



MICROCHIP

Adaptec® SmartRAID 3100 Series and SmartHBA 2100 Series Host Bus Adapters Installation and User Guide

Released / July 2021

Revision History : July 2021

Revision	Revision Date	Details of Change
10	July 2021	Updated for SR2.6.2 release: Update driver installation procedures, add Linux secure boot installation, remove unsupported drivers.
9	March 2021	Updated for SR2.6 release: add SLES 11 driver upgrade procedure with "by-uuid" method.
8	February 2020	Updated for SR2.5.2 release: Add specs, illustrations, features, installation procedures, and regulatory compliance for SmartRAID 3101E-4i and SmartRAID 3102E-8i adapters. Add new UEFI/HII options: Modify Cache Settings, Out of Band Messaging Settings (PBI/MCTP configuration).
7	August 2019	Updated for SR2.4.8 release: update Solaris SmartPQI driver installation instructions; add "SmartRAID/SmartHBA Physical and Logical Device Support" appendix.
6	January 2019	Updated for SR2.4 release. Add support for new SKU: SmartHBA 2100-16i. Add support for UEFI Configure Controller Port Mode; revise UEFI Encryption Manager Full Setup task flow; add caution and describe effects of UEFI Reset Controller to Factory Defaults.
5	April 2018	Clarify cache protection options and revise board illustrations for SmartRAID 3151-4i and SmartRAID 3154-8i controllers. Update max supported drives with expanders.
4	April 2018	Updated for SR2.3 release. Add support for new skus: SmartRAID 3162-8i, SmartRAID 3162-8i /e, SmartRAID 3154-8i8e, SmartRAID 3154-8i16e, SmartHBA 2100-8i8e. Add support for UEFI Encryption Manager, Create maxCache Array, and Reset controller to factory defaults.
3	December 2017	Updated supported operating systems
2	November 2017	<ol style="list-style-type: none"> 1. Updated supported operating systems. 2. Revised controller airflow requirements.
1	October 2017	First Production Release.

Regulatory Compliance Statements

Federal Communications Commission Radio Frequency Interference Statement



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

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

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

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

UL Compliance Statement

	Microchip Adaptec products are tested and listed by Underwriters Laboratories, Inc. to UL 60950-1 Second Edition and IEC-60950-1 Second Edition standards, file numbers E175975. Microchip Adaptec products are for use only with UL listed ITE.	
	Microchip Corporation	Use only with the listed ITE:
	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 Adaptec SmartHBA 2100-8i/ Adaptec SmartHBA 2100-24i/ Adaptec SmartHBA 2100-4i4e/ Adaptec SmartHBA 2100-8i8e/ Adaptec SmartHBA 2100-16i	
 Tested to Comply With FCC Standards FOR HOME OR OFFICE USE		

Regulatory Compliance Statements

European Union Compliance Statement



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

- EN55032 (2014) Emissions:
 - Class B ITE radiated and conducted emissions
- EN55024 (2010) Immunity:
 - EN61000-4-2 (2009) Electrostatic discharge: ± 4 kV contact, ± 8 kV air
 - EN61000-4-3 (2010) Radiated immunity: 3V/m
 - EN61000-4-4 (2012) Electrical fast transients/burst: ± 1 kV AC, ± 0.5 kV I/O
 - EN61000-4-5 (2014) Surges: ± 1 kV differential mode, ± 2 kV common mode
 - EN61000-4-6 (2014) Conducted immunity: 3 V
 - EN61000-4-11 (2004) Supply dips and variations: 30% and 100%
- EN50581 (2012) Technical Documentation:
 - For the assessment of electrical and electronic products with respect to the restriction of hazardous substances

In addition, all equipment requiring UL listing has been found to comply with EMC Directive 2014/35/EU, in accordance with EN60950 with amendments A1, A2, A3, A4, A11, A12, and with UL 62368-1:2014 and IEC 62368-1:2014.

Australian/New Zealand Compliance Statement



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

Canadian Compliance Statement



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

Japanese Compliance (Voluntary Control Council Initiative)



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

Korean Compliance (KCC) Statement



Microchip Adaptec products are tested and certified by KCC:
Korean Compliance (KCC) Statement:

MSIP-REM-M2C-3154-8i

The above certification covers the following series:

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 SmartHBA 2100-8i

Korean Compliance (KCC) Statement:

MSIP-REM-M2C-3154-8e

The above certification covers the following series:

Regulatory Compliance Statements

Adaptec SmartRAID 3154-8e

Korean Compliance (KCC) Statement:

MSIP-REM-M2C-3154-24i

The above certification covers the following series:

Adaptec SmartRAID 3154-16i w/ ASCM-35F

Adaptec SmartRAID 3154-24i w/ ASCM-35F

Adaptec SmartHBA 2100-24i

Korean Compliance (KCC) Statement:

MSIP-REM-M2C-3154-8i16e

The above certification covers the following series:

Adaptec SmartRAID 3154-8i16e w/ ASCM-35F

Adaptec SmartRAID 3154-8i8e w/ ASCM-35F

Adaptec SmartHBA 2100-8i8e

Korean Compliance (KCC) Statement:

MSIP-REM-M2C-2100-4i4e

The above certification covers the following series:

Adaptec SmartHBA 2100-4i4e

Korean Compliance (KCC) Statement:

MSIP-REM-M2C-3162-8i

The above certification covers the following series:

Adaptec SmartRAID 3162-8i

Adaptec SmartRAID 3162-8i /e

B급 기기

(가정용 방송통신기자재)

Class B Equipment

(For Home Use Broadcasting & Communication Equipment)

이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

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

Table of Contents

1 About This Guide.....	1
1.1 What You Need to Know Before You Begin.....	1
1.2 Terminology Used in this Guide.....	1
1.3 How to Find More Information.....	1
2 Kit Contents and System Requirements.....	3
2.1 Kit Contents.....	3
2.2 System Requirements.....	3
3 About Your SmartRAID 3100 Series Host Bus Adapter	4
3.1 Standard Features.....	4
3.2 Mechanical Information	4
3.2.1 Board Dimensions.....	4
3.2.2 Heat Sink.....	4
3.3 Visual Indicators.....	5
3.4 About the Adaptec SmartRAID 3101-4i/3151-4i.....	7
3.5 About the Adaptec SmartRAID 3101E-4i.....	8
3.6 About the Adaptec SmartRAID 3102-8i/3152-8i/3154-8i.....	9
3.7 About the Adaptec SmartRAID 3102E-8i.....	10
3.8 About the Adaptec SmartRAID 3154-8e.....	11
3.9 About the Adaptec SmartRAID 3154-8i8e.....	12
3.10 About the Adaptec SmartRAID 3154-8i16e.....	13
3.11 About the Adaptec SmartRAID 3154-16i.....	14
3.12 About the Adaptec SmartRAID 3154-24i.....	15
3.13 About the SmartRAID 3162-8i/SmartRAID 3162-8i /e Adapter.....	16
4 About Your SmartHBA 2100 Series Host Bus Adapter	17
4.1 Standard Features.....	17
4.2 Mechanical Information	17
4.2.1 Board Dimensions.....	17
4.2.2 Heat Sink.....	17
4.3 Visual Indicators.....	18
4.4 About the Adaptec SmartHBA 2100-4i4e.....	19
4.5 About the Adaptec SmartHBA 2100-8i.....	20
4.6 About the Adaptec SmartHBA 2100-8i8e.....	21
4.7 About the Adaptec SmartHBA 2100-16i.....	22
4.8 About the Adaptec SmartHBA 2100-24i.....	23
5 Installing the Controller and Disk Drives.....	24
5.1 Before You Begin.....	24
5.2 Selecting Disk Drives and Cables	24
5.2.1 Disk Drives.....	24
5.2.2 Cables.....	24
5.3 Installing the Host Bus Adapter.....	25
6 Installing the Driver and an Operating System.....	28
6.1 Download the Driver Package.....	28
6.2 Installing with Windows.....	28
6.3 Installing with Red Hat Linux or CentOS.....	28
6.4 Installing with SuSE Linux Enterprise Server.....	29

6.5 Installing with Oracle Linux.....	30
6.6 Installing with Ubuntu Linux.....	30
6.7 Installing with Debian Linux.....	30
6.8 Installing with FreeBSD.....	31
6.9 Installing with Solaris.....	33
6.9.1 Installing with Solaris Live Media.....	33
6.9.2 Installing with Solaris Text Installer.....	34
6.10 Installing with Citrix XenServer.....	35
6.11 Installing with VMware.....	36
7 Installing the Driver on an Existing Operating System.....	38
7.1 Download the Driver Package.....	38
7.2 Installing on Windows.....	38
7.3 Installing on Red Hat or CentOS.....	38
7.4 Installing on SuSE Linux Enterprise Server.....	39
7.5 Installing on Oracle Linux.....	39
7.6 Installing on Ubuntu Linux.....	39
7.7 Installing on Debian Linux.....	40
7.8 Installing on FreeBSD.....	40
7.9 Installing on Solaris.....	40
7.10 Installing on Citrix XenServer.....	42
7.11 Installing on VMware.....	42
8 Solving Problems	44
8.1 Troubleshooting Checklist.....	44
8.2 Resetting the Adapter	44
Appendix A Using the Microchip SAS/SATA Configuration Utility.....	45
A.1 Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?.....	45
A.2 Controller Information.....	46
A.3 Creating an Array.....	46
A.4 Creating a maxCache Array.....	46
A.5 Managing Arrays and Logical Drives.....	47
A.5.1 Viewing Logical Drive Properties.....	47
A.5.2 Creating Logical Drives.....	47
A.5.3 Enabling IO Bypass.....	48
A.5.4 Editing Logical Drive Properties.....	48
A.5.5 Deleting a Logical Drive.....	48
A.5.6 Assigning Spares.....	49
A.5.7 Deleting a Spare Drive.....	49
A.5.8 Identifying the Drives in an Array.....	49
A.5.9 Deleting an Array.....	50
A.6 Modifying SmartHBA 2100/SmartRAID 3100 controller Settings.....	50
A.7 Clearing the Controller Configuration.....	52
A.8 Backup Power Source.....	52
A.9 Managing Power Settings.....	52
A.10 Out of Band Messaging Settings.....	53
A.11 Using the Encryption Manager.....	54
A.11.1 Encryption Manager Full Setup.....	54
A.11.2 Modifying the Encryption Manager Configuration.....	55
A.11.3 Modifying User Account Settings.....	56
A.11.4 Resetting a Forgotten Password.....	56
A.11.5 Clearing the Encryption Manager Configuration.....	57
A.11.6 Re-Keying a Logical Drive.....	57
A.11.7 Converting Plaintext Data to Encrypted Data.....	58
A.11.8 Erasing an Encrypted Logical Drive.....	58

A.11.9 Importing a Foreign Master Key.....	58
A.12 Configuring the Controller Port Mode.....	59
A.13 Device Information.....	59
A.14 Identifying a Disk Drive.....	59
A.15 Erasing a Disk Drive.....	60
A.16 Updating Drive Firmware.....	60
A.17 Clearing Configuration Meta-data.....	61
A.18 Setting the Bootable Device(s) for Legacy Boot Mode.....	61
A.19 Updating the SmartHBA 2100/SmartRAID 3100 controller Firmware.....	62
A.20 Creating a Support Archive.....	62
A.21 Resetting the Controller to Factory Defaults.....	62
Appendix B Installing the SmartPQI Drivers from Source	64
B.1 Installation Instructions for Supported Linux OS's.....	64
B.2 Using the Installation DVD as the Repository.....	66
Appendix C SmartRAID/SmartHBA Physical and Logical Device Support.....	68
Appendix D Safety Information.....	69
D.1 Electrostatic Discharge (ESD).....	69
Appendix E Technical Specifications.....	70
E.1 Environmental Specifications.....	70
E.2 DC Power Requirements.....	70
E.3 Current and Power Requirements	70
Appendix F The Microchip Web Site.....	72
F.1 Customer Change Notification Service.....	72
F.2 Customer Support.....	72
F.3 Microchip Devices Code Protection Feature.....	72
F.4 Legal Notice.....	73
F.5 Trademarks.....	73
F.6 Quality Management System Certified by DNV.....	73
F.7 Worldwide Sales and Service.....	74

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 SmartRAID 3100 Series and SmartHBA 2100 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 SmartRAID 3100 Series or SmartHBA 2100 Series Host Bus Adapter by referring to these documents.

- *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)
- *Adaptec SmartRAID 3100 and SmartHBA 2100 Software/Firmware Release Notes*—Includes updated product information, known issues, and limitations. (ESC-2161026)

2 Kit Contents and System Requirements

This section lists the contents of your SmartRAID 3100 Series or SmartHBA 2100 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 storage.microsemi.com. For more information, see [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 the descriptions in [About Your Host Bus Adapter](#))
- One of these operating systems:
 - Microsoft® Windows®
 - Red Hat® Enterprise Linux
 - CentOS
 - SuSE Linux Enterprise Server
 - Ubuntu Linux
 - Debian Linux
 - Oracle Linux
 - Citrix XenServer
 - Solaris
 - FreeBSD
 - VMware ESXi

See the *Release Notes* for a complete list of supported OS versions.

- USB flash drive or CD burner, for creating driver disks and bootable media

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 pre-boot BIOS, CTRL-A 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 [Environmental Specifications](#) on page 70.

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 [Figure 1 • SmartRAID 3100 Series LED Locations](#) on page 5), and include DDR LEDs (also referred to as Flash-Based Write Cache, or FBWC, LEDs) and status LEDs. The LED states are described in [Table 3-2 • SmartRAID 3100 Series Status LEDs](#) on page 5 and [Table 3-3 • SmartRAID 3100 Series DDR/FBWC LED States](#) on page 6.

