

vantage[™]

12T1

Turin BIOS User Guide

Version 1.1

Vantageo Enterprise Platform Solutions

CONTENTS

1	GENERAL OVERVIEW.....	5
2	BIOS FEATURES OVERVIEW.....	6
2.1	BIOS DESCRIPTION	6
2.2	PROCESSOR.....	6
2.3	MEMORY.....	7
2.3.1	Bad DIMM Location	7
2.4	STORAGE	8
2.5	NETWORKING	8
2.6	POWER MANAGEMENT	8
2.7	SECURITY.....	9
2.7.1	Strong BIOS Password	9
2.7.2	Trusted Computing (TPM)	10
2.7.3	RoT (Optional)	10
2.7.3.1	PFR T-1	11
2.7.3.2	Anti-Rollback	11
2.7.3.3	Seamless Update.....	12
2.8	SMBIOS	12
2.9	BMC	13
2.10	MISC.....	14
2.10.1	BIOS Recovery Mode	14
2.10.2	Hot Key	14
2.10.3	Fixed Boot Order.....	14
2.10.4	Clear CMOS.....	15
2.10.5	Endless Boot	15
2.10.6	Chassis Intrusion.....	15
2.10.7	HW Monitor (Optional)	16
2.11	POST INFORMATION	20
2.11.1	Early Console POST Information.....	20
2.11.2	Quiet Boot	21
2.11.3	POST Information	21
3	SYSTEM EVENT LOG	22
3.1	MEMORY.....	22
3.2	PROCESSOR.....	23
3.3	PCIE	25
3.4	SEL FOR AMD RAS.....	26
3.4.1	NBIO	26
3.4.2	SMN.....	26
3.4.3	CXL.....	27
3.4.4	PMIC.....	27
4	SMBIOS	28
4.1	TYPE 0	28
4.2	TYPE 1	28
4.2.1	SMBIOS UUID to BMC GUID Format	28
4.3	TYPE 2	29
4.4	TYPE 3	29
5	UTILITY	30
5.1	FLASH BIOS UTILITieS.....	30
5.2	AMISCE.....	30
5.3	DMIEDIT (OPTIONAL)	30
6	BIOS SETUP.....	32

6.1	MAIN MENU	32
6.2	ADVANCED MENU	34
6.2.1	<i>Trusted Computing</i>	36
6.2.2	<i>PSP Firmware Versions</i>	37
6.2.3	<i>Redfish Host Interface Settings</i>	38
6.2.4	AMD CBS	39
6.2.4.1	CPU Common Options	40
6.2.4.1.1	Performance	44
6.2.4.1.1.1	Custom Core Pstates	45
6.2.4.1.1.2	CCD/Core/Thread Enablement	48
6.2.4.1.2	Prefetched settings	49
6.2.4.1.3	Core Watchdog	50
6.2.4.2	DF Common Options	51
6.2.4.2.1	Memory Addressing	53
6.2.4.2.2	ACPI	55
6.2.4.2.3	Link	56
6.2.4.2.3.1	xGMI Global Preset List	58
6.2.4.2.3.2	xGMI Initial Preset	59
6.2.4.2.3.3	xGMI TXEQ Search Mask	68
6.2.4.2.3.4	xGMI AC/DC Coupled Link	77
6.2.4.2.3.5	xGMI Channel Type	78
6.2.4.2.4	SDCI	79
6.2.4.2.5	Probe Filter	80
6.2.4.3	UMC Common Options	82
6.2.4.3.1	DDR Addressing Options	83
6.2.4.3.2	DDR Controller Configuration	84
6.2.4.3.2.1	DDR Power Options	85
6.2.4.3.2.2	Memory Channel Disable	87
6.2.4.3.2.3	Refresh Management (RFM)	89
6.2.4.3.3	DDR MBIST Options	91
6.2.4.3.3.1	Data Eye	93
6.2.4.3.4	DDR RAS	95
6.2.4.3.4.1	ECC Configuration	97
6.2.4.3.4.2	DRAM Scrubbers	99
6.2.4.3.5	DDR Bus Configuration	103
6.2.4.3.5.1	P-state 0 Dram ODT Impedance	105
6.2.4.3.5.2	P-state 1 Dram ODT Impedance	107
6.2.4.3.6	DDR Timing Configuration	109
6.2.4.3.6.1	DDR Timing Configuration-Accept	110
6.2.4.3.7	DDR Training Options	116
6.2.4.3.7.1	Periodic Phase Training	117
6.2.4.3.8	DDR Security	118
6.2.4.3.9	DDR PMIC Configuration	119
6.2.4.3.10	DDR Thermal Throttling	121
6.2.4.3.11	DDR Miscellaneous	123
6.2.4.4	NBIO Common Options	124
6.2.4.4.1	SMU Common Options	126
6.2.4.4.2	NBIO RAS Common Options	129
6.2.4.4.3	PCIE	131
6.2.4.4.4	nBif Common Options	134
6.2.4.4.4.1	RCD_DEV0	135
6.2.4.4.5	IOMMU/Security	138
6.2.4.4.6	Enable Port Bifurcation	139
6.2.4.4.7	Link EQ Preset Options	140
6.2.4.4.7.1	GEN3	141
6.2.4.4.7.2	GEN4	142
6.2.4.4.7.3	GEN5	143
6.2.4.5	FCH Common Options	144
6.2.4.5.1	I3c/I2c Configuration Options	145
6.2.4.5.2	SATA Configuration Options	147
6.2.4.5.2.1	SATA Controller Options	148
6.2.4.5.3	USB Configuration Options	161

6.2.4.5.3.1	MCM USB enable	162
6.2.4.5.4	AC Power Loss Options.....	163
6.2.4.5.5	Uart Configuration Options	164
6.2.4.5.6	FCH RAS Options	165
6.2.4.5.7	Miscellaneous Options.....	166
6.2.4.6	Soc Miscellaneous Control	167
6.2.4.6.1	Firmware Anti-rollback (FAR).....	169
6.2.4.7	CXL Common Options	170
6.2.4.7.1	CXL RAS.....	172
6.2.5	S5 RTC Wake Settings	173
6.2.6	Serial Port Console Redirection	174
6.2.6.1	COM0 Console Redirection Setting	175
6.2.6.2	Legacy Console Redirection Settings.....	177
6.2.6.3	Console Redirection Setting	178
6.2.7	CPU Configuration.....	180
6.2.7.1	Node 0 Information.....	181
6.2.7.2	Node 1 Information.....	182
6.2.8	PCI Subsystem Settings.....	183
6.2.9	USB Configuration.....	184
6.2.10	Network Stack Configuration	186
6.2.11	NVME Configuration	187
6.2.12	SATA Configuration.....	188
6.2.13	System Configuration	189
6.2.14	AMD Mem Configurations Status.....	190
6.2.14.1	Socket 0.....	191
6.2.14.1.1	Channel 0.....	192
6.2.14.1.2	Channel 1.....	193
6.2.14.1.3	Channel 2.....	194
6.2.14.1.4	Channel 3.....	195
6.2.14.1.5	Channel 4.....	196
6.2.14.1.6	Channel 5.....	197
6.2.14.1.7	Channel 6.....	198
6.2.14.1.8	Channel 7.....	199
6.2.14.1.9	Channel 8.....	200
6.2.14.1.10	Channel 9.....	201
6.2.14.1.11	Channel 10.....	202
6.2.14.1.12	Channel 11.....	203
6.2.14.2	Socket 1.....	204
6.2.14.2.1	Channel 0.....	205
6.2.14.2.2	Channel 1.....	206
6.2.14.2.3	Channel 2.....	207
6.2.14.2.4	Channel 3.....	208
6.2.14.2.5	Channel 4.....	209
6.2.14.2.6	Channel 5.....	210
6.2.14.2.7	Channel 6.....	211
6.2.14.2.8	Channel 7.....	212
6.2.14.2.9	Channel 8.....	213
6.2.14.2.10	Channel 9.....	214
6.2.14.2.11	Channel 10.....	215
6.2.14.2.12	Channel 11.....	216
6.2.15	Tls Auth Configuration.....	217
6.2.15.1	Server CA Configuration	218
6.2.15.1.1	Enroll Cert	219
6.2.15.1.2	Delete Cert.....	220
6.2.16	AMD PBS.....	221
6.2.16.1	RAS.....	222
6.2.16.2	Range Encryption	224
6.3	CHIPSET.....	226
6.3.1	North Bridge.....	227
6.3.1.1	Socket 0 Information.....	228
6.3.1.2	Socket 1 Information.....	229

6.4	SECURITY.....	230
6.4.1	Secure Boot	231
6.4.1.1	Expert Key Management.....	232
6.5	BOOT.....	235
6.5.1	UEFI NETWORK Drive BBS Priorities.....	237
6.5.2	UEFI NVME Drive BBS Priorities	238
6.5.3	UEFI USB Drive BBS Priorities	239
6.6	SAVE & EXIT	240
6.7	SERVER MGMT	241
6.7.1	System Event Log.....	243
6.7.2	View FRU information	244
6.7.3	Bmc Self-Test log	245
6.7.4	BMC network Configuration.....	246
6.7.5	View System Event Log.....	250
6.7.6	BMC User Settings.....	251
6.7.6.1	Add User	252
6.7.6.2	Delete User	253
6.7.6.3	Change User Settings	254
7	STATUS CODES LIST	255
7.1	AMI STANDARD STATUS CODE	255
7.1.1	SEC Phase	255
7.1.2	PEI Phase.....	256
7.1.3	DXE Phase.....	259

1 GENERAL OVERVIEW

This document specifies the system BIOS requirements of **Vantageo 12T1** project.

2 BIOS FEATURES OVERVIEW

2.1 BIOS DESCRIPTION

Item	Description
Code base vendor	AMI Aptio Core Base Version : Aptio V
BIOS image size	32 MB
ROM image size	32 MB

2.2 PROCESSOR

Intel Features	Description
Intel Hyper-Threading Technology	Support
Intel Boot Guard	
Intel VT-d	Support
Intel TDX	Support
Intel Turbo Boost Technology	Support
Intel SpeedStep Technology (P-States)	Support
Intel C-State	Support
Intel SST-PP	Support
Intel SST-BF	Support
Intel SST-TF	Support
Intel SST-CP	Support
Intel QAT	
Intel SGX	Support
AMD Features	Description
AMD SMT Control	Support
AMD SVM	Support

2.3 MEMORY

Features	Description
Interleaving Mode	Support
Independent Channel Mode	
Rank Sparing Mode	
Lockstep Channel Mode	
Mirroring Mode	Support
ECC (Error-correcting code)	Support
Memory re-mapping above 4GB	
Demand Scrubbing	
Patrol Scrubbing	
Vantageo Features	Description
Bad DIMM Location	Support

2.3.1 Bad DIMM Location

BIOS should correctly report bad DIMM location at early console out. DIMM location must match to DIMM silkscreen.

```
Copyright(c) 2024 American Megatrends International, LLC.
System Information:
Platform Name: TypeArcherCityRP, Core Version: 5.32
AMI BIOS Version: ES322IMS.228, Intel RC Version: 106.D62, Build Date: "06/11/20
24"

-----
System Boot Status

0x31 : Memory Initialization Complete
Major,Minor(0x46,:0x4)Socket,Channel,Dimm(0x0,:0x2:0x0)
CPU0_DIMM_C1
```

2.4 STORAGE

Features	Description
SATA HDD	Support
SATA CD-ROM/DVD-ROM	Support
USB HDD	Support
USB CD-ROM/DVD-ROM	Support
SAS HDD	Support
U.2 NVMe	Support
M.2 NVMe	Support
E1.S NVMe	Support
Intel Features	Description
Intel VROC	Support
Intel VMD	Support
Vantageo Features	Description
Hotplug	Support

2.5 NETWORKING

Features	Description
IPv4 PXE Boot	Support
IPv4 HTTP Boot	Support
Ipv6 PXE Boot	Support
IPv6 HTTP Boot	Support
Vantageo Features	Description
Enable/Disable Network port	

2.6 POWER MANAGEMENT

Features	Description
ACPI S0 (Working)	Support
ACPI S1	
ACPI S2	
ACPI S3	
ACPI S4 (Hibernate)	
ACPI S5 (Shut down)	Support
Processor C0	Support
Processor C1E	Support

Features	Description
Processor C1	Support
Processor C2	Support
Processor C3	Support
Processor C4	Support
Processor C5	Support
Processor C6	Support
Vantageo Features	Description
Restore on AC Power Loss	Support
Wake On Lan (WOL)	Support
Wake On RTC	Support
Power Capping	

2.7 SECURITY

Features	Description
Secure Boot	Support
TPM 1.2	
TPM 2.0	Support
Secure Flash BIOS	
Password on BIOS Setup Utility	Support
Password Clear	
Intel Features	Description
Intel TXT	
Vantageo Features	Description
Rot	
PFR	
Secure Erase Support (Security Freeze Lock)	Support
Strong BIOS Password	Support

2.7.1 Strong BIOS Password

Strong password policy

- At least 8 characters long
- Must with mixed-case letters, numbers and symbols
- Must start with English alphabet and case sensitive
- Symbols allow !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
- Do not contain spaces
- Old password is not allowed (keep 3 old password)
- Show warning message "Please change another password" when use old password

2.7.2 Trusted Computing (TPM)

Trusted platform module technology helps keep servers secure by offering hardware-level protection against malware and sophisticated cyber-attacks. TPM technology can be embedded into modern CPUs and “securely store artifacts used to authenticate the platform.”

- BIOS Setup Item

Item	Settings	Description
Security Device Support	[Disabled] [Enabled]	Enables or Disables BIOS support for security device.

2.7.3 RoT (Optional)

More detail information please refer to Vantageo_PRoT_Specification_R05.PDF

2.7.3.1 PFR T-1

The PFR software creates a special pre-boot environment on the platform and it is designed to allow the software operation in isolation from any external platform interfaces, while CPU, PCH, BMC, network, etc. are all held in power-off or in reset states.

In T-1 mode the AST1060 has full ownership of all platform flash storage to perform authentication, recovery and update actions.

Platform Status	Active	Recovery	Staging	Action/Comments
Boot	Good (n)	Good (<=n)	Don't Care	No action required, SPI flash is in correct operational state
Boot	Bad	Good (<=n)	Don't Care	Active partition is corrupted, recovery action required
Boot	Good (n)	Bad	Good (n)	Most probable power failure during Recovery update, corrective action required: copy Staging over to Recovery if staged firmware matches active firmware
Boot	Bad	Bad	Good (x)	Critical platform error; corrective action required: copy Staging over to Recovery, then perform recovery action
Boot	Good (n)	Bad	Bad	Critical platform error; allow platform boot but restrict Active updates; BMC/PCH is required to provide a Recovery update with firmware that matches active firmware. Reject recovery update and log error if staged firmware doesn't match active firmware.
Boot	Bad	Bad	Bad	Critical platform error; Hold this platform component in reset. When BMC FW is good and PCH/CPU FW is bad, user can attempt to update PCH/CPU FW via BMC to get the platform back to the good state. When BMC is bad, system will be held in T-1 with both BMC and PCH in reset. Note that a PCH/CPU recovery update is needed to recover from this scenario via BMC.
Update	Good (n)	Good (<=n)	Good (> n)	Correct update image staged; perform update action

2.7.3.2 Anti-Rollback

Anti-Rollback Protection is a security mechanism that prevents the system from being downgraded to a previous BIOS version with known vulnerabilities. It uses the Security Version Number (SVN) to determine the legitimacy of the firmware update.

SVN Number Usage Guideline

The Security Version Number (SVN) ranges from 0 to 64.

- **Before MP release:** SVN values are limited to SVN 1 or SVN 2 for internal testing purposes only.
- **After MP release:** The SVN value is incremented by 1 for each official BIOS release to enforce anti-rollback protection and maintain firmware security.

This mechanism ensures that once a BIOS version is released for production, future updates must carry a higher SVN to be accepted by the platform.

2.7.3.3 Seamless Update

Seamless technology allows platform administrators to perform a firmware update to SPI Flash without shutting down the running OS. Through handshake with BMC, CPLD can take over both SPI flashes and perform an update to a specific firmware volume on SPI flash.

2.8 SMBIOS

Type	Name	Description
0	BIOS Information	Support
1	System Information	Support
2	Base-Board Information	Support
3	System Enclosure or Chassis	Support
4	Processor Information	Support
5	Memory Controller Information	
6	Memory Module Information	
7	Cache Information	Support
8	Port Connector Information	Support
9	System Slots	Support
10	On Board Device Information	
11	OEM String	Support
12	System Configuration Options	Support
13	BIOS Language Information	Support
14	Group Associations	
15	System Event Log	
16	Physical Memory Array	Support
17	Memory Device	Support
18	32-bit Memory Error Information	
19	Memory Array Mapped Address	Support
20	Memory Device Mapped Address	Support
21	Built-in Pointing Device	
22	Portable Battery	
23	System Reset	
24	Hardware Security	
25	System Power Controls	
26	Voltage Probe	
27	Cooling Device	
28	Temperature Probe	
29	Electrical Current Probe	
30	Out-Of-Band Remote Access	
31	BIS Entry Point	
32	System Boot Information	Support
33	64-bit Memory Error Information	
34	Management Device	

Type	Name	Description
35	Management Device Component	
36	Management Device Threshold Data	
37	Memory Channel	
38	IPMI Device Information	Support
39	System Power Supply	Support
41	Onboard Device Extended Information	Support
42	Management Controller Host Interface	Support
43	TPM Device	Support
44	Processor Additional Information	
45	Firmware Inventory Information	
46	String Property	
126	Inactive	
127	End-of-Table	Support

2.9 BMC

Features	Description
Console Redirection via Serial Port	Support
Wait for BMC	Support
Sync The Timer With BMC	Support
IPMI Boot (Choice boot device via IPMI command)	Support
BMC LAN Control in BIOS Setup Utility	Support
BMC User Configuration in BIOS Setup Utility	Support
FRB2 (Fault Resilient Booting 2)	Support
Vantageo Features	Description
"Post Start" Event To BMC	
"Post End" Event To BMC	
BMC BIST	
IPMI LAN Select	

2.10 MISC

Features	Description
BIOS Recovery Mode	Support
Quiet Boot	Support
SEL (Self Error Log)	Support
Legacy Boot Mode (CSM)	
Hot Key	Support
Change Logo	Support
Fixed Boot Order	Support
Early Console	Support
Vantageo Features	Description
Clear CMOS Mode	Support
Dynamic PCIE Routing Configuration For Different Chassis SKU (1U/2U...)	Support
NMI Event And Log	
Endless Boot	Support
Chassis Intrusion	Support
HW Monitor	(optional)

2.10.1 BIOS Recovery Mode

A BIOS recovery can be accomplished from an USB Disk-On-Key. The recovery media must include the BIOS image file in the root directory.

- Recovery image – VANTAGEOBOOT.ROM.

2.10.2 Hot Key

Features	Description
Del	Enter BIOS setup menu
F2	Enter BIOS setup menu
F11	Enter Boot menu
F12	Enter network boot

2.10.3 Fixed Boot Order

1 st	2 nd	3 rd	4 th	5 th	
UEFI Network	UEFI Hard Disk	UEFI NVME	UEFI CD/DVD	UEFI USB	

2.10.4 Clear CMOS

When CMOS was clear by remove RTC battery or Clear CMOS jumper, BIOS will reload the default settings, including BIOS SETUP, RTC Date and Time. The default Date would be the first of January of the year of project kick-off. The default Time is 00:00:00.

- Error message
"Error: RTC Power Status Failed, BIOS Defaults are Loaded"
"Press F1 Skip, F10 Enter Setup"
Note: Passwords will be preserved even after clear CMOS

2.10.5 Endless Boot

If BIOS can't find boot OS from boot devices, BIOS will repeatedly try all boot devices until boot device was found.

- BIOS Setup item

Item	Settings	Description
Endless Boot Support	[Enabled] [Disabled]	Enable or disable repeatedly try all boot devices until boot device was found.

2.10.6 Chassis Intrusion

When chassis intrusion is detected, BIOS will popup error information during POST.

- Error message
"Error: The Chassis has been opened"
"Press F1 Skip, F10 Enter Setup and Clear Status"
- BIOS Setup Item

Item	Settings	Description
Chassis Intrusion	[Enabled] [Disabled]	Enable or disable chassis intrusion detection.

2.10.7 HW Monitor (Optional)

System with BMC support can monitor these sensors through WebUI or IPMI command. Hence, this SETUP page only available when system without BMC support and sensors are connected to SIO.

Hardware Monitor Main Page

Aptio Setup - AMI						
Main	Advanced	Chipset	Security	Boot	Save & Exit	Server Mgmt
Hardware Monitor						
BMC FW Product		AST2600				
BMC FW Revision		01.05				
▶ Temperature status ▶ Voltage status ▶ Fan status						
		→ ←: Select Screen ↑ ↓: Select Item - Enter: Select +/-: Change Opt. - F1: General Help - F2: Previous values - F3: Optimized Defaults - F4: Save & Exit - ESC: Exit				
Version 2.22.1284. Copyright © 2022 AMI						

Temperature Status

[illegible]

Voltage Status

Aptio Setup - AMI	
Main	Advanced
Chipset	Security
Boot	Save & Exit
Server Mgmt	

Voltage status	
P12V	: +12.00 V
P12V_BP	: +12.00 V
P3V3_SCALED	: +3.24 V
P5V_SCALED	: +5.00 V
P5V_AUX_SCALED	: +5.04 V
PM_VDD_P1V8	: +1.79 V
PM_VDD_P1V0_AUX	: +0.99 V
PM_VDD_P1V0	: +0.99 V
PVDDBT_RTC_G	: +2.96 V
PVDDIO_MEM_AUX	: +1.08 V
PVDD_P1V8_AUX	: +1.75 V
PVDD_P1V8	: +1.77 V
PVDD_MISC_AUX	: +0.73 V
PVDD_MISC	: +1.10 V
VDDCR_CPU	: + 1.34 V
VDDCR_SOC	: +1.01 V

→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
--

Version 2.22.1284. Copyright © 2022 AMI

Fan Status

Aptio Setup - AMI		
Main	Advanced	Chipset Security Boot Save & Exit Server Mgmt

Fan status

FAN1	: 1600 RPM
FAN2	: 1600 RPM
FAN3	: 1600 RPM
FAN4	: 1600 RPM
FAN5	: 1600 RPM
FAN6	: 1600 RPM
FAN7	: N/A
FAN8	: N/A

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

2.11 POST INFORMATION

Display system configuration, error information, and hotkey information during POST. User can be press hot key or <F2> into BIOS setup Menu during POST.

2.11.1 Early Console POST Information

Provide system information, processor information, and memory information.

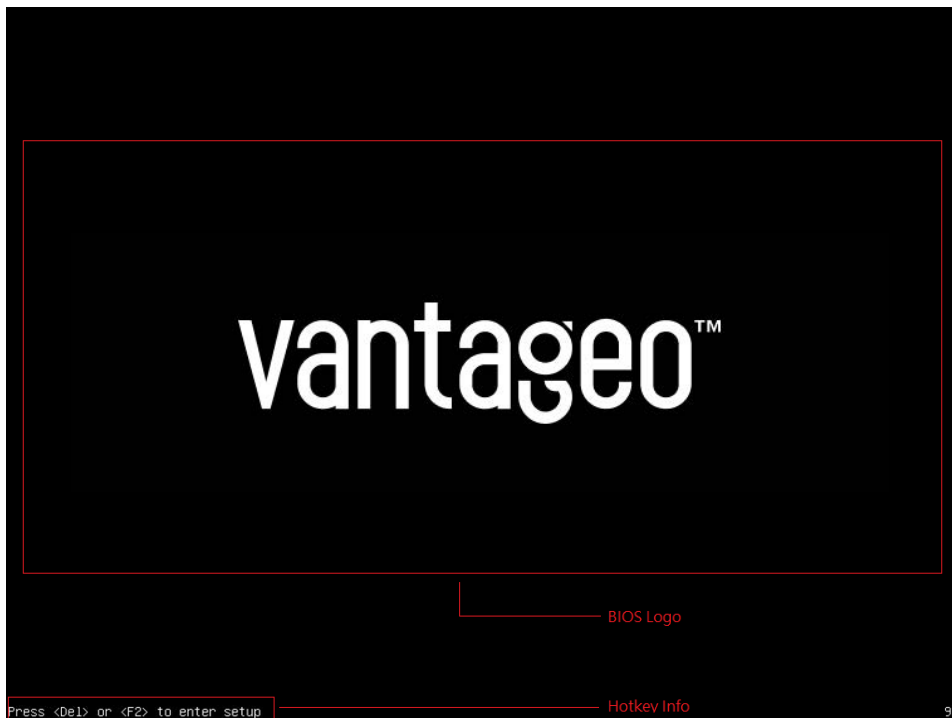
Below information are mandatory. Other information can be displayed according to different platform.

System Information	
BIOS Version:	ESXXXXXX.XXX
Build Date:	MM/DD/YYYY
Processor Information	
Name:	
Stepping:	
Speed:	MHz
Processors:	
Cores:	
Memory Information	
Total Memory:	GB
Memory Speed:	MT/s

System Information:	
BIOS Version: ES368IMS.A01	
Build Date: 08/20/2024	
Intel RC Version: 3376D01	
Processor Informaiton:	
Name: Intel(R) Xeon(R) 6756E, Stepping: SRF HDCC Cx, Speed: 1800 MHz	
Processors: 2, Cores: 256	
S3M Information:	
Series: S3M IBL	
Memory Information:	
Total Memory: 2048GB, Memory Speed: 5200MT/s,	RAS Mode: Indep
0x4F : DXE IPL Start	
0x33 : CPU Cache initialization	
0x60 : DXE Core Started.	
Mandatory information	

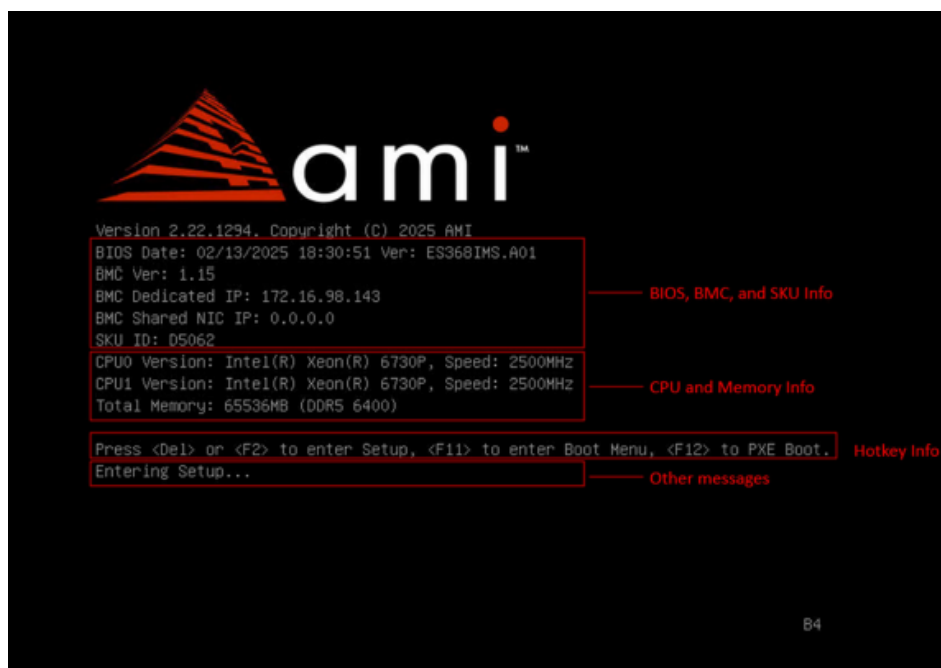
2.11.2 Quiet Boot

Display logo and hotkey information.



2.11.3 POST Information

Provide BIOS version, BIOS build date, BMC version, BMC IP address, SKU ID, processor version, processor speed, total memory, hotkey information, and other messages. If the system does not have a BMC, the POST information will not display any BMC-related details.



