S3071
BIOS User Guide

Version 1.1

MSI Enterprise Platform Solutions

CONTENTS

Copyright and Trademarks Notice

Technical Support

If a problem arises with your product and no solution can be obtained from the user's manual, please contact your place of purchase or local distributor. Alternatively, please visit https://eps.msi.com/support for further guidance.

1 GENERAL OVERVIEW

This document specifies the system BIOS requirements of **S3071** project.

2 BIOS FEATURES OVERVIEW

2.1 BIOS DESCRIPTION

Item	Description
Code base vendor	AMI Aptio Core Base Version : 5.35
BIOS image size	64 MB
ROM image size	38 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	Support
Intel SGX	Support

2.3 MEMORY

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

2.3.1 Bad DIMM Location

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

2.4 STORAGE

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

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

2.6.1 Restore on AC Power Loss

The power control policy is managed by the BMC. When the system's power is restored, the BMC will control the system's power state as "Power Restore," "Do Not PowerUp," or "Last Power State."

- BIOS Setup Item

Item	Settings	Description
Power Control Policy	[Do Not PowerUp] [Last Power State] **[Power Restore]**	Configure how the system should respond if AC Power is lost, Reset not required as selected Power policy will be set in BMC when policy is saved.

Note: Power control policy default setting will sync to BMC chassis power restore policy setting instead of BIOS default setting when clear CMOS occurs.

The state after G3 is managed by CPU or PCH. BIOS default set to “S5 State” since power control managed by BMC. The item name could differ across platforms.

- BIOS Setup Item

Item	Settings	Description
State After G3	[S0 State] **[S5 State]** [Last State]	Specify what state to go to when power is re-applied after a power failure (G3 state).

Note: It is recommended to keep this default setting and manage the system's power restore behavior through the power control policy.

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	Support
Intel Features	**Description**
Intel TXT	Support
msi Features	**Description**
Rot	
PFR	
Secure Erase Support (Security Freeze Lock)	
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 MSI_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	
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	
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

Type	Name	Description
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 commond)	Support
BMC LAN Control in BIOS Setup Utility	Support
BMC User Configuration in BIOS Setup Utility	Support
FRB2 (Fault Resilient Booting 2)	Support
msi 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
msi 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	

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 – MSIBOOT.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

1st	2nd	3rd	4th	5th
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, Quiet Boot, Secure Boot 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

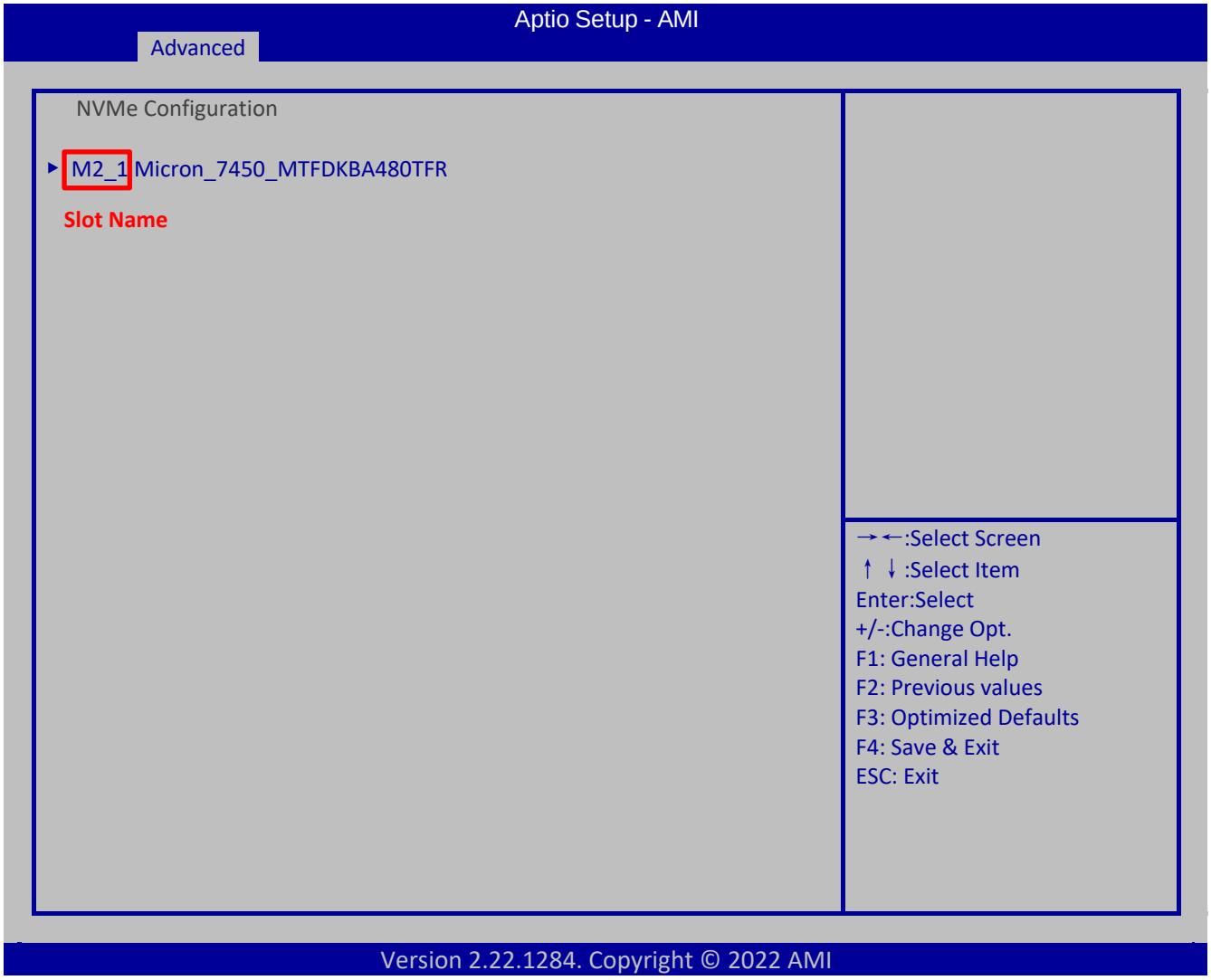
When chassis intrusion is detected, BIOS will popup error information during POST.

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

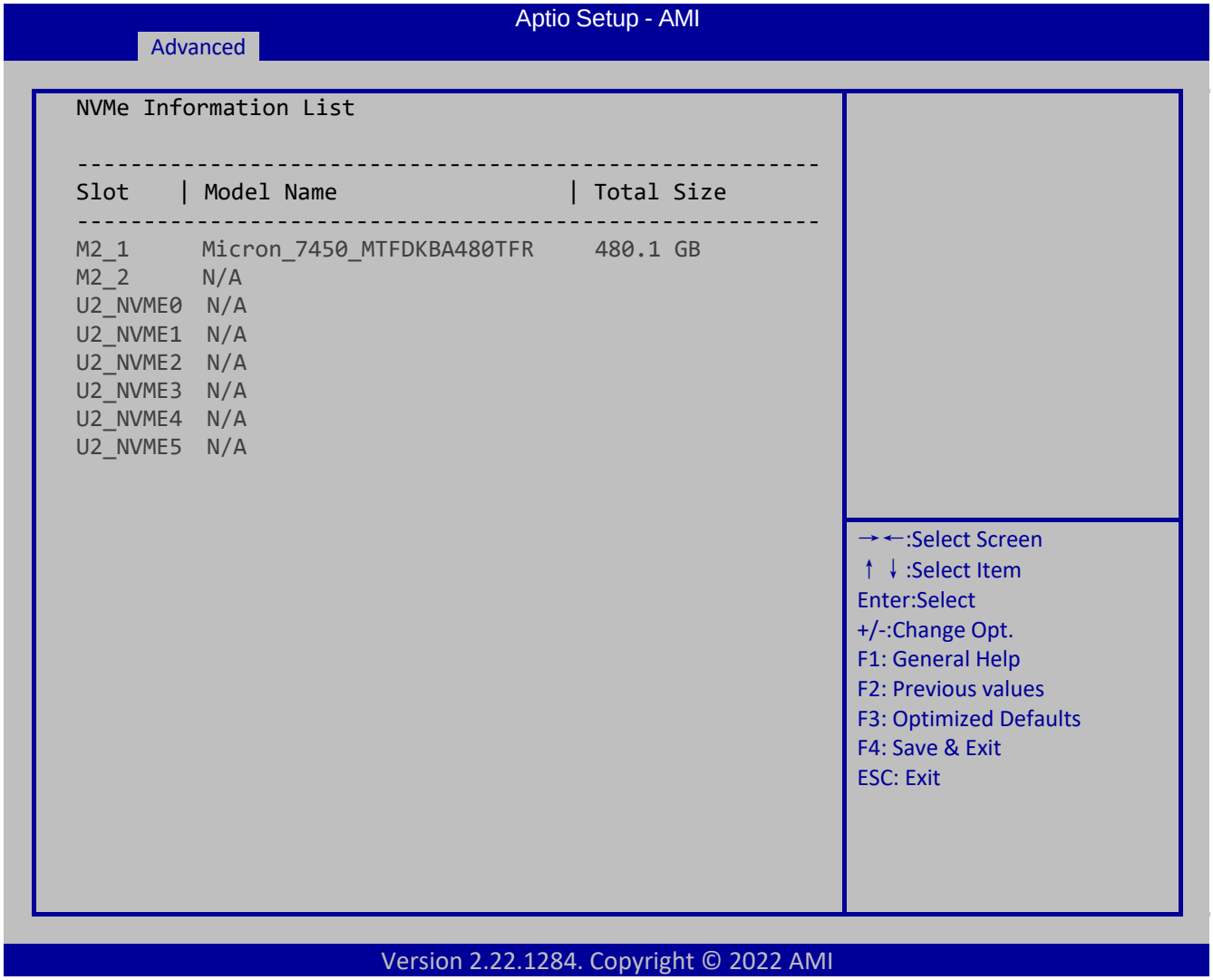
Item	Settings	Description
Chassis Intrusion	**[Enabled]** [Disabled]	Enable or disable chassis intrusion detection.

2.10.7 Nvme Setup Information

BIOS supports list all Nvme devices information in setup that user can check Nvme device exist or not. Also add system slot name in original Nvme configuration page that user can recognize Nvme device and control their OptionRom settings. Nvme slot name must match to slot silkscreen.



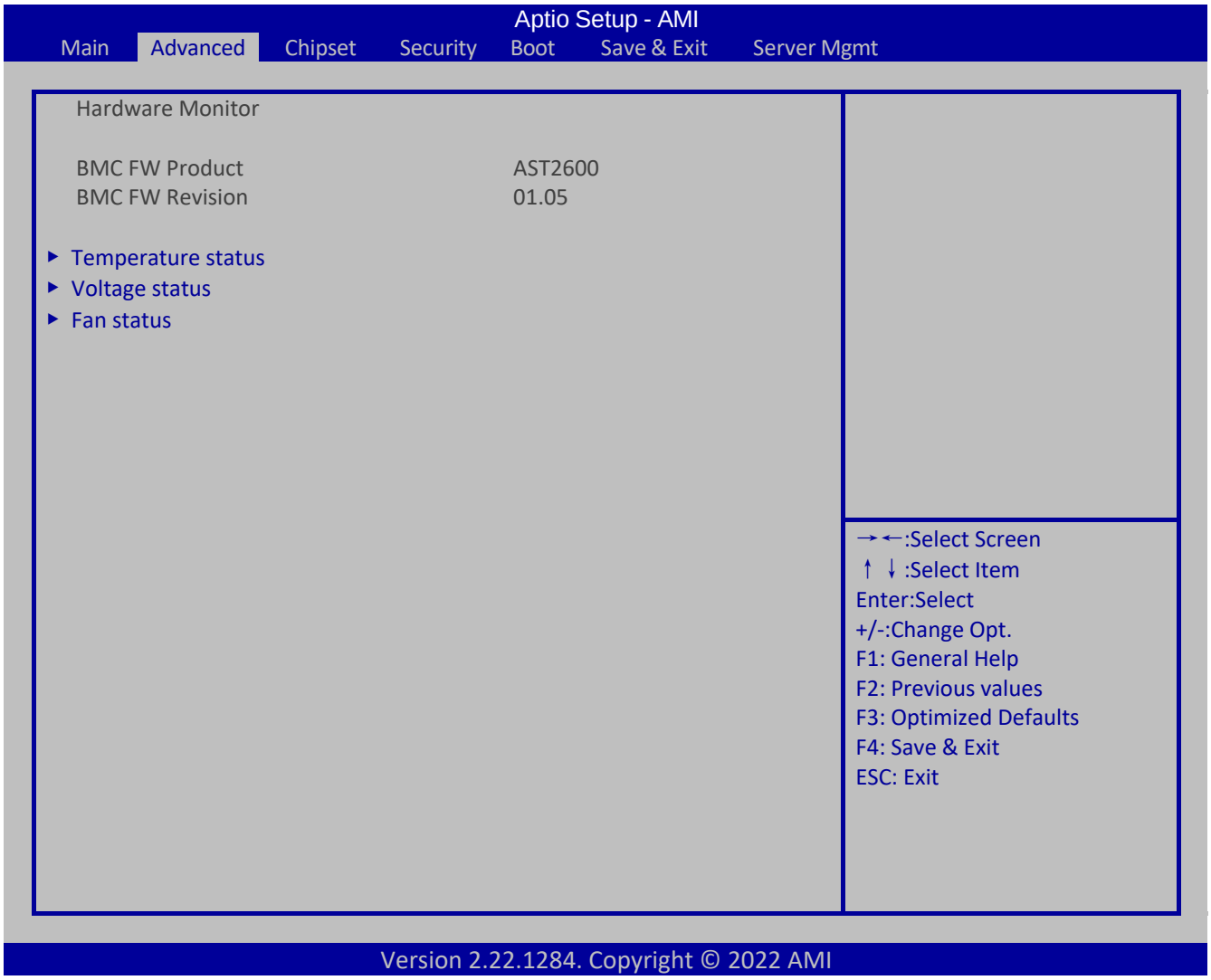
NVMe Information List



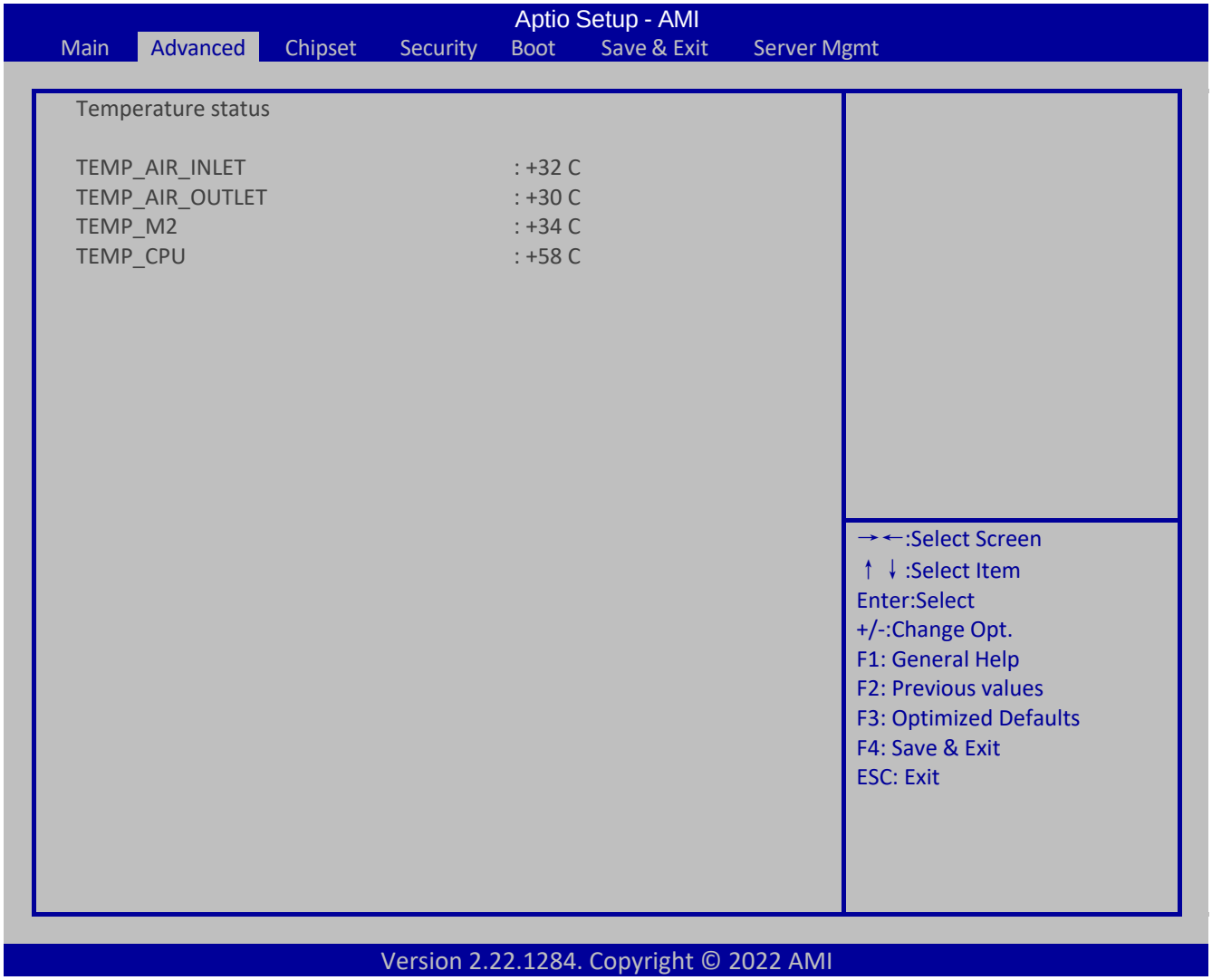
2.10.8 HW Monitor (Not Supported)

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.