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

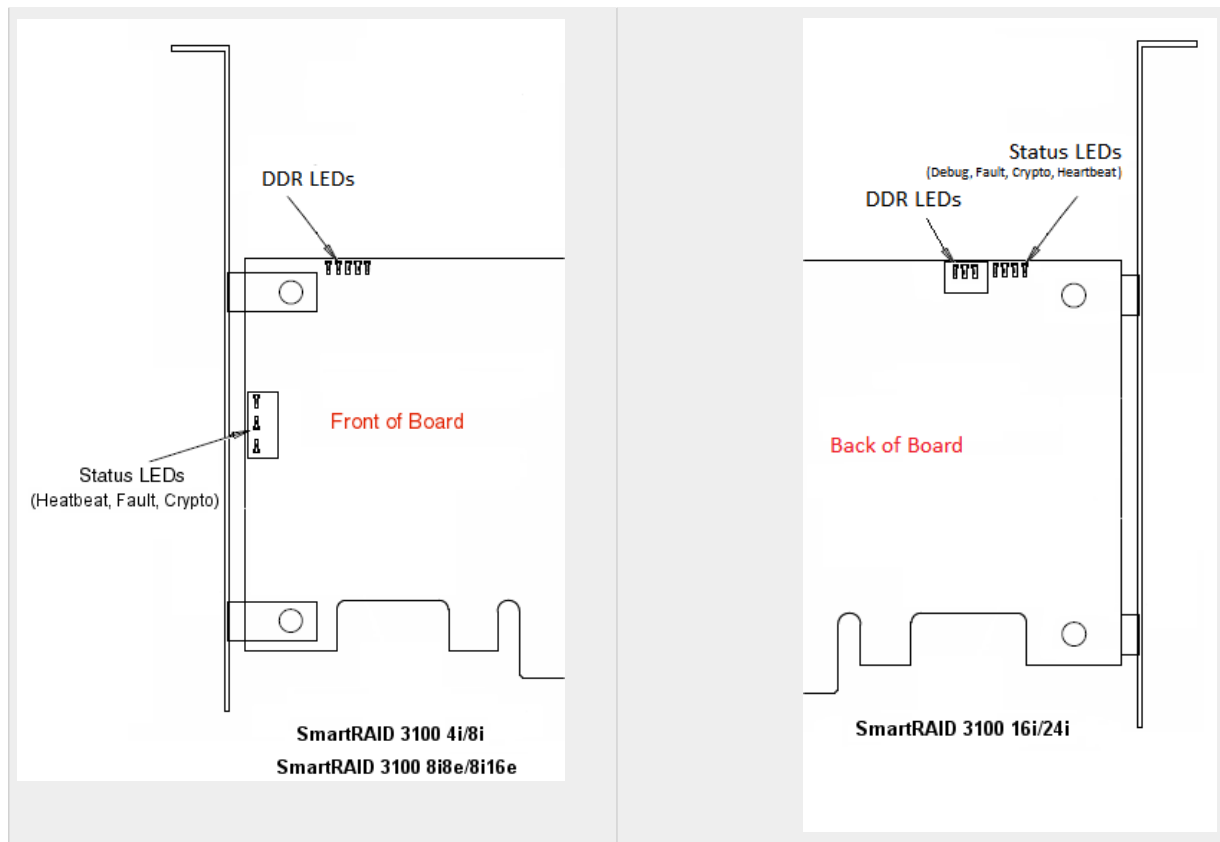


Table 3-2 • SmartRAID 3100 Series Status LEDs

LED	Color	Meaning
DDR_LED1	Yellow	Cache backup error (see Table 3-3 • SmartRAID 3100 Series DDR/FBWC LED States on page 6)
DDR_LED2	Green	Dirty cache (see Table 3-3 • SmartRAID 3100 Series DDR/FBWC LED States on page 6)
DDR_LED3	Green	Charge status (see Table 3-3 • SmartRAID 3100 Series DDR/FBWC LED States on page 6)
HEARTBEAT	Green	Heartbeat (blinks once per/second when firmware operating normally)
FAULT	Yellow	Hardware Lockup/Fault

About Your SmartRAID 3100 Series Host Bus Adapter

LED	Color	Meaning
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 Note: 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

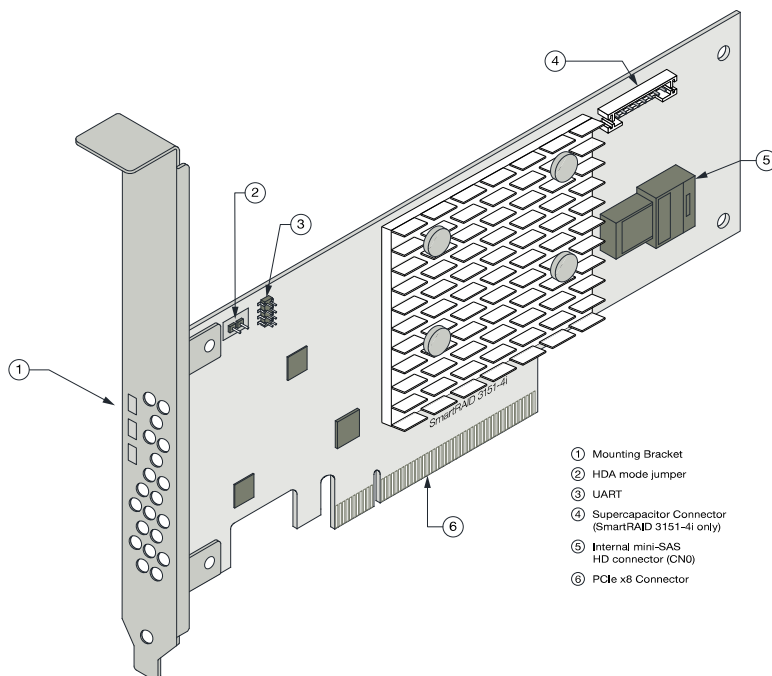
Table 3-3 • SmartRAID 3100 Series DDR/FBWC LED States

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

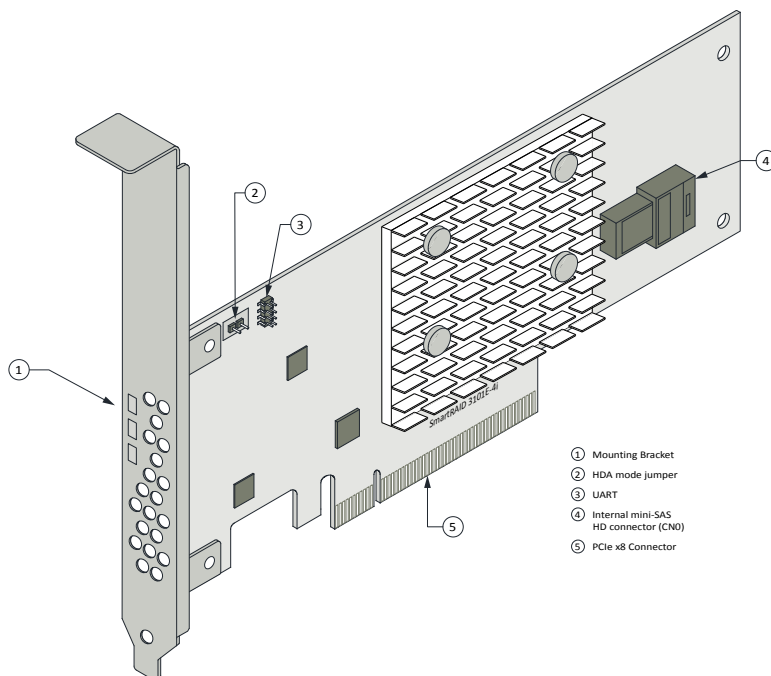


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	4
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1Mb MRAM
Cache	1 GB
Connectors, internal	1 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	4 direct-attached (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	SmartRAID 3101-4i: No (non-upgradeable) SmartRAID 3151-4i: Integrated ASCM-35F backup module with external super-capacitor

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

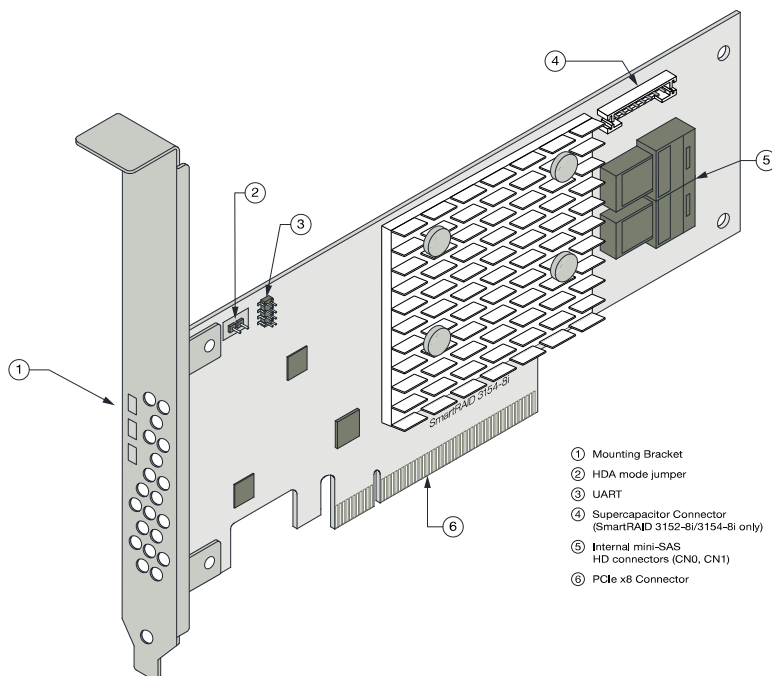


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	4
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1Mb MRAM
Cache	1 GB
Connectors, internal	1 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	4 direct-attached
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

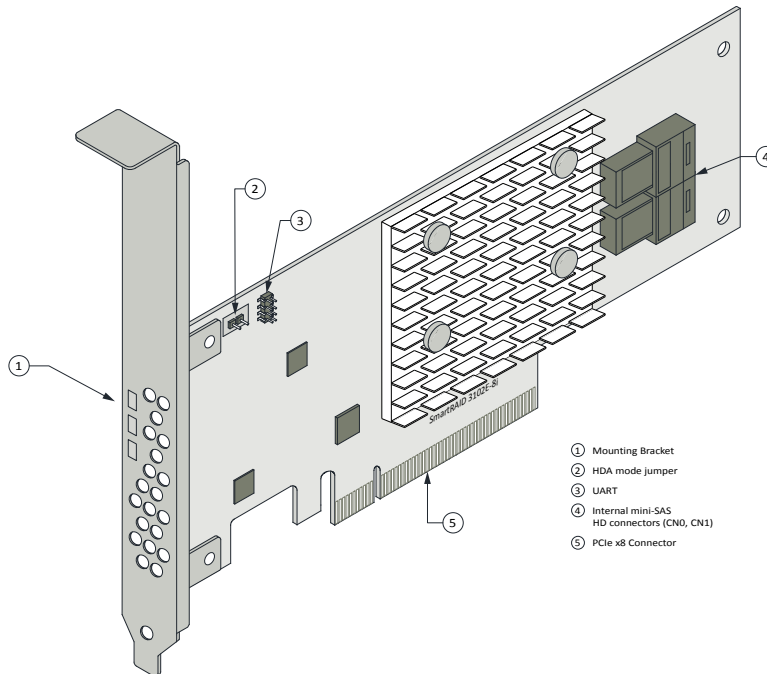


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1Mb MRAM
Cache	SmartRAID 3102-8i/3152-8i: 2 GB SmartRAID 3154-8i: 4 GB
Connectors, internal	2 mini-SAS HD x4 (SFF-8643)
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	SmartRAID 3102-8i: No (non-upgradeable) SmartRAID 3152-8i/3154-8i: 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

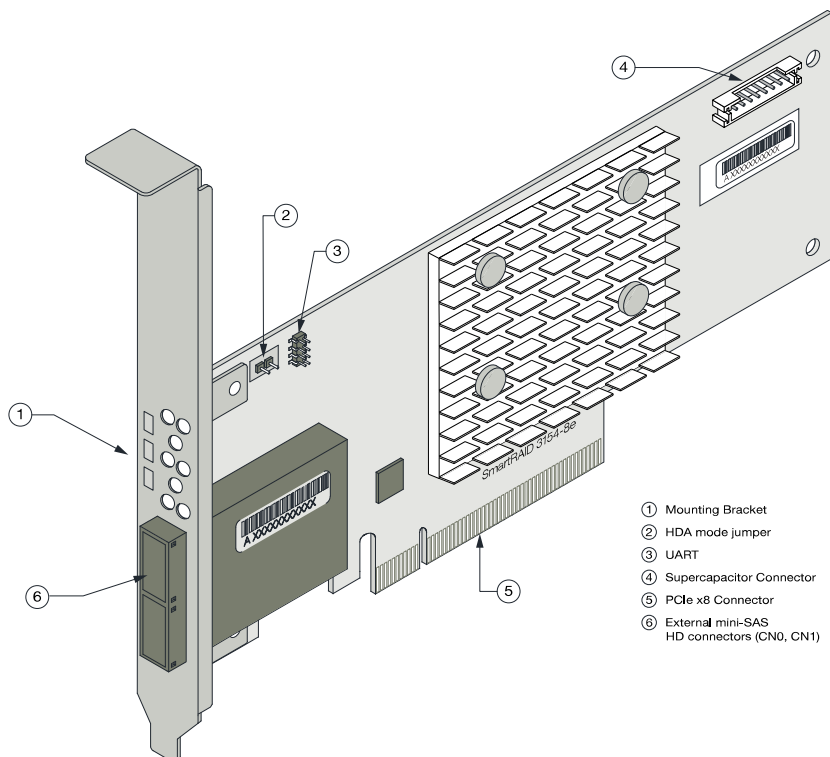


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb EEPROM, 1Mb MRAM
Cache	2 GB
Connectors, internal	2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	8 direct-attached
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