3 SYSTEM EVENT LOG

3.1 MEMORY

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0x0C
12	Sensor #	0x00
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error type 0x00 = Correctable ECC 0x01 = Uncorrectable ECC 0x04 = Memory device disabled 0x05 = Correctable error threshold reached
15	Event Data 2	Intel [7:4] – Reserved [3] – Dimm valid bit. [2] – Channel valid bit. [1] – Socket valid bit. [0] – Happened in the boot. 0x00 = Current boot 0x01 = Last boot AMD [7:0] - Reserved
16	Event Data 3	[7:5] – Socket ID Number 0x00 = Socket 0 0x01 = Socket 1 0x02 = Socket 2 0x03 = Socket 3 [4:1] – Memory Channel Number 0x00 = Memory channel A 0x01 = Memory channel B 0x02 = Memory channel C 0x03 = Memory channel D 0x04 = Memory channel E 0x05 = Memory channel F 0x06 = Memory channel G

Byte	Field	Description
		0x07 = Memory channel H 0x08 = Memory channel I 0x09 = Memory channel J 0x0A = Memory channel K 0x0B = Memory channel L 0x0C = Memory channel M 0x0D = Memory channel N 0x0E = Memory channel O 0x0F = Memory channel P [0] – Memory Dimm Number 0x00 = Dimm 0 of channel 0x01 = Dimm 1 of channel

3.2 PROCESSOR

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0x07
12	Sensor #	0x00
13	Event Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] 0x05 = Configuration Error 0x0B = Machine Check Exception (Uncorrectable) 0x0C = Correctable Machine Check Error
15	Event Data 2	[7:4] –Socket ID Number 0x00 = Socket 0 0x01 = Socket 1 Intel [3:0] – Bank Type 0x00 = None 0x01 = IFU 0x02 = DCU 0x03 = DTLB 0x04 = MLC 0x05 = PCU

Byte	Field	Description
		0x06 = IIO 0x07 = CHA 0x08 = KTI AMD [3:0] – Die ID
16	Event Data 3	Intel [7:4] –Error Type 0x00 = Unknow 0x01 = Cache Error 0x02 = TLB Error 0x03 = Bus Error 0x04 = Micro Arch Error [3:1] –Error Severity of ACPI 0x00 = Recoverable 0x01 = Fatal 0x02 = Corrected 0x03 = None [0] – Happened in the boot. 0x00 = Current boot 0x01 = Last boot AMD [7:0] – MCA OEM Error Type 0x8A = CPU PSP 0x8B = CPU SMU 0x8E = CPU Gen 0x8F = CPU GMI 0x90 = CPU xGMI 0x93 = WAFL

3.3 PCIE

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0x13
12	Sensor #	0x00
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error type 0x04 = PCIE Bus PERR 0x05 = PCIE Bus SERR 0x07 = PCIE Bus Correctable Error 0x08 = PCIE Bus Uncorrectable Error 0x0A = PCIE Bus Fatal Error 0x0F = Latest Boot PCIE Error
15	Event Data 2	[7:0] – PCI Bus Number
16	Event Data 3	[7:3] – PCI Device Number [2:0] – PCI Function Number

3.4 SEL FOR AMD RAS

3.4.1 NBIO

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0x13
12	Sensor #	0x00
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error Type
15	Event Data 2	[7:0] – 0x00
16	Event Data 3	[7:4] – RAS ELog Type 0x04 = NBIO

3.4.2 SMN

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0xC0
12	Sensor #	0x00
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error Type 0x01 = Correctable Error 0x02 = Uncorrectable Error
15	Event Data 2	[7:0] – Bus ID
16	Event Data 3	[7:4] – RAS ELog Type 0x06 = SMN [3:0] – Error Source

3.4.3 CXL

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0xC1
12	Sensor #	0x02
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:2] – CXL Error Log Type 0x0 = CXL IO 0x1 = CXL Memory 0x2 = CXL Component Event [1] – CXL Agent Type [0] – Error Type 0x00 = Correctable Error 0x01 = Uncorrectable Error
15	Event Data 2	[7:0] – Bus Number
16	Event Data 3	[7:3] – Device Number [2:0] – Function Number

3.4.4 PMIC

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04
11	Sensor Type	0xC0
12	Sensor #	0x00
13	Enent Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error Type 0x01 = Correctable Error 0x02 = Uncorrectable Error
15	Event Data 2	[7:6] – Reserved [5] – Socket [4] – DIMM [3:0] – Channel
16	Event Data 3	[7:0] – RAS ELog Type 0x95 = PMIC

4 SMBIOS

4.1 TYPE 0

Name	Description
Vendor	American Megatrends International, LLC.
BIOS Version	(Should follow BIOS Naming Rule)
BIOS Characteristics	0000 0001 340B 9A80
BIOS Characteristics Extension Bytes	0D03
System BIOS Major Release	AMI Core Major Version
System BIOS Minor Release	AMI Core Minor Version

4.2 TYPE 1

SMBIOS	FRU	
Name	Area	Field
Manufacturer	Product Info	Product Manufacturer
Product Name	Product Info	Product Name
Version	Product Info	Product Version
Serial Number	Product Info	Product Serial Number
UUID	IPMI	System GUID
SKU Number	Product Info	Product Part Number
Family		

4.2.1 SMBIOS UUID to BMC GUID Format

RFC 1422 Name	Field	Bytes	BIOS UUID	BMC GUID
time low	Data1	4	UUID[0] UUID[1] UUID[2] UUID[3]	GUID[12] GUID[13] GUID[14] GUID[15]
time mid	Data2	2	UUID[4] UUID[5]	GUID[10] GUID[11]
time high and version	Data3	2	UUID[6] UUID[7]	GUID[8] GUID[9]
clock seq and reserved	Data4	2	UUID[8] UUID[9]	GUID[7] GUID[6]
node	Data5	6	UUID[10] UUID[11] UUID[12] UUID[13] UUID[14] UUID[15]	GUID[5] GUID[4] GUID[3] GUID[2] GUID[1] GUID[0]

Reading of UUID Structure and Conversion

UUID Type	UUID
SMBIOS UUID	AABBCCDD-EEFF-GGHH-IIJJ-KKLLMMNNOOPP
BMC Get Device GUID	MMNNOOPP-KKLL-IIJJ-HHGG-FFEEDDCCBBAA

4.3 TYPE 2

SMBIOS	FRU	
Name	Area	Field
Manufacturer	Board Info	Board Manufacturer
Product	Board Info	Board Product Name
Version	Board Info	Board Part Number
Serial Number	Board Info	Board Serial Number
Asset Tag		

4.4 TYPE 3

SMBIOS	FRU	
Name	Area	Field
Manufacturer	Product Info	Product Manufacturer
Type	Chassis Info	Chassis Type
Version		
Serial Number	Chassis Info	Chassis Serial Number
Asset Tag Number		
SKU Number	Chassis Info	Chassis Part Number

5 UTILITY

5.1 FLASH BIOS UTILITIES

AFU (AMI Firmware Update) is a package of utilities used to update the system BIOS under various operating systems. AFU only works for APTIO with SMI FLASH support.

Utilities	Description
Flash BIOS Image Under EFI Shell	AFUEFIX64.EFI
Flash BIOS Image Under Linux	AFULNX_64
Flash BIOS Image Under Windows	AFUWINGUI.EXE

5.2 AMISCE

AMI Setup Control Environment (AMISCE) is a command line tool available in both 32-bit and 64-bit flavors. AMISCE provides you an easy way to update NVRAM variables from within the EFI, Linux, or Windows based environment. The user can extract variables directly from the BIOS, and also allows the user to change settings using either a text editor or a setup program, and then update the BIOS. Each of these actions may take place on a different system.

AMISCE produces a script file that lists all setup questions on the system where AMISCE is running. The user can then modify the script file and use it as input to change the current NVRAM setup variables.

Utilities	Description
AMISCE Under EFI Shell	SceEfi64.efi

5.3 DMIEDIT (OPTIONAL)

AMIDEEFI (DMIEEdit) is a Desktop Management Interface utility with command line interface. It allows you to modify strings associated with SMBIOS tables on AMIBIOS host system.

The utility offers you to modify following SMBIOS table:

- * BIOS Information (Type 0)
- * System (Type 1)
- * Base Board (Type 2)
- * Chassis (Type 3)
- * Processor Information (Type 4)
- * OEM String (Type 11)
- * System Configuration Options (Type 12)
- * Portable Battery (Type 22)
- * System Power Supply (Type 39)

Utilities	Description
DMIEDIT Under EFI Shell	DMIDEEFIx64.EFI
DMIEDIT Under Linux	AMIDELNX_64
DMIEDIT Under Windows	DMIEDITx64.EXE AMIDEWINx64.EXE

Note: DMI modification might not effect when data was synchronized from FRU.

6 BIOS SETUP

6.1 MAIN MENU

Aptio Setup - AMI

Main

Advanced

Chipset

Security

Boot

Save & Exit

Server Mgmt

BIOS Information

BIOS Vendor

Core Version

Compliance

Project Version

Build Date and Time

Access Level

Memory Information

Total Memory

System Language

System Date

System Time

American Megatrends

5.35

UEFI 2.9; PI 1.7

ES312AMS.XXX

01/01/20XX 00:00:00

Administrator

Total Memory :16384 MB

[English]

[Sat 01/01/2022]

[00:00:00]

→ ← :Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Main		
Menu Fields	Settings	Comments
BIOS Information		
BIOS Vendor	American Megatrends	
Core Version	x.xx	Displays the Core version.
Compliance	UEFI x.x: PI x.x	Displays the Compliance name.
Project Version	x.xx	Displays the BIOS version.
Build Date and Time	xx/xx/xx xx:xx:xx	Displays the BIOS build date and time.
Access Level	Administrator	Displays the control level of setup menu
Memory Information		
Total memory	Y MB	Displays the available memory size

Main		
Menu Fields	Settings	Comments
System time	[Sat 01/01/2023]	Displays the current time.
System date	[00:00:00]	Displays the current date.

6.2 ADVANCED MENU

Aptio Setup - AMI
Main Advanced Chipset Security Boot Save & Exit Server Mgmt

- ▶ Trusted Computing
- ▶ PSP Firmware Version
- ▶ Redfish Host Interface Settings
- ▶ AMD CBS
- ▶ S5 RTC Wake Settings
- ▶ Serial Port Console Redirection
- ▶ CPU Configuration
- ▶ PCI Subsystem Settings
- ▶ USB Configuration
- ▶ Network Stack Configuration
- ▶ NVMe Configuration
- ▶ SATA Configuration
- ▶ System Configuration

- ▶ AMD Mem Configuration Status
- ▶ Tls Auth Configuration
- ▶ AMD PBS

- ▶ Intel(R) I350 Gigabit Network Connection - 00:00:00:00:...
- ▶ Intel(R) I350 Gigabit Network Connection - 00:00:00:00:...

→ ←: Select Screen
↑ ↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced		
Menu Fields	Settings	Comments
Trusted Computing	Selects sub-menu.	Trusted Computing Settings.
PSP Firmware Versions	Selects sub-menu.	PSP Firmware Versions
Redfish Host Interface Settings	Selects sub-menu.	Redfish Host Interface Parameters.
AMD CBS	Selects sub-menu.	AMD CBS Setup Page
S5 RTC Wake Settings	Selects sub-menu.	Enable System to Wake from S5 using RTC alarm
Serial Port Console Redirection	Selects sub-menu.	Serial Port Console Redirection
CPU Configuration	Selects sub-menu.	CPU Configuration Parameters
PCI Subsystem Settings	Selects sub-menu.	PCI Subsystem Settings
USB Configuration	Selects sub-menu.	USB Configuration Parameters
Network Stack Configuration	Selects sub-menu.	Network Stack Settings
NVMe Configuration	Selects sub-menu.	NVMe Device Options Settings
SATA Configuration	Selects sub-menu.	SATA Devices Information

Advanced		
Menu Fields	Settings	Comments
System Configuration	Selects sub-menu.	System Configuration
AMD Mem Configuration Status	Selects sub-menu.	To display memory configuration (initialized by ABL) status
Tls Auth Configuration	Selects sub-menu.	Press <Enter> to select Tls Auth Configuration
AMD PBS	Selects sub-menu.	AMD PBS Setup Page
Intel(R) I350 Gigabit Network Connection - 00:00:00:00:...	Selects sub-menu.	Configure Gigabit Ethernet device parameters
Intel(R) I350 Gigabit Network Connection - 00:00:00:00:...	Selects sub-menu.	Configure Gigabit Ethernet device parameters

6.2.1 Trusted Computing

Aptio Setup - AMI	
Advanced	
Configuration	
Security Device Support	[Enabled]
No Security Device Found	
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

6.2.2 PSP Firmware Versions

Aptio Setup - AMI

Advanced

PSP Firmware Versions

ABL Version	1005F011
PSP BootLoader Version	00.3D.00.73
PSP BootLoader 2 Version	00.3D.00.73
PSP TEE Version	00.3D.00.73
SMU FW Version	00.5E.7A.00
SEV FW Version	01.01.37.3D
PHY FW Version	00.01.49.00
MPIO FW Version	01.00.1B.00
TF MPDMA FW Version	00.5E.24.00
PM MPDMA FW Version	00.5E.1D.00
GMI FW Version	BB.05.53.00
RIB FW version	0B.00.05.1F
SEC FW version	0E.11.40.59
PMU FW version	00.00.9C.13
EMCR FW version	00.00.EC.13
uCode C1 version	B002147
APCB Version	0000
APOB Version	0000
APPB Version	0000

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.2.3 Redfish Host Interface Settings

Aptio Setup - AMI

Advanced

Redfish Host Interface Settings

Redfish

[Enable]

BMC Redfish Version

1.15.1

BIOS Redfish Version

1.15.1

Authentication mode

[Basic Authentication]

Redfish BMC Settings

IP address

169.254.0.17

IP Mask address

255.255.0.0

IP Port

443

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.2.4 AMD CBS

Aptio Setup - AMI

Advanced

AMD CBS

AMD CBS Revision Number 0x0

- ▶ CPU Common Options
- ▶ DF Common Options
- ▶ UMC Common Options
- ▶ NBIO Common Options
- ▶ FCH Common Options
- ▶ SOC Miscellaneous Control
- ▶ CXL Common Options

→ ← :Select Screen
 ↑ ↓ :Select Item
 Enter:Select
 +/-:Change Opt.
 F1: General Help
 F2: Previous values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS		
Menu Fields	Settings	Comments
CPU Common Options	Selects sub-menu.	
DF Common Options	Selects sub-menu.	
UMC Common Options	Selects sub-menu.	
NBIO Common Options	Selects sub-menu.	
FCH Common Options	Selects sub-menu.	
SOC Miscellaneous Control	Selects sub-menu.	
CXL Common Options	Selects sub-menu.	

6.2.4.1 CPU Common Options

Aptio Setup - AMI

Advanced

CPU Common Options

► Performance

REP-MOV/STOS Streaming [Enabled]

► Perfetcher settings

► Core Watchdog

RedirectForReturnDis [Auto]

Platform First Error Handling [Auto]

Core Performance Boost [Auto]

Global C-state Control [Auto]

Power Supply Idle Control [Auto]

Streaming Stores Control [Auto]

Local APIC Mode [Auto]

ACPI _CST C1 Declaration [Auto]

ACPI CST C2 Latency 100

MCA error thresh enable [Auto]

MCA FruText [True]

SMU and PSP Debug Mode [Auto]

PPIN Opt-in [Auto]

SMEE [Auto]

Action on BIST Failure [Auto]

Enhanced REP MOVSB/STOSB (ERSM) [Auto]

Log Transparent Errors [Auto]

AVX512 [Auto]

ERMSB Caching Behavior [Auto]

CPU Speculative store Modes [Auto]

Fast short REP MOVSB (FSRM) [Auto]

PauseCntSel_1_0 [Auto]

Prefetch/Request Throttle [Auto]

Scan Dump Debug Enable [Disabled]

MCAX 64 bank support [Auto]

Adaptive Allocation (AA) [Auto]

Latency under Load (LUL) [Auto]

Core Trace Dump Enable [Disabled]

FP512 [Auto]

AMD_ERMSB Reporting [Auto]

→ ←:Select Screen

↑ ↓:Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

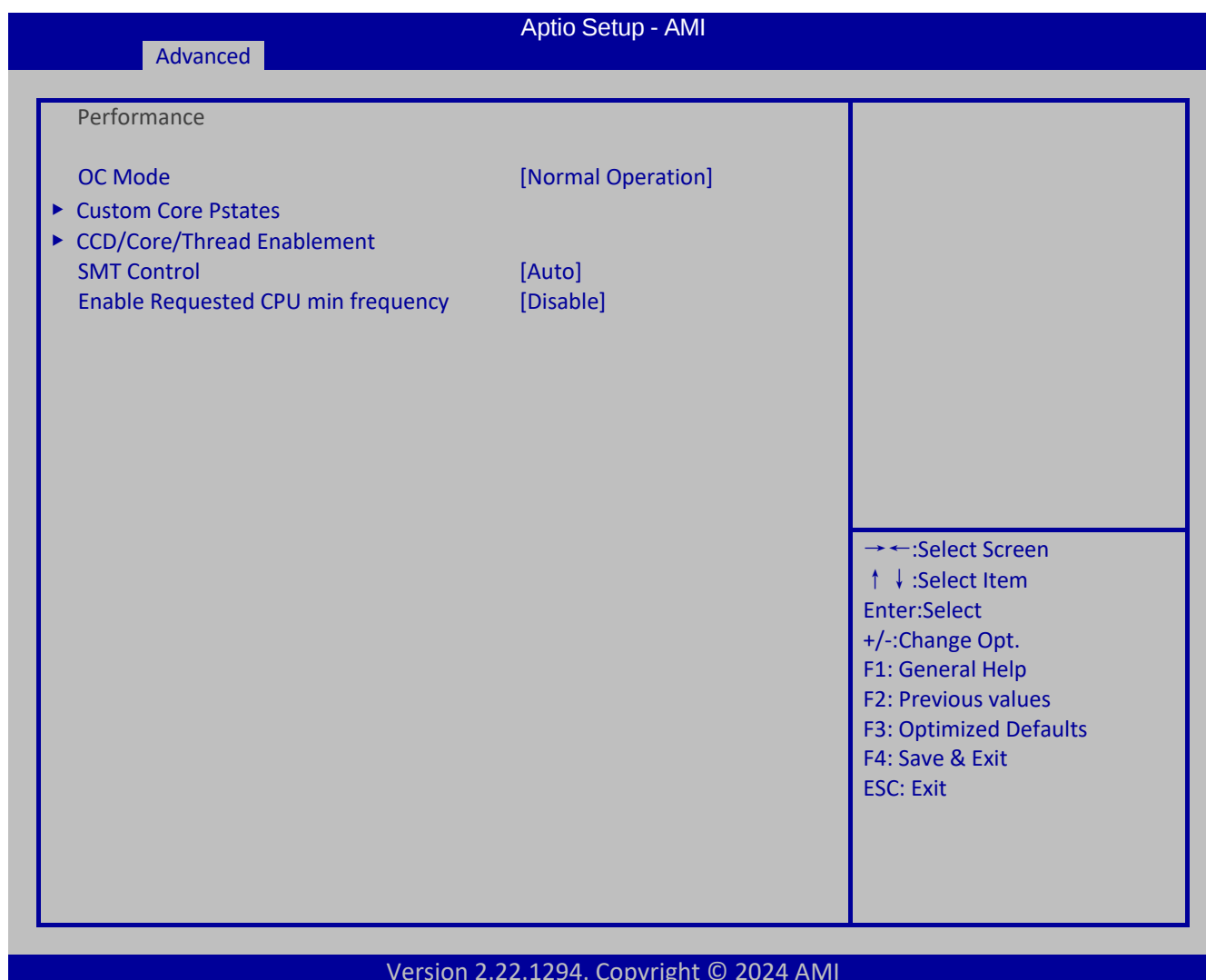
Advanced \ AMD CBS \ CPU Common Options		
Menu Fields	Settings	Comments
Performance	Select sub-menu	
REP-MOV/STOS Streaming	[Disabled] [Enabled]	Allow REP-MOV/STOS to use non-caching streaming stores for large sizes.
Perfetcher settings	Select sub-menu	
Core Watchdog	Select sub-emnu	

Advanced \ AMD CBS \ CPU Common Options		
Menu Fields	Settings	Comments
RedirectForReturnDis	[Auto] [1] [0]	From a workaround for GCC/C000005 issue for XV core on CZ A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrctForReturns] to 1
Platform First Error Handling	[Enabled] [Disabled] [Auto]	Enable/disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank.
Core Performance Boost	[Disabled] [Auto]	Disable CPB
Global C-state Control	[Disabled] [Enabled] [Auto]	Controls IO base C-state generation and DF C-states.
Power Supply Idle Control	[Low Current Idle] [Typical Current Idle] [Auto]	Power Supply Idle Control.
Streaming Stores Control	[Disabled] [Enabled] [Auto]	Enables or disables the streaming stores functionality.
Local APIC Mode	[xAPIC] [x2APIC] [Auto]	Select local APIC operation modes.
ACPI _CST C1 Declaration	[Disabled] [Enabled] [Auto]	Determines whether or not to declare the C1 state to the OS.
ACPI CST C2 Latency	x	Enter in microseconds (decimal value). Larger C2 latency value will reduce the number of C2 transitions and reduce C2 residency. Fewer transitions can help when performance is sensitive to the latency of C2 entry and exit. Higher residency can improve performance by allowing higher frequency boost and reduce idle core power. With Linux kernel 6.0 or later, the C2 transition cost is significantly reduced. The best value will be dependent on kernel version, use case, and workload.
MCA error thresh enable	[False] [True] [Auto]	Enable MCA error thresholding
MCA FruText	[False] [True]	Enable MCA FruText
SMU and PSP Debug Mode	[Disabled] [Enabled] [Auto]	When this option is enabled, uncorrected errors detected by the PSP FW or SMU FW that should cause a cold reset, will hang and not reset the system
PPIN Opt-in	[Disabled] [Enabled] [Auto]	Turn on PPIN feature
SMEE	[Disabled] [Enabled] [Auto]	Control secure memory encryption enable Enabling both SMEE and SME-MK is not supported. Results in #GP.
Action on BIST Failure	[Do nothing] [Down-CCD] [Auto]	Action to take when a CCD BIST failure is detected
Enhanced REP MOVSB/STOSB (ERSM)	[Disabled] [Enabled] [Auto]	Default is 1, can be set to zero for analysis purposes as long as OS supports it.

Advanced \ AMD CBS \ CPU Common Options		
Menu Fields	Settings	Comments
Log Transparent Errors	[Auto] [Disabled] [Enabled]	Log transparent errors in MCA in addition to debug registers.
AVX512	[Disabled] [Enabled] [Auto]	Enable/Disable AVX512
ERMSB Caching Behavior	[Disabled] [Enabled] [Auto]	Enable: Optimized caching for REPs. Disable: Legacy caching behavior for REPs.
CPU Speculative store Modes	[Balanced] [More Speculative] [Less Speculative] [Auto]	Balanced: Store instructions may delay sending out their invalidations to remote cacheline copies when the cacheline is present but not in a writable state in the local cache. More Speculative: Store instructions will send out invalidations to remote cacheline copies as soon as possible. Less Speculative: Store instructions may delay sending out their invalidations to remote cacheline copies when the cacheline is not present in the local cache or not in a writable state in the local cache.
Fast short REP MOVSB (FSRM)	[Auto] [Enabled] [Disabled]	Default is 1, can be set to zero for analysis purposes as long as OS supports it.
PauseCntSel_1_0	[Auto] [16 cycles] [32 cycles] [64 cycles] [128 cycles]	Number of cycles dispatch is stalled for a thread after dispatching PAUSE instruction. POR is 64 cycles.
Prefetch/Request Throttle	[Disabled] [Enabled] [Auto]	Enables XI logic which calculates average latency, updates throttle level, and sends throttle level messages to L2
Scan Dump Debug Enable	[Disable] [Enable]	This option operates like below setting (when enabled) to avoid the reset caused by Syncflood, etc APCB_TOKEN_UID_PSP_ENABLE_DEBUG_MODE = 1 (Enabled) APCB_TOKEN_UID_DF_EXT_IP_SYNC_FLOOD_PROP = 1 (Sync flood disabled) PcdResetCpuOnsyncFlood = 0 (Disable)
MCAX 64 bank support	[Disabled] [Enabled] [Auto]	Enable 64 MCA banks per thread mapping.
Adaptive Allocation (AA)	[Enabled] [Disabled] [Auto]	Disable to use fixed L2 replacement/allocation policy
Latency under Load (LUL)	[Auto] [Enabled] [Disabled]	Enabling may improve latency in heavy BW scenarios. May slightly reduce peak CCD BW.
Core Trace Dump Enable	[Disable] [Enable]	Enable/Disable Core Trace Dump Feature.

Advanced \ AMD CBS \ CPU Common Options		
Menu Fields	Settings	Comments
FP512	[Disabled]	Indicates support for downgrading FP512 datapath to FP256. Enable = 512bit datapath, Disable = 256bit datapath.
	[Enabled]	
	[Auto]	
AMD_ERMSB Reporting	[Auto]	Report presence of AMD_ERMSB via CUID. By default, this is reported as true (Enable), the field can be set to false for analysis purposes as long as OS supports it.
	[Disable]	
	[Enable]	

6.2.4.1.1 Performance



Advanced \ AMD CBS \ CPU Common Options \ Performance		
Menu Fields	Settings	Comments
OC Mode	[Normal Operation] [Customized]	Select overlock operation modes
Custom Core Pstats	Select sub-menu	
CCD/Core/Thread Enablement	Select sub-menu	
SMT Control	[Disable] [Enable] [Auto]	Can be used to disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after selecting the 'Enable' option. Select 'Auto' based on BIOS PCD(PcdAmdSmtMode) default setting. WARNING – S3 is NOT SUPPORTED on systems where SMT is disabled.
Enable Requested CPU min frequency	[Disable] [Enable]	This allows for minimum requested CPU frequency to be used.

6.2.4.1.1.1 Custom Core Pstates

Advanced

Aptio Setup - AMI

Custom Core Pstates

WARNING – DAMAGE CAUSED BY USE OF YOUR AMD PROCESSOR OUTSIDE OF SPECIFICATION OR IN EXCESS OF FACTORY SETTINGS ARE NOT COVERED UNDER YOUR AMD PRODUCT WARRANTY AND MAY NOT BE COVERED BY YOUR SYSTEM MANUFACTURER’S WARRANTY.

Operating your AMD processor outside of specification or in excess of factory settings, including but not limited to overclocking, may damage or shorten the life of your processor or other system components, create system instabilities (e.g., data loss and corrupted images) and in extreme cases may result in total system failure. AMD does not provide support or service for issues or damages related to use of an AMD processor outside of processor specifications or in excess of factory settings.

► Decline

► Accept

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ CPU Common Options \ Performance \ Custom Core Pstates		
Menu Fields	Settings	Comments
Decline	Selects Previous-menu	
Accept	Selects sub-menu	

6.2.4.1.1.1.1 Custom Core Pstates - Accept

Aptio Setup - AMI

Advanced

Accept

Custom Pstate0 [Auto]

Pstate0 Freq (MHz) 0

→ ←: Select Screen

↑ ↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ CPU Common Options \ Performance \ Custom Core Pstates \ Accept		
Menu Fields	Settings	Comments
Custom Pstate0	[Custom] [Auto]	Disable – disable this Pstate Custom – customize this Pstate, applicable only if PcdOcDisable=FALSE WARNING – DAMAGE CAUSED BY USE OF YOUR AMD PROCESSOR OUTSIDE OF SPECIFICATION OR IN EXCESS OF FACTORY SETTINGS ARE NOT COVERED UNDER YOUR AMD PRODUCT WARRANTY AND MAY NOT BE COVERED BY YOUR SYSTEM MANUFACTURER'S WARRANTY. Operating your AMD processor outside of specification or in excess of factory settings, including but not limited to overclocking, may damage or shorten the life of your processor or other system components, create system instabilities (e.g., data loss and corrupted images) and in extreme cases may result in total system failure. AMD does not provide support or

Advanced \ AMD CBS \ CPU Common Options \ Performance \ Custom Core Pstates \ Accept		
Menu Fields	Settings	Comments
		service for issues or damages related to use of an AMD processor outside of processor specifications or in excess of factory settings.
Pstate0 Freq (MHz)	x	Specifies core frequency (MHz)

6.2.4.1.1.2 CCD/Core/Thread Enablement

Advanced

Aptio Setup - AMI

CCD/Core/Thread Enablement

CCD Control

Core control

[Auto]

[Auto]

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ CPU Common Options \ Performance \ CCD/Core/Thread Enablement		
Menu Fields	Settings	Comments
CCD Control	[Auto]	Sets the number of active CCDs. Once this option has been used to remove any CCDs, a POWER CYCLE is required in order for future selections to take effect.
	[2 CCDs]	
	[4 CCDs]	
	[6 CCDs]	
	[8 CCDs]	
	[10 CCDs]	
Core control	[Auto]	Set the number of cores to be used. Once this Option has been used to remove any cores, a POWER CYCLE is required in order for future selections to take effect.
	[ONE (1+0)]	
	[TWO (2+0)]	
	[THREE (3+0)]	
	[FOUR (4+0)]	
	[FIVE (5+0)]	
	[SIX (6+0)]	
	[SEVEN (7+0)]	

6.2.4.1.2 Prefetched settings

Advanced

Aptio Setup - AMI

Prefetcher settings

L1 Stream HW Prefetcher

[Auto]

L1 Stride Prefetcher

[Auto]

L1 Region Prefetcher

[Auto]

L2 Stream HW Prefetcher

[Auto]

L2 Up/Down Prefetcher

[Auto]

L1 Burst Prefetch Mode

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ CPU Common Options \Prefetcher settings		
Menu Fields	Settings	Comments
L1 Stream HW Prefetcher	[Disable] [Enable] [Auto]	Option to Enable Disable L1 Stream HW Prefetcher.
L1 Stride Prefetcher	[Disable] [Enable] [Auto]	Uses memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous.
L1 Region Prefetcher	[Disable] [Enable] [Auto]	Uses memory access history to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses.
L2 Stream HW Prefetcher	[Disable] [Enable] [Auto]	Option to Enable Disable L2 Stream HW prefetcher
L2 Up/Down Prefetcher	[Disable] [Enable] [Auto]	Uses memory access history to determine whether to fetch the next or previous line for all memory access
L1 Burst Prefetch Mode	[Disable] [Enable] [Auto]	Option to Enable Disable L1 Burst prefetch Mode

6.2.4.1.3 Core Watchdog

Aptio Setup - AMI

Advanced

Core Watchdog

Core Watchdog Timer Enable

[Auto]

Core Watchdog Timer Interval

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ CPU Common Options \ Core Watchdog		
Menu Fields	Settings	Comments
Core Watchdog Timer Enable	[Disabled]	Enable or disable CPU Watchdog Timer
	[Enabled]	
	[Auto]	
Core Watchdog Timer Interval	[2.681s]	Select CPU Watchdog Timer interval
	[1.340s]	
	[669.41ms]	
	[334.05ms]	
	[166.37ms]	
	[82.53ms]	
	[40.61ms]	
	[20.970ms]	
	[10.484ms]	
	[5.241ms]	
	[2.620ms]	
	[1.309ms]	
	[654.08us]	
	[326.4us]	
	[162.56us]	
	[80.64us]	
	[39.68us]	
	[Auto]	

6.2.4.2 DF Common Options

Aptio Setup - AMI	
Advanced	
DF Common Options ▶ Memory Addressing ▶ ACPI ▶ Link ▶ SDCI ▶ Probe Filter DF Watch Timer Interval [Auto] Disable DF to external IP [Auto] SyncFloodPropagation Sync Flood Propagation to DF Components [Auto] Freeze DF module queues on error [Auto] CC6 memory region encryption [Auto] CCD B/W Balance Throttle Level [Auto] Number of PCI Segments [Auto] CCM Throttler [Auto] Clean Victim FTI Cmd Balancing [Auto] CXL Strongly Ordered Writes [Disable] Enhanced Partial Writes to Same Address [Auto]	
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options		
Menu Fields	Settings	Comments
Memory Addressing	Select sub-menu	Memory Addressing
ACPI	Select sub-menu	ACPI
Link	Select sub-menu	Link
SDCI	Select sub-menu	SDCI
Probe Filter	Select sub-menu	Probe Filter
DF Watch Timer Interval	[Auto]	Configure the Data Fabric watchdog timer interval.
	[41 ms]	
	[166 ms]	
	[334 ms]	
	[669 ms]	
	[1.34 seconds]	
	[2.68 seconds]	
Disable DF to external IP SyncFloodPropagation	[Auto]	Disable SyncFlood to UMC & downstream slaves.
	[Sync flood disabled]	
	[Sync flood enabled]	

Advanced \ AMD CBS \ DF Common Options		
Menu Fields	Settings	Comments
Sync Flood Propagation to DF Components	[Sync flood disabled] [Sync flood enabled] [Auto]	Control DF::PIEConfig[DisSyncFloodProp]
Freeze DF module queues on error	[Disabled] [Enabled] [Auto]	Controls DF::DfGlobalCtrl [DisImmSyncFloodOnFatalError] Disabling this option sets DF::DfGlobalCtrl [DisImmsyncFloodOnFatalError]
CC6 memory region encryption	[Disabled] [Enabled] [Auto]	Control Whether or not the CC6 save/restore memory is encrypted
CCD B/W Balance Throttle Level	[Auto] [Level 0] [Level 1] [Level 2] [Level 3] [Level 4]	Enables throttling of memory traffic pre CCD. Increased throttling can reduce imbalance across CCDs (expected to be rare).
Number of PCI Segments	[1 Segment] [2 Segments] [4 Segments] [Auto]	No help string
CCM Throttler	[Auto] [Enabled] [Disabled]	Limit peak CCM throughput
Clean Victim FTI Cmd Balancing	[Disabled] [Enabled] [Auto]	Control Clean Victim FTI Cmd Balancing feature
CXL Strongly Ordered Writes	[Disabled] [One at a time]	Determines how the host treats Strongly ordered Writes(ItoMWr and MemWr) from CXL.cache devices. When disabled is chosen Strongly ordered Writes are downgraded to Weakly ordered Writes within the host. When one at a time is chosen the host throttles processing Strongly ordered Writes to a one at a time cadence.
Enhanced Partial Writes to Same Address	[Disabled] [Enabled] [Auto]	Controls enhanced writes to the same address for requests less than 64B.

