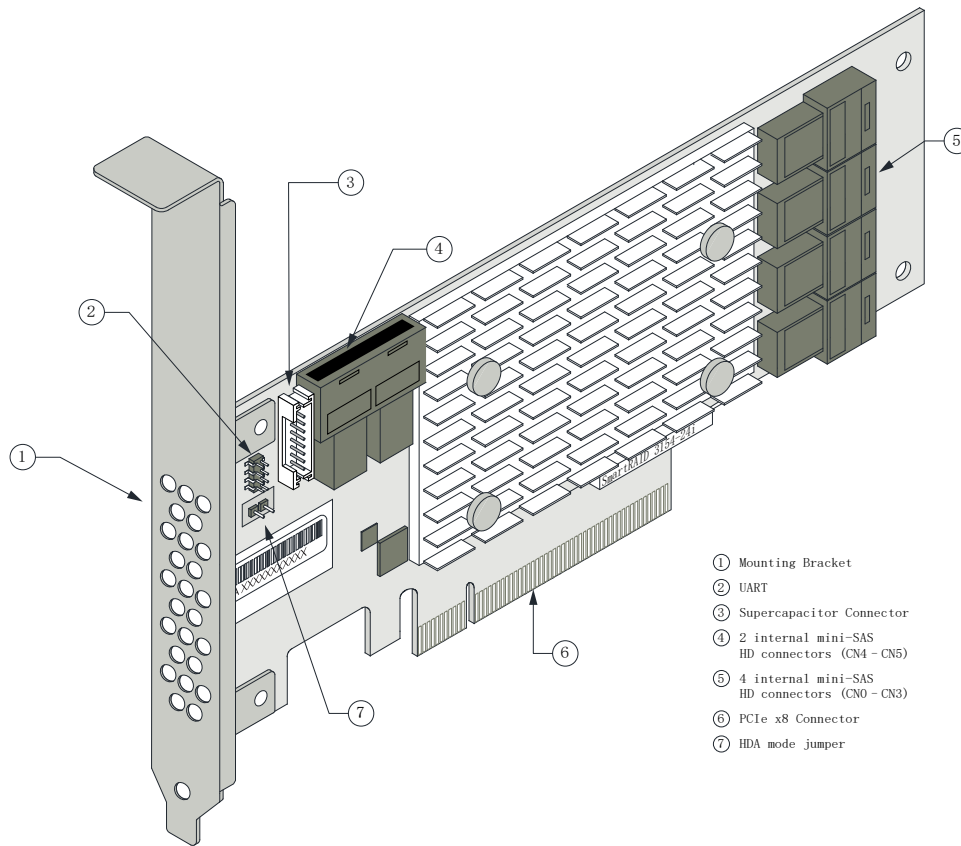
- ① Mounting Bracket
- ② UART
- ③ Supercapacitor Connector
- ④ 4 internal mini-SAS HD connectors (CN0-CN3)
- ⑤ PCIe x8 Connector
- ⑥ HDA mode jumper

Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB boot flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	4 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	16 direct-attached (or up to 238 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Thermal sensor	Processor temperature, Ambient temperature
Cache Protection/Backup	Integrated ASCM-35F backup module with external supercapacitor

### 3.12 About the Adaptec SmartRAID 3154-24i

The Adaptec SmartRAID 3154-24i is a SAS Host Bus Adapter with these features:

Figure 3-10. Adaptec SmartRAID 3154-24i

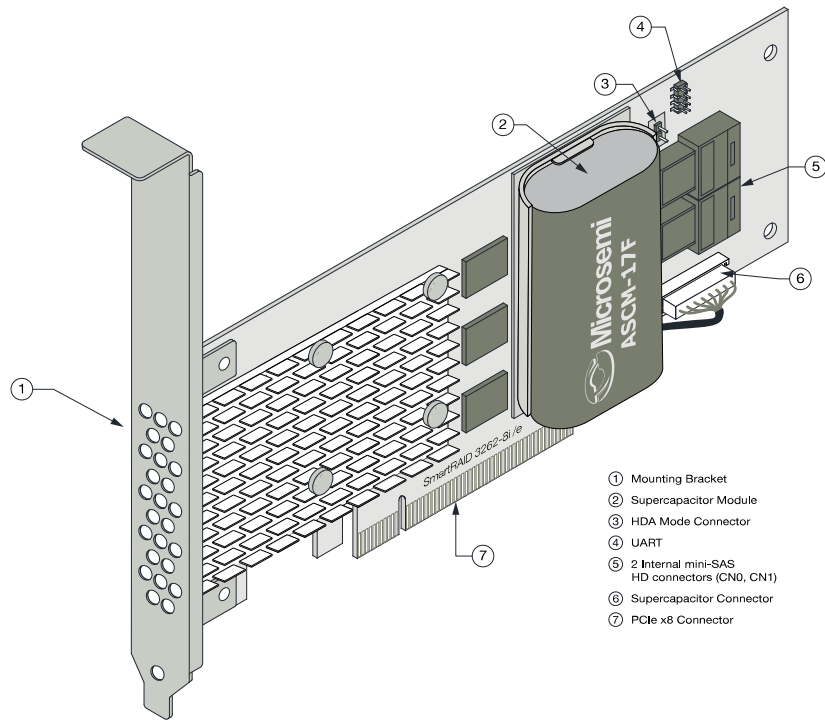


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	24
Standard memory	32 MB Boot Flash, 128 Kb EEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	6 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	24 direct-attached (or up to 230 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
Thermal sensor	Processor temperature, Ambient temperature
Cache Protection/Backup	Integrated ASCM-35F backup module with external supercapacitor

### 3.13 About the SmartRAID 3162-8i/SmartRAID 3162-8i /e Adapter

The SmartRAID 3162-8i/SmartRAID 3162-8i /e is a SAS Host Bus Adapter with these features:

Figure 3-11. Adaptec SmartRAID 3162-8i



Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 16 KB Boot SEEPROM, 128 KB MRAM, 256 KB Crypto SEEPROM (SmartRAID 3162-8i /e only)
Cache	2 GB
Connectors, internal	2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	8 direct-attached (or up to 246 with expanders)
Enclosure Support	SES2, SES3, IBPI and SGPIO
maxCrypto Controller-Based Encryption	<b>SmartRAID 3162-8i:</b> No <b>SmartRAID 3162-8i /e:</b> Yes
Thermal sensor	Processor temperature, Ambient temperature
Cache Protection/Backup	Integrated flash backup module ASCM-17F, with board-mounted supercapacitor

## 4. About Your SmartHBA 2100 Series Host Bus Adapter

This section provides an overview of the features of the SmartHBA 2100 Series adapter.

### 4.1 Standard Features

- Support for SAS and SATA Hard Disk Drives (HDD) and Solid State Drives (SSD)
- UEFI Driver, HII configuration utility
- Flash ROM for updates to firmware and BIOS
- Up-to 24 ports, 12 Gbps I/O
- SAS 3.0, PCIe 3.0
- Low-profile MD2 form factor
- Mini-SAS HD connectors
- Support for disk drive enclosures with SES 2.x/3.x inband support, TWI, IBPI and SGPIO enclosure management
- Thermal sensors, with logging capabilities
- Support for RAID 0, 1, 5, 10
- Universal asynchronous receiver/transmitter (UART) debug/diagnostic port

### 4.2 Mechanical Information

#### 4.2.1 Board Dimensions

This table shows the board dimensions of the SmartHBA 2100 Series adapters, in inches.