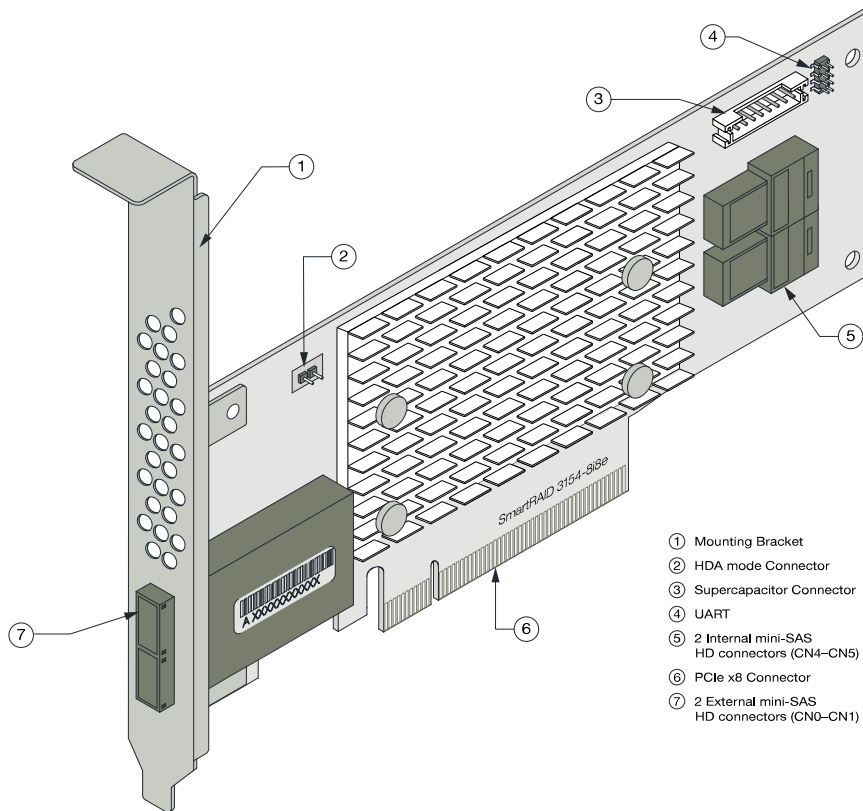


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 256 Kb SEEPROM, 1 Mb MRAM
Cache	4 GB
Connectors, external	2 mini-SAS HD x4 (SFF-8644)
Maximum number of disk drives	8 direct-attached (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

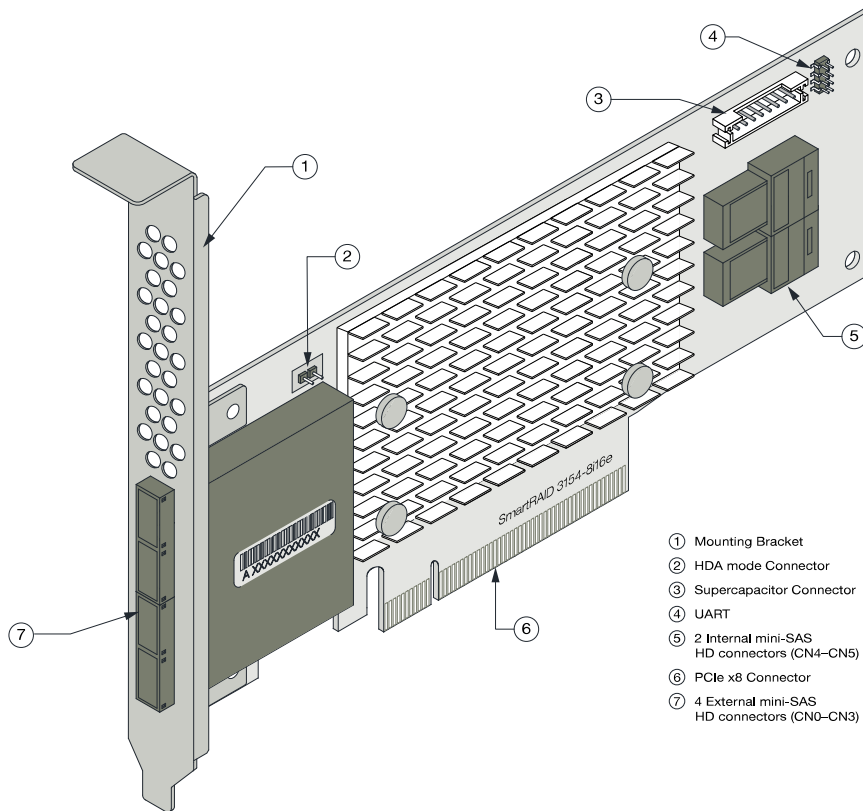


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	2 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum 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

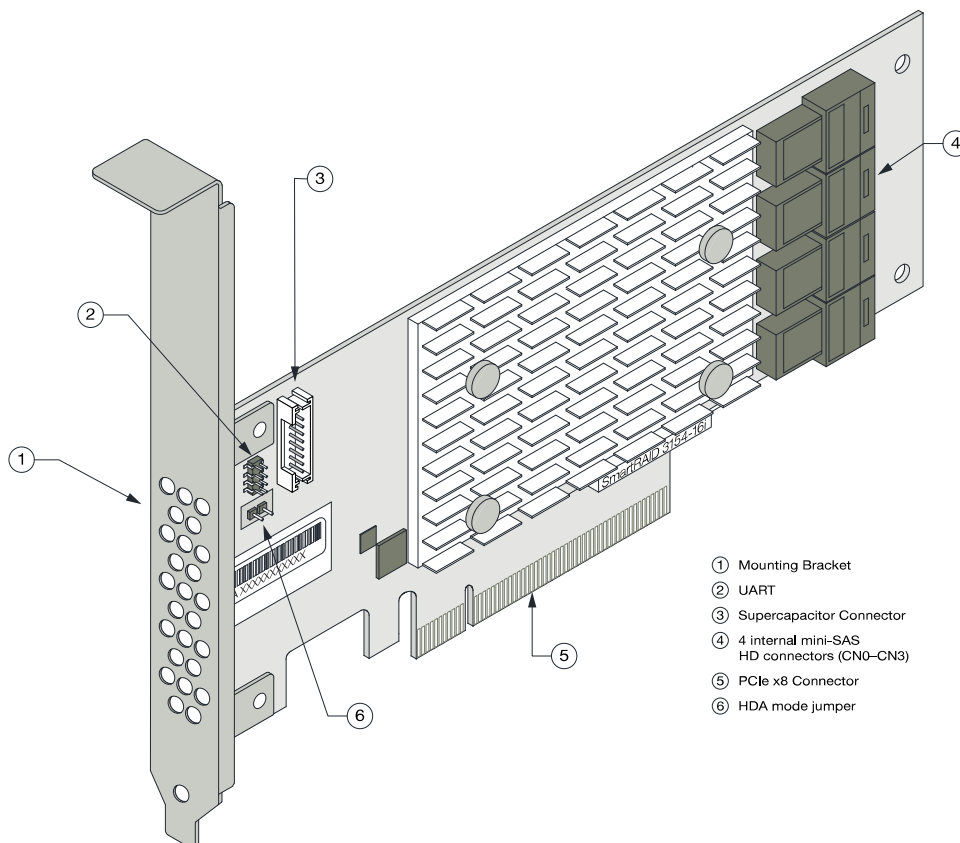


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	24
Standard memory	32 MB boot flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	4 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum 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

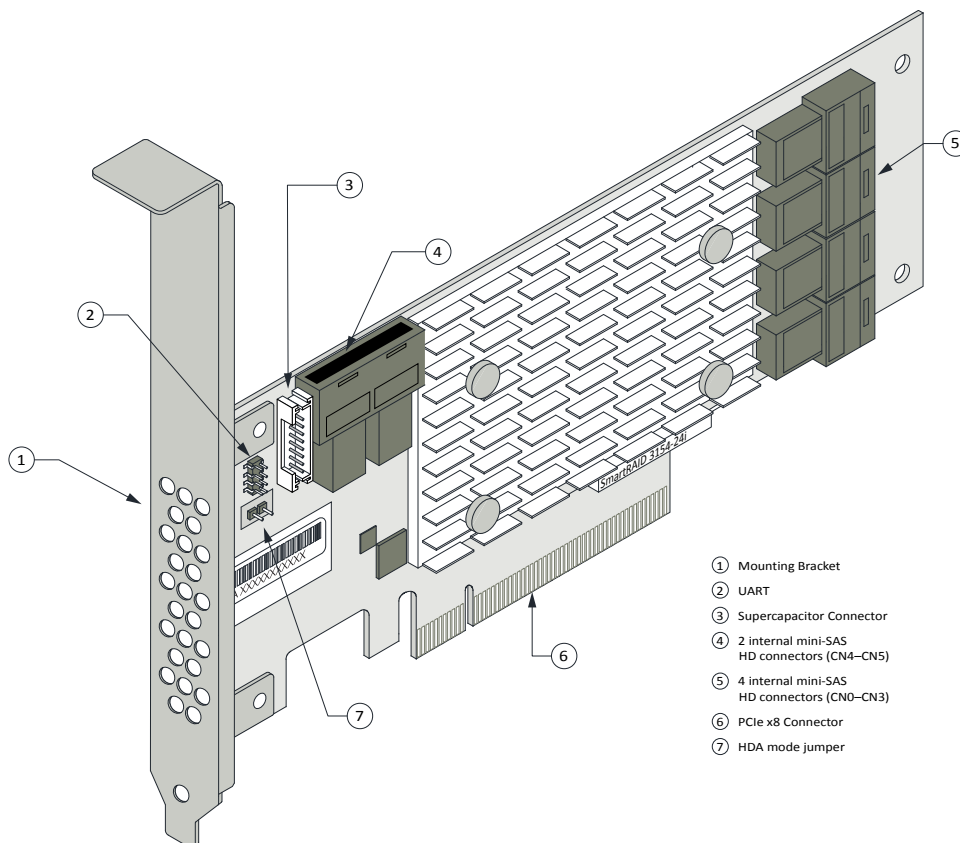


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB boot flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	4 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	16 direct-attached (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

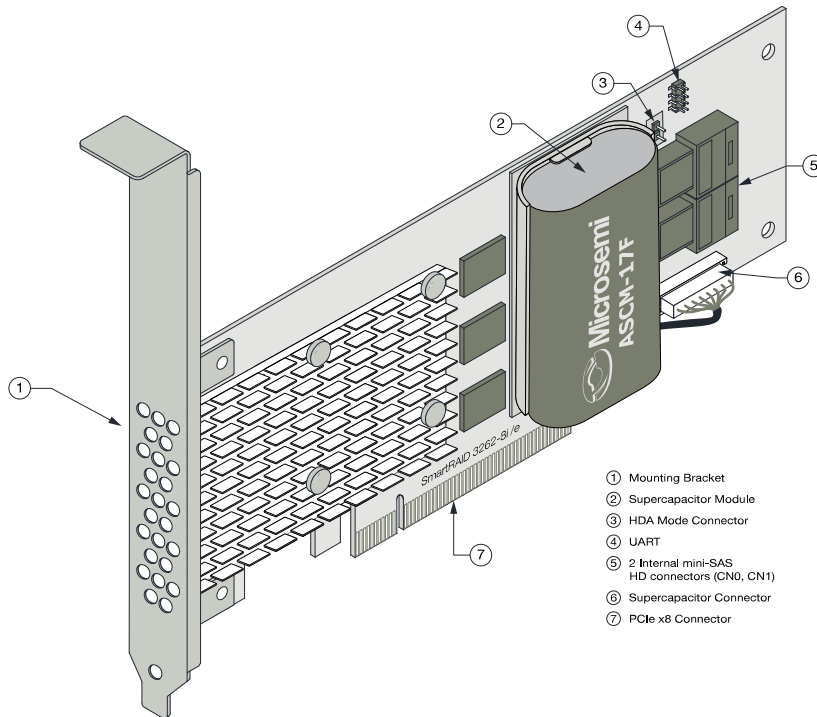


Form Factor	Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	24
Standard memory	32 MB Boot Flash, 128 Kb SEEPROM, 128 KB MRAM
Cache	4 GB
Connectors, internal	6 mini-SAS HD x4 (SFF-8643)
Maximum number of disk drives	24 direct-attached (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	SmartRAID 3162-8i: No SmartRAID 3162-8i /e: 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 pre-boot BIOS, CTRL-A 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

4.2 Mechanical Information

4.2.1 Board Dimensions

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

Table 4-4 • 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. For airflow requirements, see [Environmental Specifications](#).

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 [Figure 12 • SmartHBA 2100 Series LED Locations](#) on page 18). The LED states are described in [Table 4-5 • SmartHBA 2100 Series Status LEDs](#) on page 18.