6.2.4.2.1 Memory Addressing

Aptio Setup - AMI	
Advanced	
Memory Addressing	
NUMA nodes pre socket	[Auto]
Memory Interleaving	[Auto]
Mixed interleaving mode	[Auto]
CXL memory interleaving	[Auto]
CXL Sublink interleaving	[Auto]
DRAM map inversion	[Auto]
Location of private memory regions	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Memory Addressing		
Menu Fields	Settings	Comments
NUMA nodes pre socket	[NPS1] [NPS2] [NPS4] [Auto]	Specifies the number of desired NUMA nodes pre socket, Zero will attempt to interleave the two sockets together.
Memory Interleaving	[Disabled] [Enabled] [Auto]	Allows for disabling memory interleaving. Note that NUMA nodes pre socket will be honored regardless of this setting.
Mixed interleaving mode	[Disabled] [Enabled] [Auto]	Allow for interleaving UMC and CXL together.
CXL memory interleaving	[Disabled] [Enabled] [Auto]	Allows for enabling/disabling CXL memory devices interleaving. Option inactive when 'CXL Memory Online/offline' is enabled.
CXL Sublink interleaving	[Enable] [Disable] [Auto]	Enable or disable CXL sublink interleaving. Option inactive when 'CXL Memory Online/offline' is enabled.

Advanced \ AMD CBS \ DF Common Options \ Memory Addressing		
Menu Fields	Settings	Comments
DRAM map inversion	[Disabled] [Enabled] [Auto]	Inverting the map will cause the highest memory channels to get assigned the lowest addresses in the system
Location of private memory regions	[Distributed] [Consolidated] [Auto]	Controls whether or not the private memory regions (PSP, SMU and CC6) are at the top of DRAM, at the top of 1st DRAM pair or distributed. Note that distributed requires memory on all dies. Note that it will always be at the top of DRAM if some dies do not have memory regardless of this option's setting. Also, Consolidation to 1st DRAM pair is only valid in the no-interleaved case.

6.2.4.2.2 ACPI

Advanced

Aptio Setup - AMI

ACPI

ACPI SRAT L3 Cache As NUMA Domain [Auto]

ACPI SLIT Distance Control [Auto]

ACPI SLIT remote relative distance [Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ ACPI		
Menu Fields	Settings	Comments
ACPI SRAT L3 Cache As NUMA Domain	[Disabled]	Enabled: Each CCX in the system will be declared as a separate NUMA domain. Disabled: Memory Addressing NUMA nodes per socket will be declared.
	[Enabled]	
	[Auto]	
ACPI SLIT Distance Control	[Manual] [Auto]	Determines how the SLIT distances are declared.
ACPI SLIT remote relative distance	[Near]	Set the remote socket distance for 2P System as near (2.8) or far (3.2).
	[Far]	
	[Auto]	

6.2.4.2.3 Link

Aptio Setup - AMI		
Advanced		
Link		
GMI encryption control	[Auto]	
xGMI encryption control	[Auto]	
xGMI Lin Configuration	[Auto]	
4-link xGMI max speed	[Auto]	
3-link xGMI max speed	[Auto]	
xGMI CRC Scale	7	
xGMI CRC Threshold	25	
xGMI Preset Control	[Enabled]	
▶ xGMI Global Preset List		
▶ xGMI Initial Preset		
▶ xGMI TXEQ Search Mask		
▶ xGMI AC/DC Coupled Link		
▶ xGMI Channel Type		
xGMI Training Err Mask	[Auto]	
		→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ Link		
Menu Fields	Settings	Comments
GMI encryption control	[Disabled] [Enabled] [Auto]	Control GMI link encryption. Program GMI key to enabling encryption.
xGMI encryption control	[Disabled] [Enabled] [Auto]	Control XGMI link encryption. Program XGMI key to enabling encryption.
xGMI Lin Configuration	[Auto] [3 xGMI Links] [4 xGMI Links] [2 xGMI Links + 2PCI Links]	Configures the number of XGMI2 link used on a multi-socket system.
4-link xGMI max speed	[20Gbps] [25Gbps] [32Gbps] [Auto]	Specifies the max frequency used for XGMI PState in a 4-link topology.
3-link xGMI max speed	[20Gbps] [25Gbps] [32Gbps]	Specifies the max frequency used for XGMI PState in a 3-link topology.

Advanced \ AMD CBS \ DF Common Options \ Link		
Menu Fields	Settings	Comments
	[Auto]	
xGMI CRC Scale	x	Configure leaky bucket scale for XGMI and WAFL CRC errors. Every scale milliseconds an error will leak from the CRC counter.
xGMI CRC Threshold	x	Configure leaky bucket threshold for XGMI and WAFL CRC error. If link CRC counter exceeds this threshold, an error will be logged.
xGMI Preset Control	[Disabled] [Enabled] [Auto]	Enable/Disable XGMI Preset Control options
xGMI Global Preset List	Selects sub-menu	xGMI Global Preset List
xGMI Initial Preset	Selects sub-menu	xGMI Initial Preset
xGMI TXEQ Search Mask	Selects sub-menu	xGMI TXEQ Search Mask
xGMI AC/DC Coupled Link	Selects sub-menu	xGMI AC/DC Coupled Link
xGMI Channel Type	Selects sub-menu	xGMI Channel Type
xGMI Training Err Mask	[Disabled] [Enabled] [Auto]	Enable/Disable XGMI training err mask

6.2.4.2.3.1 xGMI Global Preset List

Aptio Setup - AMI

Advanced

xGMI Global Preset List

▶ Preset P11

▶ Preset P12

▶ Preset P13

▶ Preset P14

▶ Preset P15

→ ← :Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Global Preset List		
Menu Fields	Settings	Comments
Preset P11	Selects sub-menu	Preset P11
Preset P12	Selects sub-menu	Preset P12
Preset P13	Selects sub-menu	Preset P13
Preset P14	Selects sub-menu	Preset P14
Preset P15	Selects sub-menu	Preset P15

6.2.4.2.3.2 xGMI Initial Preset

Aptio Setup - AMI	
Advanced	
xGMI Initial Preset	
▶ Initial Preset Socket 0 Link 0 ▶ Initial Preset Socket 0 Link 1 ▶ Initial Preset Socket 0 Link 2 ▶ Initial Preset Socket 0 Link 3 ▶ Initial Preset Socket 1 Link 0 ▶ Initial Preset Socket 1 Link 1 ▶ Initial Preset Socket 1 Link 2 ▶ Initial Preset Socket 1 Link 3	→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset		
Menu Fields	Settings	Comments
Initial Preset Socket 0 Link 0	Selects sub-menu	Initial Preset Socket 0 Link 0
Initial Preset Socket 0 Link 1	Selects sub-menu	Initial Preset Socket 0 Link 1
Initial Preset Socket 0 Link 2	Selects sub-menu	Initial Preset Socket 0 Link 2
Initial Preset Socket 0 Link 3	Selects sub-menu	Initial Preset Socket 0 Link 3
Initial Preset Socket 1 Link 0	Selects sub-menu	Initial Preset Socket 1 Link 0
Initial Preset Socket 1 Link 1	Selects sub-menu	Initial Preset Socket 1 Link 1
Initial Preset Socket 1 Link 2	Selects sub-menu	Initial Preset Socket 1 Link 2
Initial Preset Socket 1 Link 3	Selects sub-menu	Initial Preset Socket 1 Link 3

6.2.4.2.3.2.1 Initial Preset Socket 0 Link 0

Aptio Setup - AMI	
Advanced	
Initial Preset Socket 0 Link 0	
Initial Preset Socket 0 Link 0 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 0 Link 0 Pstate0	4
Initial Preset Socket 0 Link 0 Pstate1	4
Initial Preset Socket 0 Link 0 Pstate2	4
Initial Preset Socket 0 Link 0 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 0		
Menu Fields	Settings	Comments
Initial Preset Socket 0 Link 0 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 0 Pstate0
Initial Preset Socket 0 Link 0 Pstate1	X	Enable/Disable Initial Preset Socket 0 Link 0 Pstate1
Initial Preset Socket 0 Link 0 Pstate2	X	Enable/Disable Initial Preset Socket 0 Link 0 Pstate2
Initial Preset Socket 0 Link 0 Pstate3	x	Enable/Disable Initial Preset Socket 0 Link 0 Pstate3

6.2.4.2.3.2.2 Initial Preset Socket 0 Link 1

Aptio Setup - AMI	
Advanced	
Initial Preset Socket 0 Link 1	
Initial Preset Socket 0 Link 1 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 0 Link 1 Pstate0	4
Initial Preset Socket 0 Link 1 Pstate1	4
Initial Preset Socket 0 Link 1 Pstate2	4
Initial Preset Socket 0 Link 1 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 1		
Menu Fields	Settings	Comments
Initial Preset Socket 0 Link 1 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 1 Pstate0
Initial Preset Socket 0 Link 1 Pstate1	X	Enable/Disable Initial Preset Socket 0 Link 1 Pstate1
Initial Preset Socket 0 Link 1 Pstate2	X	Enable/Disable Initial Preset Socket 0 Link 1 Pstate2
Initial Preset Socket 0 Link 1 Pstate3	x	Enable/Disable Initial Preset Socket 0 Link 1 Pstate3

6.2.4.2.3.2.3 Initial Preset Socket 0 Link 2

Aptio Setup - AMI	
Advanced	
Initial Preset Socket 0 Link 2	
Initial Preset Socket 0 Link 2 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 0 Link 2 Pstate0	4
Initial Preset Socket 0 Link 2 Pstate1	4
Initial Preset Socket 0 Link 2 Pstate2	4
Initial Preset Socket 0 Link 2 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 2		
Menu Fields	Settings	Comments
Initial Preset Socket 0 Link 2 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 2 Pstate0
Initial Preset Socket 0 Link 2 Pstate1	X	Enable/Disable Initial Preset Socket 0 Link 2 Pstate1
Initial Preset Socket 0 Link 2 Pstate2	X	Enable/Disable Initial Preset Socket 0 Link 2 Pstate2
Initial Preset Socket 0 Link 2 Pstate3	x	Enable/Disable Initial Preset Socket 0 Link 2 Pstate3

6.2.4.2.3.2.4 Initial Preset Socket 0 Link 3

Aptio Setup - AMI	
Advanced	
Initial Preset Socket 0 Link 3	
Initial Preset Socket 0 Link 3 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 0 Link 3 Pstate0	4
Initial Preset Socket 0 Link 3 Pstate1	4
Initial Preset Socket 0 Link 3 Pstate2	4
Initial Preset Socket 0 Link 3 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 3		
Menu Fields	Settings	Comments
Initial Preset Socket 0 Link 3 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 3 Pstate0
Initial Preset Socket 0 Link 3 Pstate1	X	Enable/Disable Initial Preset Socket 0 Link 3 Pstate1
Initial Preset Socket 0 Link 3 Pstate2	X	Enable/Disable Initial Preset Socket 0 Link 3 Pstate2
Initial Preset Socket 0 Link 3 Pstate3	x	Enable/Disable Initial Preset Socket 0 Link 3 Pstate3

6.2.4.2.3.2.5 Initial Preset Socket 1 Link 0

Aptio Setup - AMI	
Advanced	
Initial Preset Socket 1 Link 0	
Initial Preset Socket 1 Link 0 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 1 Link 0 Pstate0	4
Initial Preset Socket 1 Link 0 Pstate1	4
Initial Preset Socket 1 Link 0 Pstate2	4
Initial Preset Socket 1 Link 0 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 1 Link 0		
Menu Fields	Settings	Comments
Initial Preset Socket 1 Link 0 Pstate0	X	Enable/Disable Initial Preset Socket 1 Link 0 Pstate0
Initial Preset Socket 1 Link 0 Pstate1	X	Enable/Disable Initial Preset Socket 1 Link 0 Pstate1
Initial Preset Socket 1 Link 0 Pstate2	X	Enable/Disable Initial Preset Socket 1 Link 0 Pstate2
Initial Preset Socket 1 Link 0 Pstate3	x	Enable/Disable Initial Preset Socket 1 Link 0 Pstate3

6.2.4.2.3.2.6 Initial Preset Socket 1 Link 1

Aptio Setup – AMI	
Advanced	
Initial Preset Socket 1 Link 1	
Initial Preset Socket 1 Link 1 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 1 Link 1 Pstate0	4
Initial Preset Socket 1 Link 1 Pstate1	4
Initial Preset Socket 1 Link 1 Pstate2	4
Initial Preset Socket 1 Link 1 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 1 Link 1		
Menu Fields	Settings	Comments
Initial Preset Socket 1 Link 1 Pstate0	X	Enable/Disable Initial Preset Socket 1 Link 1 Pstate0
Initial Preset Socket 1 Link 1 Pstate1	X	Enable/Disable Initial Preset Socket 1 Link 1 Pstate1
Initial Preset Socket 1 Link 1 Pstate2	X	Enable/Disable Initial Preset Socket 1 Link 1 Pstate2
Initial Preset Socket 1 Link 1 Pstate3	x	Enable/Disable Initial Preset Socket 1 Link 1 Pstate3

6.2.4.2.3.2.7 Initial Preset Socket 1 Link 2

Aptio Setup – AMI	
Advanced	
Initial Preset Socket 1 Link 2	
Initial Preset Socket 1 Link 2 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 1 Link 2 Pstate0	4
Initial Preset Socket 1 Link 2 Pstate1	4
Initial Preset Socket 1 Link 2 Pstate2	4
Initial Preset Socket 1 Link 2 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 1 Link 2		
Menu Fields	Settings	Comments
Initial Preset Socket 1 Link 2 Pstate0	X	Enable/Disable Initial Preset Socket 1 Link 2 Pstate0
Initial Preset Socket 1 Link 2 Pstate1	X	Enable/Disable Initial Preset Socket 1 Link 2 Pstate1
Initial Preset Socket 1 Link 2 Pstate2	X	Enable/Disable Initial Preset Socket 1 Link 2 Pstate2
Initial Preset Socket 1 Link 2 Pstate3	x	Enable/Disable Initial Preset Socket 1 Link 2 Pstate3

6.2.4.2.3.2.8 Initial Preset Socket 1 Link 3

Aptio Setup – AMI	
Advanced	
Initial Preset Socket 1 Link 3	
Initial Preset Socket 1 Link 3 Pstate0/1/2/3 (APCB)	4444
Initial Preset Socket 1 Link 3 Pstate0	4
Initial Preset Socket 1 Link 3 Pstate1	4
Initial Preset Socket 1 Link 3 Pstate2	4
Initial Preset Socket 1 Link 3 Pstate3	4
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 1 Link 3		
Menu Fields	Settings	Comments
Initial Preset Socket 1 Link 3 Pstate0	X	Enable/Disable Initial Preset Socket 1 Link 3 Pstate0
Initial Preset Socket 1 Link 3 Pstate1	X	Enable/Disable Initial Preset Socket 1 Link 3 Pstate1
Initial Preset Socket 1 Link 3 Pstate2	X	Enable/Disable Initial Preset Socket 1 Link 3 Pstate2
Initial Preset Socket 1 Link 3 Pstate3	x	Enable/Disable Initial Preset Socket 1 Link 3 Pstate3

6.2.4.2.3.3 xGMI TXEQ Search Mask

Aptio Setup – AMI	
Advanced	xGMI TXEQ Search Mask ▶ TXEQ Search Mask Socket 0 Link 0 ▶ TXEQ Search Mask Socket 0 Link 1 ▶ TXEQ Search Mask Socket 0 Link 2 ▶ TXEQ Search Mask Socket 0 Link 3 ▶ TXEQ Search Mask Socket 1 Link 0 ▶ TXEQ Search Mask Socket 1 Link 1 ▶ TXEQ Search Mask Socket 1 Link 2 ▶ TXEQ Search Mask Socket 1 Link 3 → ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 0 Link 0	Selects sub-menu	TXEQ Search Mask Socket 0 Link 0
TXEQ Search Mask Socket 0 Link 1	Selects sub-menu	TXEQ Search Mask Socket 0 Link 1
TXEQ Search Mask Socket 0 Link 2	Selects sub-menu	TXEQ Search Mask Socket 0 Link 2
TXEQ Search Mask Socket 0 Link 3	Selects sub-menu	TXEQ Search Mask Socket 0 Link 3
TXEQ Search Mask Socket 1 Link 0	Selects sub-menu	TXEQ Search Mask Socket 1 Link 0
TXEQ Search Mask Socket 1 Link 1	Selects sub-menu	TXEQ Search Mask Socket 1 Link 1
TXEQ Search Mask Socket 1 Link 2	Selects sub-menu	TXEQ Search Mask Socket 1 Link 2
TXEQ Search Mask Socket 1 Link 3	Selects sub-menu	TXEQ Search Mask Socket 1 Link 3

6.2.4.2.3.3.1 TXEQ Search Mask Socket 0 Link 0

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 0 Link 0	
TXEQ Search Mask Socket 0 Link 0 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 0 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 0 Pstate0	7A
TXEQ Search Mask Socket 0 Link 0 Pstate1	7A
TXEQ Search Mask Socket 0 Link 0 Pstate2	7A
TXEQ Search Mask Socket 0 Link 0 Pstate3	7A
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 0		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 0 Link 0 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 0 Pstate0
TXEQ Search Mask Socket 0 Link 0 Pstate1	X	Enable/Disable TXEQ Search Make Socket 0 Link 0 Pstate1
TXEQ Search Mask Socket 0 Link 0 Pstate2	X	Enable/Disable TXEQ Search Make Socket 0 Link 0 Pstate2
TXEQ Search Mask Socket 0 Link 0 Pstate3	X	Enable/Disable TXEQ Search Make Socket 0 Link 0 Pstate3

6.2.4.2.3.3.2 TXEQ Search Mask Socket 0 Link 1

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 0 Link 1	
TXEQ Search Mask Socket 0 Link 1 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 1 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 1 Pstate0	7A
TXEQ Search Mask Socket 0 Link 1 Pstate1	7A
TXEQ Search Mask Socket 0 Link 1 Pstate2	7A
TXEQ Search Mask Socket 0 Link 1 Pstate3	7A
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 0 Link 1 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate0
TXEQ Search Mask Socket 0 Link 1 Pstate1	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate1
TXEQ Search Mask Socket 0 Link 1 Pstate2	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate2
TXEQ Search Mask Socket 0 Link 1 Pstate3	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate3

6.2.4.2.3.3 TXEQ Search Mask Socket 0 Link 2

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 0 Link 2 TXEQ Search Mask Socket 0 Link 2 Pstate 0/1 AP CB TXEQ Search Mask Socket 0 Link 2 Pstate 2/3 AP CB TXEQ Search Mask Socket 0 Link 2 Pstate0 TXEQ Search Mask Socket 0 Link 2 Pstate1 TXEQ Search Mask Socket 0 Link 2 Pstate2 TXEQ Search Mask Socket 0 Link 2 Pstate3 7A007A 7A007A 7A 7A 7A 7A	
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 2		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 0 Link 2 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 2 Pstate0
TXEQ Search Mask Socket 0 Link 2 Pstate1	X	Enable/Disable TXEQ Search Make Socket 0 Link 2 Pstate1
TXEQ Search Mask Socket 0 Link 2 Pstate2	X	Enable/Disable TXEQ Search Make Socket 0 Link 2 Pstate2
TXEQ Search Mask Socket 0 Link 2 Pstate3	X	Enable/Disable TXEQ Search Make Socket 0 Link 2 Pstate3

6.2.4.2.3.3.4 TXEQ Search Mask Socket 0 Link 3

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 0 Link 3	
TXEQ Search Mask Socket 0 Link 3 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 3 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 0 Link 3 Pstate0	7A
TXEQ Search Mask Socket 0 Link 3 Pstate1	7A
TXEQ Search Mask Socket 0 Link 3 Pstate2	7A
TXEQ Search Mask Socket 0 Link 3 Pstate3	7A
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 3		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 0 Link 3 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 3 Pstate0
TXEQ Search Mask Socket 0 Link 3 Pstate1	X	Enable/Disable TXEQ Search Make Socket 0 Link 3 Pstate1
TXEQ Search Mask Socket 0 Link 3 Pstate2	X	Enable/Disable TXEQ Search Make Socket 0 Link 3 Pstate2
TXEQ Search Mask Socket 0 Link 3 Pstate3	X	Enable/Disable TXEQ Search Make Socket 0 Link 3 Pstate3

6.2.4.2.3.3.5 TXEQ Search Mask Socket 1 Link 0

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 1 Link 0	
TXEQ Search Mask Socket 1 Link 0 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 0 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 0 Pstate0	7A
TXEQ Search Mask Socket 1 Link 0 Pstate1	7A
TXEQ Search Mask Socket 1 Link 0 Pstate2	7A
TXEQ Search Mask Socket 1 Link 0 Pstate3	7A
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 1 Link 0		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 1 Link 0 Pstate0	X	Enable/Disable TXEQ Search Make Socket 1 Link 0 Pstate0
TXEQ Search Mask Socket 1 Link 0 Pstate1	X	Enable/Disable TXEQ Search Make Socket 1 Link 0 Pstate1
TXEQ Search Mask Socket 1 Link 0 Pstate2	X	Enable/Disable TXEQ Search Make Socket 1 Link 0 Pstate2
TXEQ Search Mask Socket 1 Link 0 Pstate3	X	Enable/Disable TXEQ Search Make Socket 1 Link 0 Pstate3

6.2.4.2.3.3.6 TXEQ Search Mask Socket 1 Link 1

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 1 Link 1	
TXEQ Search Mask Socket 1 Link 1 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 1 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 1 Pstate0	7A
TXEQ Search Mask Socket 1 Link 1 Pstate1	7A
TXEQ Search Mask Socket 1 Link 1 Pstate2	7A
TXEQ Search Mask Socket 1 Link 1 Pstate3	7A
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 1 Link 1		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 1 Link 1 Pstate0	X	Enable/Disable TXEQ Search Make Socket 1 Link 1 Pstate0
TXEQ Search Mask Socket 1 Link 1 Pstate1	X	Enable/Disable TXEQ Search Make Socket 1 Link 1 Pstate1
TXEQ Search Mask Socket 1 Link 1 Pstate2	X	Enable/Disable TXEQ Search Make Socket 1 Link 1 Pstate2
TXEQ Search Mask Socket 1 Link 1 Pstate3	X	Enable/Disable TXEQ Search Make Socket 1 Link 1 Pstate3

6.2.4.2.3.3.7 TXEQ Search Mask Socket 1 Link 2

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 1 Link 2	
TXEQ Search Mask Socket 1 Link 2 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 2 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 2 Pstate0	7A
TXEQ Search Mask Socket 1 Link 2 Pstate1	7A
TXEQ Search Mask Socket 1 Link 2 Pstate2	7A
TXEQ Search Mask Socket 1 Link 2 Pstate3	7A
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 1 Link 2		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 1 Link 2 Pstate0	X	Enable/Disable TXEQ Search Make Socket 1 Link 2 Pstate0
TXEQ Search Mask Socket 1 Link 2 Pstate1	X	Enable/Disable TXEQ Search Make Socket 1 Link 2 Pstate1
TXEQ Search Mask Socket 1 Link 2 Pstate2	X	Enable/Disable TXEQ Search Make Socket 1 Link 2 Pstate2
TXEQ Search Mask Socket 1 Link 2 Pstate3	X	Enable/Disable TXEQ Search Make Socket 1 Link 2 Pstate3

6.2.4.2.3.3.8 TXEQ Search Mask Socket 1 Link 3

Aptio Setup – AMI	
Advanced	
TXEQ Search Mask Socket 1 Link 3	
TXEQ Search Mask Socket 1 Link 3 Pstate 0/1 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 3 Pstate 2/3 AP CB	7A007A
TXEQ Search Mask Socket 1 Link 3 Pstate0	7A
TXEQ Search Mask Socket 1 Link 3 Pstate1	7A
TXEQ Search Mask Socket 1 Link 3 Pstate2	7A
TXEQ Search Mask Socket 1 Link 3 Pstate3	7A
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 1 Link 3		
Menu Fields	Settings	Comments
TXEQ Search Mask Socket 1 Link 3 Pstate0	X	Enable/Disable TXEQ Search Make Socket 1 Link 3 Pstate0
TXEQ Search Mask Socket 1 Link 3 Pstate1	X	Enable/Disable TXEQ Search Make Socket 1 Link 3 Pstate1
TXEQ Search Mask Socket 1 Link 3 Pstate2	X	Enable/Disable TXEQ Search Make Socket 1 Link 3 Pstate2
TXEQ Search Mask Socket 1 Link 3 Pstate3	X	Enable/Disable TXEQ Search Make Socket 1 Link 3 Pstate3

6.2.4.2.3.4 xGMI AC/DC Coupled Link

Aptio Setup – AMI

Advanced

xGMI AC/DC Coupled Link

xGMI AC/DC Coupled Link Control

[Auto]

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI AC/DC Coupled Link		
Menu Fields	Settings	Comments
xGMI AC/DC Coupled Link Control	[Manual] [Auto]	Control XGMI AC/DC Coupled Link. Valid value: 0: AC Coupled 1: DC Coupled

6.2.4.2.3.5 xGMI Channel Type

Advanced

Aptio Setup – AMI

xGMI Channel Type

xGMI Chanel Type Control

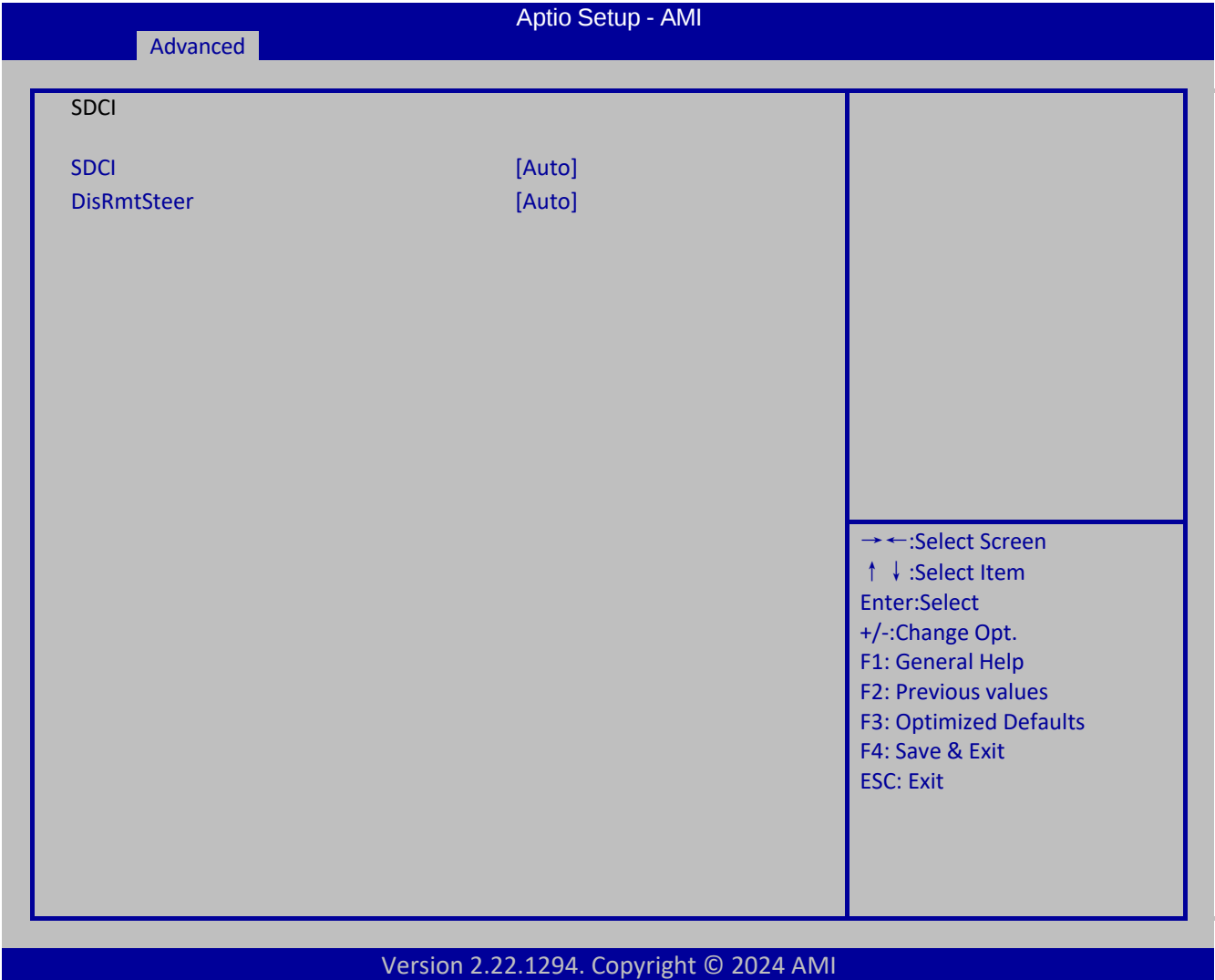
[Auto]

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Channel Type		
Menu Fields	Settings	Comments
xGMI Channel Type Control	[Manual] [Auto]	Control XGMI Channel Type. Valid Channel Type: 0: Disable 1: Long Reach

6.2.4.2.4 SDCI



Advanced \ AMD CBS \ DF Common Options \ SDCI		
Menu Fields	Settings	Comments
SDCI	[Disabled] [Enabled] [Auto]	Enable or Disable smart Data Cache Injection feature.
DisRmtSteer	[Disabled] [Enabled] [Auto]	When set, this bit disables the sending of steering probes to remote socket.

6.2.4.2.5 Probe Filter

Aptio Setup - AMI

Advanced

Probe Filter

Organization

[Auto]

Periodic Directory Rinse (PDR) Tuning

[Auto]

Tracking Granularity

[Auto]

PDR Mode

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ DF Common Options \ Probe Filter		
Menu Fields	Settings	Comments
Organization	[Auto] [Dedicated] [Shared]	Specifies whether multiple memory/CXL Channels will share probe filter storage. For memory sizes of 16TB or larger , this feature is ignored as it is auto-selected to 'shared'
Periodic Directory Rinse (PDR) Tuning	[Periodic] [Blended] [Auto]	Control PDR Settings that may impact performance by workload and/or processor. Periodic (RefClock Based Floss Only): Rate based Directory Rinse. Blended (Cache Load Based Floss with Background RefClock Based Floss): Demand based Directory Rinse.
Tracking Granularity	[Finer-Grain] [Coarser-Grain] [Auto]	Finer-Grain tracking enables higher memory efficiency and is expected to be the preferred performance option. Coarser-grain tracking may improve memory performance for a narrow set of workloads.

Advanced \ AMD CBS \ DF Common Options \ Probe Filter		
Menu Fields	Settings	Comments
PDR Mode	[Auto] [Selective] [All]	Selective: [Recommended setting] Rinsing applied only to the minimum set of memory addresses. All: Rinsing applied to all memory addresses.