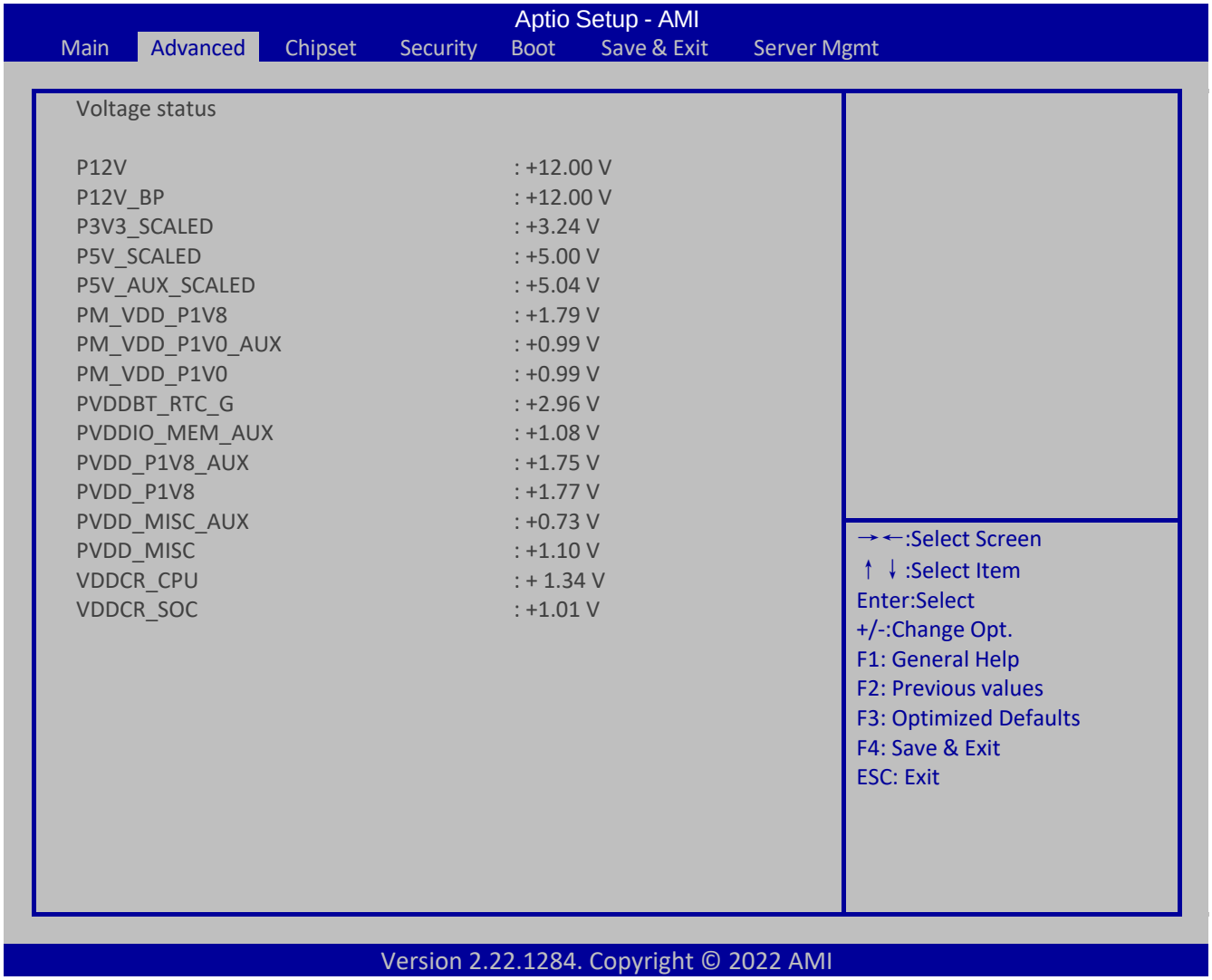
Hardware Monitor Main Page



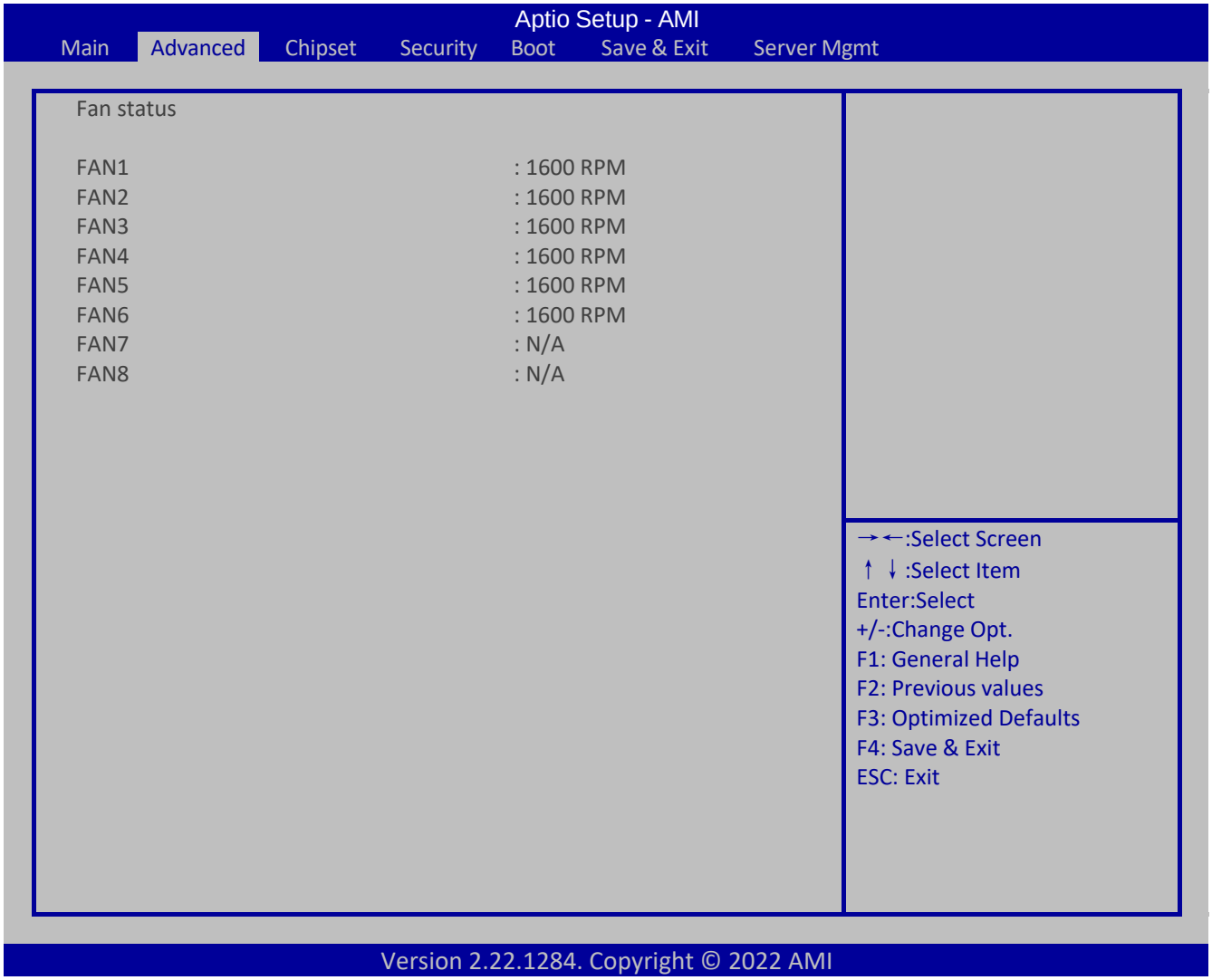
Temperature Status



Voltage Status



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 <Del> or <F2> into BIOS setup Menu during POST.

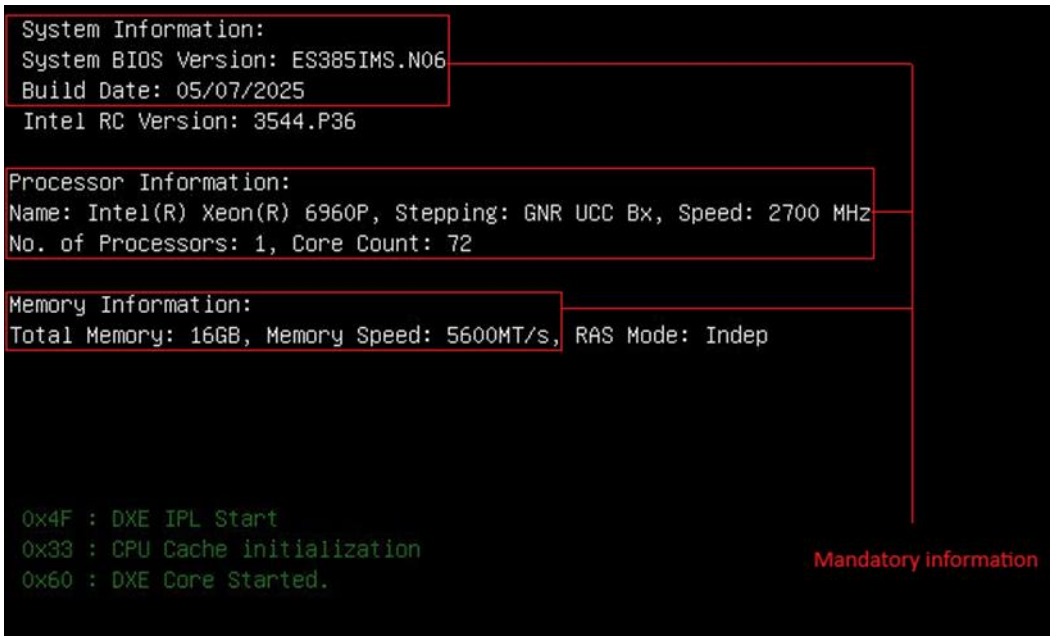
2.11.1 Early Console POST Information

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

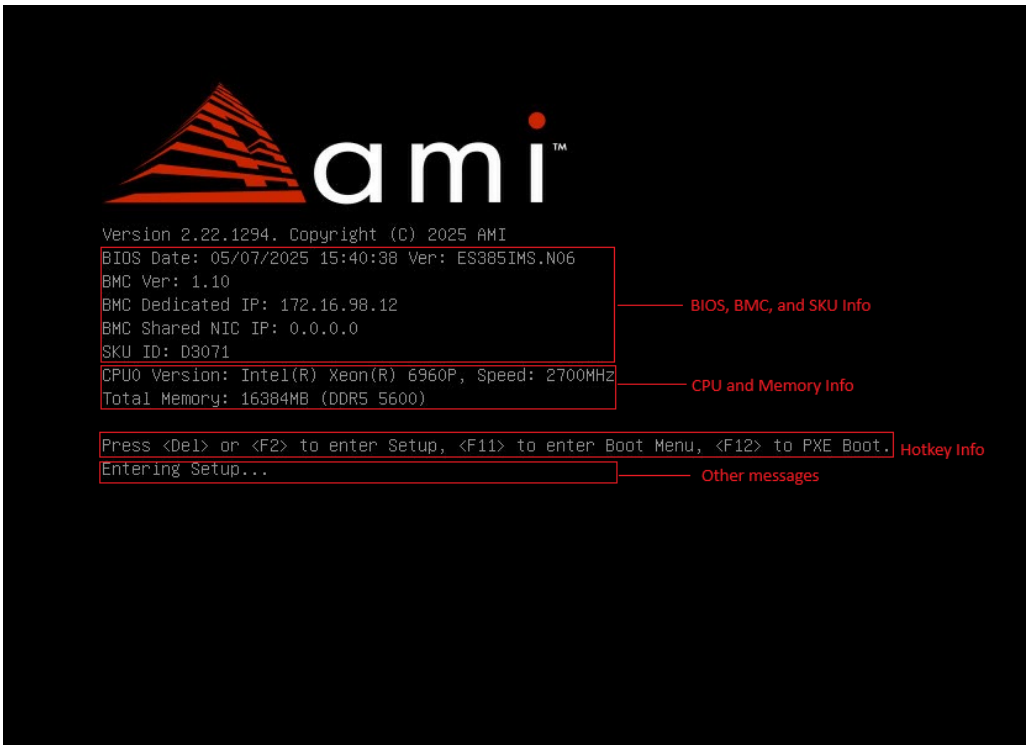


2.11.2 Quiet Boot

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	[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
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 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

Byte	Field	Description
		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	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 0x05 = Configuration Error 0x0B = Machine Check Exception (Uncorrectable) 0x0C = Correctable Machine Check Error
15	Event Data 2	[7:4] –Socket ID Number [3:0] – Bank Type 0x00 = None 0x01 = IFU 0x02 = DCU 0x03 = DTLB 0x04 = MLC 0x05 = PCU 0x06 = IIO 0x07 = CHA 0x08 = KTI
16	Event Data 3	[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

Byte	Field	Description
		[0] – Happened in the boot. 0x00 = Current boot 0x01 = Last boot

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 PERR 0x05 = PCIE SERR 0x07 = Bus Correctable Error 0x08 = Bus Uncorrectable Error 0x0A = 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 INTEL RAS

3.4.1 Spare Core Error

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	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 0x5 = Configuration Error
15	Event Data 2	[7-4] – CPU Socket Number [3-0] – Error Severity 0x0 = Correctable Error