Figure 4-12 • SmartHBA 2100 Series LED Locations

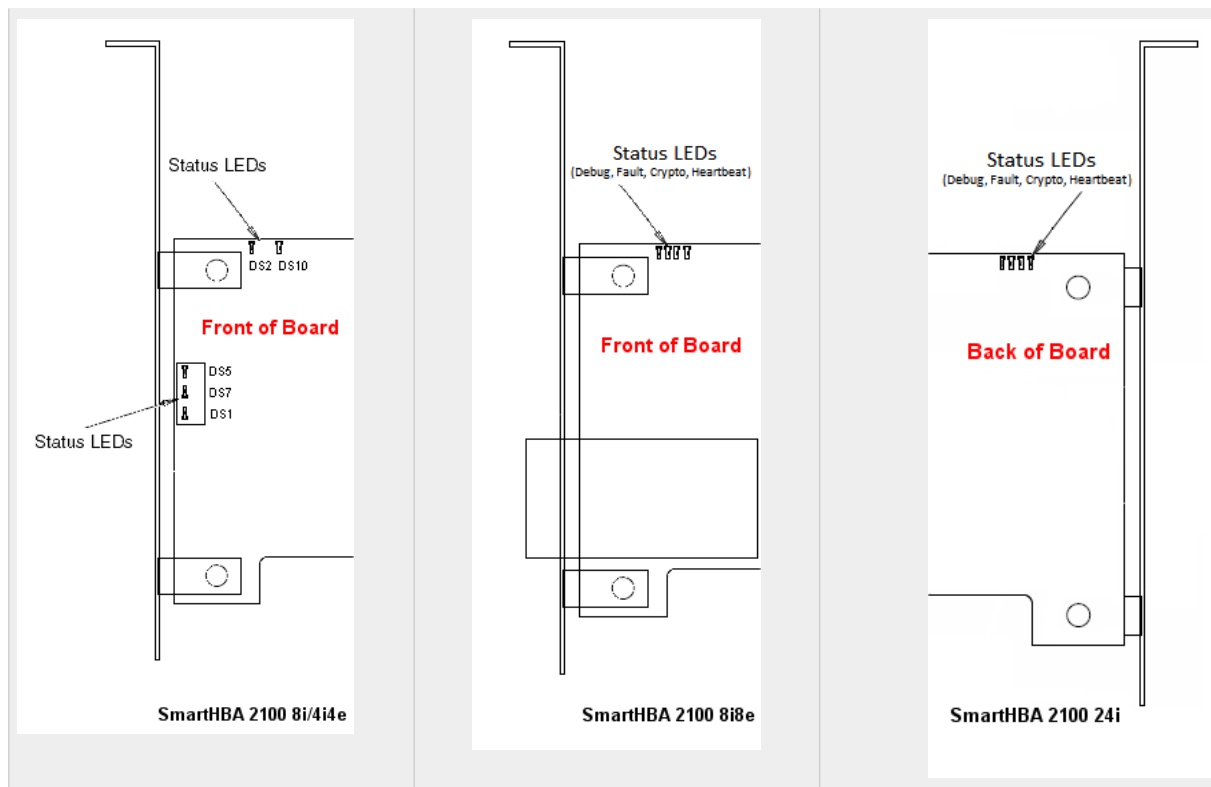


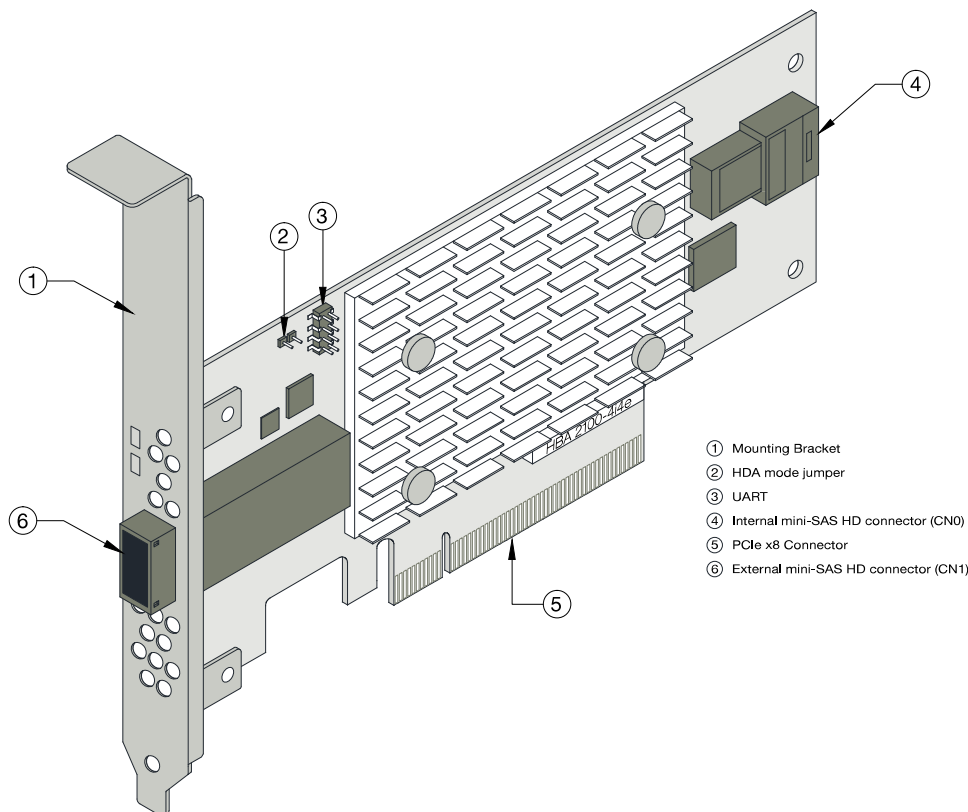
Table 4-5 • SmartHBA 2100 Series Status LEDs

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 4-13 • Adaptec SmartHBA 2100-4i4e

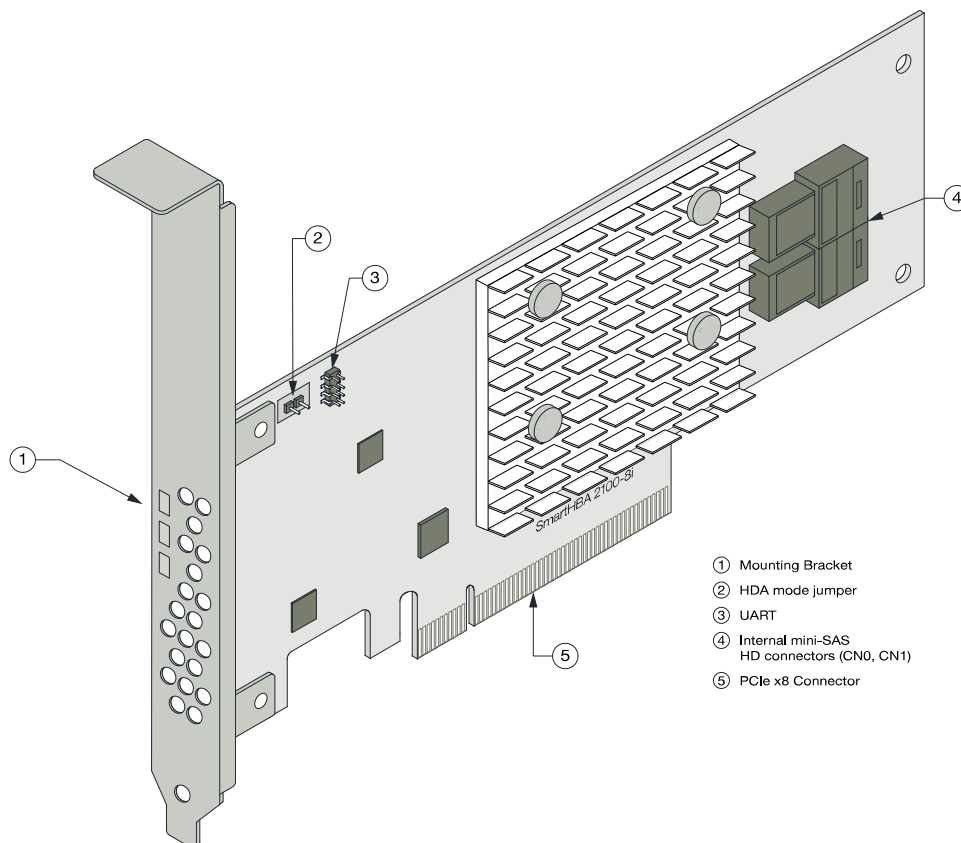


Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 16 KB SEEPROM, 128 KB MRAM
Connectors, internal	1x1 mini-SAS HD x4 (SFF-8643)
Connectors, external	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 4-14 • Adaptec SmartHBA 2100-8i Features

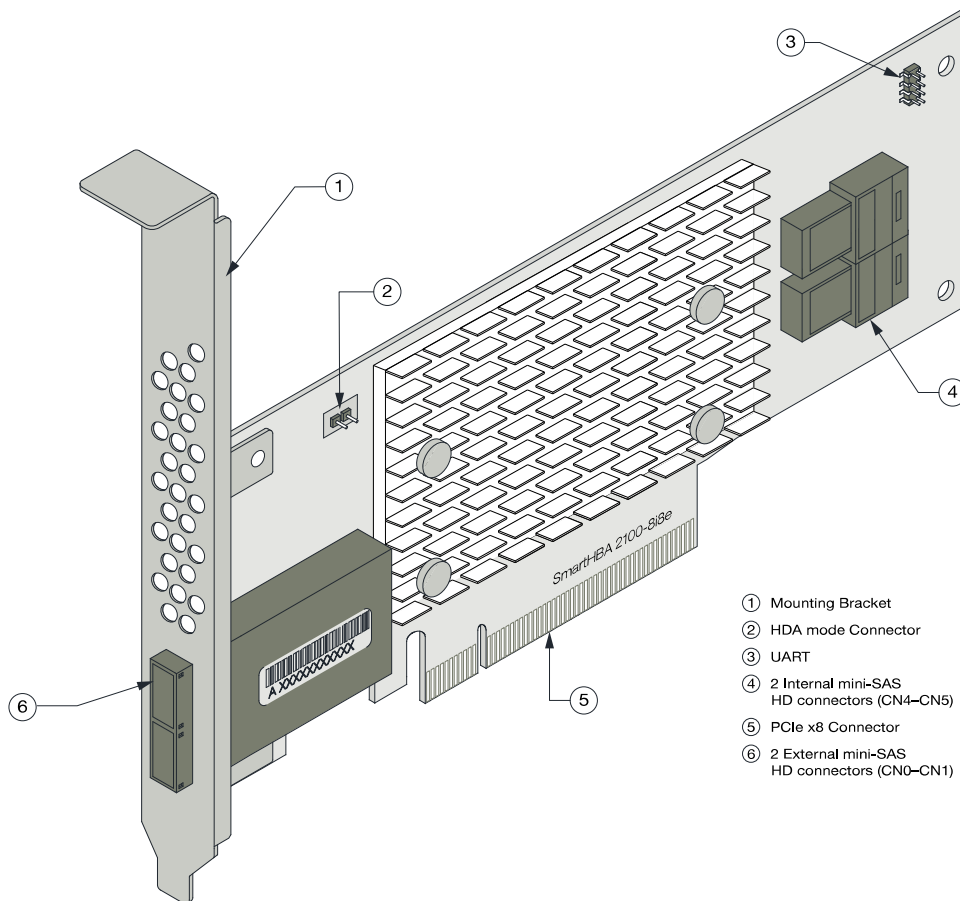


Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	8
Standard memory	32 MB Boot Flash, 32 KB SEEPROM, 128 KB MRAM
Connectors, internal	1x2 mini-SAS HD x4 (SFF-8643)
Maximum number of disk 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 4-15 • Adaptec SmartHBA 2100-8i8e Features

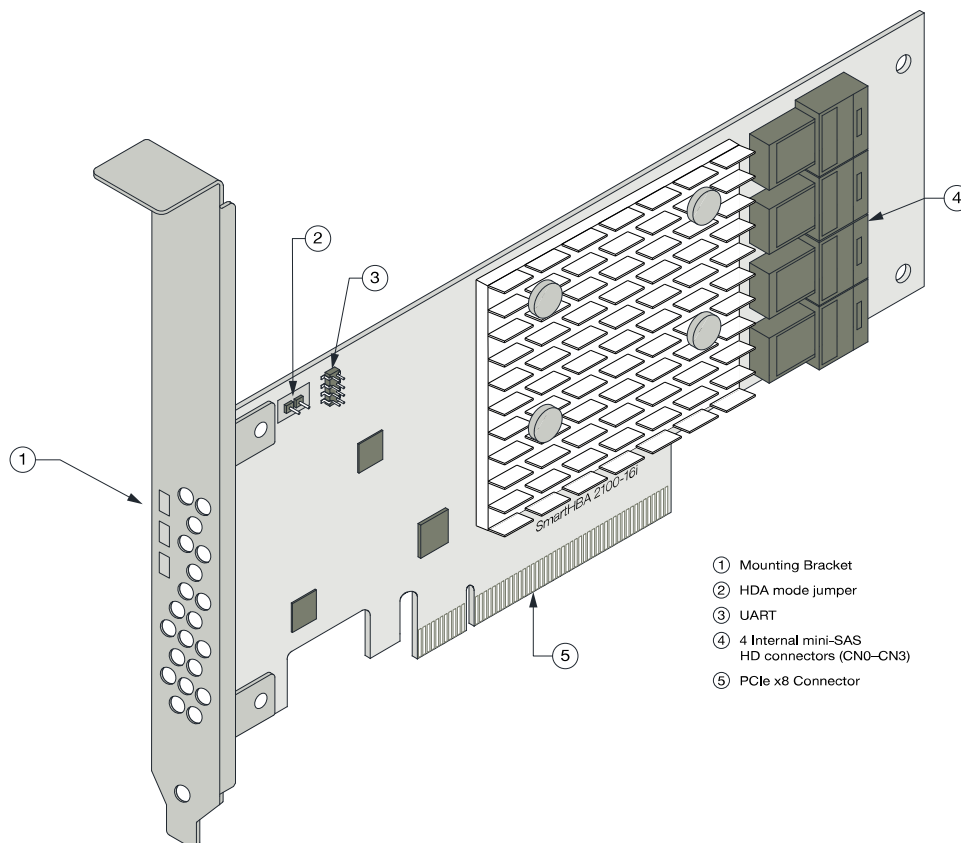


Form Factor	PCIe Low-profile MD2
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate	12 Gb/s per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 128 Kb EEPROM, 128 KB MRAM
Connectors, internal	2 mini SAS HD x4 (SFF-8644) and 2 mini SAS HD x4 (SFF-8643)
Maximum number 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 4-16 • Adaptec SmartHBA 2100-16i Features

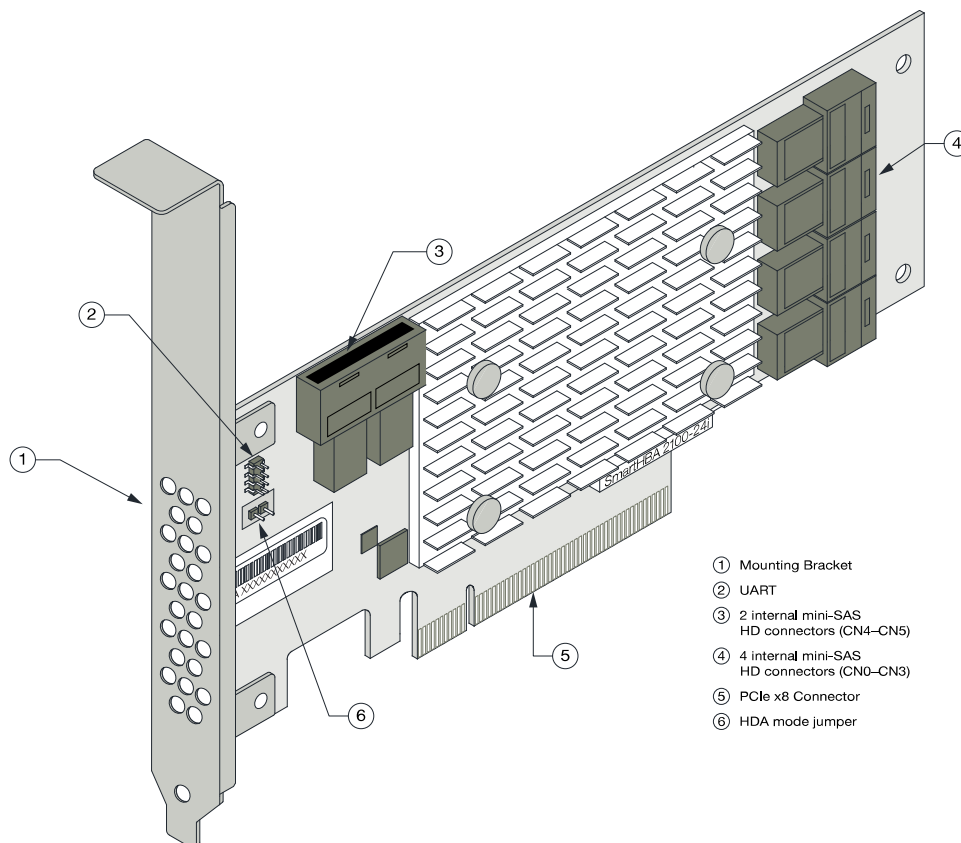


Form Factor	PCIe Low-profile MD2 (smaller than MD2)
Bus compatibility	PCIe 3.0
PCIe bus width	x8
Data transfer rate (SAS)	12 Gbps per port
Phys (Unified Serial Ports)	16
Standard memory	32 MB Boot Flash, 32 KB SEEPROM, 128 KB MRAM
Connectors, internal	4 mini-SAS HD x4 (SFF-8643)
Maximum number of disk 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 4-17 • 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 SmartRAID 3100 Series or SmartHBA 2100 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