6.2.4.3 UMC Common Options

Aptio Setup - AMI

Advanced

UMC Common Options

- ▶ DDR Addressing Options
- ▶ DDR Controller Configuration
- ▶ DDR MBIST Options
- ▶ DDR RAS
- ▶ DDR Bus Configuration
- ▶ DDR Timing Configuration
- ▶ DDR Training Options
- ▶ DDR Security
- ▶ DDR PMIC Configuration
- ▶ DDR Thermal Throttling
- ▶ DDR Miscellaneous

→ ← :Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options		
Menu Fields	Settings	Comments
DDR Addressing Options	Selects sub-menu.	
DDR Controller Configuration	Selects sub-menu.	
DDR MBIST Options	Selects sub-menu.	
DDR RAS	Selects sub-menu.	
DDR Bus Configuration	Selects sub-menu.	
DDR Timing Configuration	Selects sub-menu.	
DDR Training Options	Selects sub-menu.	
DDR Security	Selects sub-menu.	
DDR PMIC Configuration	Selects sub-menu.	
DDR Thermal Throttling	Selects sub-menu.	
DDR Miscellaneous	Selects sub-menu.	

6.2.4.3.1 DDR Addressing Options

Aptio Setup - AMI	
Advanced	
DDR Addressing Options	
Chipselect Interleaving	[Auto]
Address Hash Bank	[Auto]
Address Hash CS	[Auto]
Address Hash Rm	[Auto]
Address Hash Subchannel	[Auto]
BankSwapMode	[Auto]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Addressing Options		
Menu Fields	Settings	Comments
Chipselect Interleaving	[Disabled] [Auto]	Interleave memory blocks across the DRAM chip selects for node 0.
Address Hash Bank	[Disabled] [Enabled] [Auto]	Enable or disable bank address hashing
Address Hash CS	[Auto] [Enabled] [Disabled]	Enable or disable CS address hashing
Address Hash Rm	[Auto] [Enabled] [Disabled]	Enable or disable RM address hashing
Address Hash Subchannel	[Auto] [Enabled] [Disabled]	Enable or disable Sub-Channel address hashing
BankSwapMode	[Auto] [Disabled] [Swap CPU]	BankSwapMode value: 0 = Disable, 1 = SwapCPU

6.2.4.3.2 DDR Controller Configuration

Aptio Setup - AMI	
Advanced	
DDR Controller Configuration ▶ DDR Power Options ▶ Memory Channel Disable ▶ Refresh Management (RFM) Memory Context Restore [Auto] DRAM Survives Warm Reset [Disabled]	
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration		
Menu Fields	Settings	Comments
DDR Power Options	Selects sub-menu.	
Memory Channel Disable	Selects sub-menu.	
Refresh Management (RFM)	Selects sub-menu.	
Memory Context Restore	[Auto] [Enabled] [Disabled]	Configure the memory context restore mode. When enabled, DRAM re-retraining is avoided when possible and the POST latency is minimized.
DRAM Survives Warm Reset	[Disabled] [Enabled]	1 - Enabled (default) 0 – Disabled If enabled – Upon warm reset DRAM content is preserved. Training values are saved & retrived.

6.2.4.3.2.1 DDR Power Options

Aptio Setup - AMI	
Advanced	
DDR Power Options	
Power Down Enable	[Auto]
Sub Urgent Refresh Lower Bound	1
Urgent Refresh Limit	4
DRAM Refresh Rate	[3.9 usec]
Self-Refresh Exit Staggering	[n = 9]
DRAM 2x Refresh Temperature Threshold	[85' – 90']
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \ DDR Power Options		
Menu Fields	Settings	Comments
Power Down Enable	[Disabled] [Enabled] [Auto]	Enable or disable DDR power down mode.
Sub Urgent Refresh Lower Bound	X	Specifies the stored refresh limit required to enter Sub-urgent refresh mode Constraint: SubUrgRefLowerBound <= UrgRefLimit Valid value: 6 ~ 1
Urgent Refresh Limit	X	Specifies the stored refresh limit required to enter urgent refresh mode Constraint: SubUrgRefLowerBound <= UrgRefLimit Valid value: 6 ~ 1
DRAM Refresh Rate	[3.9 usec] [1.95 usec]	DRAM refresh rate: 1.95us or 3.9us(default)
Self-Refresh Exit Staggering	[Disabled] [n = 1]	Tcksrx += (Trfc/n * (UMC_Number %3)) Selectable by CBS Option:

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \ DDR Power Options		
Menu Fields	Settings	Comments
	[n = 2] [n = 3] [n = 4] [n = 5] [n = 6] [n = 7] [n = 8] [n = 9]	Disabled Staggering n = 1 <= Stagger channels by ~270 ns n = 2 n = 3 n = 4 . . . n = 9 <= Stagger Channels By ~30 ns (Default)
DRAM 2x Refresh Temperature Threshold	[85' – 90'] [90' – 95'] [95' – 100'] [> 100']	Determine the DDR temperature threshold to activate 2x REF rate per the DRAM MR readout.

6.2.4.3.2.2 Memory Channel Disable

Aptio Setup - AMI

Advanced

Memory Channel Disable

Memory Channel Disable Float Power [Disabled]
Good

Memory Channel Disable Bitmask 0

Socket 0 Channel 0 [Enabled]
Socket 0 Channel 1 [Enabled]
Socket 0 Channel 2 [Enabled]
Socket 0 Channel 3 [Enabled]
Socket 0 Channel 4 [Enabled]
Socket 0 Channel 5 [Enabled]
Socket 0 Channel 6 [Enabled]
Socket 0 Channel 7 [Enabled]
Socket 0 Channel 8 [Enabled]
Socket 0 Channel 9 [Enabled]
Socket 0 Channel 10 [Enabled]
Socket 0 Channel 11 [Enabled]
Socket 1 Channel 0 [Enabled]
Socket 1 Channel 1 [Enabled]
Socket 1 Channel 2 [Enabled]
Socket 1 Channel 3 [Enabled]
Socket 1 Channel 4 [Enabled]
Socket 1 Channel 5 [Enabled]
Socket 1 Channel 6 [Enabled]
Socket 1 Channel 7 [Enabled]
Socket 1 Channel 8 [Enabled]
Socket 1 Channel 9 [Enabled]
Socket 1 Channel 10 [Enabled]
Socket 1 Channel 11 [Enabled]

→ ←: Select Screen
↑ ↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \Memory Channel Disable		
Menu Fields	Settings	Comments
Memory Channel Disable Float Power	[Disabled]	Float Power Good When Channel is disabled by BIOS setup options.
Good	[Enabled]	
Memory Channel Disable Bitmask	X	
Socket 0 Channel 0	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 1	[Disabled] [Enabled]	
Socket 0 Channel 2	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 3	[Disabled] [Enabled]	
Socket 0 Channel 4	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 5	[Disabled] [Enabled]	

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \Memory Channel Disable		
Menu Fields	Settings	Comments
Socket 0 Channel 6	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 7	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 8	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 9	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 10	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 0 Channel 11	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 0	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 1	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 2	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 3	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 4	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 5	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 6	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 7	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 8	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 9	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 10	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.
Socket 1 Channel 11	[Disabled] [Enabled]	SPD reading will be skipped when channel is disabled.

6.2.4.3.2.3 Refresh Management (RFM)

Aptio Setup - AMI	
Advanced	
Refresh Management (RFM)	
Refresh Management	[Auto]
Adaptive Refresh Management	[Auto]
RAA Initial Management Threshold	[Auto]
RAA Maximum Management Threshold	[Auto]
RAA Refresh Decrement Multiplier	[Auto]
DRFM Enable	[Auto]
Bounded Refresh Configuration	[BRC4]
DRFM Hash Enable	[Auto]
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \ Refresh Management (RFM)		
Menu Fields	Settings	Comments
Refresh Management	[Auto] [Disable] [Enable] [Force Enable]	Auto Disable: Disable RFM for all Ranks. Enable: Enable RFM for Ranks which support RFM. Force Enable: Enable RFM for all Ranks regardless of support. Selecting 'Force Enable' will cause REFpb/REFsb to be disabled if all ranks do not support RFM<
Adaptive Refresh Management	[Auto] [Disable] [ARFM Level A] [ARFM Level B] [ARFM Level C]	Apply the Settings for RAAIMT, RAAMMT, and RefDecrement which are associated with the selected level.
RAA Initial Management Threshold	[Auto] [32] [40] [48] [56]	Override Rolling Accumulated ACT Initial Management Threshold Auto: BIOS will choose the lowest supported value from SPD.

Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \ Refresh Management (RFM)		
Menu Fields	Settings	Comments
	[64] [72] [80]	Choices from list are for Normal Refresh Mode. In Fine Granularity Mode, the value will be divided by 2
RAA Maximum Management Threshold	[Auto] [3X] [4X] [5X] [6X]	Override Rolling Accumulated ACT Maximum Management Threshold Auto: BIOS will choose the lowest supported value from SPD. Choices from list are for Normal Refresh Mode. Logic handles adjustment for Fine Granularity Mode
RAA Refresh Decrement Multiplier	[Auto] [0.5] [1]	Override RAA Refresh Decrement Multiplier Auto: BIOS will choose the lowest supported value from SPD
DRFM Enable	[Auto] [Disable] [Enable]	Enable DRFM for any ranks that support it. (Enable/Disable)
Bounded Refresh Configuration	[BRC2] [BRC3] [BRC4]	Set Bounded Refresh Configuration Level. The selected level will be used for each rank that supports it. For ranks that only support a BRC of 2, then 2 will be used regardless of this selection.
DRFM Hash Enable	[Auto] [Disable] [Enable]	Enable DRFM Hashing for all channels

6.2.4.3.3 DDR MBIST Options

Aptio Setup - AMI	
Advanced	
DDR MBIST Options	
MBIST Enable	[Auto]
MBIST Test Mode	[Auto]
MBIST Aggressors	[Auto]
DDR Healing BIST	[Disabled]
DDR Healing BIST Execution Mode	[One Time]
DDR Healing BIST Repair Type	[Soft Repair]
▶ Data Eye	
→ ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options		
Menu Fields	Settings	Comments
MBIST Enable	[Disabled] [Enabled] [Auto]	Enable or disable Memory MBIST
MBIST Test Mode	[Interface Mode] [Data Eye Mode] [Both] [Auto]	Select MBIST Test Mode – Interface Mode (Tests Single and Multiple CS transactions and Basic Connectivity) or Data Eye Mode (Measures Voltage vs. Timing)
MBIST Aggressors	[Disabled] [Enabled] [Auto]	Enable or disable MBIST Aggressor test
DDR Healing BIST	[Disabled] [PMU Mem BIST] [Self-Healing Mem BIST] [PMU and Self-Healing Mem BIST]	This item enables a full memory test. Please note that this is a memory content test and is separate and distinct from the MBIST test of Interface and Data Eye. PMU Mem BIST: this uses PMU firmware to test memory on all channels simultaneously. Failing

Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options		
Menu Fields	Settings	Comments
		memory will be repaired using soft or hard PPR depending on the PPR configuration. Self-Healing Mem BIST: this runs the JEDEC DRAM self healing, if the device and DIMM support the feature. The DRAM will do a hard repair for failing memory. PMU and Self-Healing Mem BIST: this option runs the PMU Mem BIST then the Self-Healing Mem BIST tests sequentially.
DDR Healing BIST Execution Mode	[One Time] [Every Boot]	[One Time]: DDR Healing BIST will only be executed one time. [Every Boot]: DDR Healing BIST will be executed on every boot.
DDR Healing BIST Repair Type	[Soft Repair] [Hard Repair] [No Repairs – Test only]	For DRAM errors found in the BIOS memory BIST select the repair type, soft, hard or test only and do not attempt to repair.
Data Eye	Selects Sub-menu	

6.2.4.3.3.1 Data Eye

Aptio Setup - AMI	
Advanced	
Data Eye	
Pattern Select	[PRBS]
Pattern Length	3
Aggressor Channel	[All Channels]
Aggressor Static Lane Control	[Disable]
Aggressor Static Lane Select Upper 32 Bits	0
Aggressor Static Lane Select Lower 32 Bits	0
Aggressor Static Lane Select ECC	0
Aggressor Static Lane Value	0
Target Static Lane Control	[Disable]
Target Static Lane Select Upper 32 Bits	0
Target Static Lane Select Lower 32 Bits	0
Target Static Lane Select ECC	0
Target Static Lane Value	0
Read Voltage Sweep Step Size	[1]
Read Timing Sweep Step Size	[1]
Write Voltage Sweep Step Size	[1]
Write Timing Sweep Step Size	[1]
Silent Execution	[Disabled]
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options \ Data Eye		
Menu Fields	Settings	Comments
Pattern Select	[PRBS] [SSO] [Both]	MBIST Data Eye Pattern Type. 0 - PRBS (default), 1 - SSO, 2 - Both
Pattern Length	X	This token determine the pattern length, available options: 3...C (input hex number, not decimal)
Aggressor Channel	[One Sub-Channel] [Half Channels] [All Channels]	One Sub-Channel enables the non-target subchannel on the target channel to be an aggressor. Half Channels enables all non-target channels on one half of the processor to be aggressors. All Channels enables all non-target channels to be aggressors.
Aggressor Static Lane Control	[Disabled] [Enabled]	This option, if enabled, will control the Aggressor Static Lane Controls.
Aggressor Static Lane Select Upper 32 Bits	X	Static Lane Select for Upper 32 bits. The bit mask represents the bits to be read

Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options \ Data Eye		
Menu Fields	Settings	Comments
Aggressor Static Lane Select Lower 32 Bits	X	Static Lane Select for Lower 32 bits. The bit mask represents the bits to be read
Aggressor Static Lane Select ECC	X	Static Lane Select for ECC Lanes. The bit mask represents the bits to be read
Aggressor Static Lane Value	X	TBD
Target Static Lane Control	[Disabled] [Enabled]	Enable Mbist Target Static Lane Control
Target Static Lane Select Upper 32 Bits	X	Static Lane Select for Upper 32 bit. The bit mask represents the bits to be read
Target Static Lane Select Lower 32 Bits	X	Static Lane Select for Lower 32 bit. The bit mask represents the bits to be read
Target Static Lane Select ECC	X	TBD
Target Static Lane Value	X	Value for Mbsit target static lane. Enable 'Target Static Lane Control' option to enter the value
Read Voltage Sweep Step Size	[1] [2] [4]	This option determines the step size for Read Data Eye voltage sweep, Supported options are 1,2 and 4
Read Timing Sweep Step Size	[1] [2] [4]	This option supports step size for Read Data Eye. Supported options are 1, 2 and 4
Write Voltage Sweep Step Size	[1] [2] [4]	This option determines the step size for write Data Eye voltage sweep, Supported options are 1,2 and 4
Write Timing Sweep Step Size	[1] [2] [4]	This option supports step size for write Data Eye. Supported options are 1, 2 and 4
Silent Execution	[Disabled] [Enabled]	Execute MBIST Data Eye silently without ABL log output Disabled - MBIST Enable will not be overridden Enabled - Execute MBIST Data Eye silently without ABL log output

6.2.4.3.4 DDR RAS

Aptio Setup - AMI

Advanced

DDR RAS

Data Poisoning [Auto]

DRAM Boot Time Post Package Repair [Disable]

DRAM Runtime Post Package Repair [Disable]

DRAM Post Package Repair Config [In-Band]

Initiator [Auto]

RCD Parity [Disabled]

Write CRC [Disabled]

Read CRC [Auto]

Memory Error Injection [False]

EcsStatus Interrupt [False]

► ECC Configuration

► DRAM Scrubbers

DRAM Corrected Error Counter Enable [LeakMode]

DRAM Corrected Error Counter Interrupt [True]

Enable

DRAM Corrected Error Counter Leak Rate 7

DRAM Corrected Error Counter Start FFF5

Count

→ ← : Select Screen

↑ ↓ : Select Item

Enter : Select

+/- : Change Opt.

F1 : General Help

F2 : Previous values

F3 : Optimized Defaults

F4 : Save & Exit

ESC : Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS		
Menu Fields	Settings	Comments
Data Poisoning	[Disabled] [Enabled] [Auto]	Enable poison data creation on uncorrectable DDR DRAM ECC errors and poison propagation to CPU cores and caches. Requires ECC memory. When FALSE, a fatal error event will occur on DDR ECC errors sets UMC_CH::EccCtrl[UcFatalEn] when MC_CH::EccCtrl[WtEccEn] is set.
DRAM Boot Time Post Package Repair	[Enable] [Disable]	Enable or Disable DRAM Boot Time Post Package Repair.
DRAM Runtime Post Package Repair	[Enable] [Disable]	Enable or Disable DRAM Run Time Post Package Repair.
DRAM Post Package Repair Config Initiator	[In-Band] [Out of Band]	This option will indicate the Post Package Repair configuration setting whether it is In-Band or Out-Of-Band Repair.
RCD Parity	[Auto] [Disabled] [Enabled]	Enable RCD command and address parity.

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS		
Menu Fields	Settings	Comments
Write CRC	[Auto] [Disabled] [Enabled]	Enable write CRC on DDR5 DRAM
Read CRC	[Auto] [Disabled] [Enabled]	Program to RecCtrl.RecEn [3]
Memory Error Injection	[False] [True] [Auto]	0=Enable. 1=Disable. Specifies UMC error injection configuration writes are disabled. True: UMC::CH::MiscCfg[DisErrInj]=1
EcsStatus Interrupt	[False] [True]	True=Enable. False=Disable. Enable interrupts from the EcsStatus Array, in lieu of ECS logging via MCA. Valid only when PcdAmdCcxCfgPFEHEnable is set to TRUE.
ECC Configuration	Selects Sub-menu	
DRAM Scrubbers	Selects Sub-menu	
DRAM Corrected Error Counter Enable	[Disable] [NoLeakMode] [LeakMode]	Configure DRAM Corrected Error Counter function. Only meaningful when PcdAmdCcxCfgPFEHEnable is TRUE
DRAM Corrected Error Counter Interrupt Enable	[False] [True]	Enable SMI when DRAM Corrected Error Counter count exceeds the threshold value.
DRAM Corrected Error Counter Leak Rate	X	Program Rate value for DRAM Corrected Error Counter function. Only meaningful when PcdAmdDdrEccErrorCounterEnable is set to LeakMode (Value :0x00-0x1F).
DRAM Corrected Error Counter Start Count	XXXX	Program starting count value for DRAM Corrected Error Counter function. Only meaningful when PcdAmdDdrEccErrorCounterEnable is not Disable (0x00 - 0xFFFF).

6.2.4.3.4.1 ECC Configuration

Aptio Setup - AMI	
Advanced	
ECC Configuration	
DRAM ECC Symbol Size	[Auto]
DRAM ECC Enable	[Auto]
DRAM UECC Retry	[Auto]
Max DRAM UECC Error Replay	8
Memory Clear	[Auto]
Address XOR after ECC	[Auto]
CypherText Hiding Enable	[Disable]
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ ECC Configuration		
Menu Fields	Settings	Comments
DRAM ECC Symbol Size	[x4] [x16] [Auto]	DRAM ECC Symbol Size (x4/x16) - UMC_CH::EccCtrl[EccSymbolSize16, EccSymbolSize]
DRAM ECC Enable	[Disabled] [Enabled] [Auto]	Use this option to enable / disable DRAM ECC. Auto will set ECC to enable.
DRAM UECC Retry	[Auto] [Disabled] [Enabled]	DRAM UECC Retry. Program to UMC::RecCtrl.RecEn [2]
Max DRAM UECC Error Replay	X	Program to UMC::RecCtrl2 [MaxEccRply], valid value:1 - 3F hex, default 8
Memory Clear	[Enabled] [Disabled] [Auto]	Clear/Zero out Dram range [DramScrubBaseAddr: DramScrubLimitAddr].When this option is disabled, Memory is not cleared after training. ECC Dimms have memory clear enabled always.

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ ECC Configuration		
Menu Fields	Settings	Comments
		Non-ECC Dimms can choose to disable/enable using this option. Default = Memclear enabled
Address XOR after ECC	[Enabled] [Disabled] [Auto]	In order to provide data integrity when data is returned from the wrong address, UMC will hash the data after ECC with the normalized address
CypherText Hiding Enable	[Disable] [Enable]	Enable or disable ciphertext hiding

6.2.4.3.4.2 DRAM Scrubbers

Aptio Setup - AMI	
Advanced	
DRAM Scrubber	
DRAM ECS Mode	[Auto]
DRAM Redirect Scrubber Enable	[Auto]
DRAM Scrub Redirection Limit	[Auto]
DRAM Scrub Time	[24 hours]
▶ ECS Config	
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers		
Menu Fields	Settings	Comments
DRAM ECS Mode	[AutoECS] [ManualECS] [Auto] [DisableECS]	0 = AutoECS Mode, 1 = ManualECS mode Disable ECS mode disables only the controller and does not disable it on the DRAM
DRAM Redirect Scrubber Enable	[Disabled] [Enabled] [Auto]	Enable/Disable Dram Redirect Scrubber and poison scrubber
DRAM Scrub Redirection Limit	[8 Scrubs] [4 Scrubs] [2 Scrubs] [1 Scrub] [Auto]	Dram ECC Scrub Redirection Limit: 0=8 scrubs, 1=4 scrubs, 2=2 scrubs, 3=1 scrub
DRAM Scrub Time	[Disabled] [1 hour] [4 hours] [6 hours] [8 hours]	Provide a value that is the number of hours to scrub memory.

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers		
Menu Fields	Settings	Comments
	[12 hours] [16 hours] [24 hours] [48 hours]	
ECS Config	Selects Sub-Menu	

6.2.4.3.4.2.1 ECS Config

Aptio Setup - AMI	
Advanced	
ECS Config	
DRAM Error Threshold Count	[Auto]
DRAM ECS Count Mode	[Auto]
DRAM AutoEcs during self Refresh	[Auto]
DRAM ECS WriteBack Suppression	[Auto]
DRAM x4 WriteBack Suppression	[Auto]
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers \ ECS Config		
Menu Fields	Settings	Comments
DRAM Error Threshold Count	[ETC_4]	List of Values: 0 = ETC_4, 1 = ETC_16, 2 = ETC_64, 3 = ETC_256 (default - Auto), 4 = ETC_1024, 5 = ETC_4096
	[ETC_16]	
	[ETC_64]	
	[ETC_256]	
	[ETC_1024]	
	[ETC_4096]	
	[Auto]	
DRAM ECS Count Mode	[Row Count Mode]	0: RowCount Mode 1: CodeWord Mode 0xFF: Auto - ABL decides default as CodeWord Mode
	[Code Word Count Mode]	
	[Auto]	
DRAM AutoEcs during self Refresh	[AutoEcs Disabled]	0: AutoEcs Disabled 1: AutoEcs Enabled 0xFF: Auto - ABL choose AutoEcs Disabled
	[AutoEcs Enabled]	
	[Auto]	
DRAM ECS WriteBack Suppression	[Disable]	To enable/Disable ECS Error Correction Writeback suppression 0: ECS Writeback Suppression Disabled
	[Enable]	
	[Auto]	

Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers \ ECS Config		
Menu Fields	Settings	Comments
		1: ECS Writeback Suppression Enabled 0xFF: Auto - ABL chooses Writeback Suppression to be Enabled by default
DRAM x4 WriteBack Suppression	[Disable] [Enable] [Auto]	To enable/Disable X4 device Error Correction Writeback suppression 0: X4 Writeback Suppression Disabled 1: X4 Writeback Suppression Enabled 0xFF: Auto

6.2.4.3.5 DDR Bus Configuration

Advanced

Aptio Setup - AMI

DDR Bus Configuration

▶ P-state 0 Dram ODT Impedance

▶ P-state 1 Dram ODT Impedance

Processor ODT Pull Up Impedance

Processor ODT Pull Down Impedance

Dram DQ drive strengths

[Auto]

[Auto]

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration		
Menu Fields	Settings	Comments
P-state 0 Dram ODT Impedance	Selects Sub-menu	
P-state 1 Dram ODT Impedance	Selects Sub-menu	
Processor ODT Pull Up Impedance	[Auto] [High Impedance] [480 ohm] [240 ohm] [160 ohm] [120 ohm] [96 ohm] [80 ohm] [68.6 ohm] [53.3 ohm] [48 ohm] [43.6 ohm] [40 ohm] [36.9 ohm] [34.3 ohm]	Select the ODT impedance for all DBYTE IOs.

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration		
Menu Fields	Settings	Comments
	[32 ohm] [30 ohm] [28.2 ohm] [26.7 ohm] [25.3 ohm]	
Processor ODT Pull Down Impedance	[Auto] [High Impedance] [480 ohm] [240 ohm] [160 ohm] [120 ohm] [96 ohm] [80 ohm] [68.6 ohm] [53.3 ohm] [48 ohm] [43.6 ohm] [40 ohm] [36.9 ohm] [34.3 ohm] [32 ohm] [30 ohm] [28.2 ohm] [26.7 ohm] [25.3 ohm]	Select The ODT pull down impedance for all DBYTE IOs.
Dram DQ drive strengths	[Auto] [48 ohm] [40 ohm] [34 ohm]	Selects the Dram Pull-up and Pull Down Output Driver Impedance for all DQ IOs.

6.2.4.3.5.1 P-state 0 Dram ODT Impedance

Advanced

Aptio Setup - AMI

P-State 0 Dram ODT Impedance

RTT_NOM_WR P-State 0

[Auto]

RTT_NOM_RD P-State 0

[Auto]

RTT_WR P-State 0

[Auto]

RTT_PARK P-State 0

[Auto]

DQS_RTT_PARK P-State 0

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration \ P-state 0 Dram ODT Impedance		
Menu Fields	Settings	Comments
RTT_NOM_WR P-State 0	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_NOM_WR P-State 0
RTT_NOM_RD P-State 0	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)]	Select the DRAMs On-die Termination impedance for RTT_NOM_RD P-State 0

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration \ P-state 0 Dram ODT Impedance		
Menu Fields	Settings	Comments
	[RZQ/7 (34)]	
RTT_WR P-State 0	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_WR P-State 0
RTT_PARK P-State 0	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_PARK P-State 0
DQS_RTT_PARK P-State 0	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for DQS_RTT_PARK P-State 0

6.2.4.3.5.2 P-state 1 Dram ODT Impedance

Advanced

Aptio Setup - AMI

P-State 1 Dram ODT Impedance

RTT_NOM_WR P-State 1 [Auto]

RTT_NOM_RD P-State 1 [Auto]

RTT_WR P-State 1 [Auto]

RTT_PARK P-State 1 [Auto]

DQS_RTT_PARK P-State 1 [Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration \ P-state 1 Dram ODT Impedance		
Menu Fields	Settings	Comments
RTT_NOM_WR P-State 1	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_NOM_WR P-State 1
RTT_NOM_RD P-State 1	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)]	Select the DRAMs On-die Termination impedance for RTT_NOM_RD P-State 1

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration \ P-state 1 Dram ODT Impedance		
Menu Fields	Settings	Comments
	[RZQ/7 (34)]	
RTT_WR P-State 1	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_WR P-State 1
RTT_PARK P-State 1	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for RTT_PARK P-State 1
DQS_RTT_PARK P-State 1	[Auto] [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance for DQS_RTT_PARK P-State 1

6.2.4.3.6 DDR Timing Configuration

Aptio Setup - AMI

Advanced

DDR Timing Configuration

WARNING - DAMAGE CAUSED BY USE OF YOUR AMD PROCESSOR OUTSIDE OF SPECIFICATION OR IN EXCESS OF FACTORY SETTINGS ARE NOT COVERED UNDER YOUR AMD PRODUCT WARRANTY AND MAY NOT BE COVERED BY YOUR SYSTEM MANUFACTURER'S WARRANTY.

Operating your AMD processor outside of specification or in excess of factory settings, including but not limited to overclocking, may damage or shorten the life of your processor or other system components, create system instabilities (e.g., data loss and corrupted images) and in extreme cases may result in total system failure. AMD does not provide support or service for issues or damages related to use of an AMD processor outside of processor specifications or in excess of factory settings.