Byte	Field	Description
		0x1 = Fatal Error 0x2 = Corrected Error
16	Event Data 3	[7-0] – CPU Failed Core Number

3.4.2 UPI Error

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	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 0x5 = Configuration Error
15	Event Data 2	[7-4] – CPU Socket Number [3-0] – Bank Type 0x8 = KTI / UPI
16	Event Data 3	[7-4] – Lan Index / UPI Port [3-1] – Error Severity 0x0 = Correctable Error 0x1 = Fatal Error 0x2 = Corrected Error [0] – Last Boot error flag 0x0 = Current Boot Error 0x1 = Last Boot Error

3.4.3 IIO Internal Error

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	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 0x5 = Configuration Error
15	Event Data 2	[7-4] – CPU Socket Number [3-1] – Stack Number [0] – Current/Last Boot Error

Byte	Field	Description
		0x0 = Current Boot Error 0x1 = Last Boot Error
16	Event Data 3	[7-0] – Error Type (See below Table)

IIO Internal Error Type Table

IIO Internal Error Type Table	
Error Types	**Description**

OTC Errors	IIO_INTERNAL_OTC_BIT00 = 0x50, // OTC_CRDT_UF, Bits[0:0]
	IIO_INTERNAL_OTC_BIT01 = 0x51, // OTC_CRDT_OF, Bits[1:1]
	IIO_INTERNAL_OTC_BIT02 = 0x52, // OTC_PAR_HDR_RF, Bits[2:2]
	IIO_INTERNAL_OTC_BIT03 = 0x53, // OTC_PAR_ADDR_RF, Bits[3:3]
	IIO_INTERNAL_OTC_BIT04 = 0x54, // OTC_ECC_UNCOR_RF, Bits[4:4]
	IIO_INTERNAL_OTC_BIT05 = 0x55, // OTC_CABORT, Bits[5:5]
	IIO_INTERNAL_OTC_BIT06 = 0x56, // OTC_MABORT, Bits[6:6]
	IIO_INTERNAL_OTC_BIT07 = 0x57, // OTC_MTC_TGT_ERR, Bits[7:7]
	IIO_INTERNAL_OTC_BIT08 = 0x58, // OTC_ECC_COR_RF, Bits[8:8]
	IIO_INTERNAL_OTC_BIT09 = 0x59, // OTC_MCTP_BCAST_TO_DMI, Bits[9:9]
	IIO_INTERNAL_OTC_BIT10 = 0x5A, // OTC_PAR_RTE, Bits[10:10]
	IIO_INTERNAL_OTC_BIT11 = 0x5B, // OTC_IRP_DAT_PAR, Bits[11:11]
	IIO_INTERNAL_OTC_BIT12 = 0x5C, // OTC_IRP_ADDR_PAR, Bits[12:12]
	IIO_INTERNAL_OTC_BIT13 = 0x5D, // OTC_HW_ASSERT, Bits[13:13]
	IIO_INTERNAL_OTC_BIT14 = 0x5E, // OTC_TXN_DUR_LOCK, Bits[14:14]
	IIO_INTERNAL_OTC_BIT15 = 0x5F, // OTC_GPSB_PAR, Bits[15:15]
	IIO_INTERNAL_OTC_BIT16 = 0x60, // OTC_MISC_SNARF_FIFO_OF, Bits[16:16]
	IIO_INTERNAL_OTC_BIT17 = 0x61, // OTC_MISC_SNARF_FIFO_UF, Bits[17:17]
	IIO_INTERNAL_OTC_BIT18 = 0x62, // OTC_MISC_OOBMSM_MULT_PEND, Bits[18:18]
	IIO_INTERNAL_OTC_BIT19 = 0x63, // VMD_CFGBAR_OVERFLOW, Bits[19:19]
	IIO_INTERNAL_OTC_BIT20 = 0x64, // OTC_POISON_MABORT, Bits[20:20]
	IIO_INTERNAL_OTC_BIT21 = 0x65, //OTC_SNAPSHOT_RELOAD, Bits[21:21]
	IIO_INTERNAL_OTC_BIT22 = 0x66, //OTC_MULT_DRAIN, Bits[22:22]
	IIO_INTERNAL_OTC_RESERVED = 0x67 // Reserved / Others

Vtd Uncorrectable Fatal/Non-Fatal Errors	IIO_INTERNAL_VTD_UNC_BIT00 = 0x70, // IOMMU_DATA_IOTLB_PAR_ERR, Bits[0:0]
	IIO_INTERNAL_VTD_UNC_BIT01 = 0x71, // PQ_REQ_PAR_ERR, Bits[1:1]
	IIO_INTERNAL_VTD_UNC_BIT02 = 0x72, // PWT_REQ_PAR_ERR, Bits[2:2]
	IIO_INTERNAL_VTD_UNC_BIT03 = 0x73, // IOMMU_MEM_RESP_ABORT, Bits[3:3]
	IIO_INTERNAL_VTD_UNC_BIT04 = 0x74, // ATS_PMR_CHECK_ABORT, Bits[4:4]
	IIO_INTERNAL_VTD_UNC_BIT16 = 0x75, // PMR_CHECK_ABORT, Bits[16:16]
	IIO_INTERNAL_VTD_UNC_BIT17 = 0x76, // HPA_OVERFLOW, Bits[17:17]
	IIO_INTERNAL_VTD_UNC_BIT18 = 0x77, // GPA_OVERFLOW, Bits[18:18]
	IIO_INTERNAL_VTD_UNC_BIT19 = 0x78, // ILLEGAL_MSI, Bits[19:19]
	IIO_INTERNAL_VTD_UNC_BIT20 = 0x79, // AT_TRANSLATED_ILLEGAL_DEVICE, Bits[20:20]
	IIO_INTERNAL_VTD_UNC_BIT21 = 0x7A, // MSI_OVERFLOW, Bits[21:21]
	IIO_INTERNAL_VTD_UNC_BIT22 = 0x7B, // CANONICAL_VIOLATION, Bits[22:22]
	IIO_INTERNAL_VTD_UNC_RESERVED = 0x7C // Reserved / Others

IIO Internal Error Type Table	
Error Types	**Description**

Vtd Corrected Errors	IIO_INTERNAL_VTD_COR_BIT00 = 0x85, // IOMMU_TAG_IOTLB_PAR_ERR, Bits[0:0]
	IIO_INTERNAL_VTD_COR_BIT01 = 0x86, // IOMMU_TAG_SL_L2_PAR_ERR, Bits[1:1]
	IIO_INTERNAL_VTD_COR_BIT02 = 0x87, // IOMMU_TAG_SL_L3_PAR_ERR, Bits[2:2]
	IIO_INTERNAL_VTD_COR_BIT03 = 0x88, // IOMMU_TAG_SL_L4_PAR_ERR, Bits[3:3]
	IIO_INTERNAL_VTD_COR_BIT04 = 0x89, // IOMMU_TAG_SL_L5_PAR_ERR, Bits[4:4]
	IIO_INTERNAL_VTD_COR_BIT05 = 0x8A, // IOMMU_TAG_FL_L2_PAR_ERR, Bits[5:5]
	IIO_INTERNAL_VTD_COR_BIT06 = 0x8B, // IOMMU_TAG_FL_L3_PAR_ERR, Bits[6:6]
	IIO_INTERNAL_VTD_COR_BIT07 = 0x8C, // IOMMU_TAG_FL_L4_PAR_ERR, Bits[7:7]
	IIO_INTERNAL_VTD_COR_BIT08 = 0x8D, // IOMMU_TAG_FL_L5_PAR_ERR, Bits[8:8]
	IIO_INTERNAL_VTD_COR_BIT09 = 0x8E, // IOMMU_TAG_PASID_PAR_ERR, Bits[9:9]
	IIO_INTERNAL_VTD_COR_BIT10 = 0x8F, // IOMMU_TAG_RCC_PAR_ERR, Bits[10:10]
	IIO_INTERNAL_VTD_COR_BIT11 = 0x90, // IOMMU_TAG_ICE_PAR_ERR, Bits[11:11]
	IIO_INTERNAL_VTD_COR_BIT12 = 0x91, // IOMMU_DATA_SL_L2_PAR_ERR, Bits[12:12]
	IIO_INTERNAL_VTD_COR_BIT13 = 0x92, // IOMMU_DATA_SL_L3_PAR_ERR, Bits[13:13]
	IIO_INTERNAL_VTD_COR_BIT14 = 0x93, // IOMMU_DATA_SL_L4_PAR_ERR, Bits[14:14]
	IIO_INTERNAL_VTD_COR_BIT15 = 0x94, // IOMMU_DATA_SL_L5_PAR_ERR, Bits[15:15]
	IIO_INTERNAL_VTD_COR_BIT16 = 0x95, // IOMMU_DATA_FL_L2_PAR_ERR, Bits[16:16]
	IIO_INTERNAL_VTD_COR_BIT17 = 0x96, // IOMMU_DATA_FL_L3_PAR_ERR, Bits[17:17]
	IIO_INTERNAL_VTD_COR_BIT18 = 0x97, // IOMMU_DATA_FL_L4_PAR_ERR, Bits[18:18]
	IIO_INTERNAL_VTD_COR_BIT19 = 0x98, // IOMMU_DATA_FL_L5_PAR_ERR, Bits[19:19]
	IIO_INTERNAL_VTD_COR_BIT20 = 0x99, // IOMMU_DATA_PASID_ERR, Bits[20:20]
	IIO_INTERNAL_VTD_COR_BIT21 = 0x9A, // IOMMU_DATA_RCC_PAR_ERR, Bits[21:21]
	IIO_INTERNAL_VTD_COR_BIT22 = 0x9B, // IOMMU_DATA_ICE_PAR_ERR, Bits[22:22]
	IIO_INTERNAL_VTD_COR_BIT23 = 0x9C, // IOMMU_DATA_PWT_OTHER_PAR_ERR, Bits[23:23]
	IIO_INTERNAL_VTD_COR_RESERVED = 0x9B // Reserved / Others

IRP Errors	IIO_INTERNAL_IRPERR_BIT00 = 0xA3, // WRCACHE_CORRECC_ERROR, Bits[0:0]
	IIO_INTERNAL_IRPERR_BIT01 = 0xA4, // WRCACHE_CORRECC_ERROR, Bits[1:1]
	IIO_INTERNAL_IRPERR_BIT02 = 0xA5, // PROTOCOL_RCVD_POISON, Bits[2:2]
	IIO_INTERNAL_IRPERR_BIT03 = 0xA6, // CSR_ACC_32B_UNALIGNED, Bits[3:3]
	IIO_INTERNAL_IRPERR_BIT04 = 0xA7, // PROTOCOL_RCVD_UNEXPRSP, Bits[4:4]
	IIO_INTERNAL_IRPERR_BIT05 = 0xA8, // PROTOCOL_PARITY_ERROR, Bits[5:5]
	IIO_INTERNAL_IRPERR_BIT06 = 0xA9, // P2P_HDR_RF_ADDR_PAR_ERROR, Bits[6:6]
	IIO_INTERNAL_IRPERR_BIT07 = 0xB0, // FAF_RF_ADDR_PAR_ERROR, Bits[7:7]
	IIO_INTERNAL_IRPERR_BIT08 = 0xB1, // ADDRCAM0_ADDR_PAR_ERROR, Bits[8:8]
	IIO_INTERNAL_IRPERR_BIT09 = 0xB2, // ADDRCAM1_ADDR_PAR_ERROR, Bits[9:9]
	IIO_INTERNAL_IRPERR_BIT10 = 0xB3, // ADDRCAM2_ADDR_PAR_ERROR, Bits[10:10]
	IIO_INTERNAL_IRPERR_BIT11 = 0xB4, // ADDRCAM3_ADDR_PAR_ERROR, Bits[11:11]
	IIO_INTERNAL_IRPERR_BIT12 = 0xB5, // PF_TIMEOUT_ERR_CS0, Bits[12:12]
	IIO_INTERNAL_IRPERR_BIT13 = 0xB6, // PF_TIMEOUT_ERR_CS1, Bits[13:13]
	IIO_INTERNAL_IRPERR_BIT14 = 0xB7, // PF_TIMEOUT_ERR_CS2, Bits[14:14]
	IIO_INTERNAL_IRPERR_BIT15 = 0xB8, // PF_TIMEOUT_ERR_CS3, Bits[15:15]
	IIO_INTERNAL_IRPERR_BIT16 = 0xB9, // PROTOCOL_QT_OVERFLOW_UNDERFLOW, Bits[16:16]
	IIO_INTERNAL_IRPERR_BIT17 = 0xBA, // IOMMU_FAF_RF_ADDR_PAR_ERROR, Bits[17:17]
	IIO_INTERNAL_IRPERR_BIT18 = 0xBB, //P2P_DATA_PAR_ERROR, Bits[18:18]
	IIO_INTERNAL_IRPERR_BIT19 = 0xBC, //IOMMU_FAF_RF_HDR_PAR_ERROR, Bits[19:19]
	IIO_INTERNAL_IRPERR_BIT20 = 0xBD, //IOMMU_FAF_RF_DATA_PAR_ERROR, Bits[20:20]
	IIO_INTERNAL_IRPERR_BIT21 = 0xBE, //IOMMU_FAF_AMAP_ABORT, Bits[21:21]
	IIO_INTERNAL_IRPERR_RESERVED = 0xBF // Reserved / Others

IIO Internal Error Type Table	
Error Types	**Description**

Ring Errors	IIO_INTERNAL_IRPRING_BIT00 = 0xC9, // BL0_PARITY_ERROR, Bits[0:0]
	IIO_INTERNAL_IRPRING_BIT01 = 0xCA, // BL1_PARITY_ERROR, Bits[1:1]
	IIO_INTERNAL_IRPRING_BIT02 = 0xCB, // SNP_ADDR_PARITY_ERROR, Bits[2:2]
	IIO_INTERNAL_IRPRING_BIT03 = 0xCC, // RXDATA1_PARITY_ERROR, Bits[3:3]
	IIO_INTERNAL_IRPRING_BIT04 = 0xCD, // RXDATA0_PARITY_ERROR, Bits[4:4]
	IIO_INTERNAL_IRPRING_BIT05 = 0xCE, // BLQ_PARITY_ERROR, Bits[5:5]
	IIO_INTERNAL_IRPRING_BIT06 = 0xCF, // BL_ECC_CORRECTED_ERROR, Bits[6:6]
	IIO_INTERNAL_IRPRING_BIT07 = 0xD0, // BL_ECC_UNCORRECTABLE_ERROR, Bits[7:7]
	IIO_INTERNAL_IRPRING_BIT08 = 0xD1, // BL0_CQID_PARITY_ERROR, Bits[8:8]
	IIO_INTERNAL_IRPRING_BIT09 = 0xD2, // BL1_CQID_PARITY_ERROR, Bits[9:9]
	IIO_INTERNAL_IRPRING_BIT10 = 0xD3, // AK0_CQID_PARITY_ERROR, Bits[10:10]
	IIO_INTERNAL_IRPRING_BIT11 = 0xD4, // AK1_CQID_PARITY_ERROR, Bits[11:11]
	IIO_INTERNAL_IRPRING_BIT12 = 0xD5, // TXQ0_ADDR_PAR_ERROR, Bits[12:12]
	IIO_INTERNAL_IRPRING_BIT13 = 0xD6, // TXQ1_ADDR_PAR_ERROR, Bits[13:13]
	IIO_INTERNAL_IRPRING_BIT14 = 0xD7, //SNPQ_RF_ADDR_PARITY_ERROR, Bits[14:14]
	IIO_INTERNAL_IRPRING_BIT15 = 0xD8, //UNEXPECTED_GO_ERR_RCVD, Bits[15:15]
	IIO_INTERNAL_IRPRING_BIT16 = 0xD9, //UNEXPECTED_IDI_U2C_RCVD, Bits[16:16]
	IIO_INTERNAL_IRPRING_BIT17 = 0xDA, //P2P_BL_PARITY_ERROR, Bits[17:17]
	IIO_INTERNAL_IRPRING_BIT18 = 0xDB, //ASF_QUEUE_OVERFLOW_UNDERFLOW, Bits[18:18]
	IIO_INTERNAL_IRPRING_RESERVED = 0xDC // Reserved / Others