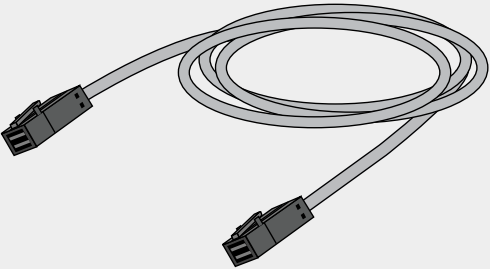
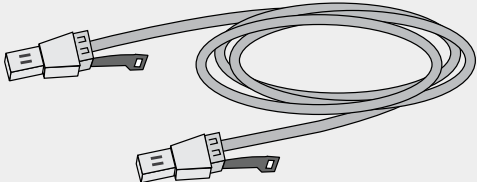
Your SmartRAID 3100 Series or SmartHBA 2100 Series adapter supports SAS and SATA disk drives, Solid State Drives (SSDs), and SAS tape drives. For more information about compatible disk drives, refer to <http://www.microsemi.com/products/storage/compatibility>.

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 SmartRAID 3100 Series or SmartHBA 2100 Series adapter, visit www.adaptec.com/cables.

Note: We recommend using 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

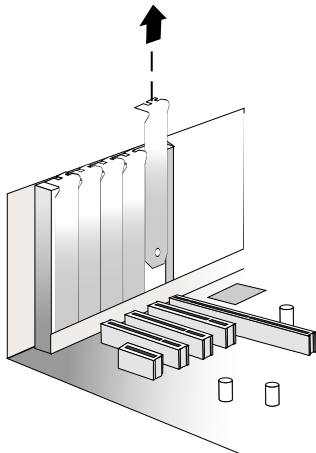
This section describes how to install your SmartRAID 3100 Series or SmartHBA 2100 Series adapter in a computer cabinet or server and connect internal and external storage devices. The SmartRAID 3100 Series and SmartHBA 2100 Series adapters have these configurations:

- 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 SmartRAID 3100 Series Host Bus Adapter](#).)

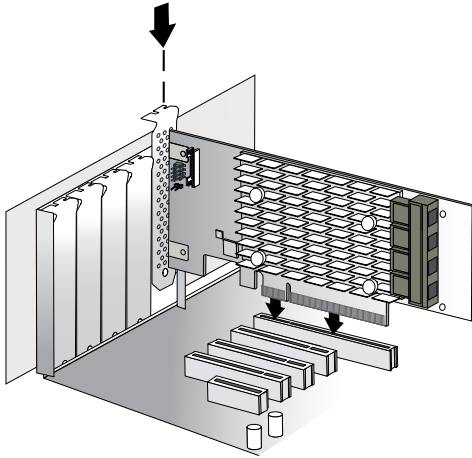
Note: For SmartRAID 3100 Series adapters with an external supercapacitor module, select a slot for the adapter that's next to an *empty* slot in the backplane, ideally, a short.

Caution: Touch a grounded metal object before handling the adapter.

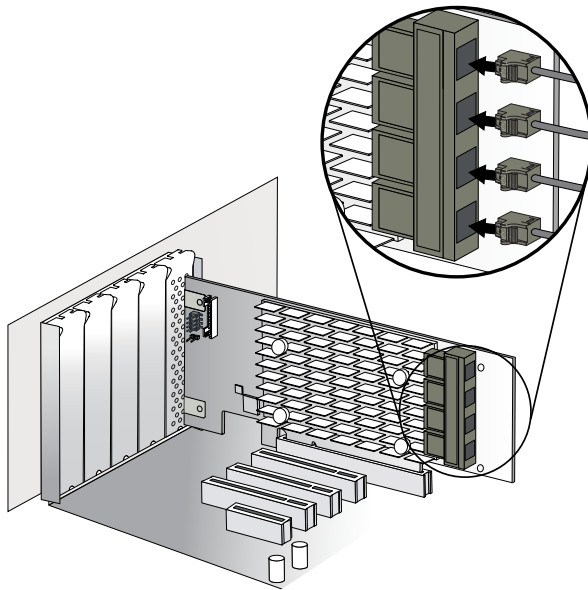


3. Insert the adapter into the expansion slot and press down gently but firmly until it clicks into place. When installed properly, the adapter should appear level with the expansion slot.

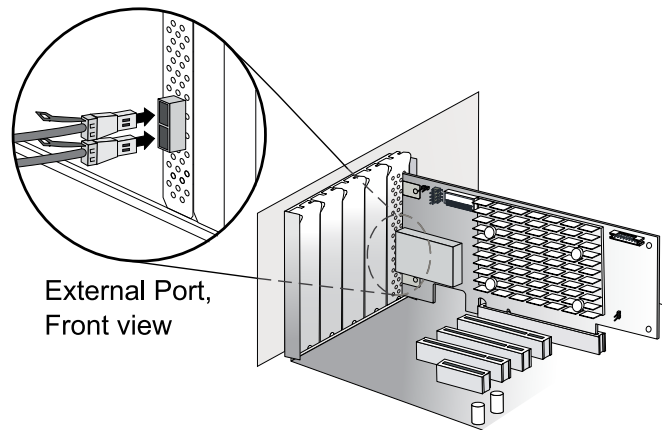
Caution: Be sure to handle the adapter by its bracket or edges only. Apply pressure only on the edges when inserting the card into expansion slot.



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:

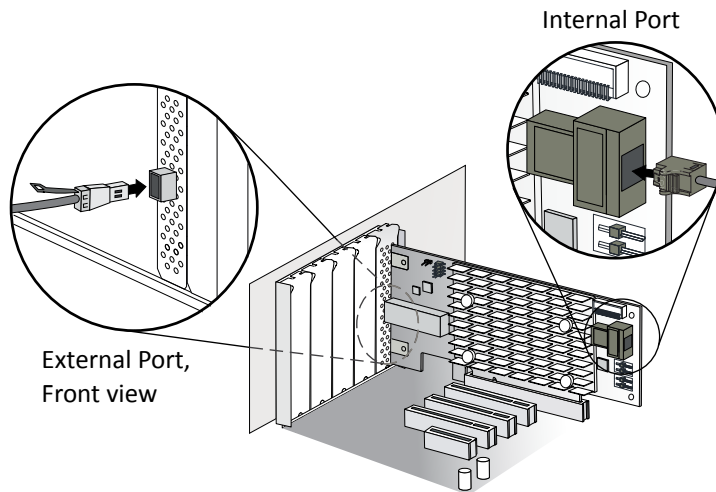


- For adapters with external ports, connect SAS HD cables between the adapter and external disk drives or enclosures:



External Port,
Front view

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



Internal Port

External Port,
Front view

6. (For SmartRAID 3100 Series adapters with external supercapacitor module only) Refer to the *Adaptec Flash Backup Module ASCM-35 Installation Instructions (ESC-2170352)* to complete the installation of the supercapacitor module.
7. 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 controller is installed in a computer or server.

Note: For information about building the SmartPQI drivers from source, see [Installing the SmartPQI Drivers from Source](#) on page 64.

6.1 Download the Driver Package

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

1. Open a browser window, then type start.adaptec.com in the address bar.
2. Enter your product or adapter model number, then select SmartRAID 3100 or SmartHBA 2100.
3. Select your operating system version, for instance, Microsoft Windows Server 2019 or Red Hat Enterprise Linux 7; then select the appropriate driver from the list.
4. Download the controller driver package (zip file archive).
5. When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (\windows 2019, \rhel7, and so on).

Note:

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

6.2 Installing with Windows

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

To install the controller SmartPQI driver while installing Windows:

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

6.3 Installing with Red Hat Linux or CentOS

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

RHEL7 Update 6 Installation and Above

To install the RHEL7 driver with a Linux system:

1. Install the Linux system using the inbox smartpqi driver.

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

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

RHEL7 Installation with Secure Boot

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

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

1. Install the Linux system using the inbox smartpqi driver in secure boot mode.
2. Enroll the Microchip public key for secure boot:
 - a. Import public key:

```
mokutil --import smart_driver_key_pub.der
```

- b. Reboot system.
- c. During boot, perform MOK key enrollment to accept the new key.

3. After the installation completes, install the signed driver rpm using the following command (where `###-###` is the build number):

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

4. Reboot.

6.4 Installing with SuSE Linux Enterprise Server

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

Installing with SLES 12 SP3 and Above

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

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

```
rpm -ivh smartpqi-ueficert-###-###.sles12sp5.x86_64.rpm
```

```
rpm -ivh smartpqi-kmp-default-###-###.sles12sp5.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.

6.5 Installing with Oracle Linux

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

Installing with Oracle Linux 7.6 and Above

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

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

```
Base Kernel: rpm -ivh kmod-smartpqi-#.#.#-###.ol7u9.x86_64.rpm
```

```
UEK Kernel: rpm -ivh kmod-smartpqi-uek-#.#.#-###.ol7u9.x86_64.rpm
```

6.6 Installing with Ubuntu Linux

To install the controller SmartPQI driver while installing Ubuntu Linux:

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

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

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

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

6.7 Installing with Debian Linux

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

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

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

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

6.8 Installing with FreeBSD

To install the controller SmartPQI driver while installing FreeBSD:

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

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

For example:

```
# gpart create -s GPT dal
# gpart add -t freebsd-ufs dal
# 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/dalpl /media
```

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

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

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

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

- iv. Add the following line:

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

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

```
# mountroot> ?
```

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

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


6.9 Installing with Solaris

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

6.9.1 Installing with Solaris Live Media

To install the SmartPQI controller driver with Solaris Live Media:

1. Copy the `smartpqi.pkg` or `iso` file and `adddriver.sh` file to a USB flash drive and insert that drive into the installation system.
2. Boot to the Solaris 11 live media DVD in the installation system. Select the Solaris version and press **Enter**.
3. Select the keyboard (default is 27) and language (default is 3).
4. Enter your login credentials.
The GUI will appear.
5. Open the terminal and switch to the root user by using the following command:

```
# su
```

Use "solaris" as the root password.

6. Adaptec controllers are shipped with the inbox aac driver, so it is necessary to remove the driver. Use the following command to remove the inbox aac driver:

```
# rem_drv aac
```

7. Open the "Device driver utility" from the desktop and enter the root password.
8. The DD utility scans and automatically highlights the controller or devices that are not claimed by the driver.
9. Click **Browse** to load the driver image from the USB flash drive.
10. Select `smartpqi.pkg` or `iso` file and click **"OK"**.
11. Click **Install**.
The **Installation Successful** message gets displayed.
12. The DD utility rescans the devices.
13. The available disks are viewable in the terminal by typing the `format` command. Press **Ctrl+L+C** to return to the command prompt.
14. Return to the desktop by typing `exit` at the `~#` prompt.
15. Double click the **Install Oracle Solaris** icon for OS installation and follow the steps to complete the OS installation.

Note: After the OS is installed, perform following procedure:

1. Open the terminal and copy the `adddriver.sh` file to `/tmp` directory.