► Decline

► Accept

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

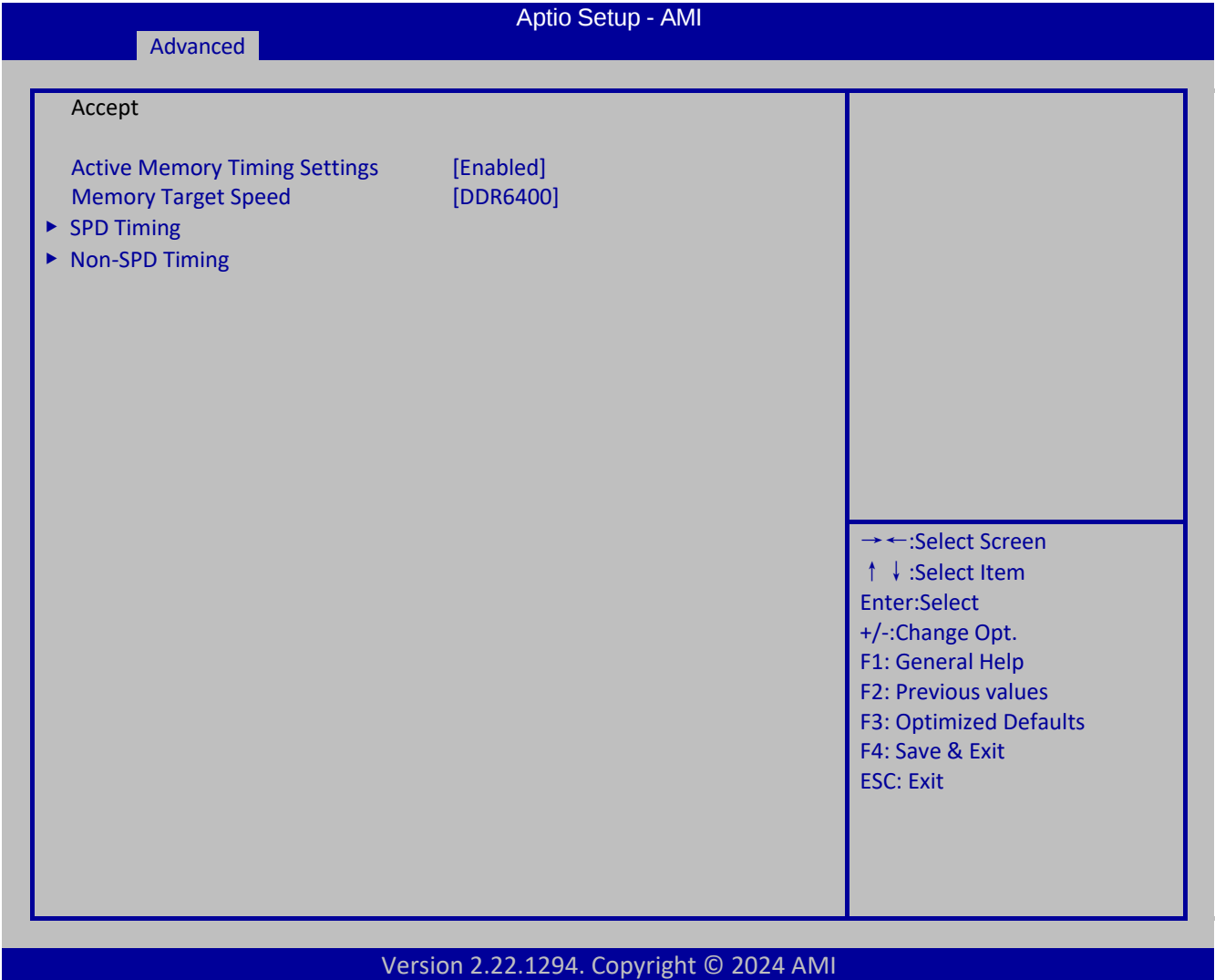
F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration		
Menu Fields	Settings	Comments
Decline	Selects Previous menu	
Accept	Selects sub-menu	

6.2.4.3.6.1 DDR Timing Configuration-Accept



Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept		
Menu Fields	Settings	Comments
Active Memory Timing Settings	[Auto] [Enabled]	Active Memory Timing Settings.
Memory Target Speed	[Auto] [DDR3600] [DDR4000] [DDR4400] [DDR4800] [DDR5200] [DDR5600] [DDR6000] [DDR6400]	Specifies the memory target speed in MT/s.
SPD Timing	Selects sub-menu	
Non-SPD Timing	Selects sub-menu	

6.2.4.3.6.1.1 SPD Timing

Aptio Setup - AMI		
Advanced		
SPD Timing		
Tcl Ctrl	[Auto]	
Tcl	16	
Trcd Ctrl	[Auto]	
Trcd	8	
Trp Ctrl	[Auto]	
Trp	8	
Tras Ctrl	[Auto]	
Tras	27	
Trc Ctrl	[Auto]	
Trc	39	
Twr Ctrl	[Auto]	
Twr	12	
Trfc1 Ctrl	[Auto]	
Trfc1	138	
Trfc2 Ctrl	[Auto]	
Trfc2	C0	
TrfcSb Ctrl	[Auto]	
TrfcSb	32	
		→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI		

Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ SPD Timing		
Menu Fields	Settings	Comments
Tcl Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Tcl	X	Specifies the CAS Latency. Valid values: 0x9 ~ 0x32. The value is in hex.
Trcd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trcd	X	Specifies the RAS# Active to CAS# Read Delay Time. Valid values: 0x8 ~ 0x3F. The value is in hex.
Trp Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trp	X	Specifies Row Precharge Delay Time. Valid values: 0x8 ~ 0x3F. The value is in hex.
Tras Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Tras	X	Specifies the minimum time in memory clock cycles from an activate

Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ SPD Timing		
Menu Fields	Settings	Comments
		command to a precharge command, both to the same bank. Valid values: 0x20 ~ 0x75.
Trc Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trc	X	Specifies Active to Active/Refresh Delay Time. Valid values 87h-1Dh.
Twr Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Twr	X	Specifies the Minimum Write Recovery Time. Valid values: 0xA ~ 0x64. The value is in hex
Trfc1 Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trfc1	X	Specifies the Refresh Recovery Delay Time (tRFC1). Valid values 3DEh-3Ch
Trfc2 Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trfc2	X	Specifies the Refresh Recovery Delay Time (tRFC2). Valid values 3DEh-3Ch
TrfcSb Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrfcSb	X	Specifies the Refresh Recovery Delay Time (tRFCsb). Valid values 0x32 ~ 0x7FF. The value is in hex.

6.2.4.3.6.1.2 Non-SPD Timing

Aptio Setup - AMI

Advanced

Non-SPD Timing

Tcwl Ctrl	[Auto]
Tcwl	C
Trtp Ctrl	[Auto]
Trtp	9
TrrdL Ctrl	[Auto]
TrrdL	4
TrrdS Ctrl	[Auto]
TrrdS	4
Tfaw Ctrl	[Auto]
Tfaw	1A
TwtrL Ctrl	[Auto]
TwtrL	3
TwtrS Ctrl	[Auto]
TwtrS	3
TrdrdScL Ctrl	[Auto]
TrdrdScL	1
TrdrdSc Ctrl	[Auto]
TrdrdSc	1
TrdrdSd Ctrl	[Auto]
TrdrdSd	3
TrdrdDd Ctrl	[Auto]
TrdrdDd	3
TwrwrScL Ctrl	[Auto]
TwrwrScL	1
TwrwrSc Ctrl	[Auto]
TwrwrSc	1
TwrwrSd Ctrl	[Auto]
TwrwrSd	3
TwrwrDd Ctrl	[Auto]
TwrwrDd	3
Twrrd Ctrl	[Auto]
Twrrd	1
Trdwr Ctrl	[Auto]
Trdwr	5

→ ← : Select Screen
↑ ↓ : Select Item
Enter : Select
+/- : Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ Non-SPD Timing		
Menu Fields	Settings	Comments
Tcwl Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Tcwl	X	Specifies the CAS Write Latency. Valid Values: 0x9 ~ 0x16
Trtp Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trtp	X	Specifies the Read CAS# to Precharge Delay Time. Valid values: 0x5 ~ 0x0E.

Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ Non-SPD Timing		
Menu Fields	Settings	Comments
TrrdL Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrrdL	X	Specifies the Activate to Activate Delay Time, same bank group(tRRD_L). Valid values: 0x4 ~ 0x0C. The value is in hex.
TrrdS Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrrdS	X	Specifies the Activate to Activate Delay Time, different bank group(tRRD_S). Valid values: 0x04 ~ 0x0C. The value is in hex.
Tfaw Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Tfaw	X	Specifies the Four Activate Window Time. Valid values 6h ~ 36h.
TwtrL Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwtrL	X	Specifies the Minimum Write to Read Time, same bank group. Valid values: 0x2 ~ 0xE
TwtrS Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwtrS	X	Specifies the Minimum Write to Read Time, different bank group. Valid values: 0x02 ~ 0x0E
TrdrdScL Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrdrdScL	X	Specifies the CAS to CAS Delay Time, same bank group. Valid values 0x1 ~ 0xF
TrdrdSc Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrdrdSc	X	Specifies the Read to Read turnaround timing in the same chipselect. Valid values: 0x1 ~ 0xF
TrdrdSd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrdrdSd	X	Specifies the Read to Read turnaround timing in the same DIMM. Valid values: 0x1 ~ 0xF.
TrdrdDd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TrdrdDd	X	Specifies the Read to Read turnaround timing in a different DIMM. Valid Values: 0x1 ~ 0xF
TwrwrScL Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwrwrScL	X	Specifies the CAS to CAS Delay Time, same bank group. Valid values 3Fh-1h
TwrwrSc Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwrwrSc	X	Specifies the Write to Write turnaround timing in the same chipselect. Valid values: 0x1 ~ 0xF
TwrwrSd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwrwrSd	X	Specifies the Write to Write turnaround timing in the same DIMM. Valid values: 0x1 ~ 0xF.

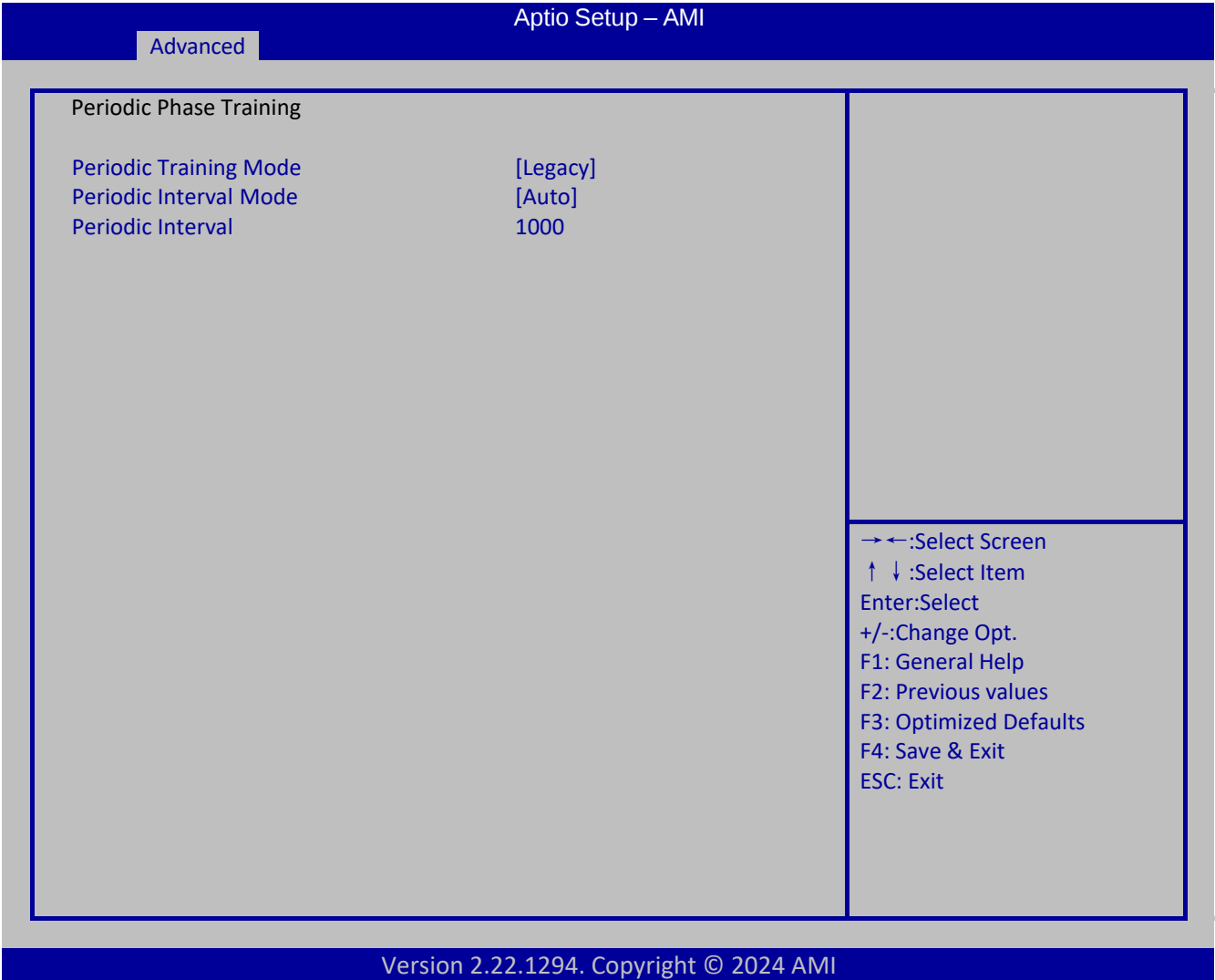
Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ Non-SPD Timing		
Menu Fields	Settings	Comments
TwrwrDd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
TwrwrDd	X	Specifies the Write to Write turnaround timing in a different DIMM. Valid values: 0x1 ~ 0xF
Twrrd Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Twrrd	X	Specifies the Write to Read turnaround timing. Valid values: 0x1 ~ 0xF. The value is in hex.
Trdwr Ctrl	[Auto] [Manual]	Auto: Follow default setting, Manual: Manually specify
Trdwr	X	Specifies the Read to Write Turnaround Timing. Valid value: 0x1 ~ 0x1F. The value is in hex.

6.2.4.3.7 DDR Training Options

Aptio Setup – AMI	
Advanced	
DDR Training Options	
DRAM PDA Enumerate ID Programming Mode [Auto] ▶ Periodic Phase Training Write Training Burst Length [4X] Training Retry Count [Auto]	→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Training Options		
Menu Fields	Settings	Comments
DRAM PDA Enumerate ID Programming Mode	[Auto] [Toggling PDA enumeration mode] [Legacy PDA enumeration mode]	Specify PDA enumeration mode Auto : default 0 : Continuous DQS toggling PDA enumeration mode (default) 1 : Legacy PDA enumeration mode
Periodic Phase Training	Selects Sub-menu	
Write Training Burst Length	[4X] [8X]	Extended sequence for write training, control PMU MsgBlock->AdvTrainOpt[6:5]
Training Retry Count	[Auto] [Disabled] [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]	Retry on PMU training failure, retry to all channels, including passed and failed channel.

6.2.4.3.7.1 Periodic Phase Training



Advanced \ AMD CBS \ UMC Common Options \ DDR Training Options \ Periodic Phase Training		
Menu Fields	Settings	Comments
Periodic Training Mode	[Disabled] [Legacy]	Specify the PPT Control
Periodic Interval Mode	[Auto] [Manual]	0: Auto. The Periodic Interval value is decided by BIOS automatically. 1: Manual. It is specified by the CBS option Periodic Interval.
Periodic Interval	X	Periodic Interval value in milli-second, in decimal. Range 100 ~ 4095 ms.

6.2.4.3.8 DDR Security

Aptio Setup – AMI	
Advanced	
DDR Security	
TSME	[Auto]
AES	[AES-256]
Data Scramble	[Enabled]
SME-MK	[Disabled]
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Security		
Menu Fields	Settings	Comments
TSME	[Auto] [Enabled] [Disabled]	Transparent SME
AES	[AES-128] [AES-256]	AES mode: AES-128 or AES-256 (default)
Data Scramble	[Enabled] [Disabled]	Data scrambling: DataScrambleEn
SME-MK	[Enabled] [Disabled]	SME-MK encryption mode. Enabling both SMEE and SME-MK is not supported. Results in #GP.

6.2.4.3.9 DDR PMIC Configuration

Aptio Setup - AMI		
Advanced		
DDR PMIC Configuration		
PMIC Error Reporting	[Auto]	
PMIC Operation Mode	[Secure Mode]	
PMIC Fault Recovery	[Always]	
PMIC SWA/SWB VDD Core	1100	
PMIC SWC VDDIO	1100	
PMIC SWD VPP	1800	
PMIC Stagger Delay	5	
Max PMCI Power On	FF	
		→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit
Version 2.22.1294. Copyright © 2024 AMI		

Advanced \ AMD CBS \ UMC Common Options \ DDR PMIC Configuration		
Menu Fields	Settings	Comments
PMIC Error Reporting	[False] [True] [Auto]	Enables support for PMIC Error Reporting.
PMIC Operation Mode	[Secure Mode] [Programmable Mode]	1 - Programmable Mode Operation (default); 0 - Secure Mode Operation Programmable mode allows certain registers to be programmed after VR enable else they will be in secure mode
PMIC Fault Recovery	[Always] [Never] [Once]	0 - Always; 1 - Never (default); 2 - Once Always - PMIC will ignore previous boot errors. No channel disabled Never - PMIC disables the channel with errors from previous boot. Once - PMIC will ignore the previous boot errors once. More than once channel will be disabled
PMIC SWA/SWB VDD Core	X	Range is from 1000mV to 1200mV; default of 1100mV

Advanced \ AMD CBS \ UMC Common Options \ DDR PMIC Configuration		
Menu Fields	Settings	Comments
		Apply to PMIC register 0x21, 0x23.
PMIC SWC VDDIO	X	Range is from 1000mV to 1200mV; default of 1100mV. Apply to PMIC register 0x25.
PMIC SWD VPP	X	Range is from 1500mV to 2135mV; default of 1800mV. Apply to PMIC register 0x27.
PMIC Stagger Delay	X	Amount of time to wait between powering on each DIMMs in milliseconds
Max PMCI Power On	X	Maximum number of DIMMs that can power on at the same time.

6.2.4.3.10 DDR Thermal Throttling

Aptio Setup - AMI	
Advanced	
DDR Thermal Throttling	
ODTS Thermal Throttle Control	[Enable]
ODTS Thermal Throttle Threshold	[Auto]
TSOD Thermal Throttle Control	[Disabled]
TSOD Thermal Throttle Start Temperature	85
TSOD Thermal Throttle Hysteresis	5
TSOD Thermal Throttle Percentage (Threshold)	10
TSOD Thermal Throttle Percentage (Threshold+5C)	20
TSOD Thermal Throttle Percentage (Threshold+10C)	40
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ UMC Common Options \ DDR Miscellaneous		
Menu Fields	Settings	Comments
ODTS Thermal Throttle Control	[Auto] [Enabled] [Disabled]	ODTS Thermal Throttle control is a HW function that is always enabled
ODTS CMD Throttle Threshold	[Auto] [> 85' C] [> 90' C] [> 95' C]	Dram MR4 Temperature status value to start ODTS Command Thermal Throttling.
TSOD Thermal Throttle Control	[Enabled] [Disabled]	TSOD = Thermal Sensor On DIMM Enables SoC (PM firmware) based thermal management of DDR5 memory, based on thermal sensor located on DIMM
TSOD Thermal Throttle Start Temperature	X	Sets an integer temperature threshold at which TSOD (Thermal Sensor on DIMM) based memory throttling begins. Applies to all installed and enabled DIMMs
TSOD Thermal Throttle Hysteresis	X	Sets an integer number of degrees the reported TSOD(Thermal Sensor On DIMM) temperature

Advanced \ AMD CBS \ UMC Common Options \ DDR Miscellaneous		
Menu Fields	Settings	Comments
		must drop below the "TSOD Thermal Throttle Start Temperature" before memory throttling is removed. Applies to all installed and enabled DIMMs
TSOD Thermal Throttle Percentage (Threshold)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded.
TSOD Thermal Throttle Percentage (Threshold+5C)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded by more than 5C.
TSOD Thermal Throttle Percentage (Threshold+10C)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded by more than 10C.

6.2.4.3.11 DDR Miscellaneous

Aptio Setup - AMI

Advanced

DDR Miscellaneous

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.2.4.4 NBIO Common Options

Aptio Setup - AMI	
Advanced	
NBIO Common Options ▶ SMU Common Option ▶ NBIO RAS Common Options ▶ PCIE ▶ nBif Common Option ▶ IOMMU/Security ▶ Enable Port Bifurcation ▶ Link EQ preset Options PCie Loopback Mode [Auto] Enable 2 SPC (Gen 4) [Auto] Enable 2 SPC (Gen 5) [Auto] Safe recovery upon a BERExceeded Error [Auto] Periodic Calibration [Auto]	
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options		
Menu Fields	Settings	Comments
SMU Common Option	Selects sub-menu.	
NBIO RAS Common Options	Selects sub-menu.	
PCIE	Selects sub-menu.	
nBif Common Option	Selects sub-menu.	
IOMMU/Security	Selects sub-menu.	
Enable Port Bifurcation	Selects sub-menu.	
Link EQ preset Options	Selects sub-menu.	
PCie Loopback Mode	[Auto] [Disabled] [Enabled]	Enable/Disable PcieLoopBackMode
Enable 2 SPC (Gen 4)	[Enable] [Disable] [Auto]	Enable this setting to use 2 symbols per clock for devices at Gen 4 speed.
Enable 2 SPC (Gen 5)	[Enable] [Disable]	Enable this setting to use 2 symbols per clock for devices at Gen 5 speed.

Advanced \ AMD CBS \ NBIO Common Options		
Menu Fields	Settings	Comments
	[Auto]	
Safe recovery upon a BERExceeded Error	[Auto] [Enable] [Disable]	No help string
Periodic Calibration	[Auto] [Enable] [Disable]	No help string

6.2.4.4.1 SMU Common Options

Aptio Setup - AMI

Advanced

SMU Common Options

TDP Control	[Auto]
PPT Control	[Auto]
Determinism Control	[Auto]
xGMI Link Width Control	[Auto]
APBDIS	[Auto]
Power Profile Selection	[Auto]
xGMI Pstate Control	[Auto]
BoostFmaxEn	[Auto]
DF PState Frequency Optimizer	[Auto]
DF Cstates	[Auto]
CPPC	[Auto]
HSMP Support	[Auto]
SVI3 SVC Speed Control	[Manual]
SVI3 SVC Speed	[5.00MHz]
3D V-Cache	[Auto]
L3 BIST	[Auto]
Diagnostic Mode	[Auto]
GMI Folding	[Auto]
Separate CPU power plane throttling	[Auto]
DfPstate Range Control	[Auto]

→ ←: Select Screen
↑ ↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	Settings	Comments
TDP Control	[Manual] [Auto]	Auto = Use the fused TDP Manual = User can set customized TDP
PPT Control	[Manual] [Auto]	Auto = Use the fused PPT Manual = User can set customized PPT
Determinism Control	[Manual] [Auto]	Auto = Use default performance determinism settings Manual = User can set custom performance determinism settings
xGMI Link Width Control	[Manual] [Auto]	Auto = Use default xGMI link width controller settings. Manual = User can set custom xGMI link width controller settings.
APBDIS	[0] [1] [Auto]	0 = not APBDIS (mission mode) 1 = APBDIS
Power Profile Selection	[High Performance Mode] [Efficiency Mode]	[0 = High Performance Mode; 1 = Efficiency Mode; 2 = Maximum IO Performance Mode; 3

Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	Settings	Comments
	[Maxumim OP Performance Mode] [Balanced Memory Performance Mode] [Balanced Core Performance Mode] Balanced Core Memory Performance Mode] [Auto]	= Balanced Memory Performance Mode; 4 = Balanced Core Performance Mode; 5 = Balanced Core Memory Performance Mode; 0xFF = Auto]
xGMI Pstate Control	[Auto] [Manual]	If manual, set XgmiPstateRangeSupportEn=1, else 0
BoostFmaxEn	[Manual] [Auto]	Auto = Use the default Fmax Manual = User can set the boost Fmax
DF PState Frequency Optimizer	[Auto] [Enabled] [Disabled]	Disabled - means disable the DFPstate CCLK effective frequency optimizer Enabled - means enable the DFPstate CCLK effective frequency optimizer
DF Cstates	[Disabled] [Enabled] [Auto]	Enable = Enable the feature : Disable = Disable the feature
CPPC	[Disabled] [Enabled] [Auto]	Enable = Enable the feature : Disable = Disable the feature
HSMP Support	[Disabled] [Enabled] [Auto]	Select HSMP support enable or disable
SVI3 SVC Speed Control	[Auto] [Manual]	Enables for programming of the SVI3 SVC speed. Auto = Use default SVI3 speed control Manual = User can set custom SVI3 speed control settings
SVI3 SVC Speed	[20.00MHz] [13.33MHz] [5.00MHz]	0=50.00MHz 1=40.00MHz 2=26.67MHz 3=20.00MHz 4=16.00MHz 5=13.33MHz 6=10.00MHz 7=8.00MHz 8=5.00MHz
3D V-Cache	[Auto] [Disable] [1 stack]	Override of X3D technology
L3 BIST	[Disable] [Enable] [Auto]	Enable or Disable L3 BIST
Diagnostic Mode	[Disabled] [Enabled] [Auto]	Select Diag mode enable or disable
GMI Folding	[Disabled] [Enabled] [Auto]	Enable = Enable the feature : Disable = Disable the feature
Separate CPU power plane throttling	[Enable] [Disable] [Auto]	Disable=link throttling for CPU planes; Enable=unlink throttling for CPU planes
DfPstate Range Control	[Disable] [Enable] [Auto]	Disable - Disable DF Pstate Range Control Enable - Enable DF Pstate Range Control

Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	Settings	Comments
		DF Pstate selection is overridden by the APBDIS BIOS option if it is selected. If this feature is enabled, the range value setting should follow the rule that the DF Pstate Max Index must be less than or equal to the DF Pstate Min Index. Otherwise, DF Pstate Range selections will not work.

6.2.4.4.2 NBIO RAS Common Options

Aptio Setup - AMI	
Advanced	
NBIO RAS Common Options	
NBIO RAS Control	[Auto]
NBIO SyncFlood Generation	[Auto]
NBIO SyncFlood Reporting	[Auto]
PCIe Aer Reporting Mechanism	[Auto]
Edpc Control	[Auto]
ACS RAS Request Value	[Auto]
NBIO Poison Consumption	[Auto]
Sync Flood on PCIe Fatal Error	[Auto]
NBIO RAS Numerical Common Options	[Disable]
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ NBIO Common Options \ NBIO RAS Common Options		
Menu Fields	Settings	Comments
NBIO RAS Control	[Disable] [MAC] [Auto]	(0) Disabled, (1) MCA
NBIO SyncFlood Generation	[Enabled] [Disabled] [Auto]	This value may be used to mask SyncFlood caused by NBIO RAS options. When set to TRUE SyncFlood from NBIO is masked. When set to FALSE NBIO is capable of generating SyncFlood.
NBIO SyncFlood Reporting	[Enabled] [Disabled] [Auto]	This value may be used to enable SyncFlood reporting to APML. When set to TRUE SyncFlood will be reported to APML. When set to FALSE that reporting will be disabled
PCIe Aer Reporting Mechanism	[Firmware First] [Firmware First but allow OS First] [OS First] [Auto]	This value selects the method of reporting AER errors from PCI Express. A value of 1 allows OS First handling of the errors through generation of a system control

Advanced \ AMD CBS \ NBIO Common Options \ NBIO RAS Common Options		
Menu Fields	Settings	Comments
		interrupt (SCI). A value of 2 provides for Firmware First handling of errors through generation of a system management interrupt (SMI).
Edpc Control	[Disabled] [Enabled] [Auto]	(0) Disabled; (1) Enabled; (3) Auto
ACS RAS Request Value	[Direct Request Access Enabled] [Request Blocking Enabled] [Request Redirect Enabled] [Auto]	No help String
NBIO Poison Consumption	[Auto] [Disabled] [Enabled]	NBIO Poison Consumption
Sync Flood on PCIe Fatal Error	[Auto] [True] [False]	When "Sync Flood on PCIe Fatal Error" is True, PcdAmdPcieSyncFloodOnFatal should be set to True. When "Sync Flood on PCIe Fatal Error" is False, PcdAmdPcieSyncFloodOnFatal should be set to False. When "Sync Flood on PCIe Fatal Error" is Auto, PcdAmdPcieSyncFloodOnFatal should retain its AGESA default.
NBIO RAS Numerical Common Options	[Disable] [Manual]	All the numerical RAS CBS options override the PCD values automatically. Disable: Keep original PCD values Manual: Display custom numerical RAS CBS options

6.2.4.4.3 PCIE

Aptio Setup - AMI

Advanced

PCIE

Data Object Exchange	[Auto]
RTM Margining Support	[Auto]
Multi Auto Speed Change On List Rate	[Auto]
Multi Upstream Auto Speed Change	[Auto]
Allow Compliance	[Auto]
EQ Bypass To Highest Rate	[Auto]
Data Link Feature Cap	[Auto]
SRIS	[Auto]
ACS Enable	[Auto]
PCIe Ten Bit Tag Support	[Auto]
PCIe ARI Enumeration	[Auto]
PCIe ARI Support	[Auto]
Presence Detect Select mode	[Auto]
Hot Plug Handling mode	[Auto]
Presence Detect State Settle Time	[Auto]
Hot Plug Port Settle Time	FF
Hotplug Support	[Auto]
Early Link Speed	[Auto]
Enable AER Cap	[Auto]
PCIe Link Speed Capability	[Auto]
PCIe Target Link Speed	[Auto]
ASPM Control	[Auto]
MCTP Enable	[Auto]
Non-PCIe Compliant Support	[Auto]
Limit hotplug devices to PCIe Boot speed	[Auto]
Enable PCIe SFI Config via OOB	[False]
PCIe Idle Power Setting	[Optimize for Perf/Power]

→ ←:Select Screen
 ↑ ↓:Select Item
 Enter:Select
 +/-:Change Opt.
 F1: General Help
 F2: Previous values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ PCIE		
Menu Fields	Settings	Comments
Data Object Exchange	[Disabled] [Enabled] [Auto]	Data Object Exchange (DOE)
RTM Margining Support	[Disable] [Enable] [Auto]	RTM Margining Support
Multi Auto Speed Change On List Rate	[Disable] [Enable] [Auto]	Force PCIe link training speed to last advertised for all ports. Disabled=Use highest data rate ever advertised. Enabled=Use last data rate advertised.
Multi Upstream Auto Speed Change	[Disabled] [Enabled] [Auto]	Defines the setting of this feature for all PCIe devices. "Auto" uses the DXIO default setting of 0 for Gen1 and 1 for Gen2/3<

Advanced \ AMD CBS \ NBIO Common Options \ PCIE		
Menu Fields	Settings	Comments
Allow Compliance	[Auto] [Disable] [Enable]	When enabled, allows the PCIe RP to enter Polling.Compliance state
EQ Bypass To Highest Rate	[Disable] [Enable] [Auto]	Controls the ability to advertise Equalization Bypass to Highest Rate Support in TSxs sent prior to LinkUp=1
Data Link Feature Cap	[Enabled] [Disabled] [Auto]	Data Link Feature Capability
SRIS	[Auto] [Disable] [Enable]	SRIS
ACS Enable	[Enable] [Disabled] [Auto]	AER must be enabled for ACS enable to work
PCIe Ten Bit Tag Support	[Disable] [Enable] [Auto]	Enables PCIe ten bit tags for supported devices. Auto = Disabled
PCIe ARI Enumeration	[Disable] [Enable] [Auto]	ARI Forwarding Enable for each downstream port
PCIe ARI Support	[Disable] [Enable] [Auto]	Enables Alternative Routing-ID Interpretation
Presence Detect Select mode	[OR] [AND] [Auto] [In-Band Only] [Out-of-Band only]	Control the Presence Detect Select mode
Hot Plug Handling mode	[OS First] [Firmware First/EDR if OS Support] [Firmware First but allow OS First] [System Firmware Intermediary] [Auto]	Control the Hot Plug Handling mode
Presence Detect State Settle Time	[Auto] [True] [False]	Presence Detect State Settle Time Enable/Disable
Hot Plug Port Settle Time	XX	Hex values. Value is between 0x1 to 0xFF (1ms to 255ms) but valid value are 0x1 to 0xFE. 0xFF: Force settle time to 0ms.
Hotplug Support	[Auto] [Disabled]	Allows disabling hot plug functionality. Auto = Normal functionality Disabled = Hot plug functionality disabled
Early Link Speed	[Max] [Gen1] [Gen2] [Auto]	Set Early Link Speed
Enable AER Cap	[Enable] [Disabled] [Auto]	Enables Advanced Error Reporting Capability
PCIe Link Speed Capability	[Maximum speed] [GEN1] [GEN2]	Set all PCIe port speed capability

Advanced \ AMD CBS \ NBIO Common Options \ PCIE		
Menu Fields	Settings	Comments
	[GEN3] [GEN4] [GEN5] [Auto]	
PCIE Target Link Speed	[Maximum speed] [GEN1] [GEN2] [GEN3] [GEN4] [GEN5] [Auto]	Set PCIe speed on all ports
ASPM Control	[Disable] [L0s] [L1] [Auto]	No help String
MCTP Enable	[Disable] [Enable] [Auto]	Enable/Disable MCTP
Non-PCIe Compliant Support	[Disable] [Enable] [Auto]	Enable this setting to send command to disable Extended EIEOS, DLF, and Gen 5 Support on training failure for non-pcie compliant devices.
Limit hotplug devices to PCIe Boot Speed	[Auto] [Enable] [Disable]	Enabled: Limit hotplug slots to Gen4 if system booted with only Gen4 devices, which optimizes idle power Disabled: Do not limit hotplug slots to Gen4 if system booted with only Gen4 devices, increases idle power
Enable PCIe SFI Config via OOB	[True] [False]	Enable PCIe SFI Config via OOB support
PCIe Idle Power Setting	[Optimize for Latency] [Optimize for Perf/Power]	Modify PCIe Power Savings Features that Can Impact Lightly Loaded Latency