ITC Errors	IIO_INTERNAL_ITC_BIT6 = 0xDD, // ITC_MULT_DRAIN, Bits[6:6]
	IIO_INTERNAL_ITC_BIT7 = 0xDE, // ITC_SNAPSHOT_RELOAD, Bits[7:7]
	IIO_INTERNAL_ITC_BIT8 = 0xDF, // ITC_SB_OF, Bits[8:8]
	IIO_INTERNAL_ITC_BIT9 = 0xE0, // ITC_SB_UF, Bits[9:9]
	IIO_INTERNAL_ITC_BIT10 = 0xE1, // ITC_IOSF_HCRED_UF, Bits[10:10]
	IIO_INTERNAL_ITC_BIT11 = 0xE2, // ITC_IOSF_HCRED_OF, Bits[11:11]
	IIO_INTERNAL_ITC_BIT12 = 0xE3, // ITC_ENQ_DATA_OVERFLOW, Bits[12:12]
	IIO_INTERNAL_ITC_BIT13 = 0xE4, // SW2IOSF_MPS_ERR, Bits[13:13]
	IIO_INTERNAL_ITC_BIT14 = 0xE5, // ITC_IOSF_DCRED_UF, Bits[14:14]
	IIO_INTERNAL_ITC_BIT15 = 0xE6, // ITC_IOSF_DCRED_OF, Bits[15:15]
	IIO_INTERNAL_ITC_BIT16 = 0xE7, // If ITC_IRP_CRED_UF, Bits[16:16]
	IIO_INTERNAL_ITC_BIT17 = 0xE8, // ITC_IRP_CRED_OF, Bits[17:17]
	IIO_INTERNAL_ITC_BIT18 = 0xE9, // ITC_PAR_IOSF_DAT, Bits[18:18]
	IIO_INTERNAL_ITC_BIT19 = 0xEA, // ITC_PAR_HDR_RF, Bits[19:19]
	IIO_INTERNAL_ITC_BIT20 = 0xEB, // ITC_VTMISC_HDR_RF, Bits[20:20]
	IIO_INTERNAL_ITC_BIT21 = 0xEC, // ITC_PAR_ADDR_RF, Bits[21:21]
	IIO_INTERNAL_ITC_BIT22 = 0xED, // ITC_ECC_COR_RF, Bits[22:22]
	IIO_INTERNAL_ITC_BIT23 = 0xEE, // ITC_ECC_UNCOR_RF, Bits[23:23]
	IIO_INTERNAL_ITC_BIT24 = 0xEF, // ITC_CABORT, Bits[24:24]
	IIO_INTERNAL_ITC_BIT25 = 0xF0, // ITC_MABORT, Bits[25:25]
	IIO_INTERNAL_ITC_BIT26 = 0xF1, // INB_UNSUCCESSFUL_CMPL, Bits[26:26]
	IIO_INTERNAL_ITC_BIT27 = 0xF2, // ITC_ENQ_OVERFLOW, Bits[27:27]
	IIO_INTERNAL_ITC_BIT28 = 0xF3, // ITC_MISC_PRH_OVERFLOW, Bits[28:28]
	IIO_INTERNAL_ITC_BIT29 = 0xF4, // ITC_HW_ASSERT, Bits[29:29]
	IIO_INTERNAL_ITC_BIT30 = 0xF5, // ITC_PAR_IOSF_CMD, Bits[30:30]
	IIO_INTERNAL_ITC_BIT31 = 0xF6, // ITC_MSGD_ILLEGAL_SIZE, Bits[31:31]
	IIO_INTERNAL_ITC_RESERVED = 0xF7 // Reserved / Others Bits

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 (DMIEdit) 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:

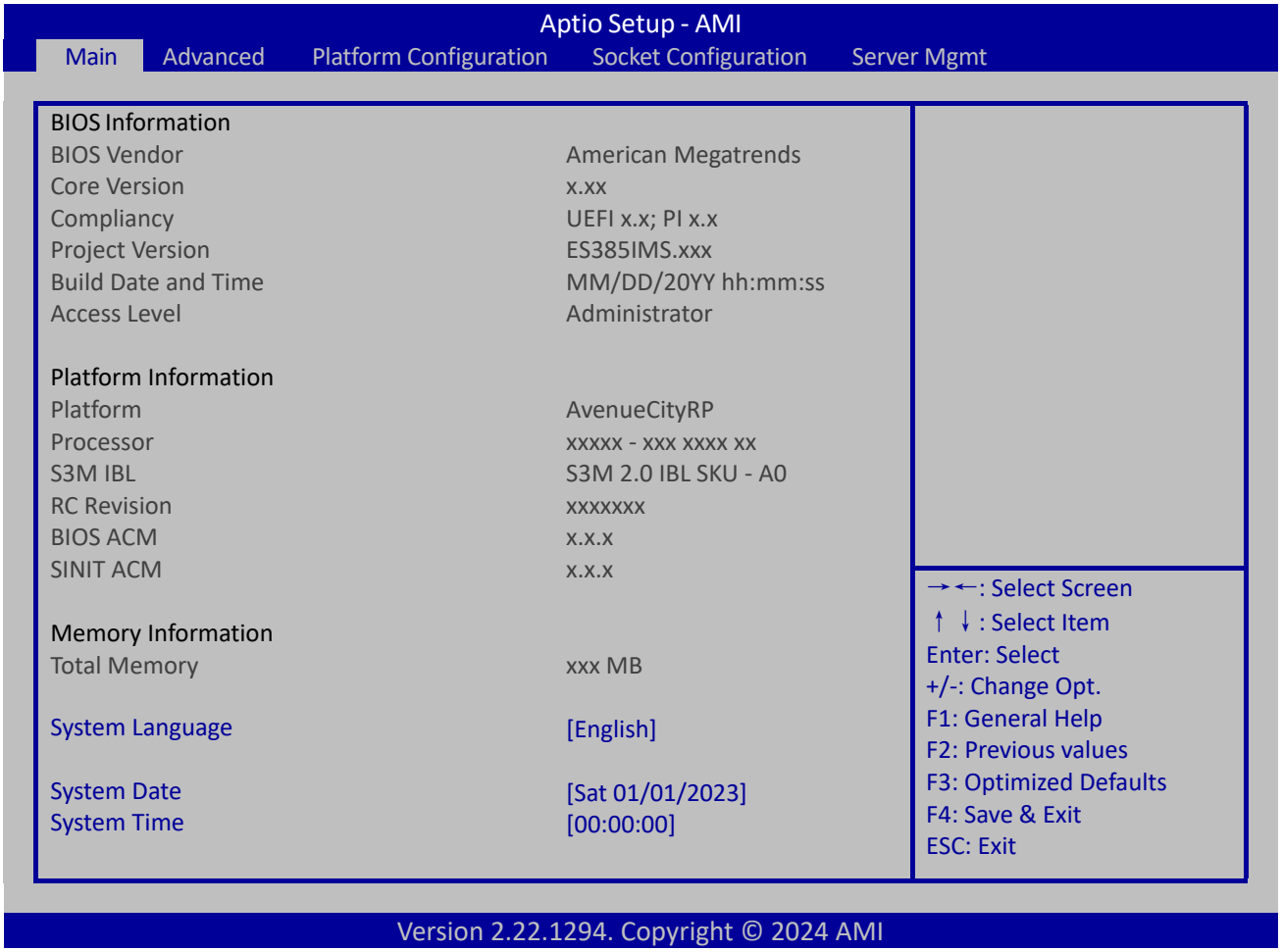
* BIOS Information (Type 0)
* System (Type 1)
* Base Board (Type 2)
* Chassis (Type 3)
* Processor Information (Type 4)
* OEM String (Type 11)
* System Configuration Options (Type 12)
* Portable Battery (Type 22)
* System Power Supply (Type 39)

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

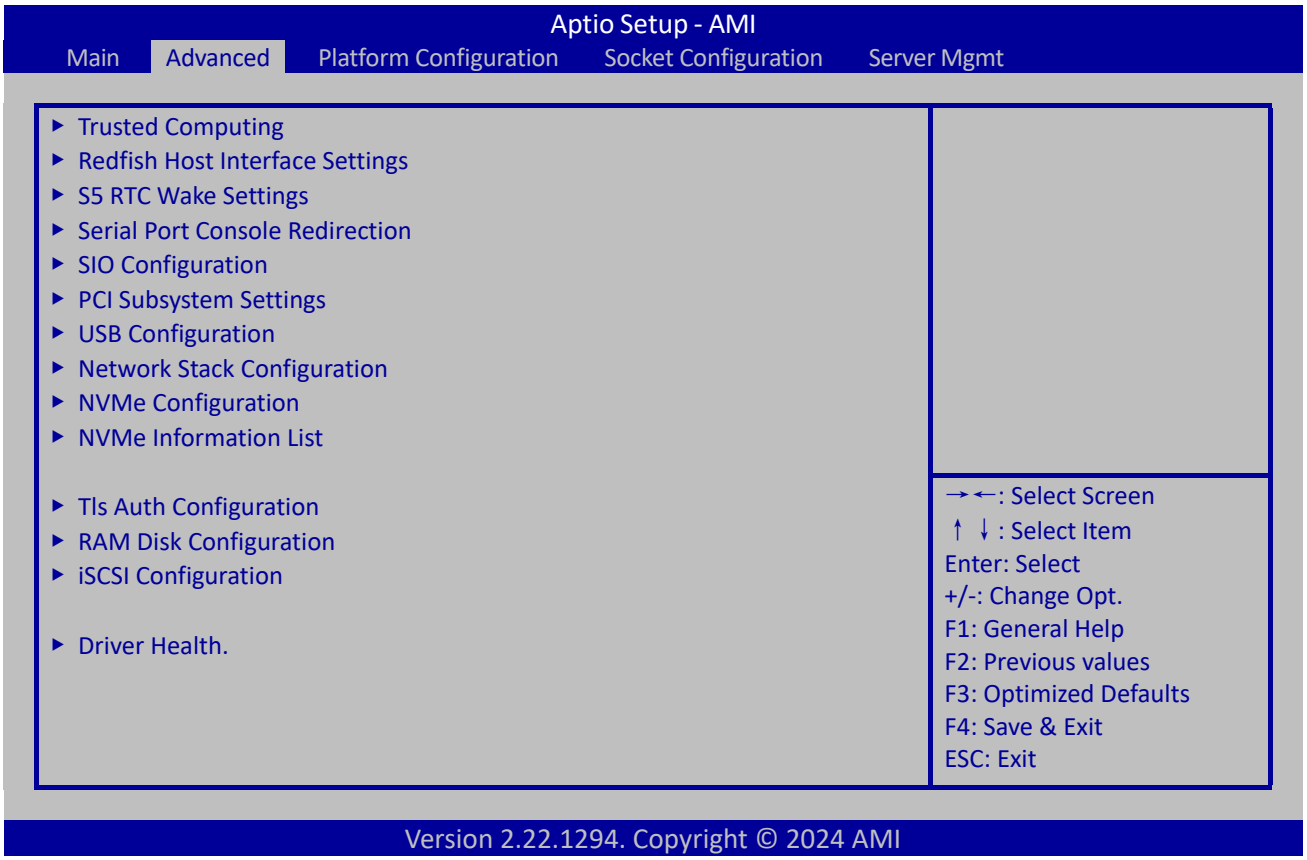
6.1 MAIN MENU



Main		
Menu Fields	**Settings**	**Comments**
BIOS Information		
BIOS Vendor	American Megatrends	
Core Version	x.xx	Displays the Core version.
Compliancy	UEFI x.x: PI x.x	Displays the Compliancy name.
Project Version	ES385IMS.xxx	Displays the BIOS version.
Build Date and Time	MM/DD/20YY hh:mm:ss	Displays the BIOS build date and time.
Access Level	Administrator	Displays the control level of setup menu.
Platform Information		
Platform	AvenueCityRP	Displays the Intel reference platform name.
Processor	xxxxx - xxx xxxx xx	Displays the Processor version.
S3M IBL	S3M 2.0 IBL SKU - A0	Displays the S3M IBL version.
RC Revision	xxxxxxx	Displays the RC Revision.

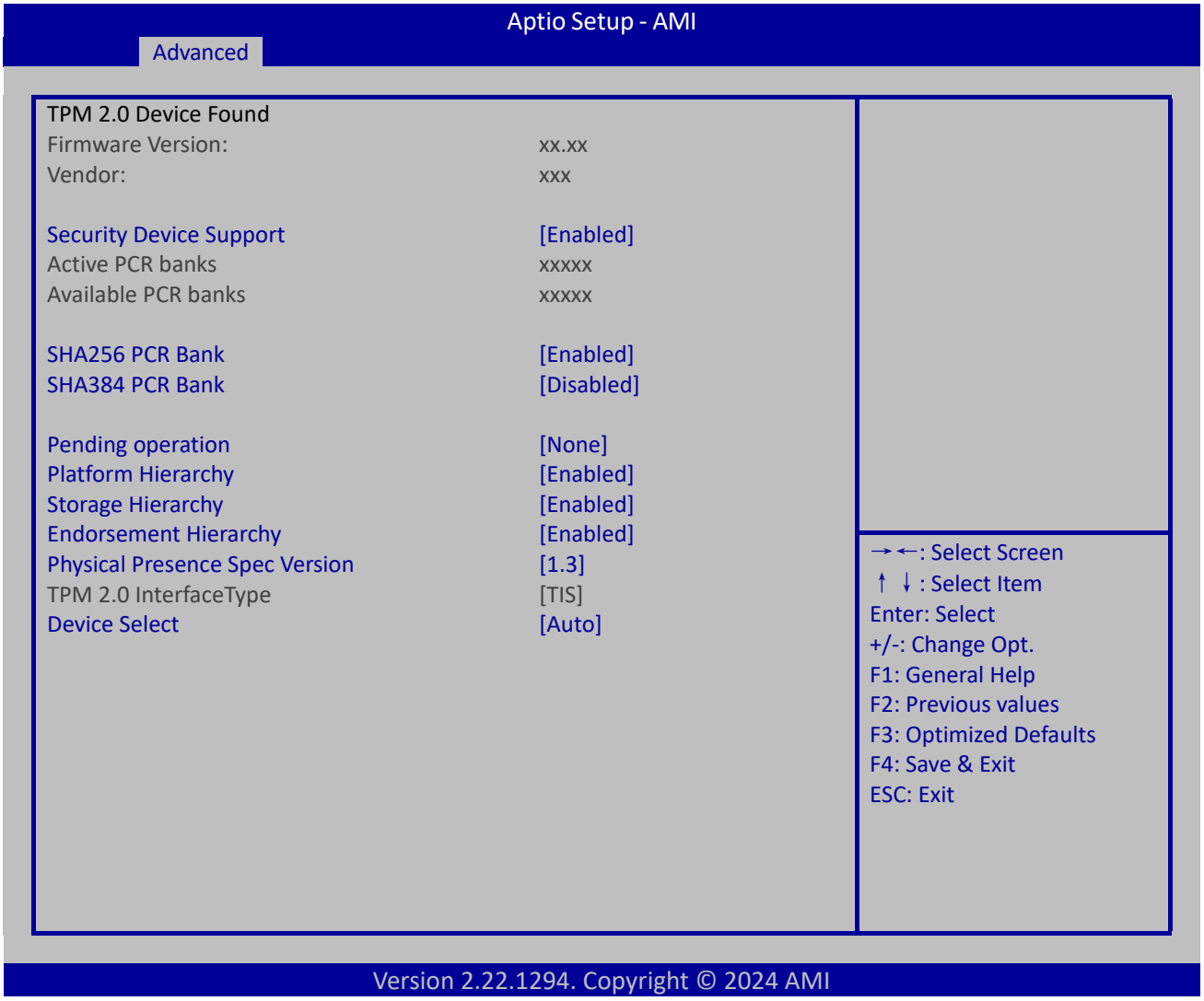
Main		
Menu Fields	**Settings**	**Comments**
BIOS ACM	x.x.x	Displays the BIOS ACM version.
SINIT ACM	x.x.x	Displays the SINIT ACM version.
Memory Information		
Total memory	xxx MB	Displays the available memory size
System time	[Sat 01/01/2023]	Displays the current time.
System date	[00:00:00]	Displays the current date.