```
# cp /media/USB_DRIVE/adddriver.sh /tmp/  
# cd /tmp
```

2. Execute the `adddriver.sh` script file with the parameter `live` as follows:

```
# chmod +x adddriver.sh
# ./adddriver.sh live
```

3. Reboot the system using the following command:

```
# reboot
```

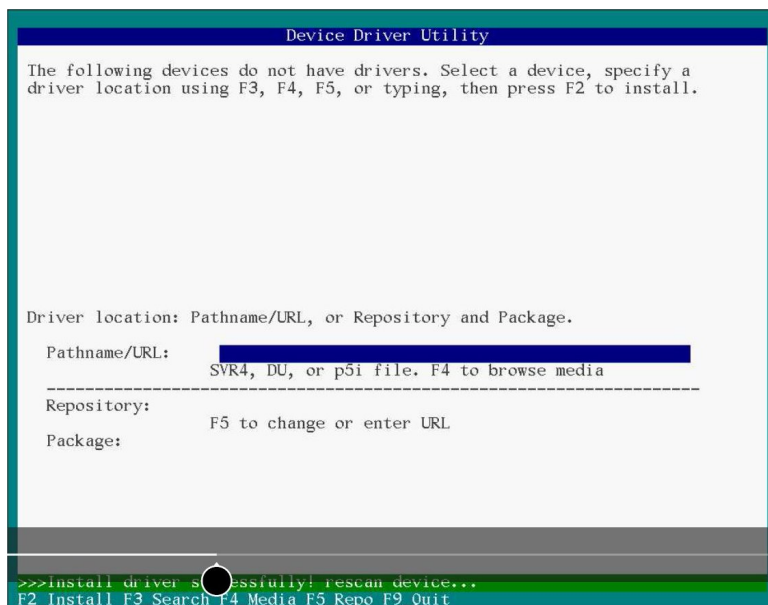
6.9.2 Installing with Solaris Text Installer

To install the SmartPQI driver with Solaris Text Installer:

1. Copy the `smartpqi.pkg` or `iso` file and `adddriver.sh` files to a USB flash drive and plug that drive into the installation system.
2. Boot to the Solaris 11.3 or 11.4 text installer DVD in the installation system, and select the keyboard and language.
3. After the DVD boots, select option 3 (**Shell**) from the list.
4. Remove the inbox `aac` driver and exit the shell using the following commands:

```
#rem_drv aac
#exit
```

5. Select option 2 (**Install Additional Drivers**) from the list. The **Device Driver Utility** screen appears.
6. Press the **F4** key (**Media**) to search for the driver image file on your flash drive.
7. Select **USB drive** and press **Enter**.
8. Find the location of the `smartpqi.pkg` or `iso` file on the flash drive, highlight it, and press the **F2** key to select it.
9. Press the **F2** key again to install the driver.
10. If the installation succeeds, the following screen will appear:



11. Press the **F9** key to exit to the **Options** menu.
12. Select option 3 (**Shell**) from the list.
13. Type the format command in the terminal window to list the available disks. Press **Ctrl+C** to return to the command prompt.
14. Type **exit** at the `~#` prompt to go back to the **Options** menu.
15. Enter option 1 to **Install Oracle Solaris**.
The **Welcome to Oracle Solaris** screen appears.
16. Press the **F2** key to continue.
17. Select the disk discovery method and press the **F2** key to continue.
18. Follow installation steps accordingly.
19. At the installation summary, press the **F2** key to install the Oracle package; or, press the **F3** key to go back to make changes.
20. After the OS has been installed, press **F9** to go back to the Options menu.
21. Select Option 3 (**Shell**).
22. Open the terminal and copy the `adddriver.sh` file to `/tmp` directory using the following commands:

```
# cp /media/USB_DRIVE/adddriver.sh /tmp/  
# cd /tmp
```

23. In the terminal, execute the `adddriver.sh` script file with the parameter text as follows:

```
# chmod +x adddriver.sh  
# ./adddriver.sh text
```

24. Reboot the system using the following command:

```
#reboot
```

6.10 Installing with Citrix XenServer

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 ESXi-Customizer tool. This tool automates the process of customizing the ESXi install-ISO and runs as a script under Microsoft PowerShell.

You can download the ESXi-Customizer tool, `ESXi-Customizer-PS-v2.5.ps1`, from <https://github.com/VFrontDe/ESXi-Customizer-PS> and other locations on the Web.

Note: Be sure to install the prerequisite software first, including Powershell and VMware POWERCLI, before you install ESXi-Customizer.

To install the SmartPQI controller driver while installing VMware:

1. Download and install Microsoft PowerShell and VMware POWERCLI, as needed. You can download PowerShell from the Microsoft Download Center at www.microsoft.com/download, and POWERCLI from my.vmware.com.

Note: PowerShell is pre-installed on many Windows systems, including Windows Server 2012/2016/2019.

2. Download the ESXi-Customizer tool from <https://github.com/VFrontDe/ESXi-Customizer-PS> or other Web location. Then, unpack the archive to a local directory on your Windows system; `C:\ESXi-Customizer`, for instance.
3. Copy the VMware driver vib for your OS version to a temp directory, such as `C:\temp\pkg`. The driver vib files (listed below, where xxxxxx is the driver version/build number) should be in the driver download directory on your Windows system.

Option	Description
ESXi 6.5	smartpqi-1.0.0-xxx-1OEM.650.0.0.xxxxxxx.x86_64.vib
ESXi 6.7	smartpqi-1.0.0-xxx-1OEM.670.0.0.xxxxxxx.x86_64.vib

4. Run ESXi-Customizer from the installation directory:

```
C:\ESXi-Customizer>ESXi-Customizer.cmd
```

5. In PowerShell, enter the following command:

```
.\ESXi-Customizer-PS-v2.5.ps1 -Vxx -pkgDir C:\temp\pkg
```

where Vxx is the VMware OS version: `v67` for VMware 6.7, `v65` for VMware 6.5.

PowerShell begins creating the custom ESXi install-ISO with embedded SmartPQI driver. It displays "All done" when the ISO is ready.

6. Burn the custom ISO image to a writable CD or USB drive.

Note: Use whatever tool you prefer to burn the CD or USB drive.

Remove the CD or USB drive after you finish burning the image.

7. On the VMware ESXi machine, insert the custom boot CD/USB, then restart your computer.
8. Follow the on-screen instructions to begin the VMware installation.

9. Complete the VMware installation, following the on-screen instructions.
10. 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 controller is installed in a computer or server and the OS is already installed.

Note:

- 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 [Installing the SmartPQI Drivers from Source](#) on page 64.

7.1 Download the Driver Package

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

1. Open a browser window, then type start.adaptec.com in the address bar.
2. Enter your product or adapter model number, then select SmartRAID 3100 or SmartHBA 2100.
3. Select your operating system version, for instance, Microsoft Windows Server 2019 or Red Hat Enterprise Linux 7; then select the appropriate driver from the list.
4. Download the controller driver package (zip file archive).
5. When the download completes, extract the package contents to a temporary location on your machine. Each driver is stored in a separate folder (\windows 2019, \rhel7, and so on).

Note:

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

7.2 Installing on Windows

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

To install the controller SmartPQI driver on Windows:

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

7.3 Installing on Red Hat or CentOS

To install the controller SmartPQI driver on Red Hat Linux or CentOS, 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):

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

2. Reboot the system.

7.4 Installing on SuSE Linux Enterprise Server

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

Installing on SLES 12 SP3 and Above

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

1. Install the latest smartpqi driver rpm by using the following command (where `###-###` is the build number):

```
rpm -ivh smartpqi-ueficert-###-###.sles12sp5.x86_64.rpm  
rpm -ivh smartpqi-kmp-default-###-###.sles12sp5.x86_64.rpm
```

2. Reboot the system.

7.5 Installing on Oracle Linux

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

Installing on Oracle Linux 7.6 and Above

To install the SmartPQI driver on an Oracle Linux system:

1. Install the latest smartpqi package using the following commands (where `###-###` is the build number):

```
Base Kernel: rpm -ivh kmod-smartpqi-###-###.ol7u9.x86_64.rpm
```

```
UEK Kernel: rpm -ivh kmod-smartpqi-uek-###-###.ol7u9.x86_64.rpm
```

```
UEK6ol7 Kernel: rpm -ivh kmod-smartpqi-uek6ol7-###-###.x86_64.rpm
```

```
UEK6ol8 Kernel: rpm -ivh kmod-smartpqi-uek6ol8-###-###.x86_64.rpm
```

7.6 Installing on Ubuntu Linux

Note:

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

To install the controller SmartPQI driver on Ubuntu:

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

```
sudo apt-get update
```

3. Load the Ubuntu unpacking tools:

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

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

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

7.7 Installing on Debian Linux

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

1. Login to the system as root, or sudo to root.
2. Install the supporting package for the SmartPQI DKMS deb package:

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

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

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

4. Reboot system.

7.8 Installing on FreeBSD

To install the controller SmartPQI driver on FreeBSD:

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

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

2. Install the SmartPQI package by using the following command:

```
# pkg add smartpqil0x-amd64.txz
```

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

```
# pkg upgrade smartpqil0x-amd64.txz
```

3. Restart the system.

```
# reboot
```

7.9 Installing on Solaris

To install the controller SmartPQI driver on Solaris, follow the steps in the sections below.

Installing the Driver on an Existing Operating System

1. Remove the inbox aac driver, since the Adaptec Smart Storage Controller is shipped with the inbox aac driver.

```
#rem_drv aac
```

2. Extract the SmartPQI driver package from a .zip or .tar file.
3. Perform the following instructions to load the driver package.
 - a. If "smartpqi.pkg" is present, execute the following command:

```
# pkgadd -d smartpqi.pkg
```

or,

- b. Ensure that the MCHPsmartpqi folder is present in the current directory. The dot (.) in following the command will read this folder as a driver package:

```
# pkgadd -d .
```

In the terminal, the following messages will appear:

```
The following packages are available:
 1 MCHPsmartpqi      MICROCHIP Smart PQI RAID Controller driver
                        (i386) 1.0.0-100,REV=2016.06.06.22.10

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Enter "1" or "all".

The following prompt will appear:

```
Do you want to continue with the installation of <MCHPsmartpqi> [y,n,?]
```

Enter "y".

The following message appears after a successful installation:

```
Installation of <MCHPsmartpqi> was successful.
```

4. Reboot the system using the following command:

```
# reboot
```

5. Use the following command to confirm whether the driver is loaded or not:

```
# modinfo -c | grep smartpqi
```

6. Use the following command to identify the driver package information:

```
# pkginfo -l MCHPsmartpqi
```

Removing the Driver Package

1. Remove the loaded driver package using the following command:

```
# pkgrm MCHPsmartpqi
```

In the terminal, the following messages will appear:

```
The following package is currently installed:
MCHPsmartpqi    MICROCHIP Smart PQI RAID Controller driver
(i386) 1.0.0-100,REV=2016.06.06.22.10
```

The following prompt will appear:

```
Do you want to remove this package? [y,n,?,q]
```

Enter "y". Once the selection is made, the following prompt will appear:

```
Do you want to continue with the removal of this package [y,n,?,q]
```

Enter "y". The following message will appear to signify the successful removal of the driver package:

```
Removal of <MCHPsmartpqi> was successful
```

2. Reboot the system using the following command:

```
# reboot
```

7.10 Installing on Citrix XenServer

Note: To copy the driver RPM file to XenServer (in Step [\[1 \]](#) below), 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 #):

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-###.xen7.6.rpm root@<xen-server-ip>:/tmp/smartpqi
```

2. Install the driver module rpm:

```
rpm -ivh /tmp/smartpqi/citrix-smartpqi-###.xen7.6.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 `xxxxxxx` is the version/build number):

```
# scp smartpqi-67.xxxx.0.xxx-10EM.670.0.0xxxxxxx.x86_64.vib root@<esxi_server_address>:/tmp
```