6.2.4.4.4 nBif Common Options

Advanced

Aptio Setup - AMI

nBif Common Options

▶ RCC_DEVO

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options		
Menu Fields	Settings	Comments
RCC_DEVO	Selects sub-menu	

6.2.4.4.4.1 RCD_DEVO

Aptio Setup - AMI	
Advanced	
RCC_DEVO	
ACS Rcc_Dev0	[Auto]
AER Rcc_Dev0	[Auto]
DlfEnableStrap1	[Auto]
Phy16GTStrap1	[Auto]
MarginEnStrap1	[Auto]
SouceValStrap5	[Auto]
TranslationalBlockingStrap5	[Auto]
P2pReq ACS Control	[Auto]
P2pCompStrap5	[Auto]
UpstreamFwStrap5	[Auto]
P2PEgressStrap5	[Auto]
DirectTranslatedStrap5	[Auto]
SsidEnStrap5	[Auto]
PriEnPageReq	[Auto]
PriResetPageReq	[Auto]
SourceVal ACS cntl	[Auto]
TranslationalBlocking ACS Control	[Auto]
P2pComp ACS Control	[Auto]
UpstreamFwd ACS Control	[Auto]
P2PEgress ACS Control	[Auto]
P2pReqStrap5	[Auto]
E2E_PREFIX	[Auto]
EXTENDED_FMT	[Auto]
AtomicRoutingStrap5	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options \ RCC_DEVO		
Menu Fields	Settings	Comments
ACS Rcc_Dev0	[Auto] [Disable] [Enable]	Enable ACS enable for RCC_DEVO ,STRAP_ACS_EN_DN_DEVO
AER Rcc_Dev0	[Auto] [Disable] [Enable]	Enable AER enable for RCC_DEVO ,STRAP_AER_EN_DN_DEVO
DlfEnableStrap1	[Auto] [Disable] [Enable]	RCC_BIF_STRAP1,STRAP_DLF_EN=1
Phy16GTStrap1	[Auto] [Disable] [Enable]	RCC_BIF_STRAP1 ,STRAP_PHY_16GT_EN=1
MarginEnStrap1	[Auto] [Disable] [Enable]	RCC_BIF_STRAP1 ,STRAP_MARGIN_EN=1
SouceValStrap5	[Auto] [Disable]	RCC_DEVO_PORT_STRAP5 = 0xAF80_0000,Source Validation bit [23]

Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options \ RCC_DEV0		
Menu Fields	Settings	Comments
	[Enable]	
TranslationalBlockingStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, Translational Blocking bit [24]
P2pReq ACS Control	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0 0x001D, P2P page request bit[2]
P2pCompStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, P2P Completion bit[26]
UpstreamFwStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, Upstream Forwarding bit[27]
P2PEgressStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, P2P Egress bit[28]
DirectTranslatedStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, ACS Direct Translated bit [29]
SsidEnStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, ACS SSID Enable bit [31]
PriEnPageReq	[Auto] [Disable] [Enable]	PCIE_PAGE_REQ_CNTL (for all nbio instances) set to 0x0001, PriEn bit set
PriResetPageReq	[Auto] [Disable] [Enable]	PCIE_PAGE_REQ_CNTL (for all nbio instances) set to 0x0001, Pri Reset bit clear
SourceVal ACS cntl	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0 = 0x001D, Source Validation bit [0] is set
TranslationalBlocking ACS Control	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0 = 0x001D, Translational blocking bit[1]
P2pComp ACS Control	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0=0x001D, P2P Completion bit[3]
UpstreamFwd ACS Control	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0 = 0x001D, Upstream Forwarding bit[4]
P2PEgress ACS Control	[Auto] [Disable] [Enable]	PCIE_ACS_CNTL_dev0 = 0x001D, P2P Egress bit[5]
P2pReqStrap5	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000, P2P request strap bit
E2E_PREFIX	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP2 has bit STRAP_E2E_PREFIX_EN_DEV0
EXTENDED_FMT	[Auto] [Disable] [Enable]	RCC_DEV0_PORT_STRAP2 has bit STRAP_EXTENDED_FMT_SUPPORTED_DEV0

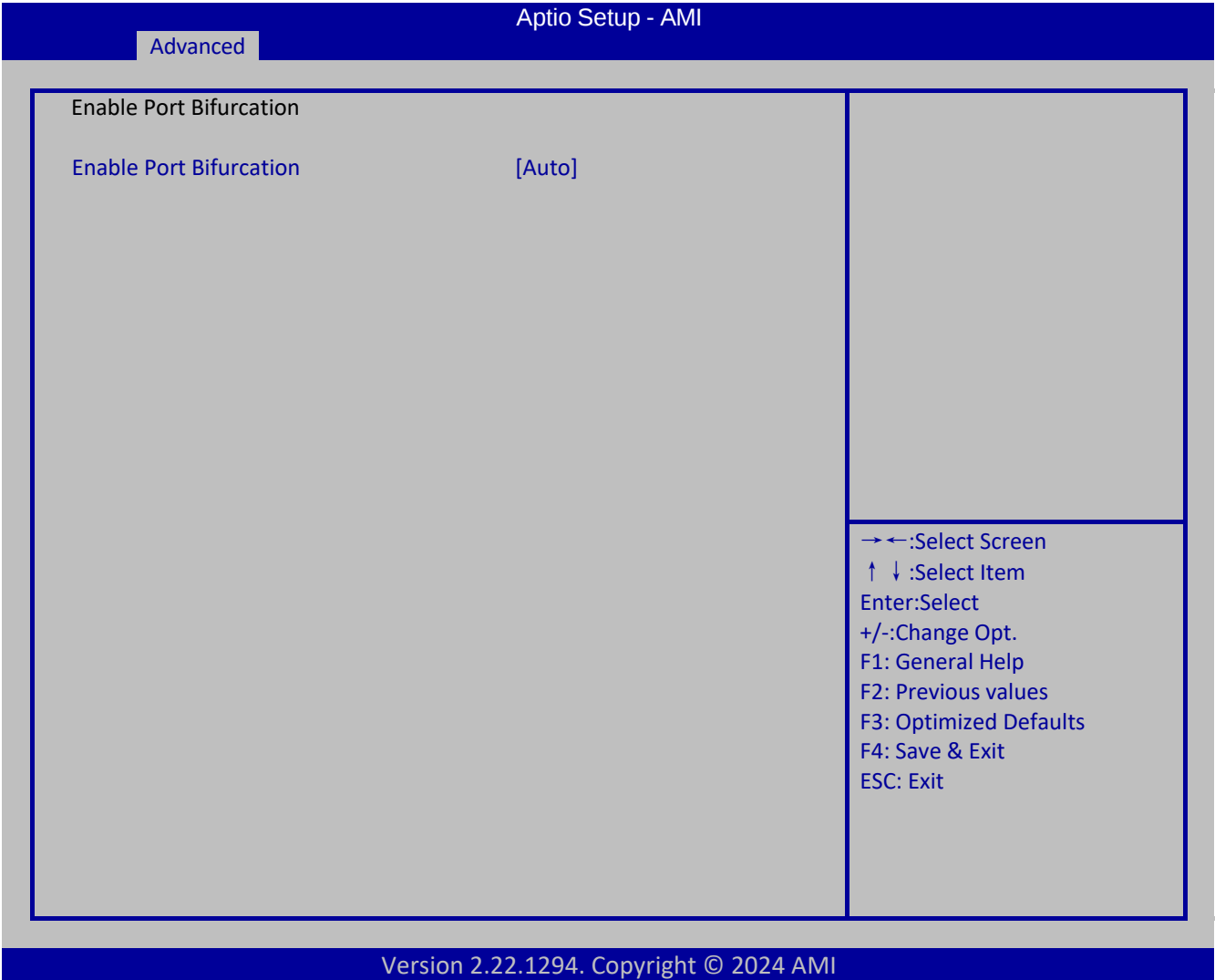
Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options \ RCC_DEV0		
Menu Fields	Settings	Comments
AtomicRoutingStrap5	[Disable]	NBIF DEV0 Enable AtomicOp Routing support in Downstream Port.
	[Enable]	
	[Auto]	

6.2.4.4.5 IOMMU/Security

Aptio Setup - AMI	
Advanced	
IOMMU/Security	
SEV-SNP Support	[Auto]
DRTM Memory Reservation	[Auto]
DRTM Virtual Device Support	[Auto]
DMA Protection	[Auto]
IOMMU	[Auto]
DMAr Suppor	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ NBIO Common Options \ IOMMU/Security		
Menu Fields	Settings	Comments
SEV-SNP Support	[Disabled] [Enabled] [Auto]	Enables support for Secure Encrypted Virtualization and Secure Nested Paging
DRTM Memory Reservation	[Disabled] [Enabled] [Auto]	Reserve 128MB memory below Bottom IO for DRTM. It is required to be enabled for Secured-Core Server function.
DRTM Virtual Device Support	[Disabled] [Enabled] [Auto]	Enable DRTM ACPI virtual device.
DMA Protection	[Auto] [Enabled] [Disabled]	Enable DMA remap support in IVRS IVinfo Field.
IOMMU	[Disabled] [Enabled] [Auto]	Enable/Disable IOMMU
DMAr Suppor	[Disabled] [Enabled] [Auto]	Enable DMAr system protection during POST.

6.2.4.4.6 Enable Port Bifurcation



Advanced \ AMD CBS \ NBIO Common Options \ Enable Port Bifurcation		
Menu Fields	Settings	Comments
Enable Port Bifurcation	[Auto] [Enable] [Disable]	Change the configuration of each PCIe link individually. By default, each link is configured 1 port of 16 lanes. (x16)

6.2.4.4.7 Link EQ Preset Options

Aptio Setup - AMI

Advanced

Link EQ Preset Options

- ▶ GEN3
- ▶ GEN4
- ▶ GEN5

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options		
Menu Fields	Settings	Comments
GEN3	Selects Sub-menu.	
GEN4	Selects Sub-menu.	
GEN5	Selects Sub-menu.	

6.2.4.4.7.1 GEN3

Aptio Setup - AMI

Advanced

GEN3

Preset Search Mask Configuration (Gen3) [Auto]

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN3		
Menu Fields	Settings	Comments
Preset Search Mask Configuration (Gen3)	[Custom] [Auto]	Configuration for Gen3 Preset Mask. Select Custom to modify Gen3 Preset Search Mask. Auto will default to platform configurations.

6.2.4.4.7.2 GEN4

Aptio Setup - AMI

Advanced

GEN4

Preset Search Mask Configuration (Gen4) [Auto]

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN4		
Menu Fields	Settings	Comments
Preset Search Mask Configuration (Gen4)	[Custom] [Auto]	Configuration for Gen4 Preset Mask. Select Custom to modify Gen4 Preset Search Mask. Auto will default to platform configurations.

6.2.4.4.7.3 GEN5

Aptio Setup - AMI

Advanced

GEN5

Preset Search Mask Configuration (Gen5) [Auto]

→←:Select Screen
↑↓:Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN5		
Menu Fields	Settings	Comments
Preset Search Mask Configuration (Gen5)	[Custom] [Auto]	Configuration for Gen5 Preset Mask. Select Custom to modify Gen5 Preset Search Mask. Auto will default to platform configurations.

6.2.4.5 FCH Common Options

Aptio Setup - AMI

Advanced

FCH Common Options

▶ I3C/I2C Configuration Options

▶ SATA Configurations Options

▶ USB Configurations Options

▶ Ac Power Loss Options

▶ Uart Configuration Options

▶ FCH RAS Options

▶ Miscellaneous Options

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options		
Menu Fields	Settings	Comments
I3C/I2C Configuration Options	Selects sub-menu.	
SATA Configurations Options	Selects sub-menu.	
USB Configurations Options	Selects sub-menu.	
Ac Power Loss Options	Selects sub-menu.	
Uart Configuration Options	Selects sub-menu.	
FCH RAS Options	Selects sub-menu.	
Miscellaneous Options	Selects sub-menu.	

6.2.4.5.1 I3c/I2c Configuration Options

Aptio Setup - AMI

Advanced

I3C/I2C Configuration Options

I3C/I2C 0 Enable

I3C/I2C 1 Enable

I3C/I2C 2 Enable

I3C/I2C 3 Enable

I2C 4 Enable

I2C 5 Enable

Release SPD Host Control

Ixc Telemetry Ports Fence Control

I2C SDA Hold Override

APML SB-TSI Mode

I3C Push Pull HCNT Value

I3C SDA Hold Value

I3C SDA Hold Override

[I3C Enabled]

[I3C Enabled]

[I3C Enabled]

[I3C Enabled]

[Auto]

[Auto]

[Enabled]

[Enabled]

[Auto]

[I2C]

8

2

[Auto]

→ ←:Select Screen

↑ ↓:Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ I3C/I2C Configuration Options		
Menu Fields	Settings	Comments
I3C/I2C 0 Enable	[Both Disabled] [I3C Enabled] [I2C Enabled] [Auto]	Enable or disable Inter-Integrated Circuit Control 0
I3C/I2C 1 Enable	[Both Disabled] [I3C Enabled] [I2C Enabled] [Auto]	Enable or disable Inter-Integrated Circuit Control 1
I3C/I2C 2 Enable	[Both Disabled] [I3C Enabled] [I2C Enabled] [Auto]	Enable or disable Inter-Integrated Circuit Control 2
I3C/I2C 3 Enable	[Both Disabled] [I3C Enabled] [I2C Enabled] [Auto]	Enable or disable Inter-Integrated Circuit Control 3
I2C 4 Enable	[Disabled]	Enable or disable Inter-Integrated Circuit Control 4

Advanced \ AMD CBS \ FCH Common Options \ I3C/I2C Configuration Options		
Menu Fields	Settings	Comments
	[Enabled] [Auto]	
I2C 5 Enable	[Disabled] [Enabled] [Auto]	Enable or disable Inter-Integrated Circuit Control 5
Release SPD Host Control	[Disabled] [Enabled]	Release SPD Host Control, so that BMC can take over the ownership of I2C/I3C bus
Ixc Telemetry Ports Fence Control	[Disabled] [Enabled]	Controls the Fencing off for I2C/I3C ports which are involved in DDR Telemetry. If this option is enabled, then the associated Ixc ports registers will be put in the secure region. Note: If this option is disabled, there is a risk of collision happening between x86 accessing IxC and PMFW running DDR Telemetry which can cause undefined behavior.
I2C SDA Hold Override	[Disabled] [Enabled] [Auto]	Override I2C SDA_TX_HOLD and SDA_RT_HOLD
APML SB-TSI Mode	[I3C] [I2C]	Select APML SB-TSI over I3C or I2C. In I3C mode, the slave controller can support both I3C and I2C(Adaptive mode).
I3C Push Pull HCNT Value	X	SCL push-pull High count for I3C transfers targeted to I3C devices
I3C SDA Hold Value	X	I3C SDA Hold Value
I3C SDA Hold Override	[Disabled] [Enabled] [Auto]	I2C3 IC SDA TX HOLD value

6.2.4.5.2 SATA Configuration Options

Advanced

Aptio Setup - AMI

SATA Configuration Options

SATA Enable

[Auto]

SATA RAS Support

[Auto]

SATA Staggered Spin-up

[Auto]

SATA Disabled AHCI Prefetch Function

[Auto]

▶ SATA Controller Options

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options		
Menu Fields	Settings	Comments
SATA Enable	[Disabled]	Disable or enable OnChip SATA controller
	[Enabled]	
	[Auto]	
SATA RAS Support	[Disabled]	Disable or enable Sata RAS Support
	[Enabled]	
	[Auto]	
SATA Staggered Spin-up	[Disabled]	Enable or disable SATA staggered spin-up.
	[Enabled]	
	[Auto]	
SATA Disabled AHCI Prefetch Function	[Disabled]	Disable or enable Sata Disabled AHCI Prefetch Function
	[Enabled]	
	[Auto]	
SATA Controller Options	Selects sub-menu.	

6.2.4.5.2.1 SATA Controller Options

Aptio Setup - AMI	
Advanced	
SATA Controller Options ▶ SATA Controller Enable ▶ SATA Controller eSATA ▶ SATA Controller DevSlp ▶ SATA Controller SGPIO	
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options		
Menu Fields	Settings	Comments
SATA Controller Enable	Selects sub-menu.	
SATA Controller eSATA	Selects sub-menu.	
SATA Controller DevSlp	Selects sub-menu.	
SATA Controller SGPIO	Selects sub-menu.	

6.2.4.5.2.1.1 SATA Controller Enable

Aptio Setup - AMI	
Advanced	
SATA Controller Enable	
Sata0 Enable	[Enabled]
Sata1 Enable	[Enabled]
Sata2 Enable	[Auto]
Sata3 Enable	[Auto]
Sata4 (Socket1) Enable	[Auto]
Sata5 (Socket1) Enable	[Auto]
Sata6 (Socket1) Enable	[Auto]
Sata7 (Socket1) Enable	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller Enable		
Menu Fields	Settings	Comments
Sata0 Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata0. Each IOD has 4 Sata Controllers.
Sata1 Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata1. Each IOD has 4 Sata Controllers.
Sata2 Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata2. Each IOD has 4 Sata Controllers.
Sata3 Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata3. Each IOD has 4 Sata Controllers.
Sata4 (Socket1) Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata4 on Socket 1 (IOD1).. Each IOD has 4 Sata Controllers.
Sata5 (Socket1) Enable	[Disabled] [Enabled]	Enable or Disable Sata5 on Socket 1 (IOD1).. Each IOD has 4 Sata Controllers.

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller Enable		
Menu Fields	Settings	Comments
	[Auto]	
Sata6 (Socket1) Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata6 on Socket 1 (IOD1).. Each IOD has 4 Sata Controllers.
Sata7 (Socket1) Enable	[Disabled] [Enabled] [Auto]	Enable or Disable Sata7 on Socket 1 (IOD1).. Each IOD has 4 Sata Controllers.

6.2.4.5.2.1.2 SATA Controller eSATA

Aptio Setup - AMI

Advanced

SATA Controller eSATA

- ▶ Sata0 eSATA
- ▶ Sata1 eSATA

→ ←: Select Screen
 ↑ ↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options \ SATA Controller Options \ SATA Controller eSATA		
Menu Fields	Settings	Comments
Sata0 eSATA	Selects sub-menu	
Sata1 eSATA	Selects sub-menu	

6.2.4.5.2.1.2.1 Sata0 eSATA

Aptio Setup - AMI	
Advanced	
Sata0 eSATA	
Sata0 eSATA Port0	[eSATA]
Sata0 eSATA Port1	[eSATA]
Sata0 eSATA Port2	[eSATA]
Sata0 eSATA Port3	[eSATA]
Sata0 eSATA Port4	[eSATA]
Sata0 eSATA Port5	[eSATA]
Sata0 eSATA Port6	[eSATA]
Sata0 eSATA Port7	[eSATA]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller eSATA \ Sata0 eSATA		
Menu Fields	Settings	Comments
Sata0 eSATA Port0	[iSATA] [eSATA] [Auto]	External SATA Port support
Sata0 eSATA Port1	[iSATA] [eSATA] [Auto]	External SATA Port support
Sata0 eSATA Port2	[iSATA] [eSATA] [Auto]	External SATA Port support
Sata0 eSATA Port3	[iSATA] [eSATA] [Auto]	External SATA Port support
Sata0 eSATA Port4	[iSATA] [eSATA] [Auto]	External SATA Port support
Sata0 eSATA Port5	[iSATA] [eSATA]	External SATA Port support

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller eSATA \ Sata0 eSATA		
Menu Fields	Settings	Comments
	[Auto]	
Sata0 eSATA Port6	[iSATA]	External SATA Port support
	[eSATA]	
	[Auto]	
Sata0 eSATA Port7	[iSATA]	External SATA Port support
	[eSATA]	
	[Auto]	

6.2.4.5.2.1.2.2 Sata1 eSATA

Aptio Setup - AMI	
Advanced	
Sata1 eSATA	
Sata1 eSATA Port0	[Enabled]
Sata1 eSATA Port1	[Enabled]
Sata1 eSATA Port2	[Enabled]
Sata1 eSATA Port3	[Enabled]
Sata1 eSATA Port4	[Enabled]
Sata1 eSATA Port5	[Enabled]
Sata1 eSATA Port6	[Enabled]
Sata1 eSATA Port7	[Enabled]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller eSATA \ Sata1 eSATA		
Menu Fields	Settings	Comments
Sata1 eSATA Port0	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port1	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port2	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port3	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port4	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port5	[Disabled] [Enabled]	External SATA Port support

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller eSATA \ Sata1 eSATA		
Menu Fields	Settings	Comments
	[Auto]	
Sata1 eSATA Port6	[Disabled] [Enabled] [Auto]	External SATA Port support
Sata1 eSATA Port7	[Disabled] [Enabled] [Auto]	External SATA Port support

6.2.4.5.2.1.3 SATA Controller DevSlp

Advanced

Aptio Setup - AMI

SATA Controller DevSlp

- ▶ Socket0 DevSlp
- ▶ Socket1 DevSlp

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller DevSlp		
Menu Fields	Settings	Comments
Socket0 DevSlp	Selects Sub-menu	
Socket1 DevSlp	Selects Sub-menu	

6.2.4.5.2.1.3.1 Socktet0 DevSlp

Aptio Setup - AMI	
Advanced	
Socket0 DevSlp	
Socket0 DevSlp0 Enable	[Auto]
Socket0 DevSlp1 Enable	[Auto]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller DevSlp \ Socket0 Devslp		
Menu Fields	Settings	Comments
Socket0 DevSlp0 Enable	[Disabled] [Enabled] [Auto]	Enable socket 0 DevSlp0. In SOC two DEVSLP pads are assigned. Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.
Socket0 DevSlp1 Enable	[Disabled] [Enabled] [Auto]	Enable socket 0 DevSlp1. In SOC two DEVSLP pads are assigned. Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.

6.2.4.5.2.1.3.2 Socktet1 DevSlp

Aptio Setup - AMI	
Advanced	
Socket1 DevSlp	
Socket1 DevSlp0 Enable	[Auto]
Socket1 DevSlp1 Enable	[Auto]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller DevSlp \ Socket1 Devslp		
Menu Fields	Settings	Comments
Socket1 DevSlp0 Enable	[Disabled] [Enabled] [Auto]	Enable socket 1 DevSlp0. In SOC two DEVSLP pads are assigned. Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.
Socket1 DevSlp1 Enable	[Disabled] [Enabled] [Auto]	Enable socket 1 DevSlp1. In SOC two DEVSLP pads are assigned. Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.

6.2.4.5.2.1.4 SATA Controller SGPIO

Aptio Setup - AMI	
Advanced	
SATA Controller SGPIO	
Sata0 SGPIO	[Enabled]
Sata1 SGPIO	[Enabled]
Sata2 SGPIO	[Auto]
Sata3 SGPIO	[Auto]
Sata4 SGPIO	[Auto]
Sata5 SGPIO	[Auto]
Sata6 SGPIO	[Auto]
Sata7 SGPIO	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller SGPIO		
Menu Fields	Settings	Comments
Sata0 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpios on Sata0
Sata1 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpios on Sata1
Sata2 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpios on Sata2
Sata3 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpios on Sata3
Sata4 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpios on Sata4 (Socket1)
Sata5 SGPIO	[Disabled] [Enabled]	Enable or Disable SataSgpios on Sata5 (Socket1)

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller SGPIO		
Menu Fields	Settings	Comments
	[Auto]	
Sata6 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpio on Sata6 (Socket1)
Sata7 SGPIO	[Disabled] [Enabled] [Auto]	Enable or Disable SataSgpio on Sata7 (Socket1)

6.2.4.5.3 USB Configuration Options

Aptio Setup - AMI

Advanced

USB Configuration Options

XHCI Controller0 Enable

[Auto]

XHCI Controller1 Enable

[Auto]

► MCM USB enable

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

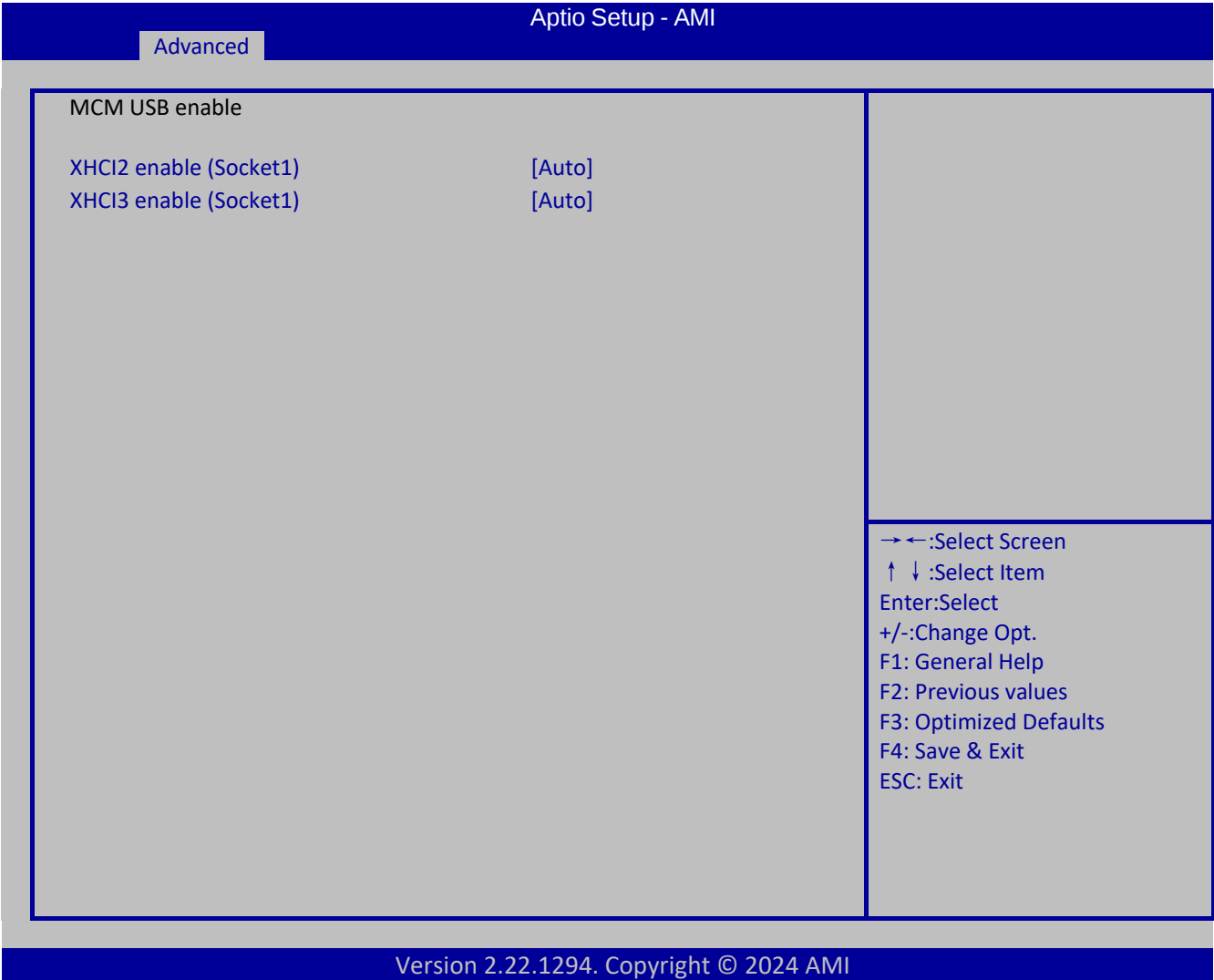
F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ USB Configuration Options		
Menu Fields	Settings	Comments
XHCI Controller0 Enable	Enabled Disabled Auto	Enable or disable USB3 controller
XHCI Controller1 Enable	Enabled Disabled Auto	Enable or disable USB3 controller
MCM USB enable	Select sub	

6.2.4.5.3.1 MCM USB enable



Advanced \ AMD CBS \ FCH Common Options \ USB Configuration Options \ MCM USB enable		
Menu Fields	Settings	Comments
XHCI2 enable (Socket1)	[Enabled]	Enable or disable USB3 controller
	[Disabled]	
	[Auto]	
XHCI3 enable (Socket1)	[Enabled]	Enable or disable USB3 controller
	[Disabled]	
	[Auto]	

6.2.4.5.4 AC Power Loss Options

Advanced

Aptio Setup - AMI

Ac Power Loss Options

Ac Loss Control

Set Fch Power failed shadow in ABL

[Always off]

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ USB Configuration Options \ Ac Power Loss Options		
Menu Fields	Settings	Comments
Ac Loss Control	[Always off]	Select Ac Loss Control Method
	[Always on]	
	[Reserved]	
	[Previous]	
Set Fch Power failed shadow in ABL	[Auto]	
	[Enabled]	
	[Disabled]	
	[Auto]	

6.2.4.5.5 Uart Configuration Options

Aptio Setup - AMI	
Advanced	
Uart Configuration Options	
Uart 0 Enable	[Auto]
Uart 1 Enable	[Auto]
Uart 2 Enable	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ Uart Configuration Options		
Menu Fields	Settings	Comments
Uart 0 Enable	[Disabled]	Enable or disable Uart0. Uart 0 has no HW flow control if Uart 2 is enabled
	[Enabled]	
	[Auto]	
Uart 1 Enable	[Disabled]	Enable or disable Uart1
	[Enabled]	
	[Auto]	
Uart 2 Enable	[Disabled]	Enable or disable Uart2. If Uart2 is enable, Uart0 has no HW flow control.
	[Enabled]	
	[Auto]	

6.2.4.5.6 FCH RAS Options

Advanced

Aptio Setup - AMI

FCH RAS Options

ALink RAS Support

Reset After Sync-Flood

[Auto]

[Auto]

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ FCH Common Options \ FCH RAS Options		
Menu Fields	Settings	Comments
ALink RAS Support	[Disabled]	Enable FCH A-Link parity error
	[Enabled]	
	[Auto]	
Reset After Sync-Flood	[Disabled]	Enable AB to forward downstream sync-flood message to system controller.
	[Enabled]	
	[Auto]	

6.2.4.5.7 Miscellaneous Options

Aptio Setup - AMI	
Advanced	
Miscellaneous Options	
FCH Spread Spectrum	[Auto]
Boot Timer Enable	[Auto]
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ FCH Common Options \ Miscellaneous Options		
Menu Fields	Settings	Comments
FCH Spread Spectrum	[Disabled] [Enabled] [Auto]	Select whether or not Enable the Spread Spectrum Feature.
Boot Timer Enable	[Disabled] [Enabled] [Auto]	Boot time enable. Enable : force PMx44 bit 27 = 1 Disable : force PMx44 bit 27 = 0 Auto: PMx44 bit 27 = PcdbootTimerEnable

6.2.4.6 Soc Miscellaneous Control

Aptio Setup - AMI

Advanced

Soc Miscellaneous Control

ABL Console Out Control [Auto]

ABL Console Out Serial Port [Auto]

ABL Console Out Serial Port IO [Auto]

ABL Serial port IO customized enabled [Disabled]

ABL Basic Console Out Control [Auto]

ABL PMU message Control [Auto]

ABL Memory Population message Control [Warning message]

Print Socket 1 PMU MsgBlock [Disabled]

Print Socket 1 PMU Training Log [Disabled]

PSP error injection Support [False]

► Firmware Anti-rollback (FAR)

SEC_I2C Voltage Mode [Auto]

→ ← : Select Screen

↑ ↓ : Select Item

Enter : Select

+/- : Change Opt.