**Table 4-1.** SmartHBA 2100 Series Board Dimensions

Dimension	SmartHBA 2100-4i4e	SmartHBA 2100-8i
Height	2.70"	2.712"
Length	5.20"	6.60"
PCB Thickness	0.062"	0.062"
Max Component Height, Top Side	0.570"	0.570"
Max Component Height, Bottom Side	0.105"	0.105"

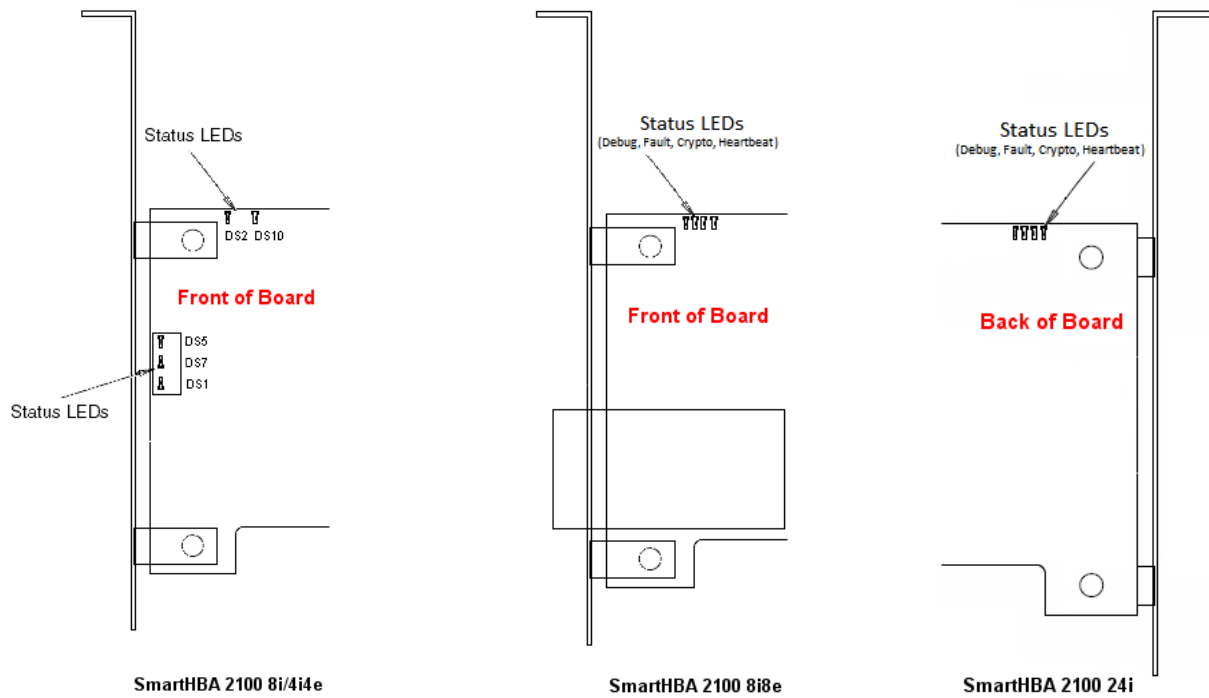
#### 4.2.2 Heat Sink

SmartHBA 2100 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 four push-pins located at its four corners to ensure an even distribution of force across the top of the ASIC.

### 4.3 Visual Indicators

LEDs on the SmartHBA 2100 Series adapters provide a visual indication of the board hardware status. The LED locations vary, and may be on the front of the board or back of the board (see figures below). The LED states are described in the following table.

**Figure 4-1. SmartHBA 2100 Series LED Locations**



**Table 4-2. SmartHBA 2100 Series Status LEDs**

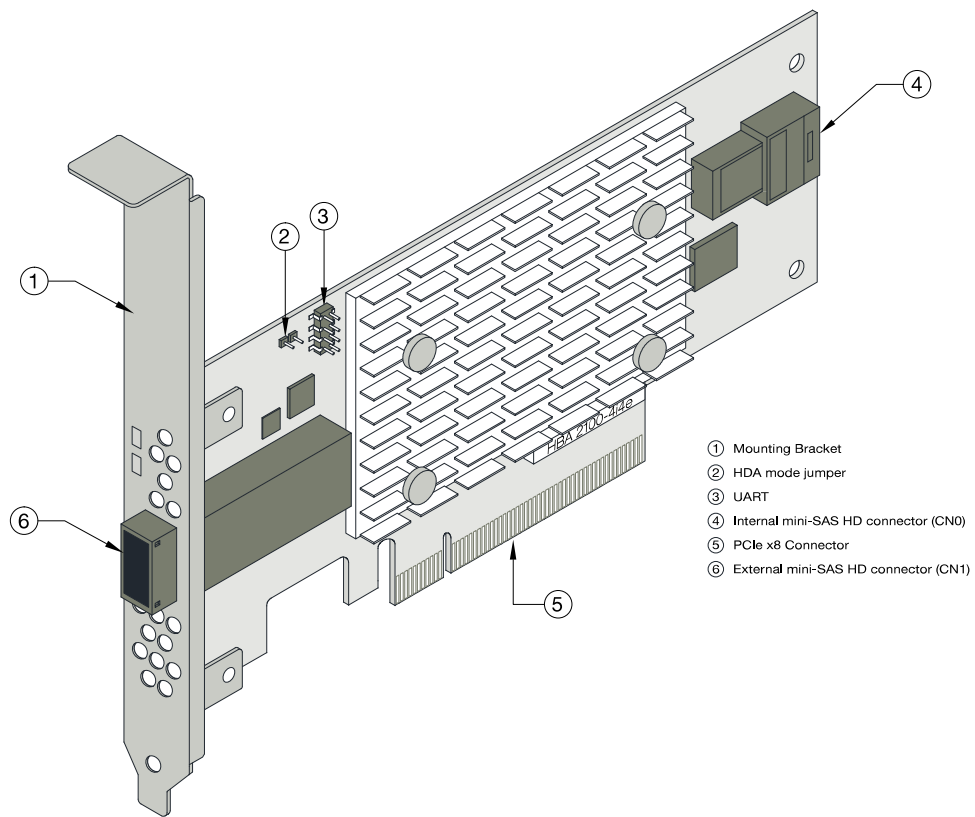
LED	Color	Meaning
HEARTBEAT (DS5)	Green	Heartbeat (blinks once per second when firmware is operating normally)
FAULT (DS7)	Yellow	Hardware Lockup/Fault
CRYPTO (DS1)	Green	Cryptographic State: always off. SmartHBA 2100 Series adapters do not support encryption.
AVS_ENB (DS2)	Green	On=Adaptive Voltage Scaling (AVS) enabled, Off=Adaptive Voltage Scaling (AVS) disabled
PAL_DEBUG (DS10)	Red	Debug LED control signal

#### 4.4 About the Adaptec SmartHBA 2100-4i4e

The Adaptec SmartHBA 2100-4i4e is a SAS Host Bus Adapter with these features:



Figure 4-2. Adaptec SmartHBA 2100-4i4e

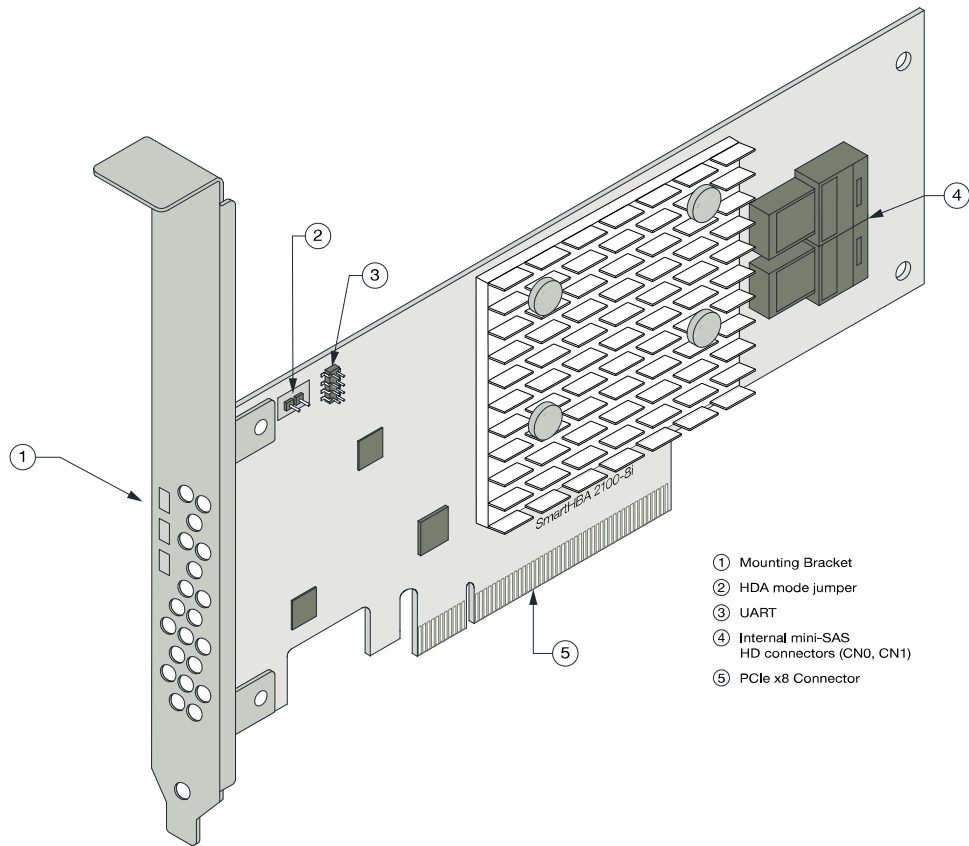


Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 16 KB SEEPROM, 128 KB MRAM
Connectors, internal	1x1 mini-SAS HD x4 (SFF-8643)
Connectors, external	1x1 mini-SAS HD x4 (SFF-8644)
Maximum number of disk drives	4/port direct-attached (or up to 250 with expanders)
Enclosure Support	SES 2.x/3.x inband support, TWI, IBPI and SGPIO
Thermal sensors	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature

#### 4.5 About the Adaptec SmartHBA 2100-8i

The Adaptec SmartHBA 2100-8i is a SAS Host Bus Adapter with these features:

Figure 4-3. Adaptec SmartHBA 2100-8i Features

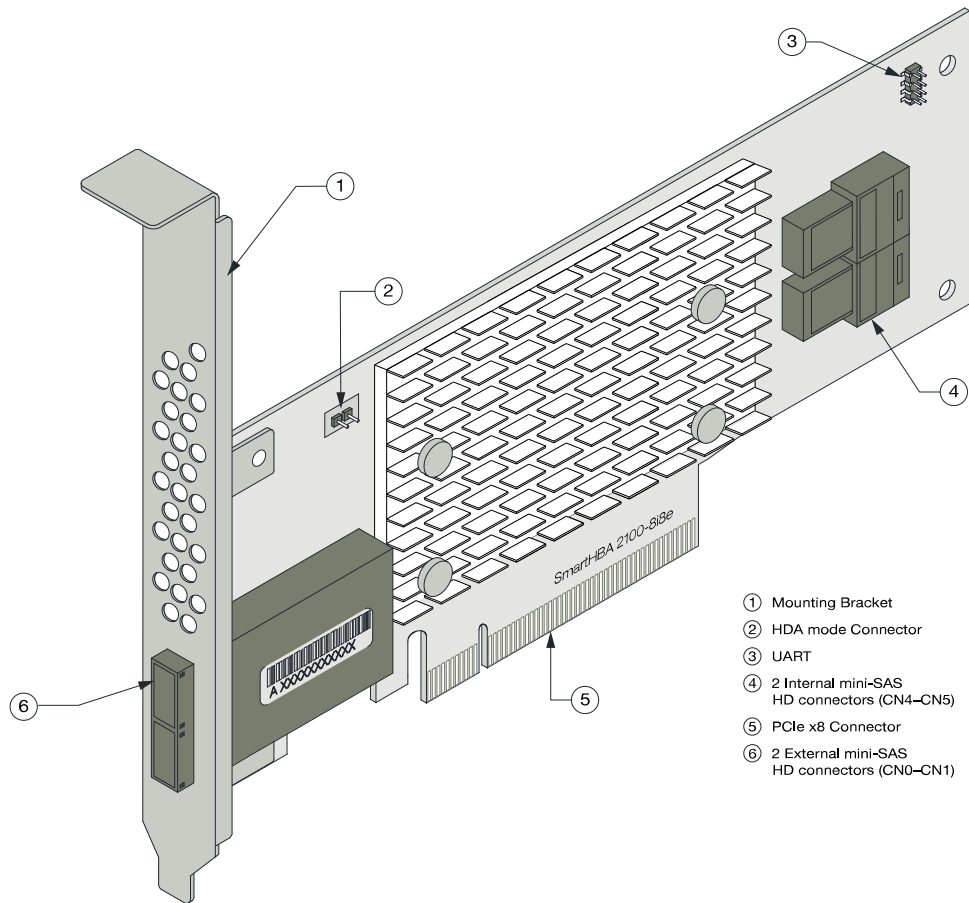


Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 32 KB SEEPROM, 128 KB MRAM
Connectors, internal	1x2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	4/port direct-attached (or up to 246 with expanders)
Enclosure Support	SES 2.x/3.x inband support, TWI, IBPI and SGPIO
Thermal sensors	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature

## 4.6 About the Adaptec SmartHBA 2100-8i8e

The Adaptec SmartHBA 2100-8i8e is a SAS Host Bus Adapter with these features:

Figure 4-4. Adaptec SmartHBA 2100-8i8e Features

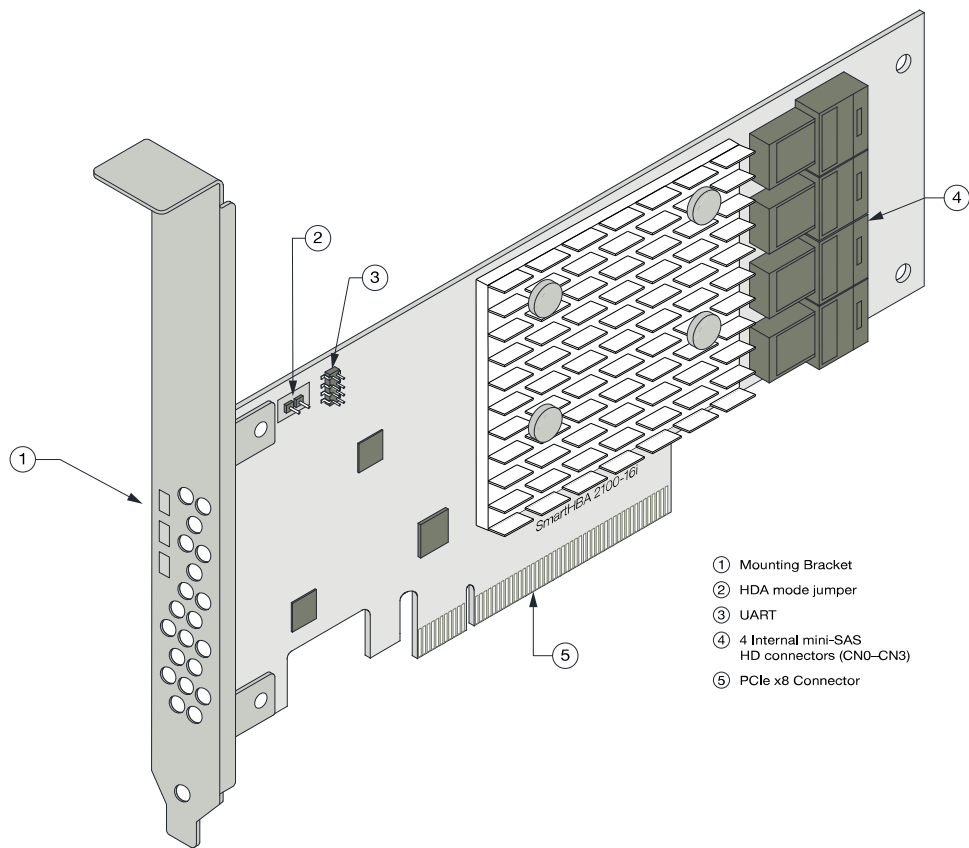


Form Factor	PCIe Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 128 Kb SEEPROM, 128 KB MRAM
Connectors, internal	2 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum number of disk drives	16 direct-attached (or up to 246 with expanders)
Enclosure Support	SES 2.x/3.x inband support, TWI, IBPI and SGPIO
Thermal sensor	Ambient temperature, ASIC die temperature

#### 4.7 About the Adaptec SmartHBA 2100-16i

The Adaptec SmartHBA 2100-16i is a SAS Host Bus Adapter with these features:

Figure 4-5. Adaptec SmartHBA 2100-16i Features



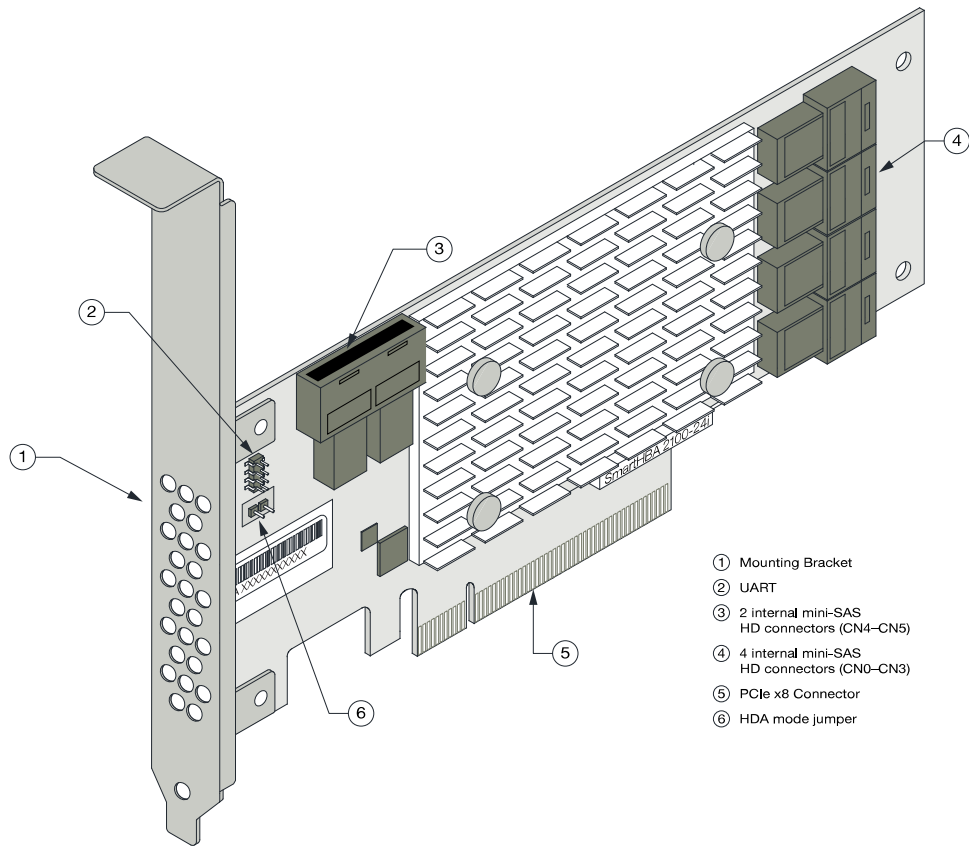
Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 32 KB SEEPROM, 128 KB MRAM
Connectors, internal	4 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	16 direct-attached (or up to 238 with expanders)
Enclosure Support	SES 2.x/3.x inband support, TWI, IBPI and SGPIO
Thermal sensors	Inlet ambient temperature, ASIC die temperature, Top-side board ambient temperature, Bottom-side board ambient temperature

## 4.8 About the Adaptec SmartHBA 2100-24i

The Adaptec SmartHBA 2100-24i is a SAS Host Bus Adapter with these features:



Figure 4-6. Adaptec SmartHBA 2100-24i Features



Form Factor	PCIe Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbp/s per port
Phys (Unified Serial Ports)	24
Standard memory	32 MB Boot Flash, 16 KB SEEPROM, 128 KB MRAM
Connectors, internal	6 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	24 direct-attached (or up to 230 with expanders)
Enclosure Support	SES 2.x/3.x inband support, TWI, IBPI and SGPIO
Thermal sensors	Inlet ambient temperature, ASIC die temperature

## 5. Installing the Controller and Disk Drives

This section explains how to install your SmartHBA 2100/SmartRAID 3100 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 (see [Standard Features](#)).
- Ensure that you have the right number of disk drives for your application (see [Selecting Disk Drives and Cables](#)).

### 5.2 Selecting Disk Drives and Cables

#### 5.2.1 Disk Drives

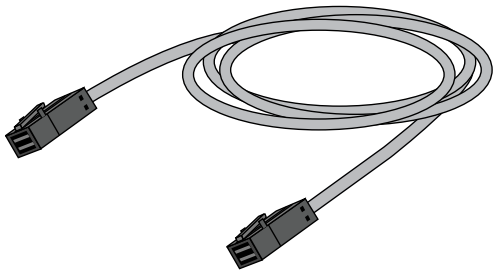
Your SmartHBA 2100/SmartRAID 3100 Series adapter supports SAS and SATA disk drives, Solid State Drives (SSDs), and SAS tape drives. For more information about compatible disk drives, refer to [adaptec.com/cables](http://adaptec.com/cables).

#### 5.2.2 Cables

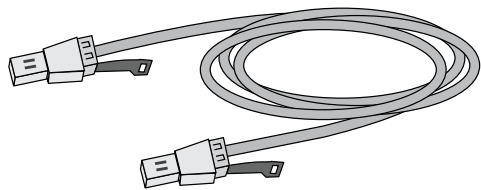
Depending on your adapter model and application requirements, you can use any of the cables listed below. For more information about cabling options for your SmartHBA 2100/SmartRAID 3100 Series adapter, visit [adaptec.com/cables](http://adaptec.com/cables)

**Note:** We recommend using Microchip Adaptec SAS cables only.

#### SAS HD Cables



Internal Mini SAS HD to SAS HD (SFF-8643 to SFF- 8643)—Connects to a backplane or enclosure.



External Mini SAS HD to SAS HD (SFF-8644 to SFF- 8644)—Connects to a backplane or enclosure.