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

```
# esxcli software vib install -v file:/tmp/ smartpqi-67.xxxx.0.xxx-10EM.670.0.0xxxxxxx.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 Solving Problems

This section provides basic troubleshooting information and solutions for solving problems with your SmartRAID 3100 Series or SmartHBA 2100 Series Host Bus Adapter.

8.1 Troubleshooting Checklist

If you encounter difficulties installing or using your SmartRAID 3100 Series or SmartHBA 2100 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 [About Your SmartRAID 3100 Series Host Bus Adapter](#).
- Ensure that your adapter is firmly seated and secured in the PCIe expansion slot.
- If your adapter is not detected during system boot, try installing it in a different compatible expansion slot. (See [Installing the Host Bus Adapter](#) for instructions.)
- Did the driver install correctly? It may need to be reloaded after a reboot or kernel update; see [Installing the Driver and an Operating System](#) on page 28.
- If you have external disk drives (or other devices), are they powered on?
- Check the Release Notes for compatibility issues and known problems.

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

8.2 Resetting the Adapter

You may need to reset your SmartHBA 2100/SmartRAID 3100 controller if it becomes inoperable or if a firmware upgrade is unsuccessful. SmartHBA 2100/SmartRAID 3100 controllers support a reset protocol called HDA mode flash. For information about HDA mode, contact your support representative. To locate the HDA mode jumper on your adapter, see the board illustrations in [About Your SmartRAID 3100 Series Host Bus Adapter](#).

A Using the Microchip SAS/SATA Configuration Utility

The Microchip SAS/SATA Configuration Utility (MSCU) is a BIOS-based utility that you can use to manage your SmartHBA 2100/SmartRAID 3100 controller 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.

A.1 Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?

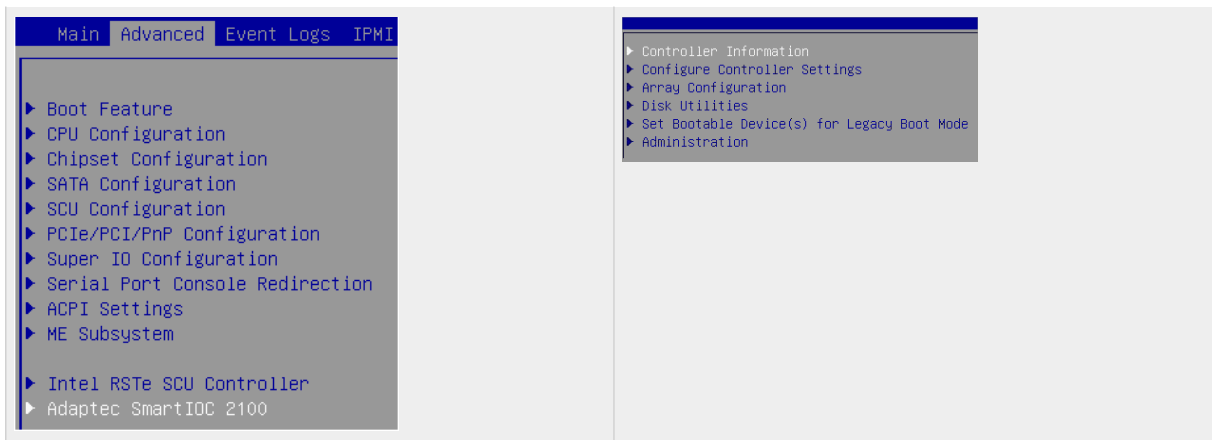
Your Adaptec SmartHBA 2100/SmartRAID 3100 controller supports two interfaces to the BIOS-level controller configuration options described in this section: Ctrl-A and UEFI/HII.

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), rather than Microchip's legacy Ctrl-A interface. UEFI/HII provides an architecture-independent mechanism for initializing add-in cards, like the SmartHBA 2100/SmartRAID 3100 controller, and rendering contents to the screen in a uniform way.

To access the SmartHBA 2100/SmartRAID 3100 controller configuration options with the Ctrl-A interface, start or restart your computer. When prompted, press `Ctrl+A`, then select your controller from the list. The Ctrl-A main menu is displayed.



In the UEFI/HII interface, the server's standard BIOS provides access to the SmartHBA 2100/SmartRAID 3100 controller configuration options. How you access the BIOS varies, depending on the server manufacturer, but typically it's started by simply pressing `DEL`. Once you enter setup, navigate to the "Advanced" menu (below, left), then select your controller from the list. The UEFI/HII main menu is displayed (below, right).



From that point on, the UEFI/HII menus and the Ctrl-A menus for configuring your controller are similar. For example, the Array Configuration menu contains the same options in both Ctrl-A and UEFI for creating and managing arrays (though the task flow differs); the Disk Utilities menu contains the same options for managing disk drives; and so on.

Note: The Administration menu is available only with the UEFI/HII interface.

In both interfaces, all the tools are menu-based and instructions for completing tasks appear on-screen. Menus can be navigated using the arrows, Enter, Esc, and other keys on your keyboard.

This appendix provides instructions for navigating and completing tasks with the UEFI/HII interface. To complete tasks with the Ctrl-A interface:

- Refer to the on-screen instructions for keyboard navigation and selection options.
- Refer to the option descriptions in this section for details about individual configuration settings.

A.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 controller information, start the Microchip SAS/SATA Configuration Utility and select **Controller Information** from the main menu.

A.3 Creating an Array

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

To create an array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press **Enter**.
3. From the main menu, select **Array Configuration**, then select **Create Array**.
4. Select each drive you want to include in the array: use the arrow keys to select a drive, press **Enter**, then **Proceed**.

Note: Be sure not to mix drive types! Select SATA drives or SAS drives only.

5. Select **Proceed to next Form**, then press **Enter**.
6. (For controllers with maxCrypto Controller-Based Encryption only) Select encryption options for the array: encrypted volume or plaintext volume (not encrypted).

Note: You will be prompted for your account credentials (Admin or User) if you are not logged into the Encryption Manager; see [Encryption Manager Full Setup](#) on page 54.

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**.

A.4 Creating a maxCache Array

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

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

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

To create a maxCache array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Create maxCache Array**.
4. Select each drive you want to include in the array: use the arrow keys to select a drive, press `Enter`, then select **Proceed to next Form**.
5. Select the RAID level, then select **Proceed to next Form**.
6. 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).
7. Select **Submit Changes**.
8. Select the data logical drive associated with the maxCache device (16 GB minimum).

A.5 Managing Arrays and Logical Drives

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

A.5.1 Viewing Logical Drive Properties

To view logical drive properties:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Use the arrow keys to select an array, press `Enter`, then select **List Logical Drives**.
5. Use the arrow keys to select a logical drive, press `Enter`, then select **Logical Drive Details**.

A.5.2 Creating Logical Drives

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

To create a logical drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Create Logical Drive**.
4. Select each drive you want 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.

5. Select **Proceed to next Form**, then press `Enter`.
6. Select the RAID level, then select **Proceed to next Form**.
7. 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).
8. Select **Submit Changes**.

A.5.3 Enabling IO Bypass

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

To adjust the IO Bypass settings:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Use the arrow keys to select an array, press `Enter`, then select **IO Bypass Settings**.
5. From the pop-up menu, select **Enabled** or **Disabled**, then press `Enter`.
6. Select **Submit Changes**.

A.5.4 Editing Logical Drive Properties

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

To edit logical drive properties:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Use the arrow keys to select an array, press `Enter`, then select **List Logical Drives**.
5. Use the arrow keys to select a logical drive, press `Enter`, then select **Edit Logical Drive**.
6. 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)
7. Select **Logical Drive Label**, then type the new label.
8. Select **Submit Changes**.

A.5.5 Deleting a Logical Drive

Note: Use this procedure to delete an individual logical drive. To delete all logical drives on an array, see [Deleting an Array](#) on page 50.

To delete a logical drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).

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

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

A.5.6 Assigning Spares

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

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

To assign a spare to an array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Use the arrow keys to select an array, press `Enter`, then select **Manage Spare Drives**.
5. 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
6. Use the arrow keys to select the drive to assign as a spare.

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

A.5.7 Deleting a Spare Drive

To delete a spare drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Array LD**.
4. Use the arrow keys to select an array, then press `Enter`.
5. Select **Manage Spare**, then select **Delete**.
6. If the array has more than one assigned spare, use the arrow keys to select a spare from the list, then press `Enter`.

A.5.8 Identifying the Drives in an Array

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

To identify the physical drives in an array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Use the arrow keys to select an array, then press `Enter`.
5. Select **Identify Device**.
6. Enter a value into **Identification Duration (seconds)**. This value determines how long the LED on the device will remain on.
7. 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)
8. Select **Start**, then press `Enter`.
9. To turn off the Identification LED(s), press `Esc` to return to the previous menu, then select **Stop**.

A.5.9 Deleting an Array

Note: Use this procedure to delete all logical drives on an array, and the array itself. To delete an individual logical drive, see [Deleting a Logical Drive](#) on page 48.

To delete an array:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Array LD**.
4. Use the arrow keys to select an array, press `Enter`, then select **Delete Array**.

A.6 Modifying SmartHBA 2100/SmartRAID 3100 controller Settings

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

Option	Description
Modify Controller Settings	
Transformation Priority	Sets the priority for array expansion: <ul style="list-style-type: none">• Low: normal system operations take priority over array expansion• Medium: normal system operations and array expansion get equal priority• High: expansion takes precedence over all other system operations
Rebuild Priority	Sets the priority for rebuilding a failed logical drive: <ul style="list-style-type: none">• Low: normal system operations take priority over rebuilds• Medium: normal system operations and rebuilds get equal priority• Medium High: rebuilds get higher priority than normal system operations• High: rebuilds take precedence over all other system operations

Using the Microchip SAS/SATA Configuration Utility

Option	Description
Surface Scan Analysis Priority	Determines the time, in seconds, that a controller must be inactive before a surface scan analysis is started on the physical drives connected to it. The scanning process checks physical drives for bad sectors and, in fault-tolerant logical drives, such as RAID 5, it also verifies the consistency of parity data. Delay value ranges from 1-30 seconds. Set the value to "0" to disable the feature. Set the value at "31" to maintain high priority.
Current Parallel Surface Scan Count	Sets the surface scan count for the controller. Set the value to "1" to disable the feature. Caution: Disabling Surface Scan Analysis is not recommended as it will prevent the controller from proactively finding and correcting disk surface errors, which may lead to data loss.
Physical Drive Write Cache State	Enables and disables physical drive write cache for all drives on the controller. Valid values are: <ul style="list-style-type: none"> Configured Unconfigured HBA
Spare Activation Mode	Sets the spare activation mode to activate on failure or predictive failure activation.
Connector Mode (CN0:CN3)	Configures the controller connectors to different operating modes: <ul style="list-style-type: none"> HBA: exposes physical drives to the operating system RAID: exposes only RAID volumes to the operating system Mixed: exposes RAID volumes and physical drives to the operating system
Modify Cache Settings	
No Battery Write Cache	Allows write caching to be enabled when a battery/supercapacitor is not present or fully charged. This setting affects all logical drives on the controller. Caution: Enabling write caching on a cache module without a fully charged battery/supercapacitor may cause data loss in the event of a power failure.
Cache Ratio (Read)	Sets the ratio of controller cache memory used for read-ahead cache versus write cache. Cache ratio values range from 0-100, in increments of 5.
Advanced Controller Settings (RAID mode or Mixed mode only):	
Degraded Mode Performance Optimization	For degraded RAID 5 logical drives, enabling this setting directs the controller to attempt to improve performance of large read requests by buffering physical drive requests. Disabling this setting forces the controller to read from the same drives multiple times.
Physical Drive Request Elevator Sort	Sets the behavior of the drive's write Elevator sort algorithm, a scheduling optimization that prioritizes I/O requests such that disk arm and head motion continues in the same direction. Enabling the elevator sort improves seek times and disabling the elevator sort improves throughput.
Alternate Inconsistent Repair Policy	Sets the surface analysis inconsistency repair policy for RAID 5 when the controller detects that the parity information does not match the data on the drives. Disabling the repair policy directs the controller to update the parity information, leaving the data untouched. Enabling the repair policy directs the controller to update the data on the drives based on the parity information.
Max Drive Request Queue Depth	Sets the queue depth for the controller. Valid values are Automatic, 2, 4, 8, 16, and 32.
Monitor and Performance Analysis Delay	Sets the Monitor and Performance Analysis delay for the controller, in minutes. Set the value to zero to disable Monitor and Performance Analysis. Default is 60 minutes.

Option	Description
HDD Flexible Latency Optimization	<p>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:</p> <ul style="list-style-type: none">• Disable (default).• Low• Middle(100ms)• High• Very High(30ms)• Very High(10ms)

A.7 Clearing the Controller Configuration

Clearing the controller configuration destroys the controller meta-data, including array configurations, partition information, and so on.

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

To clear the controller configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Clear Configuration**.
4. Select **Delete All Array Configurations** or **Delete Configuration Metadata on All Physical Drives**.
5. Select **Submit Changes**.

A.8 Backup Power Source

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

A.9 Managing Power Settings

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

- **Maximum Performance** (default): All settings are selected based on maximum performance. Power savings options that affect performance are disabled.
- **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 (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press **Enter**.
3. From the main menu, select **Controller Configuration**.
4. Select **Manage Power Settings**, then select **Power Mode**.
5. Press **Tab** to select the power mode.
6. Select **Survival Mode**, then press **Tab** to select Enabled or Disabled.
7. Select **Submit Changes**.

A.10 Out of Band Messaging Settings

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

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

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

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press **Enter**.
3. From the main menu, select **Configure Controller Settings**.
4. Select **Out of Band Messaging Settings**.
5. Select **OOB Interface** and press **Enter**.
6. From the pop-up menu, select **PBSI**, **MCTP**, or **Disable OOB interface**.
7. To configure Out of Band Messaging for PBSI, set these parameters:

PBSI Parameters	Description
SMBus Slave Address	Sets the SMBus (System Management Bus) slave address of the controller to a valid hexadecimal address value.
SMBus Clock Speed	Sets the SMBus clock speed: <ul style="list-style-type: none">• Feature Disabled (Default)• SMBus clock speed 100 kHz• SMBus clock speed 400 kHz
SMBus Clock Stretching	Sets the SMBus Clock Stretching mode: <ul style="list-style-type: none">• Enable: Enables SMBus clock stretching• Disable: Disables SMBus clock stretching

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

MCTP Parameters	Description
SMBus Slave Address	Sets the SMBus (System Management Bus) slave address of the controller to a valid hexadecimal address value. (For valid range, refer to the Management Component Transport Protocol (MCTP) SMBus/I2C Transport Binding Specification document.)
SMBus Device Type	Sets the SMBus Device Type: <ul style="list-style-type: none">• Default• Fixed• ARP (Address Resolution Protocol)
SMBus Physical Channel	Sets the SMBus Channel mode: <ul style="list-style-type: none">• Enable: Enables SMBus channel• Disable: Disables SMBus channel
Use Static EIDs during Initialization	Sets the Static End Point Identifier (EID) mode: <ul style="list-style-type: none">• Enable: Enables Static EID• Disable: Disables Static EID
VDM Discovery Notify	Sets the Vendor Defined Message (VDM) discovery notification mode: <ul style="list-style-type: none">• Enable: Enables VDM discovery notification• Disable: Disables VDM discovery notification

9. Select **Submit Changes**.

A.11 Using the Encryption Manager

Note:

1. This option is available only in the UEFI/HII interface; UEFI version 2.4A or higher, recommended.
2. This option is available only for controllers that support maxCrypto Controller-Based Encryption. See [About Your SmartRAID 3100 Series Host Bus Adapter](#) on page 4 for more information.

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

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

Once you configure the Encryption Manager, you can encrypt arrays and logical drives, and create storage spaces with mixed encrypted and plaintext volumes. For more information about creating and managing encrypted volumes, see [Creating an Array](#) on page 46.

A.11.1 Encryption Manager Full Setup

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

To configure the Encryption Manager:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press **Enter**.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **Full setup**.

5. Using the arrow keys and Enter key, configure basic encryption settings:

a. In the Encryption Mode field, select one of these options:

- **Enable and Allow future...** to enable encryption and allow plaintext logical devices to be created in addition to encrypted logical devices.
- **Enable and Disallow future...** to enable encryption and allow only encrypted logical devices to be created.
- **Disable** to disable the Encryption Manager. If encryption is disabled, all encrypted logical drives are set to offline and the data becomes inaccessible; newly created logical drives will not be encrypted. (They will be created as plaintext logical drives.)

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

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

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

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

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

6. Select **Proceed to Next Form**.

The Terms of Use form opens.

7. Select **Accept** to accept the Terms and Conditions.

8. Select **Submit Changes**.

A.11.2 Modifying the Encryption Manager Configuration

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

Note: This option is available only after you complete the Encryption Manager Full setup; see [Encryption Manager Full Setup](#) on page 54.

To modify the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **Crypto Officer Settings**.
5. Using the arrow keys and Enter key, modify basic encryption settings, as needed (encryption enable/disable, master encryption key, allow/disallow future plaintext volumes).
6. In the Firmware Update field, select **Unlock** to allow controller firmware upgrades. Select **Lock** to block (prevent) firmware upgrades.
7. Using the arrow keys and Enter key, configure the Crypto Officer and User account settings:
 - a. Change the Crypto Officer password, as needed: press `Enter`, type the password in the pop-up window, then press `Enter` to submit.

- b. Enter the Password Recovery Question for a forgotten password: press `Enter`, type the recovery question in the pop-up window, then press `Enter` to submit.
The recovery question is 16-255 characters, comprising all printable ASCII characters.
 - c. In the Password Recovery Answer field, enter the answer to the recovery question.
The recovery answer is 16-64 characters and is case sensitive, comprising all printable ASCII characters.
Note: Password recovery is available only for the Crypto Officer account.
 - d. In the User Password field, enter the User account password: press `Enter`, type the password in the pop-up window, then press `Enter` to submit.
8. Select **Proceed to Next Form**.
The Terms of Use form opens.
 9. Select **Accept** to accept the Terms and Conditions.
 10. Select **Submit Changes**.

A.11.3 Modifying User Account Settings

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

Note: This option is available only after you complete the Encryption Manager Full setup; see [Encryption Manager Full Setup](#) on page 54.

To modify the User Account Settings:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **User Settings**.
5. Modify the User account password, as needed: press `Enter`; when the pop-up window opens, type the password, then press `Enter` to submit.
The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (`#,!,@,...`).
6. 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.
7. Select **Proceed to Next Form**.
8. Select **Submit Changes**.

A.11.4 Resetting a Forgotten Password

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

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

To reset a forgotten password:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.

3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Manage Encryption Settings**, then select **Forgot Crypto Officer Password**.
5. Enter the answer to the password recovery question; see [Modifying the Encryption Manager Configuration](#) on page 55.
6. Enter the Crypto Officer's new password: press `Enter`; when the pop-up window opens, type the password, then press `Enter` to submit.
7. Select **Submit Changes**.

A.11.5 Clearing the Encryption Manager Configuration

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

Note: Clearing the configuration does not affect the encrypted logical drives in your storage space. However, to continue accessing or managing encrypted volumes, you must reconfigure the basic encryption settings in the Encryption Manager; see [Encryption Manager Full Setup](#) on page 54.

To clear the Encryption Manager configuration:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Clear Configuration**.
5. If your storage space includes encrypted volumes, enter the Encryption Master Key. The Master Key is a 10-32 character string, comprising all printable ASCII characters.
6. Select **Submit Changes**.

A.11.6 Re-Keying a Logical Drive

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

To re-key a logical drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Select an array, then select **List Logical Drives**.
5. Select an encrypted logical drive, then select **Volume key rekey**.
Note: Use Logical Drive Details to check encryption status.
6. Enter your Encryption Manager password: press `Enter`; type your password in the pop-up window, then press `Enter` to submit.
7. Select your account type: Crypto Officer or User.
8. Select **Submit Changes**.

A.11.7 Converting Plaintext Data to Encrypted Data

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

To convert plaintext data:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Select an array, then select **List Logical Drives**.
5. Select a plaintext logical drive, then select **Convert Plaintext Data to Encrypted Data**.
Note: Use Logical Drive Details to check encryption status.
6. Enter your Encryption Manager password: press `Enter`; type your password in the pop-up window, then press `Enter` to submit.
7. Select your account type: Crypto Officer or User.
8. In the Convert Plaintext Data to Encrypted Data field, select discard existing data or preserve existing data during conversion.
9. Select **Submit Changes**.

A.11.8 Erasing an Encrypted Logical Drive

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

To erase an encrypted logical drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Array Configuration**, then select **Manage Arrays**.
4. Select an array, then select **List Logical Drives**.
5. Select an encrypted logical drive, then select **Secure erase**.
Note: Use Logical Drive Details to check encryption status.
6. Enter your Encryption Manager password: press `Enter`; type your password in the pop-up window, then press `Enter` to submit.
7. Select your account type: Crypto Officer or User.
8. Select **Submit Changes**.

A.11.9 Importing a Foreign Master Key

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

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

To import a foreign master key:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Configure Controller Settings**, then select **Encryption Manager**.
4. Select **Import Foreign Local Key**.
5. Enter the master key used to encrypt the logical drive.
The Master Key is a 10-32 character string, comprising all printable ASCII characters.
6. Enter the Crypto Officer password: press `Enter`; when the pop-up window opens, type the password, then press `Enter` to submit.
7. Select **Submit Changes**.

A.12 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 [Modifying SmartHBA 2100/SmartRAID 3100 controller Settings](#) on page 50.) 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

Note:

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 (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
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**.

A.13 Device Information

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

A.14 Identifying a Disk Drive

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

To identify a disk drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Disk Utilities**.
4. Select the disk drive you want to locate, then press `Enter`.
5. Select **Identify Device**, then enter a value into **Identification Duration (seconds)**. This value determines how long the LED on the device will remain on.
6. Select **Start**, then press `Enter`.
7. To turn off the Identification LED, press `Esc` to return to the previous menu, select **Stop** and press `Enter`.

A.15 Erasing a Disk Drive

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

To erase a disk drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Disk Utilities**.
4. Select the disk drive you want to erase, then press `Enter`.
5. Select **Erase Disk**, then select **Continue**.

A.16 Updating Drive Firmware

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

To update drive firmware:

1. Copy the firmware binary file to a USB flash drive, then connect the USB drive to the machine. Alternatively, copy the firmware binary to a known location on your machine.
2. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
3. Select your controller, then press `Enter`.
4. From the main menu, select **Disk Utilities**, then select **Update Drive Firmware**.
5. 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
6. 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.
7. Select **Proceed**.

8. 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.
9. When the update is complete, reboot the server.

A.17 Clearing Configuration Meta-data

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

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

To clear the configuration meta-data from a drive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Disk Utilities**.
4. Select a disk drive with configuration meta-data, then press `Enter`.
5. Select **Clear Configuration Metadata**, then select **Continue**.

A.18 Setting the Bootable Device(s) for Legacy Boot Mode

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

This option sets the primary and secondary logical or physical boot device(s) for Legacy Boot Mode. The secondary boot device acts as a failover to the primary boot device. By default, the SmartHBA 2100/SmartRAID 3100 controller boots from the first logical drive.

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

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Set Bootable Device(s) for Legacy Boot Mode**, then select **Select Bootable Logical Drive**.
4. To set the default bootable device, select a logical drive from the list, then select **Set as Primary Bootable Device**.
5. To set the secondary bootable device, select a logical drive from the list, then select **Set as Secondary Bootable Device**.

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

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the menu, select **Set Bootable Device(s) for Legacy Boot Mode**, then select **Select Bootable Physical Drive**.
4. To set the default bootable device, select a physical drive from the list, then select **Set as Primary Bootable Device**.

5. 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)**.

A.19 Updating the SmartHBA 2100/SmartRAID 3100 controller Firmware

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

To update the SmartHBA 2100/SmartRAID 3100 controller firmware:

1. Copy the firmware binary file (.bin) to a USB flash drive, then connect the USB drive to the machine. Alternatively, copy the firmware binary to a known location on your machine.
2. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
3. Select your controller, then press **Enter**.
4. From the main menu, select **Administration**, then select **Flash Controller Firmware**.
5. Select **Continue with flashing Firmware**.
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 controller.
7. When the update is complete, reboot the server.

A.20 Creating a Support Archive

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

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

To create a support archive:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press **Enter**.
3. From the main menu, select **Administration**, then select **Save Support Archive**.
4. 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.
5. Press any key to complete the operation and exit.

A.21 Resetting the Controller to Factory Defaults

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

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

Use this option to reset the SmartHBA 2100/SmartRAID 3100 controller to factory default settings.

To reset the controller:

1. Start the Microchip SAS/SATA Configuration Utility in UEFI mode (see [Running the Microchip SAS/SATA Configuration Utility: Ctrl-A or UEFI/HII?](#) on page 45).
2. Select your controller, then press `Enter`.
3. From the main menu, select **Administration**.
4. Select **Reset controller settings to factory defaults**.
5. Select **Submit Changes**.

B Installing the SmartPQI Drivers from Source

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

B.1 Installation Instructions for Supported Linux OS's

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

- RHEL-based OS images (including CentOS)
- Ubuntu 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 [Using the Installation DVD as the Repository](#) on page 66.

RHEL-Based OS Images

The instructions below apply to the following RHEL-based OS images:

- Red Hat® Enterprise Linux/CentOS 7.4, 7.3, 7.2, 7.1, 7.0 (64-bit only)
- Red Hat® Enterprise Linux/CentOS 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. Rebuild initramfs with the newly installed smartpqi driver by using the following command:

```
# dracut -v -f --add-drivers smartpqi
```

9. Reboot the system to load the new initramfs, which will contain the newly installed smartpqi.ko driver.

Ubuntu OS Images

The instructions below apply to the following Ubuntu OS images:

- Ubuntu Linux 16.04.x (64-bit only)
- Ubuntu Linux 14.04.5, 14.04.4 (64-bit only)

To install the SmartPQI driver from source for Ubuntu 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:

```
# apt-get install build-essential linux-headers-`uname -r`
```

3. Extract the driver source code from the source tar 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:

```
# update-initramfs -k `uname -r` -c -v
```

Note: Ubuntu provides update-initramfs 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.

B.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
```

C SmartRAID/SmartHBA Physical and Logical Device Support

Table C-6 • SmartRAID/SmartHBA Physical and Logical Device Support

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

D 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.

D.1 Electrostatic Discharge (ESD)

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

To prevent ESD damage:

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

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

E Technical Specifications

E.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.

E.2 DC Power Requirements

Bus Type	Description	Requirements
PCIe	DC Voltage	3.3 V \pm 9%, 12 V \pm 8%, 3.3 V \pm 9% (auxiliary power from PCIe slot)

E.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

Adapter Model	Typical Power	Typical Current
		(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
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)

F The Microchip Web Site

Microchip provides online support via our web site at <http://www.microchip.com/>. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user guides and hardware support documents, latest software releases, and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, and Microchip consultant 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

F.1 Customer Change Notification Service

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

To register, access the Microchip web site at <http://www.microchip.com/>. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

F.2 Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: <http://www.microchip.com/support>

F.3 Microchip Devices Code Protection Feature

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

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be

a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

F.4 Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. 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.

F.5 Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Helder, JukeBlox, KeeLoq, Klear, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire 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, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KlearNet, KlearNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQL, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, 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.

Silicon Storage Technology is a registered trademark 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.

© 2021, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

F.6 Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and

analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

F.7 Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com	Australia - Sydney Tel: 61-2-9868-6733 China - Beijing Tel: 86-10-8569-7000 China - Chengdu Tel: 86-28-8665-5511 China - Chongqing Tel: 86-23-8980-9588 China - Dongguan Tel: 86-769-8702-9880 China - Guangzhou Tel: 86-20-8755-8029 China - Hangzhou Tel: 86-571-8792-8115 China - Hong Kong SAR Tel: 852-2943-5100 China - Nanjing Tel: 86-25-8473-2460 China - Qingdao Tel: 86-532-8502-7355 China - Shanghai Tel: 86-21-3326-8000 China - Shenyang Tel: 86-24-2334-2829 China - Shenzhen Tel: 86-755-8864-2200 China - Suzhou Tel: 86-186-6233-1526 China - Wuhan Tel: 86-27-5980-5300 China - Xian Tel: 86-29-8833-7252 China - Xiamen Tel: 86-592-2388138 China - Zhuhai Tel: 86-756-3210040	India - Bangalore Tel: 91-80-3090-4444 India - New Delhi Tel: 91-11-4160-8631 India - Pune Tel: 91-20-4121-0141 Japan - Osaka Tel: 81-6-6152-7160 Japan - Tokyo Tel: 81-3-6880-3770 Korea - Daegu Tel: 82-53-744-4301 Korea - Seoul Tel: 82-2-554-7200 Malaysia - Kuala Lumpur Tel: 60-3-7651-7906 Malaysia - Penang Tel: 60-4-227-8870 Philippines - Manila Tel: 63-2-634-9065 Singapore Tel: 65-6334-8870 Taiwan - Hsin Chu Tel: 886-3-577-8366 Taiwan - Kaohsiung Tel: 886-7-213-7830 Taiwan - Taipei Tel: 886-2-2508-8600 Thailand - Bangkok Tel: 66-2-694-1351 Vietnam - Ho Chi Minh Tel: 84-28-5448-2100	Austria - Wels Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 Denmark - Copenhagen Tel: 45-4450-2828 Fax: 45-4485-2829 Finland - Espoo Tel: 358-9-4520-820 France - Paris Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 Germany - Garching Tel: 49-8931-9700 Germany - Haan Tel: 49-2129-3766400 Germany - Heilbronn Tel: 49-7131-67-3636 Germany - Karlsruhe Tel: 49-721-625370 Germany - Munich Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 Germany - Rosenheim Tel: 49-8031-354-560 Israel - Ra'anana Tel: 972-9-744-7705 Italy - Milan Tel: 39-0331-742611 Fax: 39-0331-466781 Italy - Padova Tel: 39-049-7625286 Netherlands - Drunen Tel: 31-416-690399 Fax: 31-416-690340 Norway - Trondheim Tel: 47-72884388 Poland - Warsaw Tel: 48-22-3325737 Romania - Bucharest Tel: 40-21-407-87-50 Spain - Madrid

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Fax: 949-462-9608 Tel: 951-273-7800 Raleigh, NC Tel: 919-844-7510 New York, NY Tel: 631-435-6000 San Jose, CA Tel: 408-735-9110 Tel: 408-436-4270 Canada - Toronto Tel: 905-695-1980 Fax: 905-695-2078			Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 Sweden - Gothenberg Tel: 46-31-704-60-40 Sweden - Stockholm Tel: 46-8-5090-4654 UK - Wokingham Tel: 44-118-921-5800 Fax: 44-118-921-5820

Index

A

adapters [4](#), [17](#), [44](#), [70](#)
flashing [44](#)
resetting [44](#)
specifications [70](#)
standard features [4](#), [17](#)
troubleshooting [44](#)
 See also controllers

B

boards , See controllers

C

cards , See controllers
contents of controller kit [3](#)
controllers [24](#)
SAS cables [24](#)

D

descriptions
disk drives [4](#), [17](#), [24](#)
solid state [4](#), [17](#), [24](#)
drive requirements [24](#)
driver and operating system installation [28](#)
driver installation
drivers [35](#)
installing with XenServer [35](#)

E

electrostatic discharge [69](#)

F

flashing adapters [44](#)

H

hard disk [1](#)
 hard disk drive [1](#)
 hard drive, See disk drive
HBA [4](#), [17](#), [50](#)
figures
modifying settings [50](#)
HDA mode [44](#)
HDA mode jumper [44](#)
HII interface [45](#)
Human Interaction Infrastructure Interface (HII) [45](#)

I

installation [28](#), [35](#), [38](#)
driver
driver and operating system [28](#)
driver and XenServer [35](#)

K

kit contents [3](#)

L

low-profile bracket [3](#)

M

mechanical information [4](#), [17](#)

O

operating systems [3](#)

R

requirements [3](#), [24](#)
drive [24](#)
resetting adapters [44](#)

S

safety information [69](#)
SAS [24](#)
cables [24](#)
Solid State Drive (SSD) [4](#), [17](#), [24](#)
specifications [70](#)
system requirements [3](#)

T

technical specifications [70](#)
terminology [1](#)
troubleshooting tips [44](#)

U

UEFI [45](#)
Unified Extensible Firmware Interface (UEFI) [45](#)

X

XenServer [35](#)
OS installation [35](#)