6.2 ADVANCED MENU



Advanced		
Menu Fields	**Settings**	**Comments**
Trusted Computing	Selects sub-menu.	
Redfish Host Interface Settings	Selects sub-menu.	
S5 RTC Wake Settings	Selects sub-menu.	
Serial Port Console Redirection	Selects sub-menu.	
SIO Configuration	Selects sub-menu.	
PCI Subsystem Settings	Selects sub-menu.	
USB Configuration	Selects sub-menu.	
Network Stack Configuration	Selects sub-menu.	
NVMe Configuration	Selects sub-menu.	
NVMe Information List	Selects sub-menu.	
Tls Auth Configuration	Selects sub-menu.	
RAM Disk Configuration	Selects sub-menu.	
iSCSI Configuration	Selects sub-menu.	
Driver Health	Selects sub-menu.	

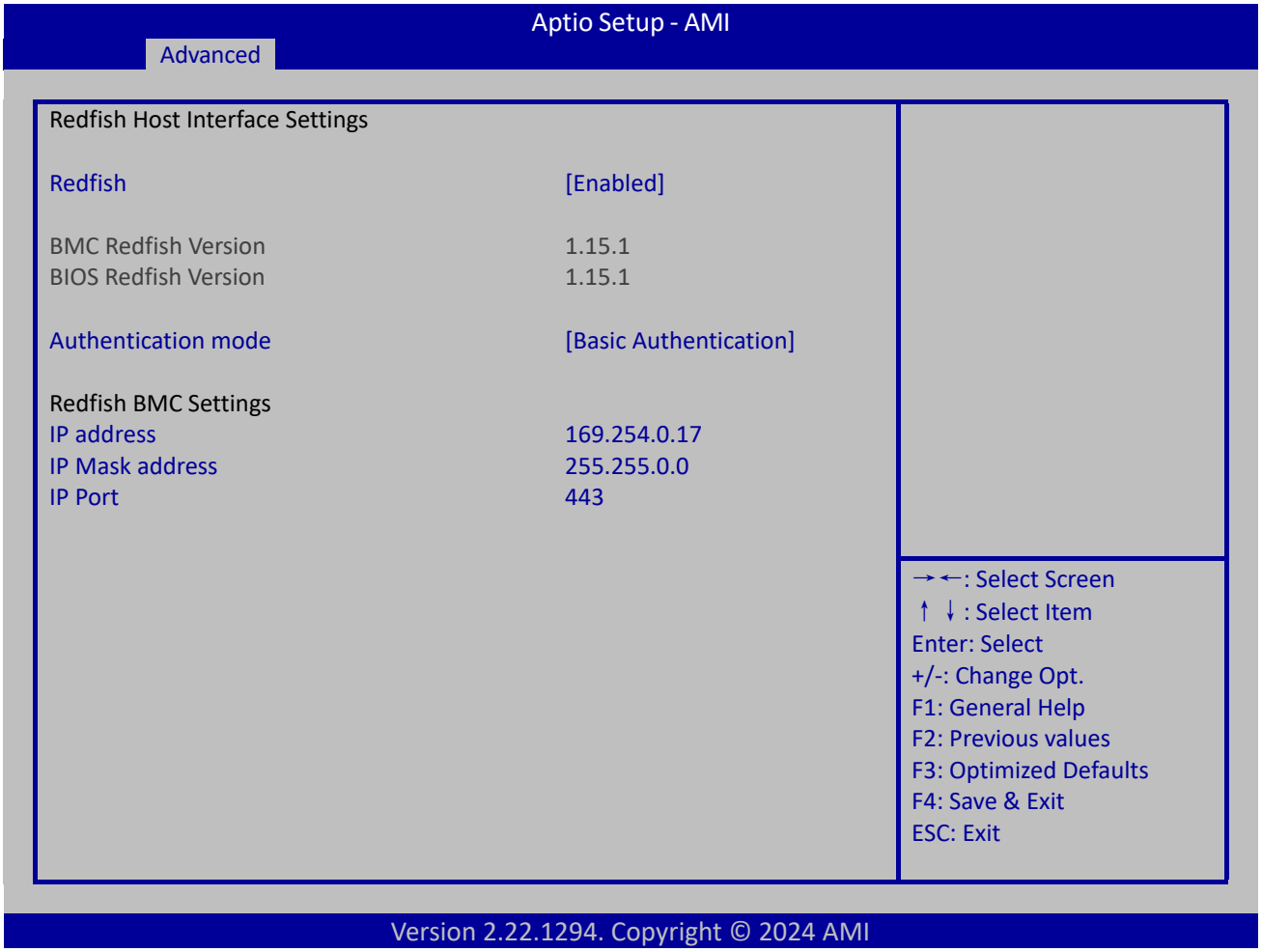
6.2.1 Trusted Computing



Advanced \ Trusted Computing		
Menu Fields	**Settings**	**Comments**
TPM 2.0 Device Found		Displays the TPM State.
Firmware Version:	xx.xx	Displays the TPM Firmware version.
Vendor:	xxx	Displays the TPM chip vendor.
Security Device Support	[Disabled] **[Enabled]**	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Active PCR banks	xxxxx	Displays the active PCR banks.
Available PCR banks	xxxxx	Displays the Available PCR banks.
SHA256 PCR Bank	[Disabled] **[Enabled]**	Enable or Disable SHA256 PCR Bank
SHA384 PCR Bank	**[Disabled]** [Enabled]	Enable or Disable SHA384 PCR Bank
Pending operation	**[None]** [TPM Clear]	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.

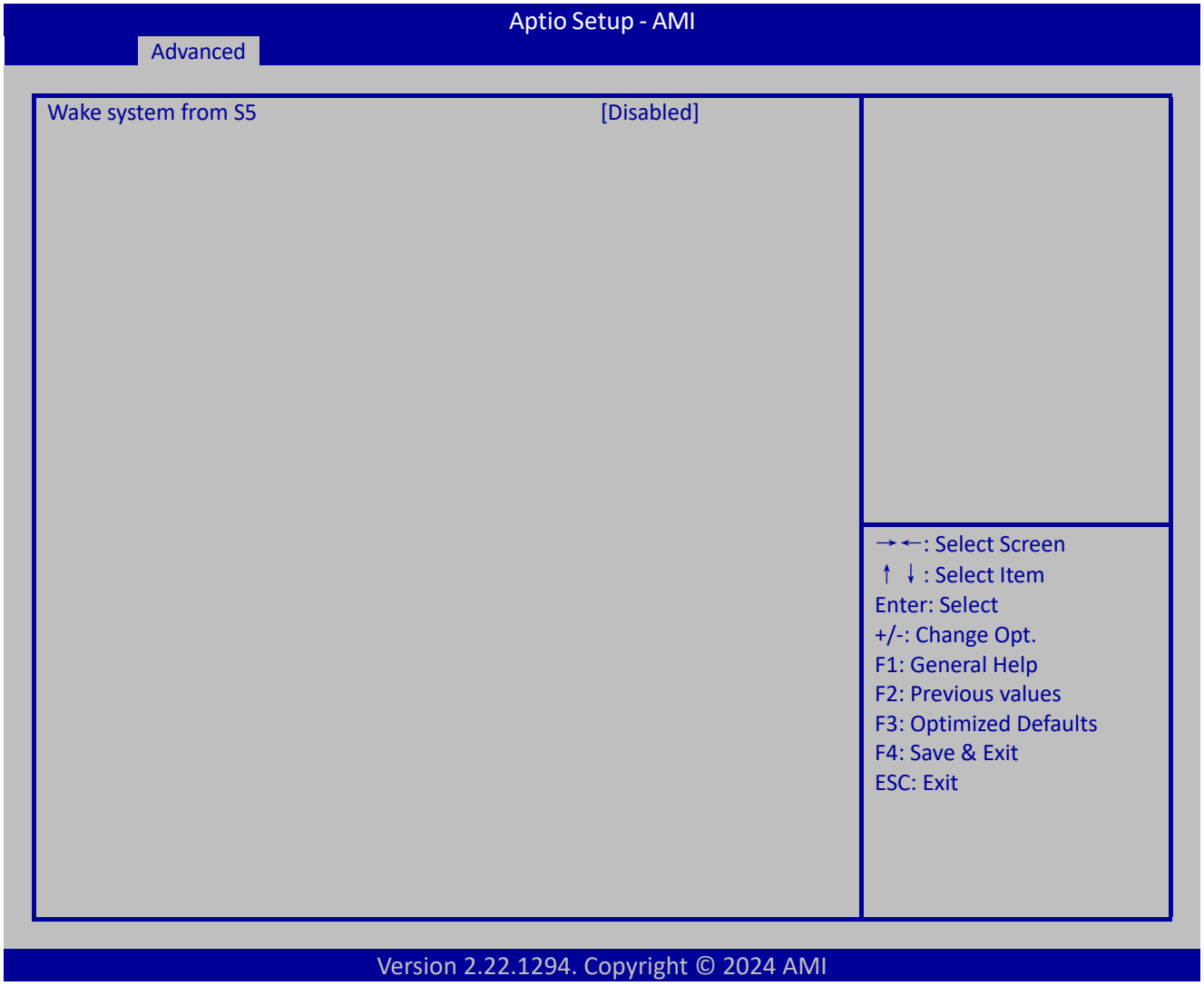
Advanced \ Trusted Computing		
Menu Fields	**Settings**	**Comments**
Platform Hierarchy	[Disabled] **[Enabled]**	Enable or Disable Platform Hierarchy
Storage Hierarchy	[Disabled] **[Enabled]**	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	[Disabled] **[Enabled]**	Enable or Disable Endorsement Hierarchy
Physical Presence Spec Version	[1.2] **[1.3]**	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
TPM 2.0 InterfaceType	**[Tis]**	Select the Communication Interface to TPM 20 Device.
Device Select	[TPM 1.2] [TPM 2.0] **[Auto]**	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

6.2.2 Redfish Host Interface Settings



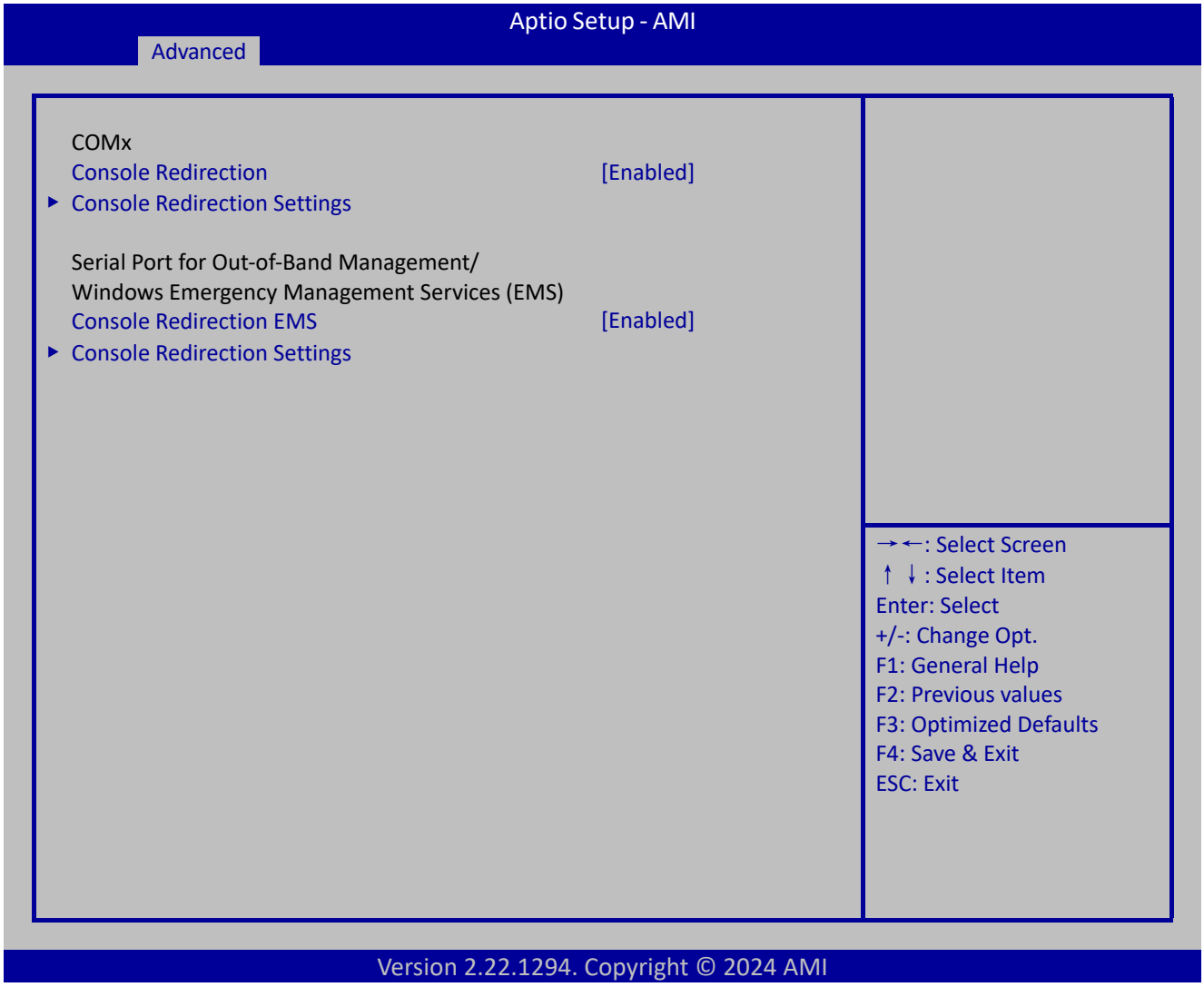
Advanced \ Redfish Host Interface Settings		
Menu Fields	**Settings**	**Comments**
Redfish Host Interface Settings		
Redfish	[Disabled] **[Enabled]**	Enable or disable AMI Redfish. When disabled, BIOS Redfish interface is turned off. BMC Redfish system inventory and BIOS configuration will no longer be updated.
BMC Redfish Version	1.15.1	Displays the BMC Redfish Version.
BIOS Redfish Version	1.15.1	Displays the BIOS Redfish Version.
Authentication mode	[Authentication None] **[Basic Authentication]** [Session Authentication]	Select authentication mode
Redfish BMC Settings		
IP address	**169.254.0.17**	Enter IP address
IP Mask address	**255.255.0.0**	Enter IP Mask address
IP Port	**443**	Enter IP Port