F1 : General Help

F2 : Previous values

F3 : Optimized Defaults

F4 : Save & Exit

ESC : Exit

Version 2.22.1294. Copyright © 2024 AMI

Advanced \ AMD CBS \ Soc Miscellaneous Control		
Menu Fields	Settings	Comments
ABL Console Out Control	[Disable] [Enable] [Auto]	Enable: Enable ConsoleOut Function for ABL Disable: Disable ConsoleOut Functions for ABL Auto: Keep default behavior
ABL Console Out Serial Port	[eSPI UART] [SOC UART0] [SOC UART1] [Auto]	eSPI UART: Enabled serial port through eSPI UART SOC UART0: Enabled serial port through SOC UART0 SOC UART1: Enabled serial port through SOC UART1 Auto: Keep default behavior
ABL Console Out Serial Port IO	[0x3F8] [0x2F8] [0x3E8] [0x2E8] [Auto]	Select Legacy Uart (SIO or eSPI) IO base 0x3F8: Set IO base to 0x3F8 0x2F8: Set IO base to 0x2F8 0x3E8: Set IO base to 0x3E8 0x2E8: Set IO base to 0x2E8 Auto: Keep default behavior Please make sure the selected eSPI IO base and length has been filled in APCB_FCH_TYPE_ESPI_INIT or APCB_FCH_TYPE_ESPI1_INIT EspilnitConfiguration table. CRB only fills 0x3F8,0x2F8 in it by default.

Advanced \ AMD CBS \ Soc Miscellaneous Control		
Menu Fields	Settings	Comments
ABL Serial port IO customized enabled	[Disabled] [Enabled]	Enabled: Can input IO based for ABL console out Serial Port IO by ABL. Console out Serial port IO Customized.
ABL Console out Serial Port IO Customized	0	0: disabled. no supported (default value). Please input your eSPI UART io based in non zero value. Also please make sure the selected eSPI IO base and length has been filled in APGB_FCH_TYPE_ESPI_INIT or APGB_FCH_TYPE_ESPI1_INIT EspiInitConfiguration table.
ABL Basic Console Out Control	[Disable] [Enable] [Auto]	Enable: Enable Basic ConsoleOut Function for ABL. Disable: Disable Basic ConsoleOut Function for ABL. Auto: Keep default behavior.
ABL PMU message Control	[Detailed debug message] [Coarse debug message] [Stage completion] [Auto]	To control the total number of PMU debug messages. Several major controls are listed below: 1. Detailed debug messages (e.g. Eye delays) 2. Coarse debug messages (e.g. rank information) 3. Stage completion
ABL Memory Population message Control	[Warning message] [Fatal error]	Non-Recommended configurations may be functional but may not be validated by AMD. Select 'warning message': To show warning messages if Memory channel configuration does Not follow SP5 Memory Population Guidelines. 'Fatal error': To show the messages and halt the system.
Print Socket 1 PMU MsgBlock	[Disabled] [Enabled]	Print Socket 1 PMU MsgBlock contents after training.
Print Socket 1 PMU Training Log	[Disabled] [Enabled]	Print Socket 1 PMU training log while 'ABL PMU message Control' == Detailed debug message.
PSP error injection Support	[False] [True]	Enable EINJ support
Firmware Anti-rollback (FAR)	Selects sub-menu.	
SEC_I2C Voltage Mode	[Auto] [1.8 V] [1.1 V]	This option allows to select SEC I2C voltage. Valid options: - Auto (Leave it to silicon initial value) - 1.8V - 1.1V

6.2.4.6.1 Firmware Anti-rollback (FAR)

Aptio Setup - AMI	
Advanced	
Firmware Anti-rollback (FAR)	
FAR enforcement state	[Enable]
SPL value in the CPU fuse	0
SPL value in the SPL table	0
FAR Switch	[Auto]
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1294. Copyright © 2024 AMI	

Advanced \ AMD CBS \ Soc Miscellaneous Control \ Firmware Anti-rollback (FAR)		
Menu Fields	Settings	Comments
FAR enforcement state	[Disabled] [Enable]	Enabled = FAR is permanently enforced in the CPU, the system can only boot from BIOS with update to date firmware stack as defined by SPL table. Disabled = FAR is NOT enforced in the CPU
SPL value in the CPU fuse	X	The current SPL value in the CPU fuse which is converted from fuse bitmask
SPL value in the SPL table	X	if Initial SPL value is set to 0, the SPL fuse in the CPU will be upgraded to the SPL value in the SPL table at next boot.
FAR Switch	[Disabled] [Enabled] [Auto]	[Enabled]: BIOS will update SPL fuse to SPL value in the SPL table. [Disable]: BIOS will not set SPL fuse.

6.2.4.7 CXL Common Options

Aptio Setup - AMI

Advanced

CXL Common Options

CXL Control [Auto]

CXL Physical Addressing [Auto]

CXL Memory attribute [Auto]

CXL Encryption [Disabled]

CXL DVSEC Lock [Auto]

CXL HDM Decoder Lock On Commit [Auto]

Temp Gen5 Advertisement [Auto]

Sync Header Bypass [Auto]

Sync Header Bypass Compatibility Mode [Auto]

► CXL RAS

CXL Memory Online/Offline [Disabled]

Override CXL Memory Size [Auto]

→ ← :Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ AMD CBS \ CXL Common Options		
Menu Fields	Settings	Comments
CXL Control	[Auto] [Enabled] [Disabled]	Force enablement of CXL on all ports. Disabled: Allow platforms to enable CXL by port Enabled: Force enablement of CXL on all ports.
CXL Physical Addressing	[Normalized address] [System address] [Auto]	Control SDP request system address. Normalized address: CS sends normalized address to SDP; System address: CS sends system address to SDP.
CXL Memory Attribute	[Auto] [Enabled] [Disabled]	Sets CXL memory as Special Purpose Memory
CXL Encryption	[Enabled] [Disabled]	CXL Encryption
CXL DVSEC Lock	[Auto] [Enabled] [Disabled]	Locks the CXL DVSEC
CXL HDM Decoder Lock On Commit	[Auto] [Enabled] [Disabled]	The CXL HDM Decoder will become read only when the decoder becomes active.
Temp Gen5 Advertisement	[Disable]	Temp Gen5 Advertisement for Alternate Protocol

Advanced \ AMD CBS \ CXL Common Options		
Menu Fields	Settings	Comments
	[Enable] [Auto]	
Sync Header Bypass	[Auto] [Enabled] [Disabled]	Enable/Disable Sync Header Bypass
Sync Header Bypass Compatibility Mode	[Auto] [Enabled] [Disabled]	Enable/Disable Sync Header Bypass Compatibility Mode
CXL RAS	Selects sub-menu.	
CXL Memory Online/Offline	[Disabled] [Enabled]	All 4 Plink slots support memory online/offline Only slot4 of Amber supports hot plug CXL memory interleaving automatically disabled globally when this CBS is enabled
Override CXL Memory Size	[32GB] [64GB] [128GB] [Auto]	No help String

6.2.4.7.1 CXL RAS

Aptio Setup - AMI	
Advanced	
CXL RAS	
CXL Protocol Error Reporting	[SameAsPcieAer]
CXL Component Error Reporting	[Debug FW-First]
CXL Root Port Isolation	[Auto]
CXL Root Port Isolation FW Notification	[Auto]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ AMD CBS \ CXL Common Options \ CXL RAS		
Menu Fields	Settings	Comments
CXL Protocol Error Reporting	[Disabled] [SameAsPcieAer] [ForceAerFWFirstIfCxlPresent]	Configure CXL Protocol Error reporting mechanism
CXL Component Error Reporting	[Allow OS-First] [Force FW-First] [Debug FW-First]	Configure CXL Component Error reporting mechanism
CXL Root Port Isolation	[Auto] [Enabled] [Disabled]	Enable/Disable CXL.mem Root Port Isolation
CXL Root Port Isolation FW Notification	[Auto] [Enabled] [Disabled]	Enable/Disable CXL.mem Root Port Isolation Notification

6.2.5 S5 RTC Wake Settings

Aptio Setup - AMI	
Advanced	
Wake system from S5	[Disabled]
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ S5 RTC Wake Settings		
Menu Fields	Settings	Comments
Wake system from S5	[Disabled] [Fixed Time] [Dynamic Time]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time + Increase minute(s)

6.2.6 Serial Port Console Redirection

Aptio Setup - AMI

Advanced

COM0

Console Redirection [Disable]

▶ Console Redirections Setting

Legacy Console Redirection

▶ Legacy Console Redirection Settings

Serial Port for Out-of-Band Management/
Windows Emergency Management Services (EMS)

Console Redirections EMS [Disabled]

▶ Console Redirection Settings

→ ←: Select Screen

↑ ↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Serial Port Console Redirection		
Menu Fields	Settings	Comments
Console Redirection	[Disabled] [Enabled]	Console Redirection Enable or Disable
Console Redirections Setting	Selects sub-menu	
Legacy Console Redirection Settings	Selects sub-menu	
Console Redirections EMS	[Disabled] [Enabled]	Console Redirection Enable or Disable
Console Redirection Settings	Selects sub-menu	

6.2.6.1 COM0 Console Redirection Setting

Aptio Setup - AMI	
Advanced	
COM0 Console Redirection Settings Terminal Type [ANSI] Bits per second [115200] Data Bits [8] Parity [None] Stop Bits [1] Flow Control [None] VT-UTF8 Combo Key Support [Enabled] Recorder Mode [Disabled] Resolution 100*31 [Disabled] Putty KeyPad [VT100]	
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	Settings	Comments
Terminal Type	[VT100] [VT100Plus] [VT-UTF8] [ANSI]	Terminal Type for Redirection Via AMI Debugger. Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	[9600] [19200] [38400] [57600] [115200] [230400] [460800] [921600]	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	[7] [8]	Data Bits
Parity	[None] [Even]	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the

Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	Settings	Comments
	[Odd] [Mark] [Space]	data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	[1] [2]	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	[None] [Hardware RTS/CTS]	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTFB Combo Key Support	[Disabled] [Enabled]	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	[Disabled] [Enabled]	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100*31	[Disabled] [Enabled]	Enables or disables extended terminal resolution
Putty KeyPad	[VT100] [LINUX] [XTERMR6] [SC0] [ESCN] [VT400]	Select FunctionKey and KeyPad on Putty.

6.2.6.2 Legacy Console Redirection Settings

Aptio Setup - AMI	
Advanced	
Legacy Console Redirection Settings	
Redirection COM Port	[COM0]
Resolution	[80X24]
Redirect After POST	[Always Enable]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ Serial Port Console Redirection \ Legacy Console Redirection Settings		
Menu Fields	Settings	Comments
Redirection COM Port	[COM0]	Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages
Resolution	[80X24] [80X25]	On Legacy OS, the Number of Rows and Columns supported redirection
Redirect After POST	[Always Enable] [BootLoader]	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

6.2.6.3 Console Redirection Setting

Aptio Setup - AMI		
Advanced		
Out-of-Band Mgmt Port	COM0	
Terminal Type EMS	[VT-UTF8]	
Bits per second EMS	[115200]	
Flow Control EMS	[None]	
Data Bits EMS	8	
Parity EMS	None	
Stop Bits EMS	1	
		→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	Settings	Comments
Out-of-Band Mgmt Port	COM0	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.
Terminal Type EMS	[VT100] [VT100Plug] [VT-UTF8] [ANSI]	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per second EMS	[9600] [19200] [57600] [115200]	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control EMS	[None] [Hardware RTS/CTS] [Software Xon/Xoff]	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
Data Bits EMS	8	Data Bits

Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	Settings	Comments
Parity EMS	None	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits EMS	1	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.

6.2.7 CPU Configuration

Advanced

Aptio Setup - AMI

CPU Configuration

SVM Mode

[Enabled]

▶ Node 0 Information

▶ Node 1 Information

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ CPU Configuration		
Menu Fields	Settings	Comments
SVM Mode	[Disabled] [Enabled]	Enable/disable CPU Virtualization
Node 0 Information	Selects sub-menu	
Node 1 Information	Selects sub-menu	

6.2.7.1 Node 0 Information

Aptio Setup - AMI	
Advanced	
Node 0 Information AMD EPYC 9655 96-Core Processor 96 Cores 192 Threads Running @ 2600 MHz 900 mV Processor Family: 1Ah Processor Model: 00h-0Fh Microcode Path Level: B00211A ----- Cache per Core ----- L1 Instruction Cache: 32 KB/12-way L1 Data Cache: 48 KB/8-way L2 Cache: 1024 KB/16-way L3 Cache per Socket: 384 MB/16-way	→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1284. Copyright © 2022 AMI	

6.2.7.2 Node 1 Information

Aptio Setup - AMI	
Advanced	
Node 1 Information AMD EPYC 9655 96-Core Processor 96 Cores 192 Threads Running @ 2600 MHz 900 mV Processor Family: 1Ah Processor Model: 00h-0Fh Microcode Path Level: B00211A ----- Cache per Core ----- L1 Instruction Cache: 32 KB/12-way L1 Data Cache: 48 KB/8-way L2 Cache: 1024 KB/16-way L3 Cache per Socket: 384 MB/16-way	→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.8 PCI Subsystem Settings

Aptio Setup - AMI	
Advanced	
AMI PCI Driver Version : A5.01.32	
PCI Settings Common for all Devices :	
Above 4G Decoding	[Enabled]
SR-IOV Support	[Enabled]
BME DMA Mitigation	[Disabled]
Hot-Plug Support	[Enabled]
Change Setting of the Following PCI Device :	
WARNING : Changing PCI Device(s) Settings may Have unwanted side effects! System may HANG! PROCEED WITH CAUTION.	
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ PCI Subsystem Settings		
Menu Fields	Settings	Comments
Above 4G Decoding	[Disabled] [Enabled]	Globally Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).
SR-IOV Support	[Disabled] [Enabled]	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.
BME DMA Mitigation	[Disabled] [Enabled]	Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked
Hot-Plug Support	[Disabled] [Enabled]	Globally Enables or Disables Hot-Plug support for the entire System. If System has Hot-Plug capable Slots and this option set to Enabled, it provides a Setup screen for selecting PCI resource padding for Hot-Plug.

6.2.9 USB Configuration

Aptio Setup - AMI	
Advanced	
USB Configuration	
USB Module Version	37
USB Controllers : 2 XHCIs	
USB Devices : 9 Drives, 4 Keyboards, 2 Mice, 3 Hubs	
Legacy USB Support	[Enabled]
XHCI Hand-off	[Enabled]
USB Mass Storage Driver Support	[Enabled]
Port 60/64 Emulation	[Enabled]
USB hardware Delays and time-outs :	
USB transfer time-out	[20 sec]
Device reset time-out	[20 sec]
Device power-up delay	[Auto]
Mass Storage Devices :	
AMI IPMI CDROM0 1.00	[Auto]
AMI Virtual CDROM0 1.00	[Auto]
AMI Virtual HDisk0 1.00	[Auto]
AMI Virtual CDROM1 1.00	[Auto]
AMI Virtual CDROM2 1.00	[Auto]
AMI Virtual CDROM3 1.00	[Auto]
AMI Virtual HDisk1 1.00	[Auto]
AMI Virtual HDisk2 1.00	[Auto]
AMI Virtual HDisk3 1.00	[Auto]
→←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ USB Configuration		
Menu Fields	Settings	Comments
Legacy USB Support	[Enabled] [Disabled] [Auto]	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	[Enabled] [Disabled]	This is a workaround for OSES without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	[Disabled] [Enabled]	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation	[Disabled] [Enabled]	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSES.
USB transfer time-out	[1 sec] [5 sec] [10 sec] [20 sec]	The time-out value for Control, Bulk, and Interrupt transfers.

Advanced \ USB Configuration		
Menu Fields	Settings	Comments
Device reset time-out	[10 sec] [20 sec] [30 sec] [40 sec]	USB mass storage device Start Unit command time-out.
Device power-up delay	[Auto] [Manual]	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.
AMI IPMI CDROM0 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual CDROM0 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual HDisk0 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual CDROM1 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual CDROM2 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual CDROM3 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual HDisk1 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual HDisk2 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.
AMI Virtual HDisk3 1.00	[Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

6.2.10 Network Stack Configuration

Aptio Setup - AMI	
Advanced	
Network Stack	[Enabled]
IPv4 PXE Support	[Enabled]
IPv4 HTTP Support	[Enabled]
IPv6 PXE Support	[Disabled]
IPv6 HTTP Support	[Disabled]
PXE boot wait time	0
Media detect Count	1
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Network Stack Configuration		
Menu Fields	Settings	Comments
Network Stack	[Disabled] [Enabled]	Enable/Disable UEFI Network Stack
IPv4 PXE Support	[Disabled] [Enabled]	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	[Disabled] [Enabled]	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	[Disabled] [Enabled]	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	[Disabled] [Enabled]	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	x	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect Count	x	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

6.2.11 NVME Configuration

Aptio Setup - AMI	
Advanced	
NVMe Configuration xxx xxxxx	
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ NVME Configuration		
Menu Fields	Settings	Comments
xxxxxx	Selects sub-menu.	Displays the NVMe Device Name and enter NVMe information page and control settings.

6.2.12 SATA Configuration

Aptio Setup - AMI	
Advanced	
SATA Configuration	
SATA Controller (S:00 B:72 D:00 F:00)	
Port 0	Not Present
Port 1	Not Present
Port 2	Not Present
Port 3	Not Present
Port 4	Not Present
Port 5	Not Present
Port 6	Not Present
Port 7	Not Present
SATA Controller (S:00 B:72 D:00 F:01)	
Port 0	Not Present
Port 1	Not Present
Port 2	Not Present
Port 3	Not Present
Port 4	Not Present
Port 5	Not Present
Port 6	Not Present
Port 7	Not Present
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.13 System Configuration

Aptio Setup - AMI	
Advanced	
Current Config: Select JMCIO2/3/4	[2U 8x SATA + 4x Tri-mode] [JMCIO2/3/4 SATA Mode]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ USB Configuration		
Menu Fields	Settings	Comments
Current Config	[2U 8x SATA + 4x Tri-mode]	Current System Configuration Auto switch by BMC, no need to select
	[1U 12x NVMe]	
	[2U 24x NVMe]	
	[2U 8x Sata + 16x NVMe]	
Select JMCIO2/3/4	[2U 12x NVMe]	Select JMCIO2/3/4 with PCIe Mode or SATA Mode
	[JMCIO2/3/4 SATA Mode]	
	[JMCIO2/3/4 PCIe Mode]	

6.2.14 AMD Mem Configurations Status

Aptio Setup - AMI

Advanced

▶ Socket 0

▶ Socket 1

Mbist Test Enable	Disabled, 0xC000
Mbist Aggressor Enable	Disabled, 0xC000
Mbist Per Bit Slave Die Report	0x0000, 0xC000
Dram Temp Controlled Refresh Enable	Disabled, 0xC001
User Timing Mode	Disabled, 0x0000
User Timing Value	Disabled, 0x0000
Mem Bus Freq Limit	Disabled, 0x0000
Enable Power Down	Disabled, 0xC000
Dram Double Refresh Rate	Disabled, 0x0000
Pmu Train Mode	0x0000, 0xC000
Ecc Symbol Size	0x0000, 0xC000
Uncorrectable Ecc Retry	Disabled, 0xC004
Ignore Spd Checksum	Disabled, 0xC000
Enable Bank Group Swap Alt	Disabled, 0x0000
Enable Bank Group Swap	Disabled, 0xC000
Ddr Route Balanced Tee	Disabled, 0xC004
Nvdimmm Power Source	0x0000, 0xC004
Odts Cmd Throt Enable	Disabled, 0xC004
Odts Cmd Throt Cycle	Disabled, 0xC004

→ ← :Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ AMD Mem Configuration Status		
Menu Fields	Settings	Comments
Socket 0	Selects Sub-menu	
Socket 1	Selects Sub-menu	

6.2.14.1 Socket 0

Aptio Setup - AMI	
Advanced	
▶ Channel 0 ▶ Channel 1 ▶ Channel 2 ▶ Channel 3 ▶ Channel 4 ▶ Channel 5 ▶ Channel 6 ▶ Channel 7 ▶ Channel 8 ▶ Channel 9 ▶ Channel 10 ▶ Channel 11	Enabled, 0xC000 Disabled, 0xC001 0x0000, 0xC000
Dram ECC Dram Parity Dimm Sensor Fine Grain Mode	→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ AMD Mem Configuration Status \ Socket 0		
Menu Fields	Settings	Comments
Channel 0	Selects Sub-menu	
Channel 1	Selects Sub-menu	
Channel 2	Selects Sub-menu	
Channel 3	Selects Sub-menu	
Channel 4	Selects Sub-menu	
Channel 5	Selects Sub-menu	
Channel 6	Selects Sub-menu	
Channel 7	Selects Sub-menu	
Channel 8	Selects Sub-menu	
Channel 9	Selects Sub-menu	
Channel 10	Selects Sub-menu	
Channel 11	Selects Sub-menu	

6.2.14.1.1 Channel 0

Aptio Setup - AMI

Advanced

DIMM0 Presence

Chipsel/Bank Interleave

Present

Enabled, 0xC000

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.1.2 Channel 1

Aptio Setup - AMI

Advanced

DIMM0 Presence
Chipsel/Bank Interleave

Present
Enabled, 0xC000

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.1.3 Channel 2

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.4 Channel 3

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.5 Channel 4

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.6 Channel 5

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.7 Channel 6

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.8 Channel 7

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.9 Channel 8

Aptio Setup - AMI

Advanced

DIMM0 Presence
Chipsel/Bank Interleave

Present
Enabled, 0xC000

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.1.10Channel 9

Aptio Setup - AMI

Advanced

DIMM0 Presence

Chipsel/Bank Interleave

Present

Enabled, 0xC000

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.1.11 Channel 10

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.1.12Channel 11

Aptio Setup - AMI

Advanced

DIMM0 Presence

Chipsel/Bank Interleave

Present

Enabled, 0xC000

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.2 Socket 1

Aptio Setup - AMI	
Advanced	
▶ Channel 0 ▶ Channel 1 ▶ Channel 2 ▶ Channel 3 ▶ Channel 4 ▶ Channel 5 ▶ Channel 6 ▶ Channel 7 ▶ Channel 8 ▶ Channel 9 ▶ Channel 10 ▶ Channel 11	Enabled, 0xC000 Disabled, 0xC001 0x0000, 0xC000
Dram ECC Dram Parity Dimm Sensor Fine Grain Mode	→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ AMD Mem Configuration Status \ Socket1		
Menu Fields	Settings	Comments
Channel 0	Selects Sub-menu	
Channel 1	Selects Sub-menu	
Channel 2	Selects Sub-menu	
Channel 3	Selects Sub-menu	
Channel 4	Selects Sub-menu	
Channel 5	Selects Sub-menu	
Channel 6	Selects Sub-menu	
Channel 7	Selects Sub-menu	
Channel 8	Selects Sub-menu	
Channel 9	Selects Sub-menu	
Channel 10	Selects Sub-menu	
Channel 11	Selects Sub-menu	

6.2.14.2.1 Channel 0

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.2 Channel 1

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.3 Channel 2

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.4 Channel 3

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.5 Channel 4

Aptio Setup - AMI

Advanced

DIMM0 Presence
Chipsel/Bank Interleave

Present
Enabled, 0xC000

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.2.6 Channel 5

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.7 Channel 6

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.8 Channel 7

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ← : Select Screen ↑ ↓ : Select Item Enter : Select +/- : Change Opt. F1 : General Help F2 : Previous values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.9 Channel 8

Aptio Setup - AMI	
Advanced	
DIMM0 Presence Chipsel/Bank Interleave	Present Enabled, 0xC000
→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

6.2.14.2.10Channel 9

Aptio Setup - AMI

Advanced

DIMM0 Presence
Chipsel/Bank Interleave

Present
Enabled, 0xC000

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.2.11Channel 10

Aptio Setup - AMI

Advanced

DIMM0 Presence

Chipsel/Bank Interleave

Present

Enabled, 0xC000

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.14.2.12Channel 11

Aptio Setup - AMI

Advanced

DIMM0 Presence
Chipsel/Bank Interleave

Present
Enabled, 0xC000

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

6.2.15 Tls Auth Configuration

Advanced

Aptio Setup - AMI

▶ Server CA Configuration

▶ Client Cert Configuration

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Tls Auth Configuration		
Menu Fields	Settings	Comments
Server CA Configuration	Selects Sub-menu	
Client Cert Configuration	Selects Sub-menu	

6.2.15.1 Server CA Configuration

Advanced

Aptio Setup - AMI

▶ Enroll Cert

▶ Delete Cert

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ Tls Auth Configuration \ Server CA Config		
Menu Fields	Settings	Comments
Enroll Cert	Selects Sub-menu	
Delete Cert	Selects Sub-menu	

6.2.15.1.1 Enroll Cert

Aptio Setup - AMI

Advanced

▶ Enroll Cert Using File

Cert GUID

▶ Commit Changes and Exit

▶ Discard Changes and Exit

→ ← : Select Screen

↑ ↓ : Select Item

Enter : Select

+/- : Change Opt.

F1 : General Help

F2 : Previous values

F3 : Optimized Defaults

F4 : Save & Exit

ESC : Exit

Version 2.22.1284. Copyright © 2022 AMI

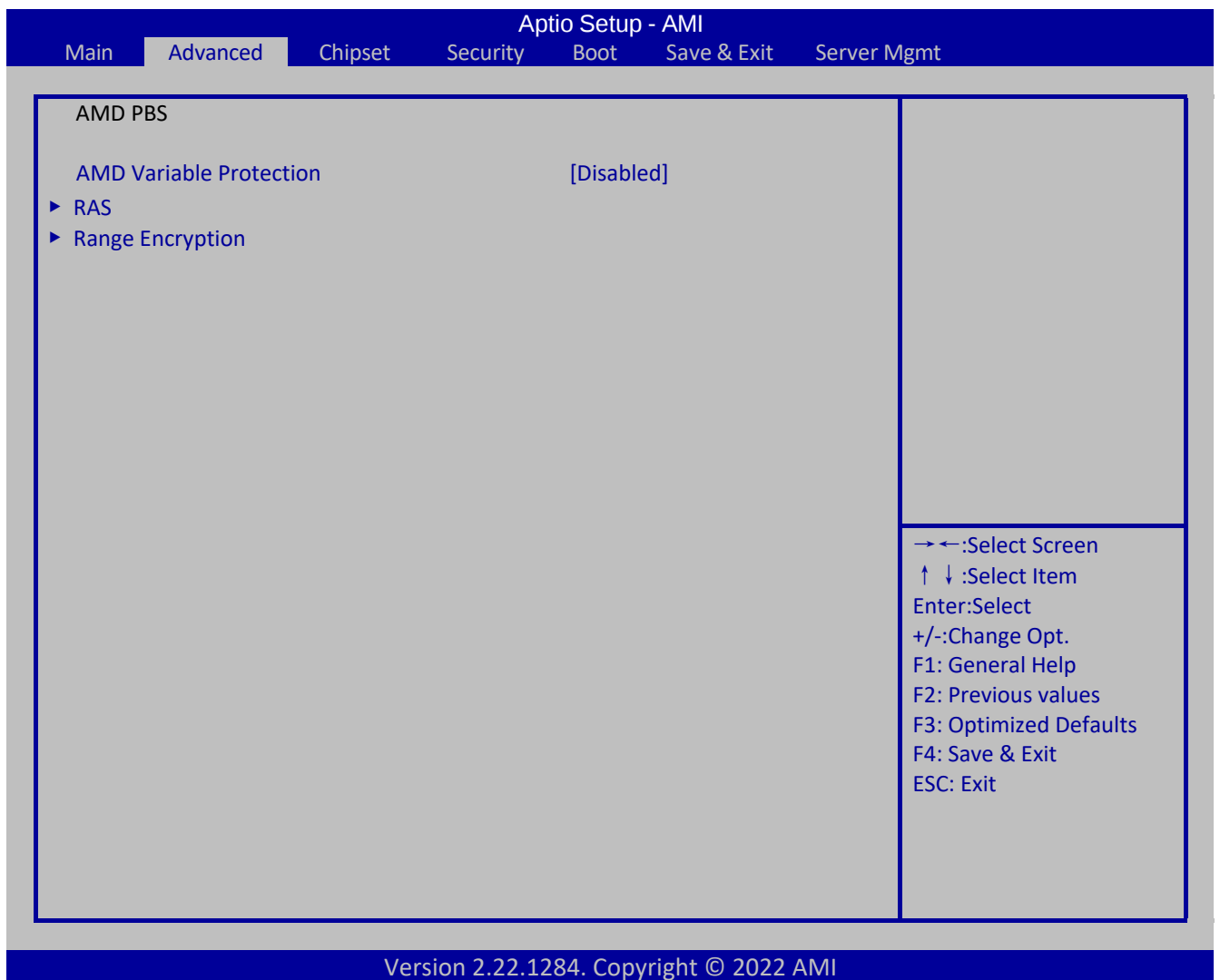
Advanced \ Tls Auth Configuration \ Server CA Config		
Menu Fields	Settings	Comments
Enroll Cert Using File	Select Storage Device	Enroll Cert Using File
Cert GUID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Input digit character in 11111111-2222-3333-4444-1234567890ab format.
Commit Changes and Exit		Commit Changes and Exit
Discard Changes and Exit		Discard Changes and Exit

6.2.15.1.2 Delete Cert

Aptio Setup - AMI	
Advanced	
FE9C6606-8B49-44A3-8B6B-DEA3A0E0324D	[Disabled]
→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1284. Copyright © 2022 AMI	

Advanced \ Tls Auth Configuration		
Menu Fields	Settings	Comments
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	[Disabled]	GUID for CERT
XXXXXXXXXXXX	[Enabled]	

6.2.16 AMD PBS



Advanced \ AMD PBS		
Menu Fields	Settings	Comments
AMD Variable Protection	[Disabled] [Enabled]	Protect some AMD Specific variables for CBS, PBS and ADD. If locked, some utilities like RU that modify variable at runtime do not work.
RAS	Selects Sub-menu	AMD CPM RAS related settings
Range Encryption	Selects Sub-menu	AMD Range Encryption Setting