### 5.3 Installing the Host Bus Adapter

This section describes how to install your SmartHBA 2100/SmartRAID 3100 Series adapter in a computer cabinet or server and connect internal and external storage devices. The SmartHBA 2100/SmartRAID 3100 Series adapters have these configurations:

- Adapters with internal connectivity
- Adapters with external connectivity
- Adapters with internal and external connectivity

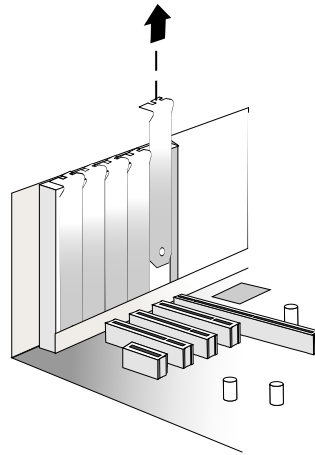
- Adapters with internal connectivity and an external supercapacitor module
1. Turn off your computer and disconnect the power cord and any network cables. Open the cabinet, following the manufacturer's instructions.
  2. Select an available PCIe expansion slot that's compatible with your adapter model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

**Note:** For SmartRAID 3100 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.

---

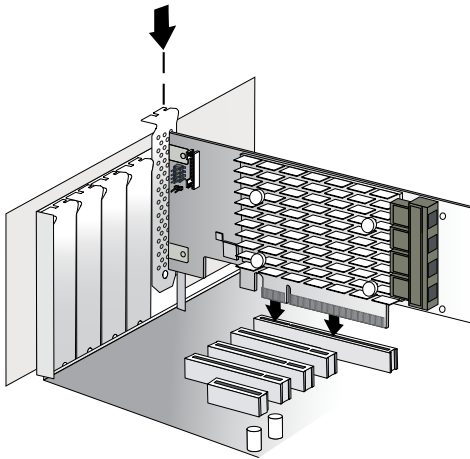


3. Insert the adapter into the expansion slot and press down gently but firmly until it clicks into place. When installed properly, the adapter should appear level with the expansion slot.

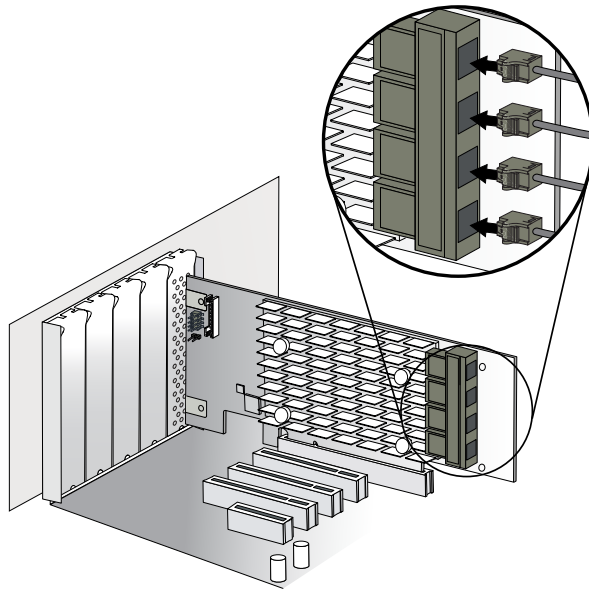
---

**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.

---

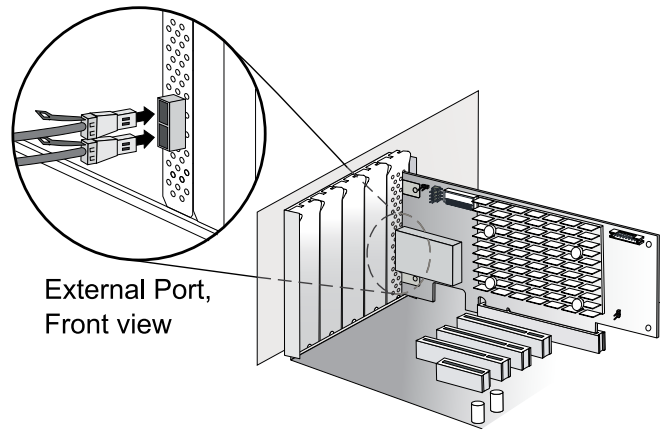


4. Secure the bracket in the expansion slot, using the retention device (for instance, a screw or lever) supplied with your computer.
5. Connect SAS HD cables between the adapter and internal or external storage devices, as required:
  - For adapters with internal ports, connect SAS HD cables between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

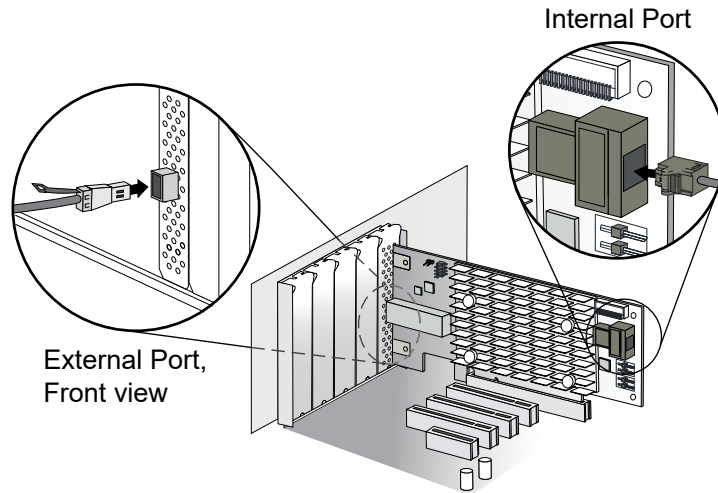


- For adapters with external ports, connect SAS HD cables between the adapter and external disk drives or enclosures:





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



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

## 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 2100/SmartRAID 3100 is installed in a computer or server.

A compatible driver is available in box 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):

- Open a browser window, then type [start.adaptec.com](http://start.adaptec.com) in the address bar.
- Navigate to the SmartHBA 2100/SmartRAID 3100 product page.
- Download the controller driver package (zip file archive).
- When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (\windows 2016, \rhel7, \rhel6, and so on).

**Note:** See the *Release Notes* for a complete list of driver files and folder structure.

### 6.2 Creating a Driver Disk

Create a driver disk by completing the steps below. You will need a USB flash drive to complete this task.

**Note:** For VMware, see [6.11. Installing with VMware](#).

- Change to the driver directory for your operating system version.
- Write the driver binary file to a USB flash drive.

For example, if the USB drive is `/dev/sdc` on the Linux system, type (where `##-###` is the build number):

Option	Description
RHEL 7	<code>dd if=smartpqi-##-###.&lt;rhel_version&gt;.x86_64.dd of=/dev/sdc</code>
SLES 12	<code>dd if=smartpqi-##-###.&lt;sles_version&gt;.x86_64.dd of=/dev/sdc</code>

**Note:** See the Release Notes for the latest build number.

- Remove and label the driver disk.
- Continue the installation with the instructions for your operating system.

### 6.3 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:

- Insert the Windows installation DVD, then restart the computer.
- Follow the on-screen instructions to begin the Windows installation.
- When prompted to specify a location for Windows, select **Load Driver**.
- 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.