6.2.3 S5 RTC Wake Settings



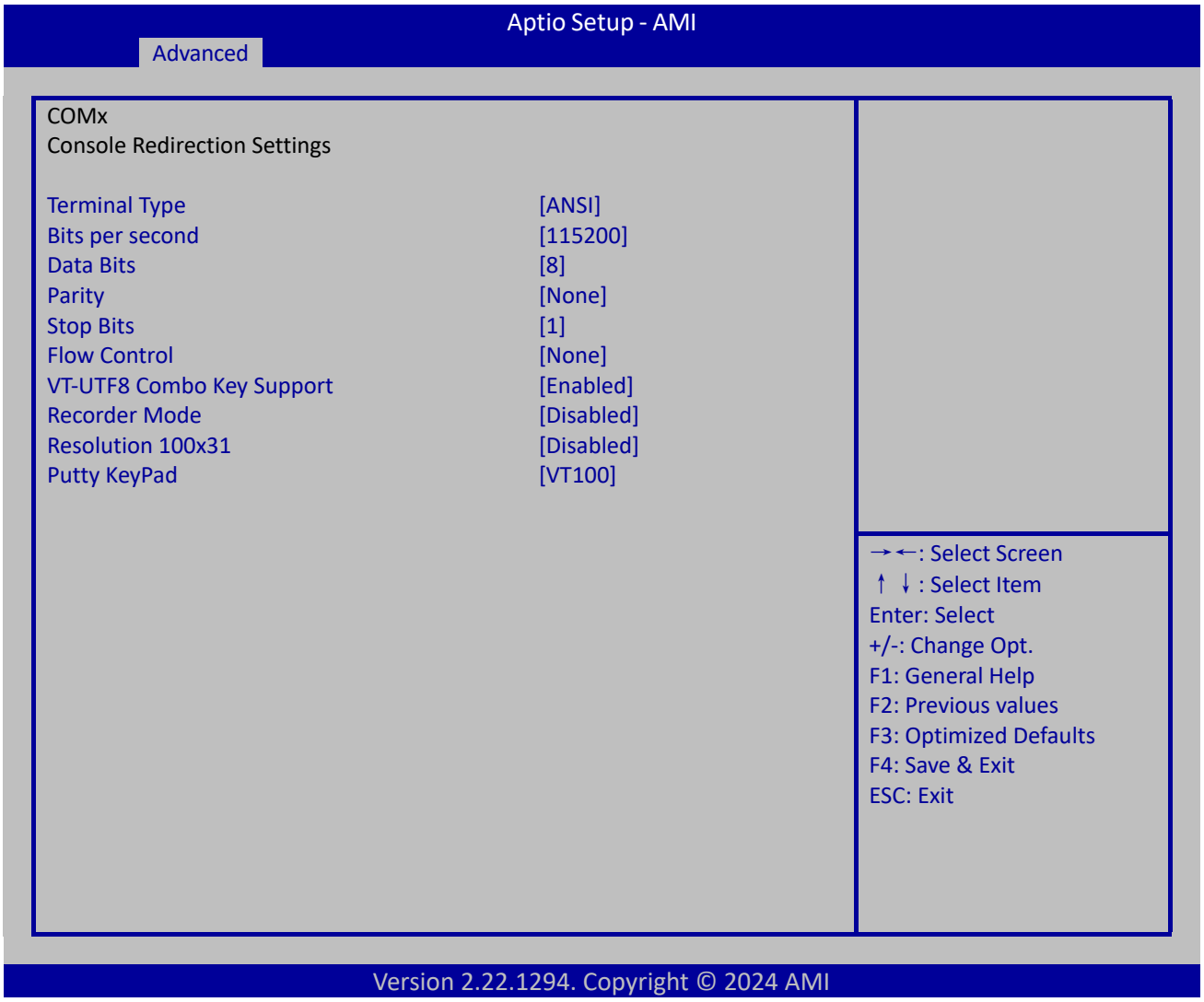
Advanced \ S5 RTC Wake Settings		
Menu Fields	**Settings**	**Comments**
Wake system from S5	**[Disabled]** [Fixed Time] [Dynamic Time]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time + Increase minute(s)
Wake up hour	**0**	select 0-23 For example enter 3 for 3am and 15 for 3pm
Wake up minute	**0**	select 0-59 for Minute
Wake up second	**0**	select 0-59 for Second
Wake up minute increase	**1**	1 - 5

6.2.4 Serial Port Console Redirection



Advanced \ Serial Port Console Redirection		
Menu Fields	**Settings**	**Comments**
COMx		
Console Redirection	[Disabled] **[Enabled]**	
Console Redirection Settings	Selects sub-menu.	
Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS)		
Console Redirection EMS	[Disabled] **[Enabled]**	
Console Redirection Settings	Selects sub-menu.	

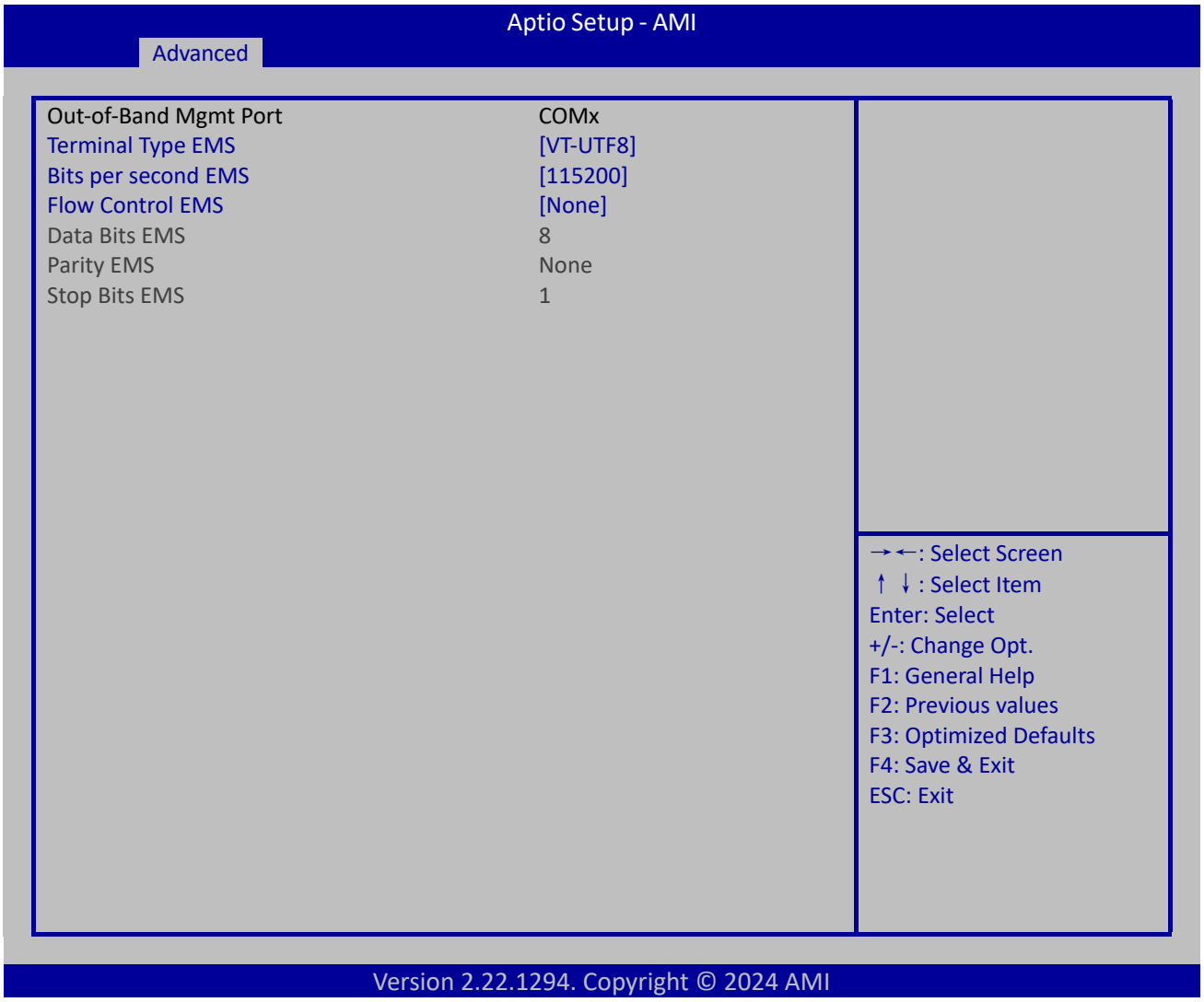
6.2.4.1 Console Redirection Settings (COMx)



Advanced \ Serial Port Console Redirection \ Console Redirection Settings (COMx)		
Menu Fields	**Settings**	**Comments**
Terminal Type	[VT100] [VT100Plug] [VT-UTF8] **[ANSI]**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: 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

Advanced \ Serial Port Console Redirection \ Console Redirection Settings (COMx)		
Menu Fields	**Settings**	**Comments**
	[Odd] [Mark] [Space]	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	**[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-UTF8 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 100x31	**[Disabled]** [Enabled]	Enables or disables extended terminal resolution
Putty KeyPad	**[VT100]** [LINUX] [XTERMR6] [SC0] [ESCN] [VT400]	Select FunctionKey and KeyPad on Putty.

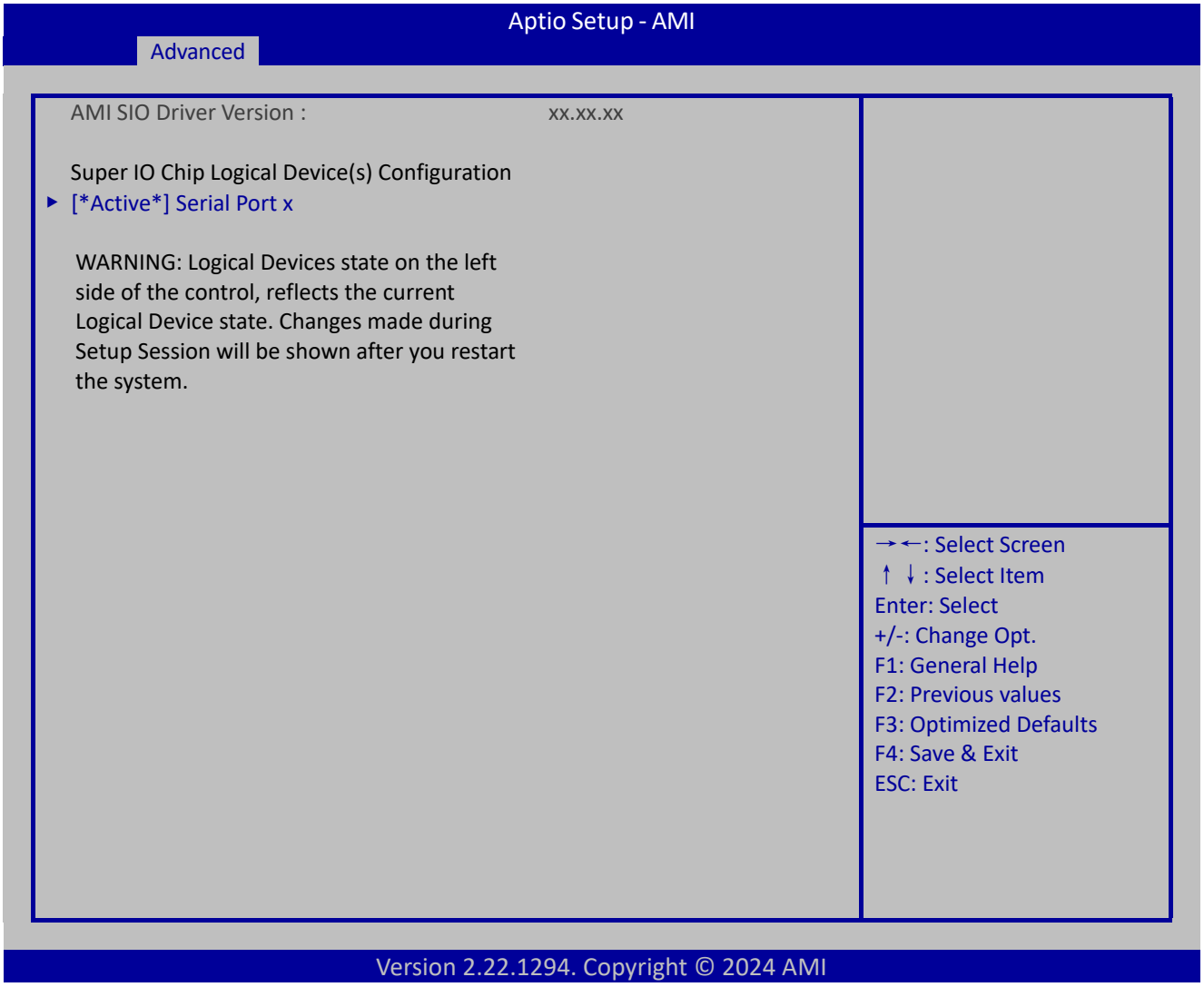
6.2.4.2 Console Redirection Settings (EMS)



Advanced \ Serial Port Console Redirection \ Console Redirection Settings (EMS)		
Menu Fields	**Settings**	**Comments**
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]** [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.
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.

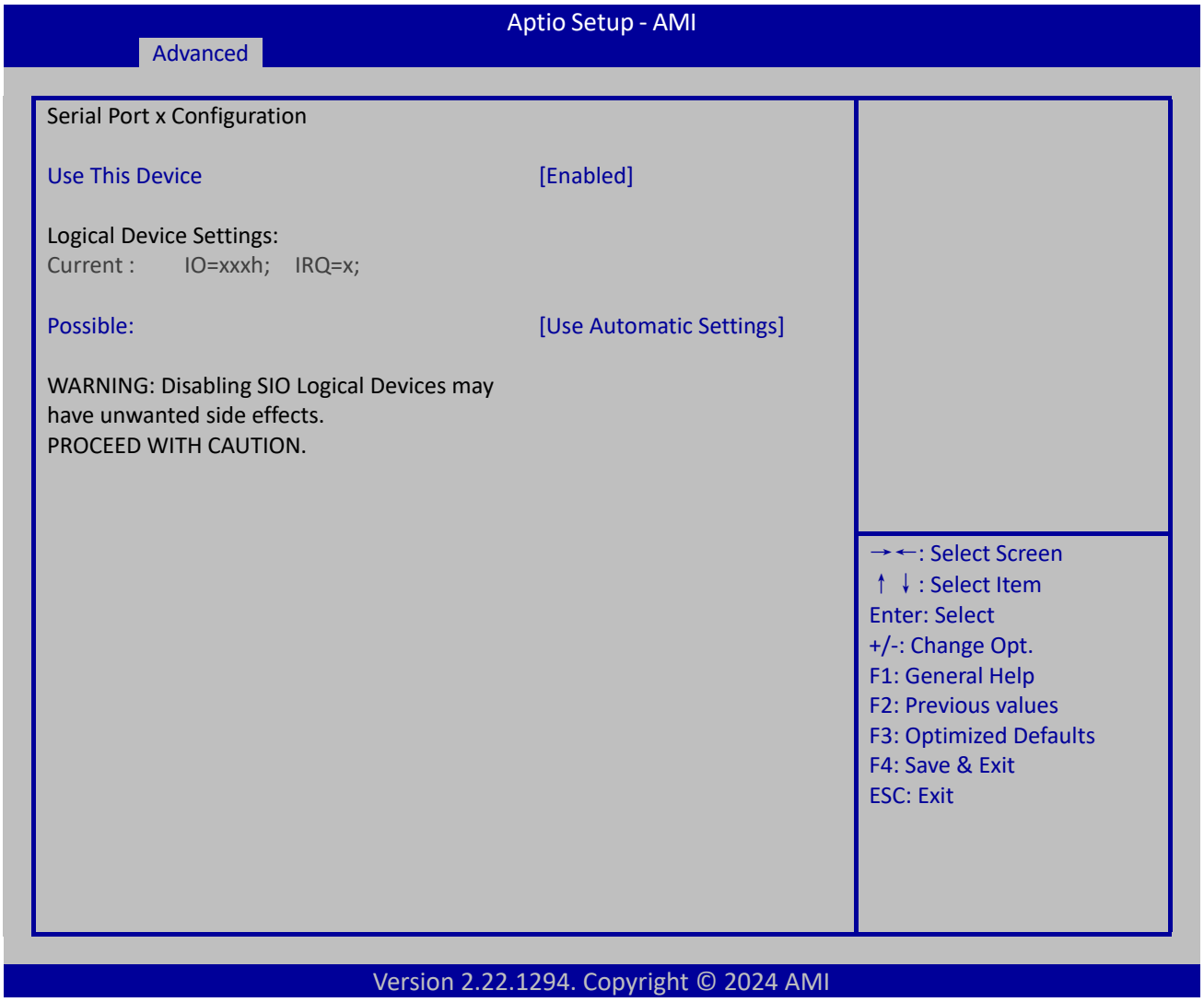
Advanced \ Serial Port Console Redirection \ Console Redirection Settings (EMS)		
Menu Fields	**Settings**	**Comments**
Data Bits EMS	[Enabled] **[Disabled]**	Data Bits
Parity EMS	**0**	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 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	**[No Access]** [Callback] [User] [Operator] [Administrator]	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.