6.2.16.1 RAS

Aptio Setup - AMI		
Main	Advanced	Chipset
Security Boot Save & Exit Server Mgmt RAS Periodic SMI Control [Enabled]		
SMI Threshold 5		
SMI Scale 1000		
SMI Scale Unit [millisecond]		
SMI Period 1000		
GHES Notify Type [Polled]		
GHES UnCorr Notify Type [NMI]		
PCIe GHES Notify Type [Polled]		
PCIe Uncorr GHES Notify Type [NMI]		
PCIe Root Port Corr Err Mask Reg 2000		
PCIe Root Port Uncorr Err Mask Reg 0		
PCIe Root Port UnCorr Error Sev Reg 57EF6030		
PCIe Device Corr Err Mask Reg 2000		
PCIe Device UnCorr Err Mask Reg 0		
PCIe Device UnCorr Error Sev Reg 57EF6030		
CXL DP CIE Mask Enable [Enabled]		
DRAM Hard Post Package Repair [Disabled]		
HEST DMC Structure Support [Disabled]		
CXL Error Report Support [Disabled]		
→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit		

Version 2.22.1284. Copyright © 2022 AMI

Advanced \ AMD PBS \ RAS		
Menu Fields	Settings	Comments
RAS Periodic SMI Control	[Disabled] [Enabled]	Enable / disable Periodic SMI for polling (MCA Threshold) error
SMI Threshold	X	The [SMI Threshold] limits the number of [MCA Threshold and Deferred Error SMI source] per a Unit time (Defined by [SMI Scale]). (Default: 5 dec interrupts)
SMI Scale	XXXX	The [SMI Scale] defines the time scale. (Default: 1000 dec)
SMI Scale Unit	[millisecond] [second] [minute]	The [SMI Scale Unit] defines the unit of time scale. (Default: ms)
SMI Period	XXXX	The [SMI Period] defines the polling interval (Default: 1000 dec, Maximum: 32767 dec, 0: Disable, Unit: ms)
GHES Notify Type	[Polled] [SCI]	Notification type for deferred/corrected errors
GHES UnCorr Notify Type	[Polled] [NMI]	Notification type for uncorrected errors
PCIe GHES Notify Type	[Polled] [SCI]	Notification type for PCIe corrected errors

Advanced \ AMD PBS \ RAS		
Menu Fields	Settings	Comments
PCIe Uncorr GHES Notify Type	[Polled] [NMI]	Notification type for PCIe uncorrected errors
PCIe Root Port Corr Err Mask Reg	XXXX	Initialize the PCIe AER Corrected Error Mask register of Root Port
PCIe Root Port Uncorr Err Mask Reg	X	Initialize the PCIe AER Uncorrected Error Mask register of Root Port
PCIe Root Port UnCorr Error Sev Reg	XXXXXXXX	Initialize the PCIe AER Uncorrected Error Severity registers of Root Port
PCIe Device Corr Err Mask Reg	XXXX	Initialize the PCIe AER Corrected Error Mask register of PCIe Device
PCIe Device UnCorr Err Mask Reg	X	Initialize the PCIe AER Uncorrected Error Mask register of PCIe Device
PCIe Device UnCorr Error Sev Reg	XXXXXXXX	Initialize the PCIe AER Uncorrected Error Severity registers of PCIe Device
CXL DP CIE Mask Enable	[Disabled] [Enabled]	Enable/Disable masking of CXL DP Correctable Error - Internal Error
DRAM Hard Post Package Repair	[Disabled] [Enabled]	This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism
HEST DMC Structure Support	[Disabled] [Enabled]	HEST DMC(Deferred Machine Check) Structure Support
CXL Error Report Support	[Disabled] [Enabled]	Enable/ disable CXL Error Reporting

6.2.16.2 Range Encryption

Aptio Setup - AMI		
Main	Advanced	Chipset
Range 1 Range 1 Memory Base 0 Range 1 Memory Limit 0 Range 2 Range 2 Memory Base 0 Range 2 Memory Limit 0 Range 3 Range 3 Memory Base 0 Range 3 Memory Limit 0 Range 4 Range 4 Memory Base 0 Range 4 Memory Limit 0 Range 5 Range 5 Memory Base 0 Range 5 Memory Limit 0 Range 6 Range 6 Memory Base 0 Range 6 Memory Limit 0 Range 7 Range 7 Memory Base 0 Range 7 Memory Limit 0 Start Range Encryption		

→ ←:Select Screen

↑ ↓:Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Advanced \ AMD PBS \ Range Encryption		
Menu Fields	Settings	Comments
Range 1 Memory Base	X	Entry memory range base address and limit address
Range 1 Memory Limit	X	Entry memory range base address and limit address
Range 2 Memory Base	X	Entry memory range base address and limit address
Range 2 Memory Limit	X	Entry memory range base address and limit address
Range 3 Memory Base	X	Entry memory range base address and limit address
Range 3 Memory Limit	X	Entry memory range base address and limit address
Range 4 Memory Base	X	Entry memory range base address and limit address
Range 4 Memory Limit	X	Entry memory range base address and limit address
Range 5 Memory Base	X	Entry memory range base address and limit address
Range 5 Memory Limit	X	Entry memory range base address and limit address
Range 6 Memory Base	X	Entry memory range base address and limit address
Range 6 Memory Limit	X	Entry memory range base address and limit address
Range 7 Memory Base	X	Entry memory range base address and limit address

Advanced \ AMD PBS \ Range Encryption		
Menu Fields	Settings	Comments
Range 7 Memory Limit	X	Entry memory range base address and limit address
Start Range Encryption	Executable item	Start to encrypt all memory ranges.

6.3 CHIPSET

Main

Advanced

Chipset

Security

Boot

Save & Exit

Server Mgmt

Aptio Setup - AMI

PCle Compliance Mode [Off]

▶ North Bridge

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Chipset		
Menu Fields	Settings	Comments
PCle Compliance Mode	[Off] [On]	PCle Link Compliance Mode.
North Bridge	Selects Sub-menu	North Bridge Paramters

6.3.1 North Bridge

Aptio Setup - AMI

Chipset

North Bridge Configuration

Memory Information

Total Memory: 393216 MB

▶ Socket 0 Information

▶ Socket 1 Information

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Chipset \ North Bridge		
Menu Fields	Settings	Comments
Socket 0 Information	Selects Sub-menu	
Socket 1 Information	Selects Sub-menu	

6.3.1.1 Socket 0 Information

Aptio Setup - AMI

Chipset

Socket 0 Information

DIMM A0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM B0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM C0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM D0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM E0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM F0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM G0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM H0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM I0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM J0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM K0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM L0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM

→←:Select Screen

↑ ↓:Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.3.1.2 Socket 1 Information

Aptio Setup - AMI

Chipset

Socket 1 Information

DIMM A0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM B0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM C0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM D0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM E0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM F0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM G0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM H0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM I0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM J0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM K0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM
DIMM L0:	SK Hynix,	Size16384 MB,	Speed 6000MT/s ,	SRx8 RDIMM

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.4 SECURITY

MainAdvancedChipsetSecurityBootSave & ExitServer Mgmt

Version 2.22.1294. Copyright © 2024 AMI

Administrator Password

User Password

Secure Boot

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Password Description

If ONLY the Administrator's Password is Set, then this only Limits access to Setup and is only asked for when entering Setup.

If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.

The password length must be

In the following range:

Minimum length3

Maximum length20

Security		
Menu Fields	Settings	Comments
Administrator Password	Executable item	Set Administrator Password
User Password	Executable item	Set User Password
Secure Boot	Selects Sub-menu	

230

6.4.1 Secure Boot

Aptio Setup - AMI		
Security		
System Mode	User	
Secure Boot	[Disabled] Not Active	
Secure Boot Mode	[Custom]	
▶ Restore Factory Keys ▶ Reset To Setup Mode ▶ Expert Key Management		
		→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Security \ Secure Boot		
Menu Fields	Settings	Comments
Secure Boot	[Disabled] [Enabled]	Secure Boot feature is Active if secure boot is enabled. Platform Key (PK) is enrolled and the System is in User mode. The mode change require platform reset.
Secure Boot Mode	[Standard] [Custom]	Secure boot mode option: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys	Executable item	Force System to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode	Executable item	Delete all Secure Boot key database from NVRAM.
Expert Key Management	Selects sub-menu	Enable expert users to modify Secure Boot Policy variables without variable authentication.

6.4.1.1 Expert Key Management

Aptio Setup - AMI

Security

Vendor Keys

Modified

Factory Key Provision [Enabled]

- ▶ Restore Factory Keys
- ▶ Reset To Setup mode
- ▶ Enroll Efi Image
- ▶ Export Secure Boot variables

Secure Boot Variable	Size	Keys	Key Source
▶ Platform Key (PK)	827	1	Factory
▶ Key ExChange Keys (KEK)	829	1	Factory
▶ Authorized Signatures (db)	2427	2	Factory
▶ Forbidden Signatures (dbx)	11788	245	Factory
▶ Authorized TimeStamps (dbt)	0	0	No keys
▶ OsRecovery Signatures (dbr)	0	0	No keys

→ ←:Select Screen
 ↑ ↓:Select Item
 Enter:Select
 +/-:Change Opt.
 F1: General Help
 F2: Previous values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Security \ Secure Boot		
Menu Fields	Settings	Comments
Factory Key Provision	[Disabled] [Enabled]	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Restore Factory Keys	Executable item	Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode	Executable item	Delete all Secure Boot key databases from NVRAM
Enroll Efi Image	Executable item	Allow Efi image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
Export Secure Boot Variables	Executable item	Save NVRAM content of Secure Boot variable to a file
Platform Key (PK)	[Details] [Export] [Update] [Delete]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER)

Security \ Secure Boot		
Menu Fields	Settings	Comments
		c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Key ExChange Keys (KEK)	[Details] [Export] [Update] [Append] [Delete]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Authorized Signatures (db)	[Details] [Export] [Update] [Append] [Delete]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Forbidden Signatures (dbx)	[Details] [Export] [Update] [Append] [Delete]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Authorized TimeStamps (dbt)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
OsRecovery Signatures (dbr)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable

Security \ Secure Boot		
Menu Fields	Settings	Comments
		3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed

6.5 BOOT

Aptio Setup - AMI						
Main	Advanced	Chipset	Security	Boot	Save & Exit	Server Mgmt
Boot Configuration Setup Prompt Timeout: 1 Bootup NumLock State: [On] Quiet Boot: [Enabled] Endless Boot: [Disabled]						
Chassis Intrusion: [Disabled] Display POST Info: [On] Fast Boot: [Disabled]						
FIXED BOOT ORDER Priorities Boot Option #1: [Network:UEFI: HTTP IPv4 Intel(R) I350 Gigabit Network Connection] Boot Option #2: [Hard Disk] Boot Option #3: [NVME: ubuntu(THNSN0256GSXA TOSHIBA)] Boot Option #4: [CD/DVD] Boot Option #5: [USB Device:UEFI: HTTP IPv4 American Megatrends Inc.]			→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit			
▶ UEFI NETWORK Drive BBS Priorities ▶ UEFI NVME Drive BBS Priorities ▶ UEFI USB Drive BBS Priorities						

Version 2.22.1294. Copyright © 2024 AMI

Boot		
Menu Fields	Settings	Comments
Setup Prompt Timeout	X	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	[On] [Off]	Select the keyboard NumLock state
Quiet Boot	[Disabled] [Enabled]	Enables or disables Quiet Boot option
Endless Boot	[Disabled] [Enabled]	Enabled: BIOS try bootable devices constantly in loop until finding a bootable device(Excluding Built-in EFI Shell)
Chassis Intrusion	[Disabled] [Enabled]	Chassis Intrusion
Display POST Info	[Off] [On]	Display POST Info after LOGO
Fast Boot	[Disabled] [Enabled]	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.

Boot		
Menu Fields	Settings	Comments
Boot Option #1	Executable item	Sets the system boot order
Boot Option #2	Executable item	Sets the system boot order
Boot Option #3	Executable item	Sets the system boot order
Boot Option #4	Executable item	Sets the system boot order
Boot Option #5	Executable item	Sets the system boot order
UEFI NETWORK Drive BBS Priorities	Selects sub-menu	Specifies the Boot Device Priority sequence from available UEFI NETWORK Drives.
UEFI NVME Drive BBS Priorities	Selects sub-menu	Specifies the Boot Device Priority sequence from available UEFI NVME Drives.
UEFI USB Drive BBS Priorities	Selects sub-menu	Specifies the Boot Device Priority sequence from available UEFI USB Drives.

6.5.1 UEFI NETWORK Drive BBS Priorities

Aptio Setup - AMI

Boot

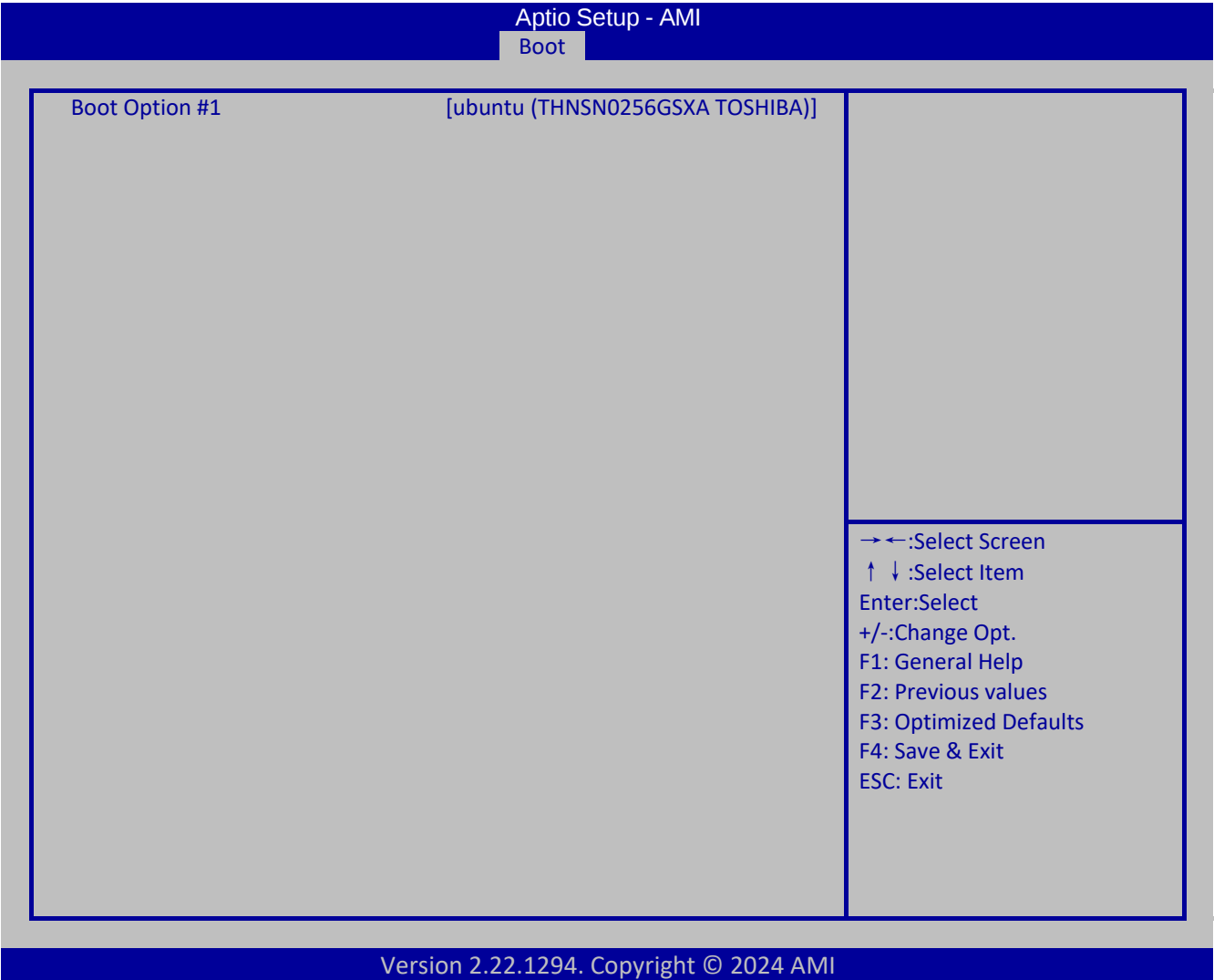
Boot Option #1	[UEFI: HTTP IPv4 Intel(R) I350 Gigabit Network Connection]	
Boot Option #2	[UEFI: PXE IPv4 Intel(R) I350 Gigabit Network Connection]	
Boot Option #3	[UEFI: HTTP IPv4 Intel(R) I350 Gigabit Network Connection]	
Boot Option #4	[UEFI: PXE IPv4 Intel(R) I350 Gigabit Network Connection]	

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Boot \ UEFI Application Drive BBS Priorities		
Menu Fields	Settings	Comments
Boot Option #1	Executable item	Sets the system boot order
Boot Option #2	Executable item	Sets the system boot order
Boot Option #3	Executable item	Sets the system boot order
Boot Option #4	Executable item	Sets the system boot order

6.5.2 UEFI NVME Drive BBS Priorities



Boot \ UEFI NVME Drive BBS Priorities		
Menu Fields	Settings	Comments
Boot Option #1	Executable item	Sets the system boot order

6.5.3 UEFI USB Drive BBS Priorities

Aptio Setup - AMI

Boot

Boot Option #1	[UEFI: HTTP IPv4 American Megatrends Inc.]	
Boot Option #2	[UEFI: PXE IPv4 American Megatrends Inc.]	

→←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Boot \ UEFI Application Drive BBS Priorities		
Menu Fields	Settings	Comments
Boot Option #1	Executable item	Sets the system boot order
Boot Option #2	Executable item	Sets the system boot order

6.6 SAVE & EXIT

Aptio Setup - AMI
Main Advanced Chipset Security Boot **Save & Exit** Server Mgmt

Save Options
Save Changes and Exit
Discard Changes and Exit

Save Changes and Reset
Discard Changes and Reset

Save Change
Discard Changes

Default Options
Restore Defaults
Save as User Defaults
Restore User Defaults

Boot Override
UEFI: HTTP IPv4 Intel(R) I350 Gigabit Network Connection
UEFI: PXE IPv4 Intel(R) I350 Gigabit Network Connection
UEFI: HTTP IPv4 Intel(R) I350 Gigabit Network Connection
UEFI: PXE IPv4 Intel(R) I350 Gigabit Network Connection
Ubuntu (THNSN0256GSXA TOSHIBA).

→ ←:Select Screen
↑ ↓:Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Save & Exit		
Menu Fields	Settings	Comments
Save Changes and Exit	Executable item	Exit system setup after saving the changes.
Discard Changes and Exit	Executable item	Exit system setup without saving any changes.
Save Changes and Reset	Executable item	Reset the system after saving the changes.
Discard Changes and Reset	Executable item	Reset system setup without saving any changes
Save Change	Executable item	Save Changes done so far to any of the setup options.
Discard Changes	Executable item	Discard Changes done so far to any of the setup options.
Restore Defaults	Executable item	Restore/Load Default values for all the setup options.
Save as User Defaults	Executable item	Save the changes done so far as User Defaults.
Restore User Defaults	Executable item	Restore the User Defaults to all the setup options.

6.7 SERVER MGMT

Aptio Setup - AMI
Main Advanced Chipset Security Boot Save & Exit **Server Mgmt**

BMC Self Test Status	PASSED	
BMC Device ID	32	
BMC Device Revision	81	
BMC Firmware Revision	1.37	
IPMI Version	2.0	
IPMI BMC Interface	KCS	
BMC Support	[Enabled]	→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
IPMI Interface Type	[Kcs Interface]	
Wait For BMC	[Disabled]	
FRB-2 Timer	[Enabled]	
FRB-2 Timer timeout	6	
FRB-2 Timer Policy	[Do Nothing]	
OS Watchdog Timer	[Disabled]	
OS Wtd Timer Timeout	10	
OS Wtd Timer Policy	[Reset]	
Serial Mux	[Disabled]	
▶ System Event Log ▶ View FRU Information ▶ BMC self test log ▶ BMC network configuration ▶ View System Event Log ▶ BMC User Settings ▶ BMC warm Reset		

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt		
Menu Fields	Settings	Comments
BMC Support	[Enabled] [Disabled]	Enable/Disable Interface to Communicate with BMC
IPMI Interface Type	[Kcs Interface] [Ipmb Interface] [Usb Interface]	Type of Interface to Communicate BMC From Host
Wait For BMC	[Enabled] [Disabled]	Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host BMC interfaces.
FRB-2 Timer	[Enabled] [Disabled]	Enable or Disable FRB-2 timer(POST timer)
FRB-2 Timer timeout	X	Enter value Between 1 to 30 min for FRB-2 Timer Expiration.
FRB-2 Timer Policy	[Do Nothing] [Reset] Power Down]	Configure how the system should respond it the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.

Server Mgmt		
Menu Fields	Settings	Comments
	[Power Cycle]	
OS Watchdog Timer	[Enabled] [Disabled]	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS success fully loaded or follows the OS Boot Watchdog Timer policy.
OS Wtd Timer Timeout	X	Enter value Between 1 to 30 min for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.
OS Wtd Timer Policy	[Do Nothing] [Reset] Power Down] [Power Cycle]	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.
Serial Mux	[Enabled] [Disabled]	Press <Enter> to enable or disable Serial Mux Configuration.
System Event Log	Selects sub-menu	Press <Enter> to change the SEL event log configuration.
View FRU Information	Selects sub-menu	Press <Enter> to view FRU information.
BMC self test log	Selects sub-menu	Logs the report returned by BMC self test command.
BMC network configuration	Selects sub-menu	Configure BMC network parameters.
View System Event Log	Selects sub-menu	Press <Enter> to view the System Event Log Records.
BMC User Settings	Selects sub-menu	Press <Enter> to Add, Delete and Set privilege level for users.
BMC warm Reset	Executable item	Press <Enter> to do Warm Reset BMC.

6.7.1 System Event Log

Aptio Setup - AMI		Server Mgmt
Enabling/Disabling Options SEL Components [Enabled]		
Erasing Settings Erase SEL [No] When SEL is Full [Do Nothing]		
Custom EFI Logging Options Log EFI Status Codes [Error code]		
NOTE: All values changed here do not take Effect until computer is restarted.		
		→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt \ System Event Log		
Menu Fields	Settings	Comments
SEL Components	[Disabled] [Enabled]	Change this to enabled or disable event logging for error/progress codes during boot.
Erase SEL	[No] [Yes, On next reset] [Yes, On every reset]	Choose options for erasing SEL.
When SEL is Full	[Do Nothing] [Erase Immediately] [Delete oldest Record]	Choose options for reactions to a full SEL.
Log EFI Status Codes	[Disabled] [Both] [Error Code] [Progress Code]	Disable the logging of EFI Status Codes or log only error code or only progress code or both.

6.7.2 View FRU information

Aptio Setup - AMI		Server Mgmt
FRU Information		
System Manufacturer	Vantageo	
System Product Name	Vantageo 12T1	
System Version	SR875462901	
System Serial Number	SR096532548	
Board Manufacturer	Vantageo	
Board Product Name	12T1	
Board Part Number	12T1-PRD	
Board Serial Number	SR452317281	
Chassis Manufacturer	Vantageo	
Chassis Part Number	12T1-CHS	
Chassis Serial Number	SR867534219	
SDR Version	1.5	
System UUID	6B0437A4-BFDE-11D3-01BC-C90A877C357E	
NOTE: No FRU information for fields indicate information needs to be filled by O.E.M		
		→ ←:Select Screen ↑ ↓:Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

6.7.3 Bmc Self-Test log

Aptio Setup - AMI		Server Mgmt
Log area usage = 00 out of 20 logs		
Erase Log	[Yes, On every reset]	
When log is full	[Clear Log]	
Log Empty		
		→ ← :Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI		

Server Mgmt \ Bmc self test log		
Menu Fields	Settings	Comments
Erase Log	[Yes, On every reset] [No]	Erase Log Options
When log is full	[Clear Log] [Do not log any more]	Select the action to be taken when log is full

6.7.4 BMC network Configuration

Aptio Setup - AMI		Server Mgmt
--BMC network configuration-- *****		
Configure IPv4 support *****		
Lan channel 1		
Configuration Address source	[Unspecified]	
Current Configuration Address source	DynamicAddressBmcDhcp	
Station IP address	xxx.xxx.xxx.xxx	
Subnet mask	xxx.xxx.xxx.xxx	
Station MAC address	xx-xx-xx-xx-xx-xx	
Router IP Address	xxx.xxx.xxx.xxx	
Router MAC Address	xx-xx-xx-xx-xx-xx	
Lan channel 2		
Configuration Address source	[Unspecified]	
Current Configuration Address source	DynamicAddressBmcDhcp	
Station IP address	xxx.xxx.xxx.xxx	
Subnet mask	xxx.xxx.xxx.xxx	
Station MAC address	xx-xx-xx-xx-xx-xx	
Router IP Address	xxx.xxx.xxx.xxx	
Router MAC Address	xx-xx-xx-xx-xx-xx	

Configure IPv6 support *****		
Lan Channel 1		
IPv6 Support	[Enabled]	
Configuration Address	[Unspecified]	
Current Configuration Address Source	DynamicAddressBmcDhcp	
Station IPv6 address	:	
Prefix Length	0	
IPv6 address status	Disabled	
IPv6 DHCP Algorithm	DHCPv6	
Configuration Router Lan1 Address source	[Unspecified]	
Current Router Configuration Address source	DynamicAddressBmcDhcp	
IPv6 Router IP Address	:	
IPv6 Router Prefix Length	255	

→ ←:Select Screen
↑ ↓:Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

IPv6 Router Prefix Value
: :

Lan Channel 2

IPv6 Support	[Enabled]
Configuration Address	[Unspecified]
Current Configuration Address Source	DynamicAddressBmcDhcp

Station IPv6 address
: :

Prefix Length
0

IPv6 address status	Disabled]
IPv6 DHCP Algorithm	DHCPv6

Configuration Router Lan2 Address source	[Unspecified]
--	---------------

Current Router Configuration Address source	DynamicAddressBmcDhcp
---	-----------------------

IPv6 Router IP Address
: :

IPv6 Router Prefix Length
255

IPv6 Router Prefix Value
: :

Configure VLAN support

Lan channel 1

VLAN Support	[Unspecified]
Current Configuration Address Source	Disabled
VLAN ID	0
VLAN Priority	0

Lan channel 2

VLAN Support	[Unspecified]
Current Configuration Address Source	Disabled
VLAN ID	0
VLAN Priority	0

Server Mgmt \ BMC network configuration		
Menu Fields	Settings	Comments

Configure IPv4 support		

Configuration Address source	[Unspecified] [Static] [DynamicBmcDhcp] [DynamicBmcNonDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
Current Configuration Address source	DynamicAddressBmcDhcp	Current LAN Configuration statically or dynamically(by BIOS or BMC). Unspecified for not Configured address space
Station IP address	Executable item	Enter station IP address
Subnet mask	Executable item	Enter subnet
Station MAC address	xx-xx-xx-xx-xx-xx	Station MAC address from BMC
Router IP Address	Executable item	Enter router IP address
Router MAC Address	Executable item	Enter router MAC address

Configure IPv6 support		

IPv6 Support	[Enabled] [Disabled]	Enable or Disable Lan IPv6 Support
Configuration Address	[Unspecified] [Static] [DynamicBmcDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
Current Configuration Address Source	DynamicAddressBmcDhcp	Current LAN Configuration statically or dynamically(by BIOS or BMC). Unspecified for not Configured address space
Station IPv6 address	Executable item	Enter Station IPv6 address
Prefix Length	Executable item	Change the prefix length
Configuration Router Lan Address Source	[Unspecified] [Static] [DynamicBmcDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
IPv6 Router IP Address	Executable item	Change the IPv6 Router IP Address
IPv6 Router Prefix Length	Executable item	Change the IPv6 Router Prefix Length
IPv6 Router Prefix Value	Executable item	Change the IPv6 Router Prefix Value

Configure VLAN support		

VLAN Support	[Enabled] [Disabled] [Unspecified]	Enabled VLAN Support to Specify the 802.1q VLAN ID.

Server Mgmt \ BMC network configuration		
Menu Fields	Settings	Comments
VLAN ID	Executable item	VLAN ID Range is from 1-4094. VLAN ID 0 & 4095 are reserved VALN ID's
VLAN Priority	Executable item	Value ranges from 0 to 7. 7is the highest priority for VLAN.

6.7.5 View System Event Log

Aptio Setup - AMI

Server Mgmt

No. of Log entries in SEL : X

DATE	TIME	SENSOR TYPE
------	------	-------------

→ ←:Select Screen
↑ ↓ :Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

6.7.6 BMC User Settings

Aptio Setup - AMI

Server Mgmt

BMC User Settings

▶ Add User

▶ Delete User

▶ Change User Setting

→ ←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt \ BMC User Settings		
Menu Fields	Settings	Comments
Add User	Selects sub-menu	
Delete User	Selects sub-menu	
Change User Settings	Selects sub-menu	

6.7.6.1 Add User

Aptio Setup - AMI

Server Mgmt

BMC Add User Details

User Name

User Password

User Access

Channel No

User Privilege Limit

[Disabled]

0

[No Access]

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt \ BMC User Settings \ Add User		
Menu Fields	Settings	Comments
User Name	Execute-item	Enter BMC User Name

6.7.6.2 Delete User

Aptio Setup - AMI	
Server Mgmt	
BMC Delete User Details User Name User Password	→ ←:Select Screen ↑ ↓ :Select Item Enter:Select +/-:Change Opt. F1: General Help F2: Previous values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt \ BMC User Settings \ Delete User		
Menu Fields	Settings	Comments
User Name	Execute-item	Enter BMC User Name

6.7.6.3 Change User Settings

Aptio Setup - AMI

Server Mgmt

BMC Change User Settings

User Name

User Password

Change User Name

Change User Password

User Access

Channel No

User Privilege Limit

[Disabled]

0

[No Access]

→←:Select Screen

↑ ↓ :Select Item

Enter:Select

+/-:Change Opt.

F1: General Help

F2: Previous values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1294. Copyright © 2024 AMI

Server Mgmt \ BMC User Settings \ Change User Settings		
Menu Fields	Settings	Comments
User Name	Execute-item	Enter BMC User Name

7 STATUS CODES LIST

7.1 AMI STANDARD STATUS CODE

The UEFI defines SEC, PEI, DXE, BDS phases during POST. AMI define several status codes during each phase for user self-check error.

7.1.1 SEC Phase

Status Code	Description
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

7.1.2 PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)

Status Code	Description
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AML error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AML progress codes
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error

Status Code	Description
0xEC-0xEF	Reserved for future AML error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AML progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AML error codes

PEI Beep Codes

# of Beeps	Description
1	Memory not installed
2	Recovery started
3	Typically for development use. The beep code is generated when DXE IPL PPI or DXE Core is not found.
4	Recovery failed
4	S3 Resume failed
7	Typically for development use. The beep code is generated when platform cannot be reset because reset PPI is not available.

7.1.3 DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect

Status Code	Description
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources

Status Code	Description
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Typically for development use. The beep code is generated when some of the Architectural Protocols are not available.
5	No Console Input or Output Devices are found (Note 1, Note 2)
6	Flash update is failed
7	Typically for development use. The beep code is generated when platform cannot be reset because reset protocol is not available.
8	Platform PCI resource requirements cannot be met

Note 1: serial console redirection is considered a console out device if enabled

Note 2: serial console redirection is considered a console in device if enabled. Also, depending on configuration PS/2 driver may always report a console in device even if one is not connected.

vantageTM