## 6.4 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 and the RHEL version is formatted as follows: `rhel7u9`):

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

## 6.5 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
```

### 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.

## 6.6 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
```

## 6.7 Installing with Ubuntu Linux

To install the controller SmartPQI driver while installing Ubuntu Linux 18.04 LTS and above:

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
```

## 6.8 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
```

## 6.9 Installing with FreeBSD

The following instructions are for FreeBSD v13.1 and earlier. For more instruction from FreeBSD v13.2, see [7.9. Installing on 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/dalpl
# mount /dev/dalpl /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/dalp1 /media
```

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

```
# cp /media/smartpqi.ko /boot/kernel/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>
```

## 6.10 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.

## 6.11 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=N4lghgNiBclJfswHMCmACAQgVwjYQBNUAnEAXyA](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-62B15826-B529-4519-B57A-98DFD0CC5522.html?hWord=N4lghgNiBclJfswHMCmACAQgVwjYQBNUAnEAXyA).
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 2100/SmartRAID 3100 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](http://start.adaptec.com) in the address bar.
2. Navigate to the SmartHBA 2100/SmartRAID 3100 product page.
3. Download the controller driver package (zip file archive).
4. When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (windows 2016, \rhel7, \rhel6, and so on).

**Note:** See the *Release Notes* for a complete list of driver files and folder structure.

### 7.2 Creating a Driver Disk

Create a driver disk by completing the steps below. You will need a USB flash drive to complete this task.

1. Change to the driver directory for your operating system version.
2. Write the driver binary file to a USB flash drive.
3. Remove and label the driver disk.
4. Continue the installation with the instructions for your operating system.

### 7.3 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. Specify the device type as a **Storage controller** and click **Next**.
7. Select the device driver you want to install.
8. Navigate to the disk location where the driver files are copied.
9. When the installation is complete, remove the driver disk and restart your computer.

### 7.4 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.

## 7.5 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. Reboot the system.

## 7.6 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`

## 7.7 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
```