6.2.5 SIO Configuration



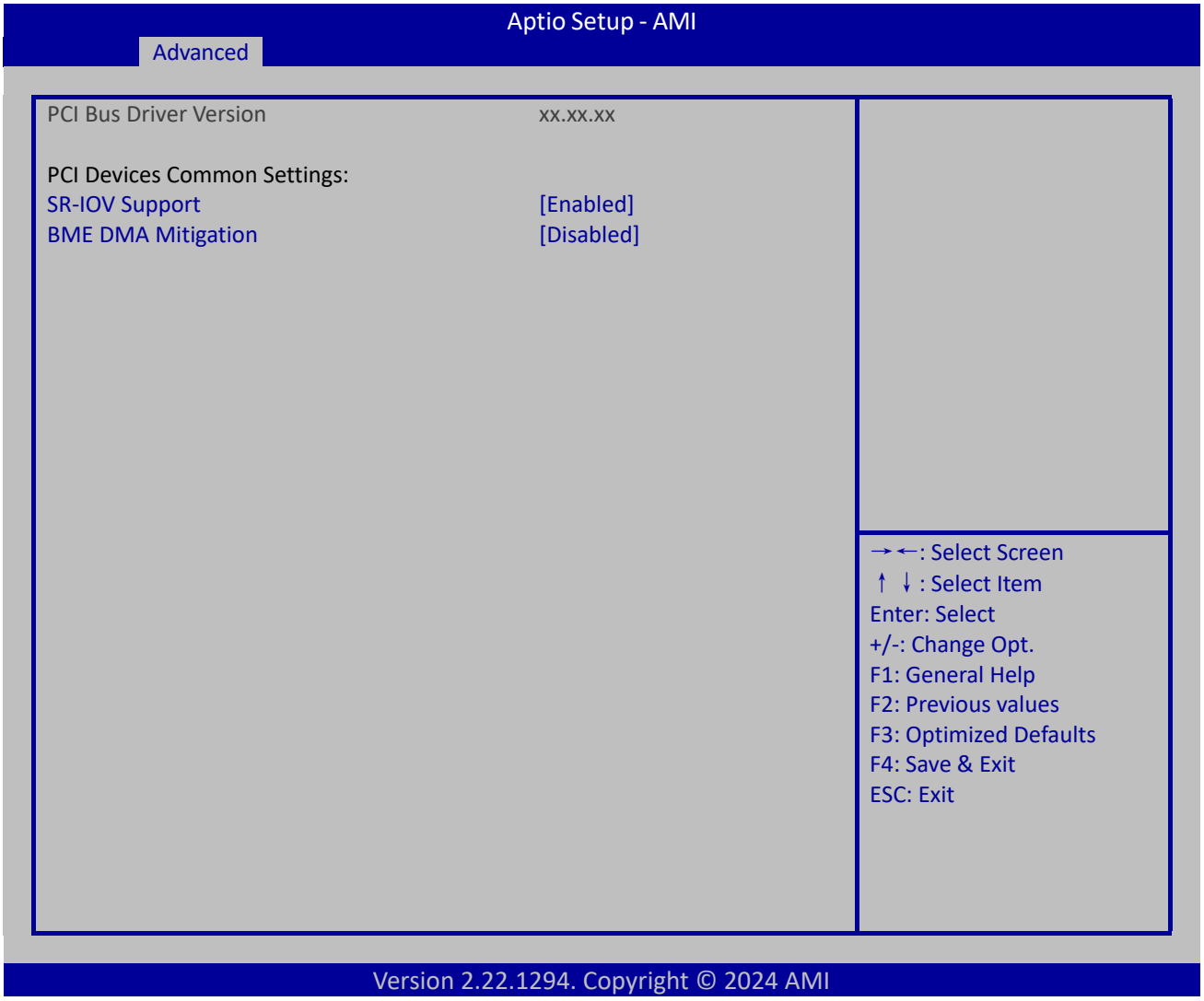
Advanced \ SIO Configuration		
Menu Fields	**Settings**	**Comments**
AMI SIO Driver Version :	xx.xx.xx	Displays the AMI SIO Driver Version.
Super IO Chip Logical Device(s) Configuration		
[*Active*] Serial Port x	Selects sub-menu.	

6.2.5.1 Serial Port x



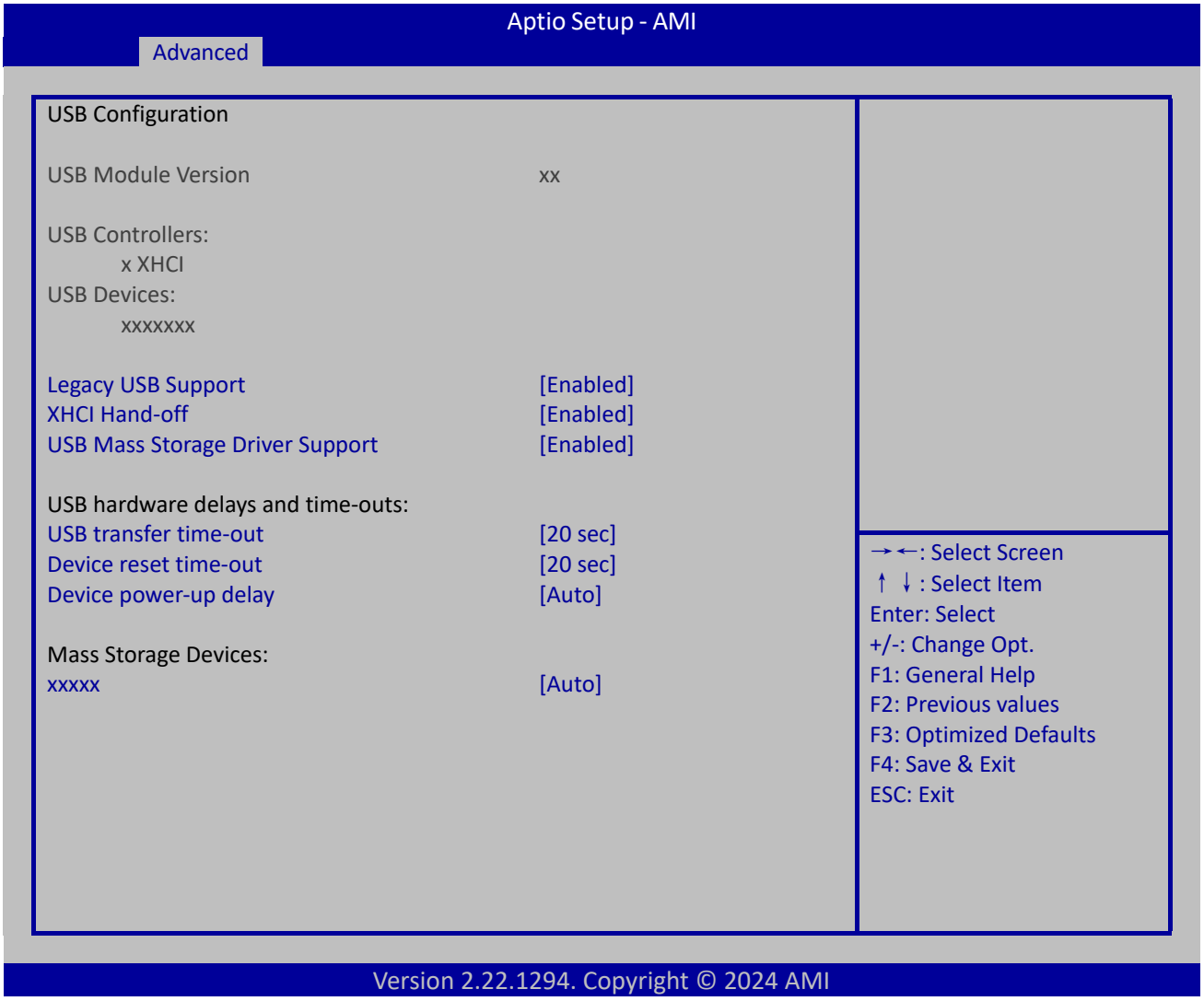
Advanced \ SIO Configuration \ Serial Port x		
Menu Fields	**Settings**	**Comments**
Serial Port x Configuration		
Use This Device	[Disabled] **[Enabled]**	Enable or Disable this Logical Device.
Logical Device Settings:		
Current :	IO=xxxh; IRQ=x;	Displays Logical Device Current Settings.
Possible:	**[Use Automatic Settings]** [IO=xxxh; IRQ=x; DMA;] [IO=xxxh; IRQ=3,4,5,6,7,9,10,11,12; DMA;] [IO=xxxh; IRQ=3,4,5,6,7,9,10,11,12; DMA;] [IO=xxxh; IRQ=3,4,5,6,7,9,10,11,12; DMA;] [IO=xxxh; IRQ=3,4,5,6,7,9,10,11,12; DMA;]	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.

6.2.6 PCI Subsystem Settings



Advanced \ PCI Subsystem Settings		
Menu Fields	**Settings**	**Comments**
PCI Bus Driver Version	xx.xx.xx	Displays the PCI Bus Driver Version.
PCI Devices Common Settings:		
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

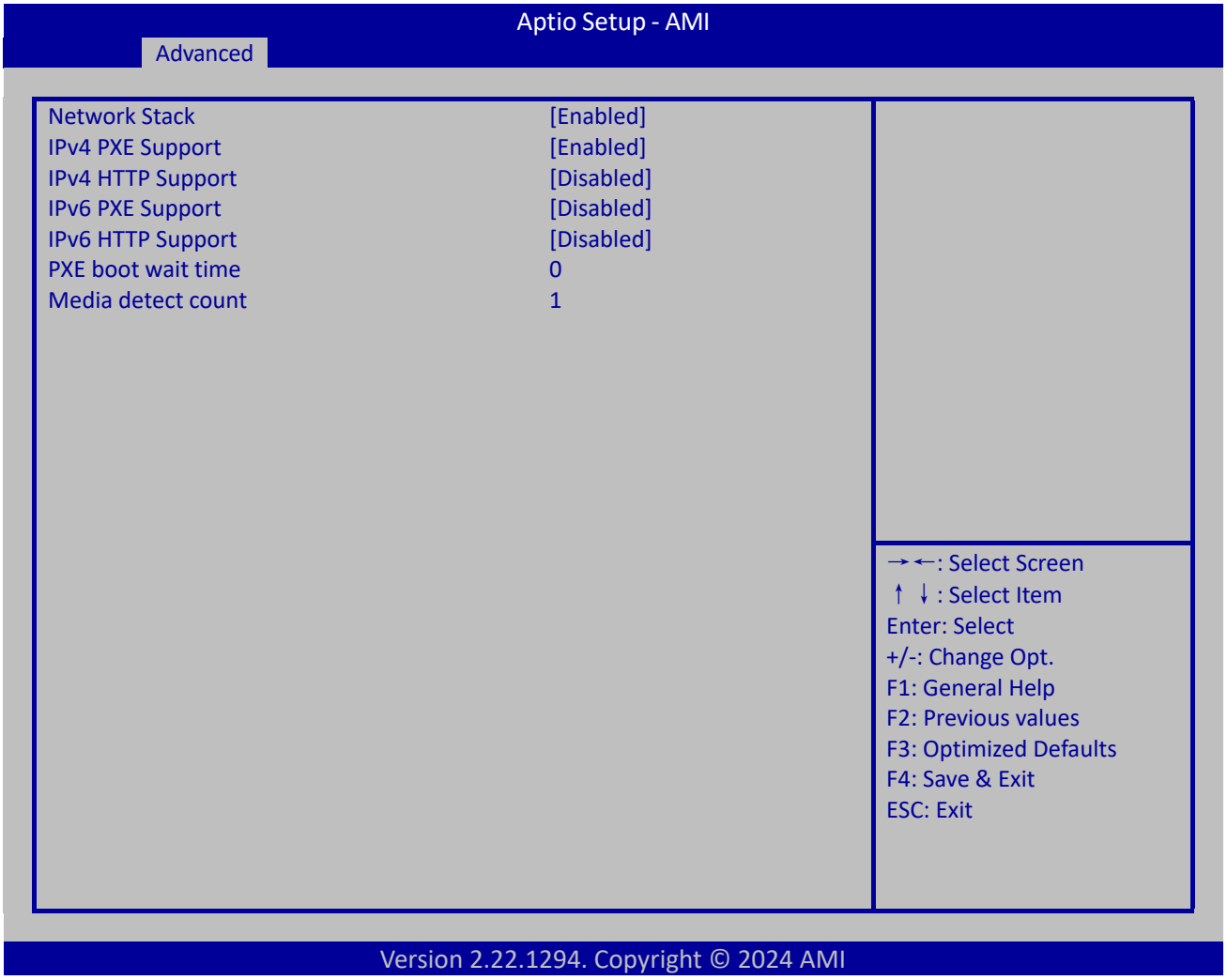
6.2.7 USB Configuration



Advanced \ USB Configuration		
Menu Fields	**Settings**	**Comments**
USB Module Version	xx	
USB Controllers:	x XHCI	
USB Devices:	xxxxxxx	
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.
USB hardware delays and time-outs:		
USB transfer time-out	[1 sec] [5 sec] [10 sec]	The time-out value for Control, Bulk, and Interrupt transfers.