## 7.8 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.

## 7.9 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
```

## 7.10 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.

## 7.11 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 `xxxxxx` 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 encryption:

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 the HII 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 2100/SmartRAID 3100 Series Host Bus Adapter.

### 9.1 Troubleshooting Checklist

If you encounter difficulties installing or using your SmartHBA 2100/SmartRAID 3100 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 [3. About Your SmartRAID 3100 Series Host Bus Adapter](#) or [4. About Your SmartHBA 2100 Series Host Bus Adapter](#) for instructions.
- 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 [3. About Your SmartRAID 3100 Series Host Bus Adapter](#) or [4. About Your SmartHBA 2100 Series Host Bus Adapter](#) for instructions.
- Did the driver install correctly? It may need to be reloaded after a reboot or kernel update.
- 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 2100/SmartRAID 3100 if it becomes inoperable or if a firmware upgrade is unsuccessful. SmartHBA 2100/SmartRAID 3100 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 [3. About Your SmartRAID 3100 Series Host Bus Adapter](#) or [4. About Your SmartHBA 2100 Series Host Bus Adapter](#) for instructions.

## 10. Using the Microchip SAS/SATA HII Configuration Utility

The Microchip SAS/SATA Configuration Utility (MSCU) is a BIOS-based utility that can manage a SmartHBA 2100/SmartRAID 3100 adapter and the devices attached to it. It comprises a set of tools for creating and managing arrays, viewing and modifying adapter properties, 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 2100/SmartRAID 3100, and rendering contents.

In the UEFI/HII interface, the server's standard BIOS provides access to the SmartHBA 2100/SmartRAID 3100 configuration options. How the BIOS is accessed, depending on the server manufacturer, but typically it's started by simply pressing **DEL**. Once setup is entered, navigate to the menu where forms of third-party vendors are displayed. The menu location depends on server manufacturer. Select the 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 the keyboard or using the 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 2100/SmartRAID 3100 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. Select drives, specify the RAID level and encryption options (if supported by the 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 the controller, then press **Enter**.
3. From the main menu, select **Array Configuration**, then select **Create Array**.
4. Select each drive to be included 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:** Account credentials (Admin or User) will be requested if not logged into the Encryption Manager; see [10.13.1. 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 Arrays with RAID0

This option will create arrays for each selected physical drives. Each array contains exactly one physical drive which has one RAID0 logical drive. Default setting will be used to create arrays.

1. From the main menu, select **Array Configuration**, then select **Create Array with RAID0**.
2. Select each drive that contains arrays.
3. Select **Submit**.

## 10.5 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. 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 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).

## 10.6 Managing Arrays and Logical Drives

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

### 10.6.1 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**.

### 10.6.2 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 to include in the array: use the space bar to 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**.

### 10.6.3 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 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**.

### 10.6.4 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**.

### 10.6.5 Deleting a Logical Drive

**Note:** Use this procedure to delete an individual logical drive. To delete all logical drives on an array, see [10.6.15. 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 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 **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, any other logical drives cannot be deleted until they all move to the Optimal state.

### 10.6.6 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 to 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.

### 10.6.7 Deleting a Spare Drive

To delete a spare drive:

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

### 10.6.8 Migrating Logical Drive

Use this option to modify the current RAID or stripe size for a logical drive. Changes in these settings can provide more or less unused space as well as allowing for fine tuning performance on the logical drive.

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 **Migrate Logical Drive**.
4. Select the new **RAID level** and **Stripe Size**.
5. Select **Submit Changes**.

### 10.6.9 Extending Logical Drive

Use this option to increase the capacity of an existing logical drive by specifying new size. Once the task is completed, OS partitioning software can be used to take advantage of the available space.

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 **Extend Logical Drive**.

4. Select the new **Size**.
5. Select **Submit Changes**.

#### 10.6.10 Re-enabling Logical Drive

This option will force the failed logical drive back to the optimal state. Re-enables a failed logical drive. Previously existing data on the logical drive may not be valid or recoverable, but the drive could be re-formatted and used by an OS.

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 **Re-Enable Logical Drive**.

#### 10.6.11 Re-enabling Logical Drive with Data Rebuild

This option will attempt to re-enable failed logical drive and rebuild data from selected drives if it meets eligibility for fault tolerance and interim recovery.

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 **Re-Enable Logical Drive with data rebuild**.
4. Select physical drives with which the logical drive was previously on fault tolerance/interim recovery state includes the recent failed drive. Check support logs to identify drive failure order.
5. Select **Submit**.



Selection of incorrect drives may lead to data loss and failed logical drive state.

---

#### 10.6.12 Consolidating Array Free Space

This option relocates the logical drives in the array and consolidate all the array free space to the end of the array.

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
2. Use the arrow keys to select the **Array**, press **Enter**.
3. Select **Consolidate Array Free Space**.

#### 10.6.13 Managing Data Drives

This menu provides options to Manage the physical data drives in the array. Expand the array by adding data drives. Shrink the array by removing current data drives.

Replace one or more data drives with new drives.

1. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
2. Use the arrow keys to select the **Array**, press **Enter**.
3. Select **Manage Data Drives**.
4. Use any of the listed options.

##### 10.6.13.1 Add Drives - Expand Array

Use this option to expand the array by adding data drives. Sub options are:

##### **Add drive to existing parity group**

Adds an equal number of drives to each parity group in 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.

#### **10.6.13.2 Remove Drives – Shrink Array**

Use this option to shrink the array by removing existing 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.

#### **10.6.13.3 Move Drives**

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

#### **10.6.14 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**.

#### **10.6.15 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 [10.6.5. 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**.

### **10.7 Modifying SmartHBA 2100/SmartRAID 3100 Settings**

To modify the SmartHBA 2100/SmartRAID 3100 settings, start the Microchip SAS/SATA Configuration Utility, select **Configure Controller Settings** from the main menu, then select **Modify Controller Settings** or **Advanced Controller Settings**. You can set the options in the table below.

Option	Description
<b>Modify Controller Settings</b>	
Transformation Priority	<p>Sets the priority for array expansion:</p> <ul style="list-style-type: none"> <li>• Low: normal system operations take priority over array expansion</li> <li>• Medium: normal system operations and array expansion get equal priority</li> <li>• High: expansion takes precedence over all other system operations</li> </ul>
Rebuild Priority	<p>Sets the priority for rebuilding a failed logical drive:</p> <ul style="list-style-type: none"> <li>• Low: normal system operations take priority over rebuilds</li> <li>• Medium: normal system operations and rebuilds get equal priority</li> <li>• Medium High: rebuilds get higher priority than normal system operations</li> <li>• High: rebuilds take precedence over all other system operations</li> </ul>
Surface Scan Analysis Priority	<p>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.</p>
Current Parallel Surface Scan Count	<p>Sets the surface scan count for the controller. Set the value to "1" to disable the feature.</p> <p> 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.</p>
Unconfigured Physical Drive Write Cache	<p>Enables and disables physical drive write cache for unconfigured drives on the controller.</p>
HBA Physical Drive Write Cache State	<p>Enables and disables physical drive write cache for HBA drives on the controller.</p>
Configured Physical Drive Write Cache State	<p>Enables and disables physical drive write cache for configured drives on the controller.</p>
<b>Modify Spare Activation Mode</b>	
Spare Activation Mode	<p>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.</p> <p>In Predictive Spare activation mode, activation is done when a drive reports a predictive failure.</p>
<b>Configure Controller Port Mode</b>	
Connector Mode (CN0:CN3)	<p>Configures the controller connectors to different operating modes:</p> <ul style="list-style-type: none"> <li>• HBA: exposes physical drives to the operating system</li> <li>• RAID: exposes only RAID volumes to the operating system</li> <li>• Mixed: exposes RAID volumes and physical drives to the operating system</li> </ul>
<b>Modify Cache Settings</b>	
No Battery Write Cache	<p>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.</p> <p> Enabling write caching on a cache module without a fully charged battery/supercapacitor may cause data loss in the event of a power failure.</p>
Cache Ratio (Read)	<p>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.</p>
Write Cache Bypass Threshold	<p>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.</p>
<b>Advanced Controller Settings (RAID mode or Mixed mode only):</b>	

.....continued

Option	Description
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.
RAID 6/60 Alternate Inconsistent Repair Policy	Sets the surface analysis inconsistency repair policy for RAID 6/60 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.
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: <ul style="list-style-type: none"> <li>• Disable (default).</li> <li>• Low</li> <li>• Middle(100 ms)</li> <li>• High</li> <li>• Very high(30 ms)</li> <li>• Very high(10 ms)</li> </ul>
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: <ul style="list-style-type: none"> <li>• View Current port Discovery Protocol</li> <li>• View Pending port Discovery Protocol</li> <li>• Set port Discovery Protocol</li> <li>• Reset port Discovery Protocol to default</li> </ul>
Modify Expander Minimum Scan Duration	This menu provides option to configure minimum scan duration for expanders. Entered value should be in seconds.
Configure Persistent Event Log Policy	Controller event logging policy setting to persist either the oldest or newest events. <ul style="list-style-type: none"> <li>• <b>Most Recently Occurred:</b> Controller shall continue to log a new event when it occurs irrespective of the event consumption status.</li> <li>• <b>Least Recently Consumed:</b> Recently occurred unconsumed events will be stored in the persistent event log.</li> </ul>
Configure Controller UEFI Driver Health Reporting	Configure controller error reporting by UEFI driver using EFI driver health protocol. <ul style="list-style-type: none"> <li>• <b>Report all errors:</b> default option, UEFI driver reports all controller configuration errors and information.</li> <li>• <b>Error reporting disabled:</b> UEFI driver will not report any controller configuration errors and information via driver health protocol.</li> </ul>

.....continued

Option	Description
Configure PCIe Max Read Request Size	<p>This option permits setting the maximum read request size which allows optimization of data flow for the purpose of tweaking controller performance. PCIe max read request size can be configured to 128/256/512/1024 bytes.</p> <p>Active PCIe Max Read Request Size shows the current set value.</p> <p>Pending PCIe Max Read Request Size shows modified value which will be applied after next reboot.</p>

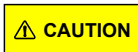
## 10.8 Recovering Cache Module

This operation is only available if the cache was disabled due to smart storage backup power source failing and the backup from RAM into FLASH memory did not complete. Ensure that the smart storage backup power source is operating properly before recovering the cache module. Controller may require a reboot after the operation to complete the cache recovery process.

From the main menu, select **Configure Controller Settings**, then select **Recover Cache Module**.

## 10.9 Clearing the Controller Configuration

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



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**.

## 10.10 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**.

## 10.11 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.
- **Minimum Power**: When settings are selected without regard to system performance, maximum power savings is achieved. This setting should only be used for very specific applications; it is not appropriate for the majority of customers. Most applications will suffer significant performance reduction.
- **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 the 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**.

## 10.12 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 the 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: <ul style="list-style-type: none"> <li>• Feature Disabled (Default)</li> <li>• SMBus clock speed 100 kHz</li> <li>• SMBus clock speed 400 kHz</li> </ul>
SMBus Clock Stretching	Sets the SMBus Clock Stretching mode: <ul style="list-style-type: none"> <li>• Enable: Enables SMBus clock stretching</li> <li>• Disable: Disables SMBus clock stretching</li> </ul>

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: <ul style="list-style-type: none"> <li>• Default</li> <li>• Fixed</li> </ul>



MCTP Parameters	Description
	<ul style="list-style-type: none"> <li>• ARP (Address Resolution Protocol)</li> </ul>
SMBus Physical Channel	Sets the SMBus Channel mode: <ul style="list-style-type: none"> <li>• Enable: Enables SMBus channel</li> <li>• Disable: Disables SMBus channel</li> </ul>
Use Static EIDs during Initialization	Sets the Static End Point Identifier (EID) mode: <ul style="list-style-type: none"> <li>• Enable: Enables Static EID</li> <li>• Disable: Disables Static EID</li> </ul>
VDM Discovery Notify	Sets the Vendor Defined Message (VDM) discovery notification mode: <ul style="list-style-type: none"> <li>• Enable: Enables VDM discovery notification</li> <li>• Disable: Disables VDM discovery notification</li> </ul>

9. Select **Submit Changes**.

## 10.13 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.

The Encryption Manager allows configuring the controller-based encryption options on the 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 the Encryption Manager is configured, logical drives can be encrypted and storage spaces created with both encrypted and plaintext logical drives. For more information about creating and managing encrypted volumes, see [10.3. Creating an Array](#).

### 10.13.1 Encryption Manager Full Setup

Use the Full Setup option to configure the Encryption Manager for initial use. This option allows setting the master encryption key, configuring the Crypto Officer account, and enabling other basic encryption settings. The Encryption Manager Terms of Use must be accepted.

To configure the Encryption Manager:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select the 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.



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**.

### 10.13.2 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 completing the Encryption Manager Full setup; see [10.13.1. Encryption Manager Full Setup](#).

To modify the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select the 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**.

### 10.13.3 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 completing 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 .  
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**.

### 10.13.4 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**.

### 10.13.5 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 the storage space. However, to continue accessing or managing encrypted volumes, reconfigure the basic encryption settings in the Encryption Manager; see [10.13.1. Encryption Manager Full Setup](#).

To clear the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode.
2. Select the controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Clear Configuration**.
5. If the 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**.

### 10.13.6 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 the account type: Crypto Officer or User.
5. Select **Submit Changes**.

### 10.13.7 Converting Plaintext Data to Encrypted Data

Use this option to convert plaintext data to encrypted data. 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 the 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**.

### 10.13.8 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 the account type: Crypto Officer or User.
5. Select **Submit Changes**.

### 10.13.9 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 press `Enter` to submit.
5. Select **Submit Changes**.

## 10.14 Configuring the Controller Port Mode

This option sets the operating mode for the ports on the controller. (To set the operating mode for individual ports, see [10.7. Modifying SmartHBA 2100/SmartRAID 3100 Settings](#).) You can set the 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 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**.

## 10.15 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 the controller, then press `Enter`. From the main menu, select **Disk Utilities**, select the disk drive, then press `Enter`.

## 10.16 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 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`.

## 10.17 Erasing a Disk Drive

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**.

## 10.18 Updating Drive Firmware

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.

## 10.19 Clearing Configuration Meta-data

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**.

## 10.20 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**.

- 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)**.

## 10.21 Updating the SmartHBA 2100/SmartRAID 3100 Firmware

To update the SmartHBA 2100/SmartRAID 3100 firmware:

- 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.
- From the main menu, select **Administration**, then select **Flash Controller Firmware**.
- Select **Continue with flashing Firmware**.
- 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.
- When the update is complete, reboot the server.

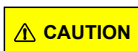
## 10.22 Creating a Support Archive

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

To create a support archive:

- From the main menu, select **Administration**, then select **Save Support Archive**.
- 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.
- Press any key to complete the operation and exit.

## 10.23 Resetting the Controller to Factory Defaults



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 2100/SmartRAID 3100 to factory default settings.

To reset the controller:

- From the main menu, select **Administration**.
- Select **Reset controller settings to factory defaults**.
- 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](#).

#### RHEL OS Images

The instructions below apply to the following RHEL OS images:

- Red Hat® Enterprise Linux 7.4, 7.3, 7.2, 7.1, 7.0 (64-bit only)
- Red Hat® Enterprise Linux 6.9, 6.8, 6.7, 6.6 (64-bit only)

To install the SmartPQI driver from source for RHEL-based OS images:

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: `# yum install kernel kernel-devel kernel-headers gcc`
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` process with the newly installed `smartpqi` driver: `# dracut -v -f --add-drivers smartpqi`  
**Note:** RHEL provides `dracut` command to place the newly installed `smartpqi.ko` driver modules into the `initramfs` file to include them in the Linux kernel.
8. Reboot the system to load the new `initramfs`, which will contain the newly installed `smartpqi.ko` driver.

#### SuSE OS Images

The instructions below apply to the following SuSE OS images:

- SuSE Linux Enterprise Server 12, SuSE Linux Enterprise Server 12 SP1, SP2, SP3 (64-bit only)



- SuSE Linux Enterprise Server 11 SP3, SP4 (64-bit only)

To install the SmartPQI driver from source for SuSE OS images:

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: `# zypper install kernel-devel gcc make`
3. Extract the driver source code from the `source_tgz` 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. Backup the already 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 kernel 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` process with the newly installed `smartpqi` driver: `# mkinitrd -v -m smartpqi`  
**Note:** SLES provides `mkinitrd` command to place the newly installed `smartpqi.ko` driver modules into the `initramfs` file to include them in the Linux kernel.
8. Reboot the system to load the new `initramfs`, 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.  
`# ls SCSI`
3. Once the DVD name is confirmed, create a location to mount the DVD, for example:  
`# mkdir /media/iso`
4. Mount the DVD to the `/media/iso` directory by using the following command:  
`/dev/srX /media/iso udf,iso9660 noauto,user,ro 0 0`
5. Use the following command to mount the DVD, once the entry is placed in `/etc/fstab`:  
`# 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.

```
# ls SCSI
```

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

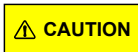
Item	SmartRAID Adapters	SmartHBA Adapters	Description
Max single/dual devices supported	256	256	# of physical SAS/SATA devices supported. Includes SEP devices, expanders. Results into 238 storage devices supported
Max # of RAID arrays supported	64	64	Maximum number of RAID arrays supported / exposed to host OS
Max # of logical drives/single cached volumes (single drive RO)	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	4/32	4/32	Number per Array/number per adapter. <b>Note:</b> 4/32 is recommended but user can assign spares up to 128.

## 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)



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:** SmartRAID 3100 Series adapters and SmartHBA 2100 Series adapters require adequate airflow to operate reliably. Forced airflow is **required**. The recommended airflow is **200 LFM** (linear feet per minute), minimum, for all controllers *except*:

- SmartRAID 3154-24i—**250 LFM**, minimum
- SmartRAID 3162-8i [e]—**150 LFM**, minimum

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.

### 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 SmartRAID 3101-4i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3101E-4i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3151-4i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3102-8i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3102E-8i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3152-8i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3154-8i	10.86 W	0.2A @ 3.3 VDC; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3154-8e	10.86 W	0.2A @ 3.3 VDC ; 0.85A @ 12.0 VDC
Adaptec SmartRAID 3154-16i	13.00 W	0.65A @ 3.3 VDC; 0.9A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartRAID 3154-24i	16.80 W	0.74A @ 3.3 VDC; 1.2A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartRAID 3154-8i8e	15.93 W	0.83A @ 3.3 VDC; 1.1 A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartRAID 3154-8i16e	17.6 W	0.97A @ 3.3 VDC; 1.2 A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartRAID 3162-8i	9.15 W	0.52A @ 3.3 VDC; 0.62 A @ 12.0 VDC
Adaptec SmartRAID 3162-8i /e	11.72 W	0.65 A @ 3.3 VDC; 0.798 A @ 12.0 VDC
Adaptec SmartHBA 2100-4i4e	7.23 W	1.1A @ 3.3 VDC; 0.3A @ 12.0 VDC
Adaptec SmartHBA 2100-8i	8.20 W	0.2A @ 3.3 VDC; 0.63A @ 12.0 VDC

.....continued

Adapter Model	Typical Power	Typical Current
Adaptec SmartHBA 2100-16i	11.93 W	0.78 A @ 3.3 VDC; 0.78 A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartHBA 2100-24i	13.80 W	0.92 A @ 3.3 VDC; 0.90 A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)
Adaptec SmartHBA 2100-8i8e	11.93 W	0.78 A @ 3.3 VDC; 0.78 A @ 12.0 VDC (3.3 V auxiliary current consumption approximately 50 mA)

## 15. Revision History

**Table 15-1.** Revision History

Revision	Date	Description
E	06/2023	Updated for SR 2.8.0.
D	02/2023	<ul style="list-style-type: none"> <li>Updated for SR 2.7.4.</li> <li>Removed <b>Securing Existing RAID Logical Drives</b> section and its references as this feature is removed.</li> </ul>
C	11/2022	Updated for SR 2.7.2.
B	06/2022	Updated for SR 2.7.0. Added <a href="#">Managing SED</a> section.
A	02/2022	Initial release in Microchip template; Assigned Microchip literature number DS-00004439A, which replaces the previous Microsemi literature number ESC-2171547.
Previous Releases 1-10	10/2017 – 07/2021	Previous releases. Contact Microchip for release details.

## Microchip Information

### The Microchip Website

Microchip provides online support via our website at [www.microchip.com/](http://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](http://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](http://www.microchip.com/support)

### Microchip Devices Code Protection Feature

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

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

### Legal Notice

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



that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at [www.microchip.com/en-us/support/design-help/client-support-services](http://www.microchip.com/en-us/support/design-help/client-support-services).

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

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

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

## Trademarks

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

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

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

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

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

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

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

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

ISBN: 978-1-6683-2647-3

## **Quality Management System**

For information regarding Microchip's Quality Management Systems, please visit [www.microchip.com/quality](http://www.microchip.com/quality).

# Worldwide Sales and Service

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