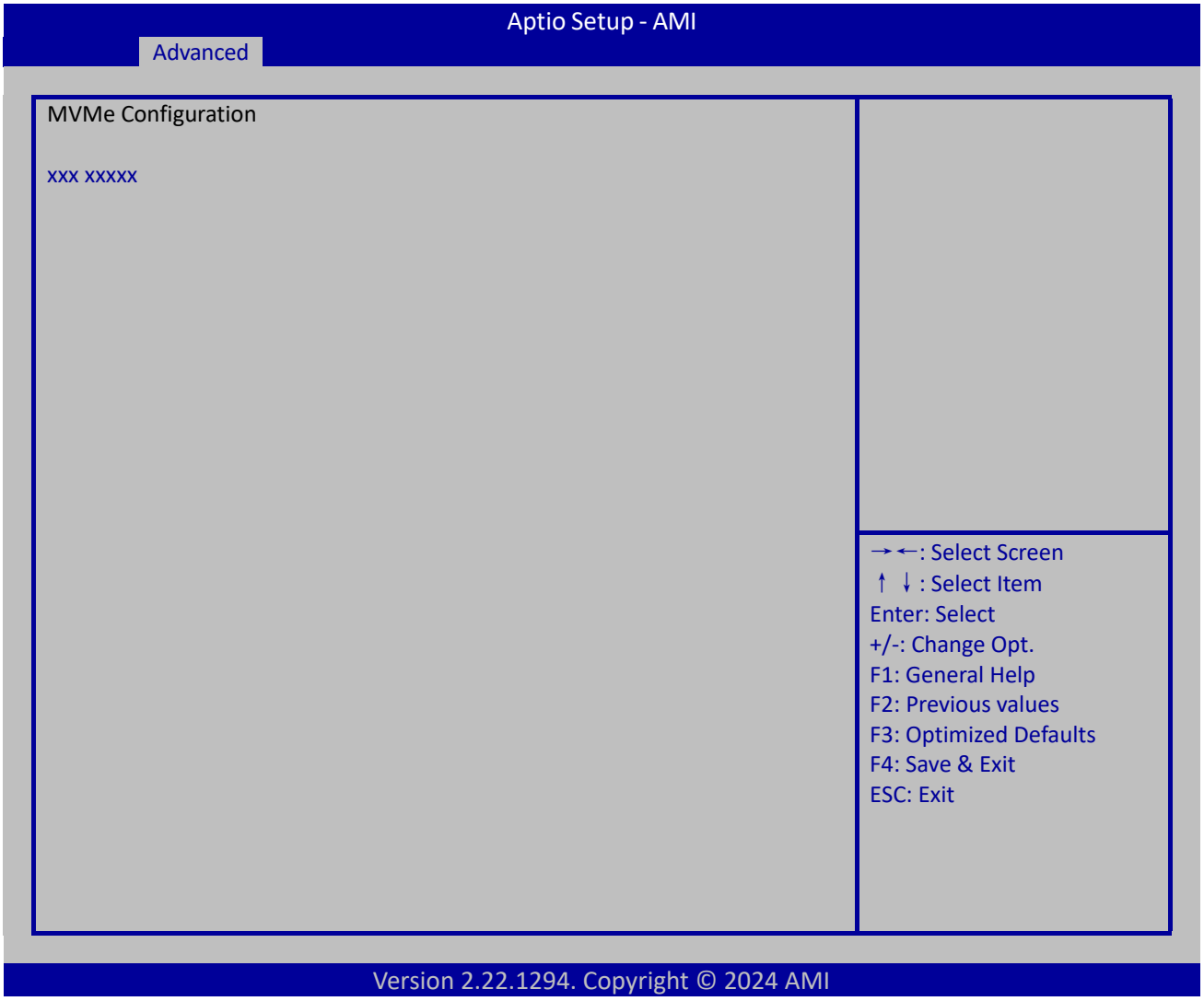
Advanced \ USB Configuration		
Menu Fields	**Settings**	**Comments**
	[20 sec]	
Device reset time-out	[10 sec] **[20 sec]** [30 sec] [40 sec]	USB mass storage device Start Unit command time-out.
Device power-up delay	**[Auto]** [Manual]	Maximum time the device will take before it properly reports itself 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.
Device power-up delay in seconds	**5**	Delay range is 1..40 seconds, in one second increments
Mass Storage Devices:		
xxxxx	**[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.

6.2.8 Network Stack Configuration



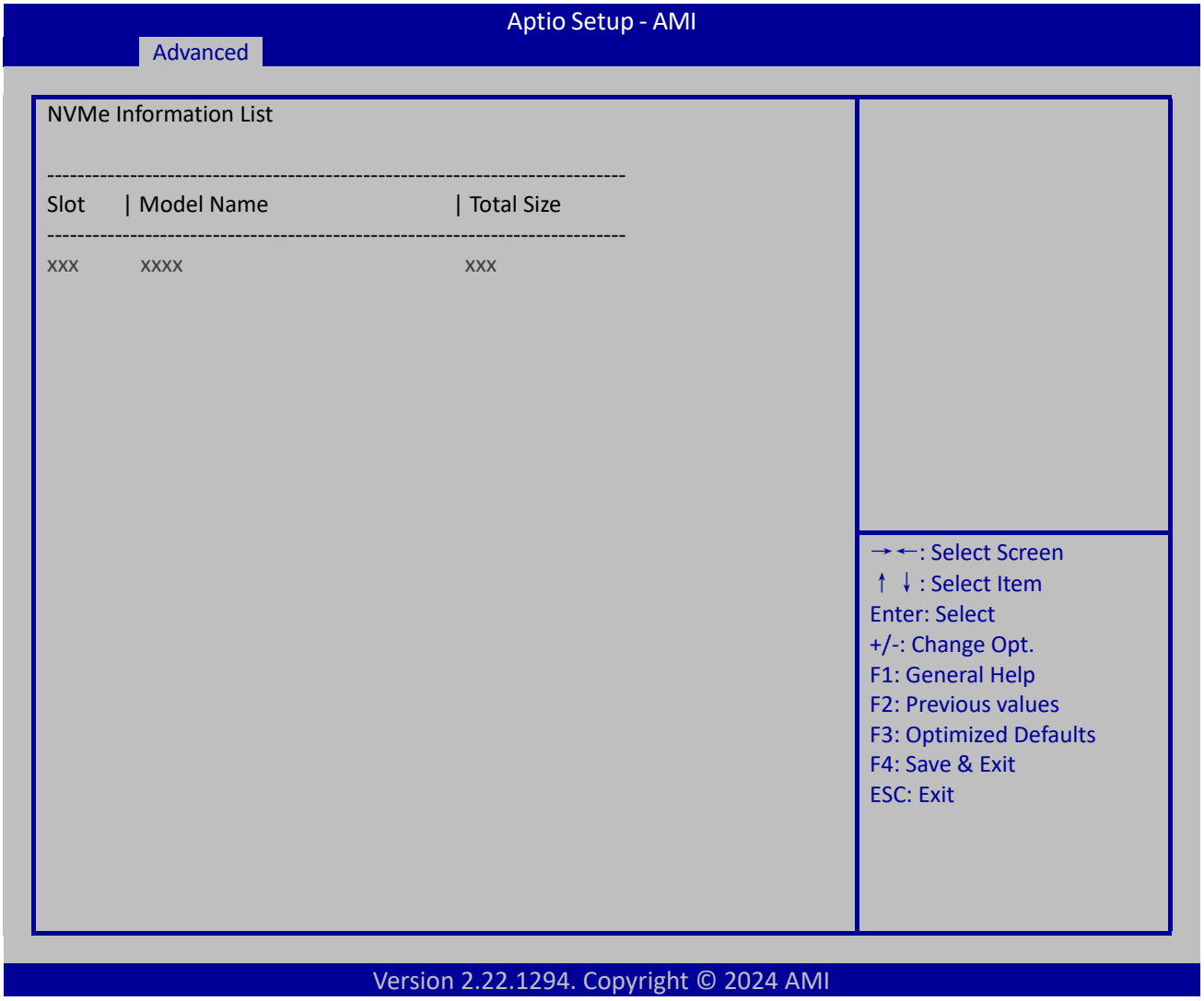
Advanced \ Network Stack Configuration		
Menu Fields	**Settings**	**Comments**
Network Stack	[Disabled] **[Enabled]**	Enable/Disable UEFI Network Stack
IPv4 PXE Support	[Disabled] **[Enabled]**	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	**[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	**0**	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	**1**	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

6.2.9 NVMe Configuration



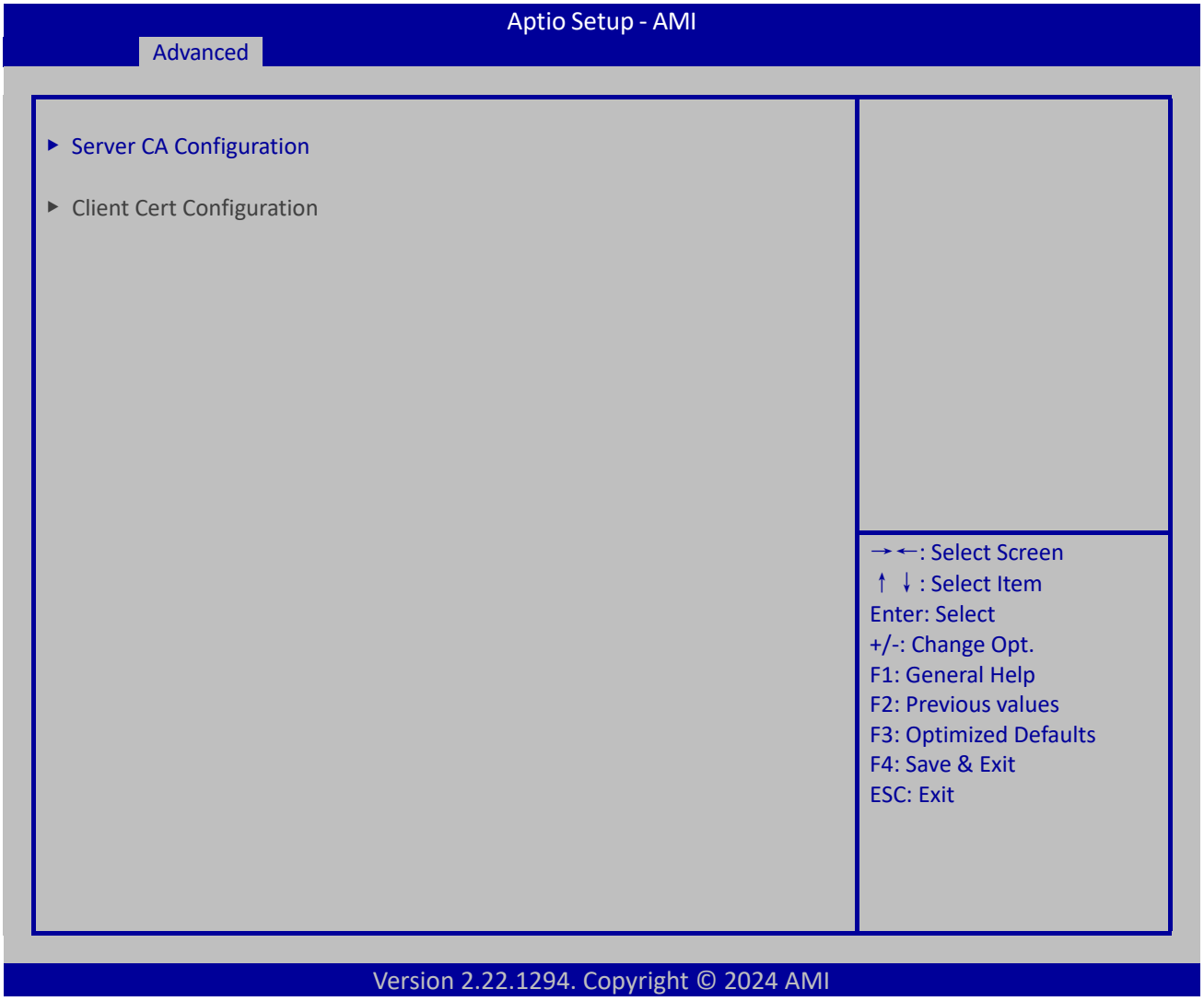
Advanced \ NVMe Configuration		
Menu Fields	**Settings**	**Comments**
xxxxx	Selects sub-menu.	Displays the NVMe Device Name and enter NVMe information page and control settings.

6.2.10 NVMe Information List



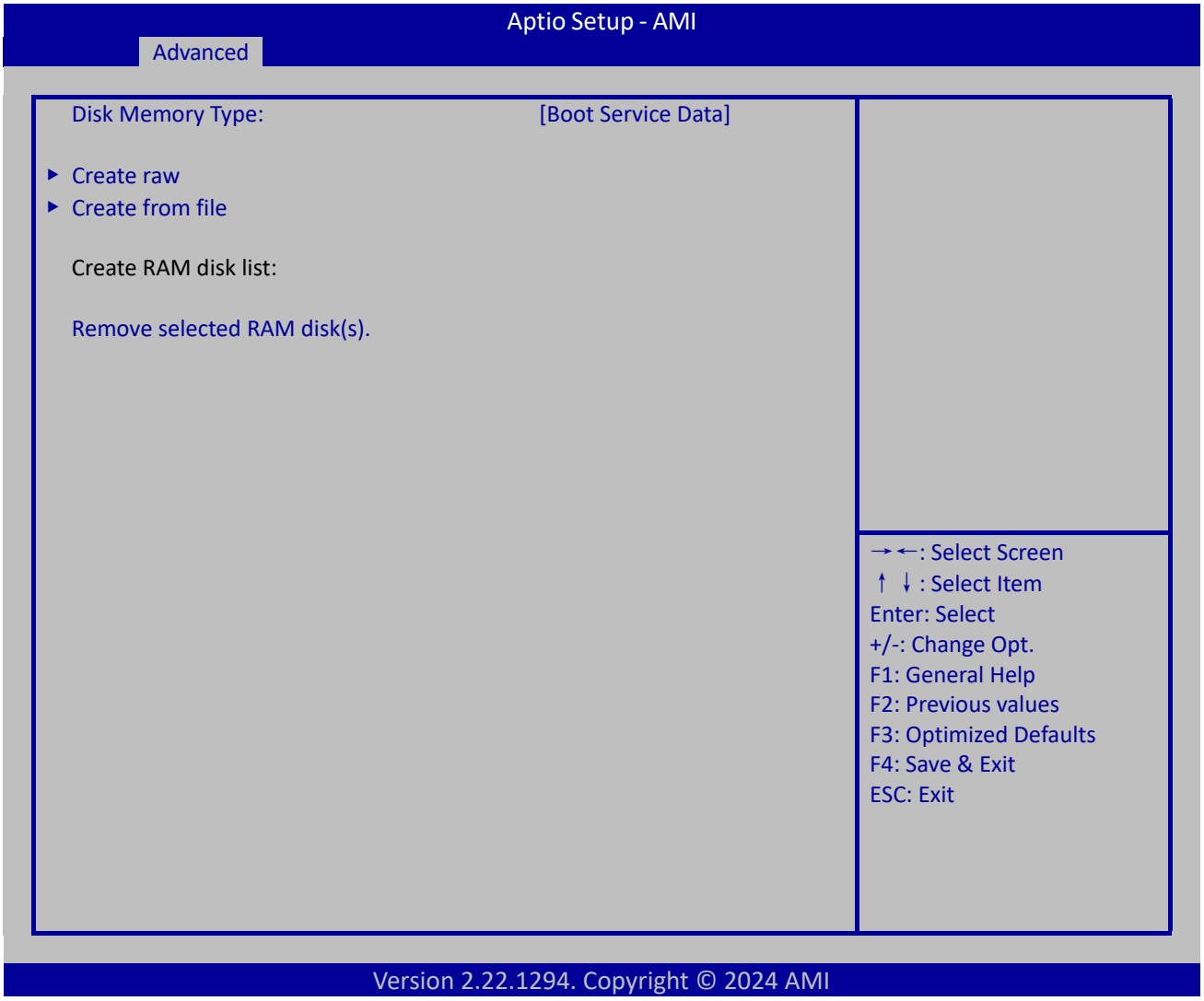
Advanced \ NVMe Information List		
Menu Fields	**Settings**	**Comments**
xxx xxxx xxx		List all NVMe information.

6.2.11 Tls Auth Configuration



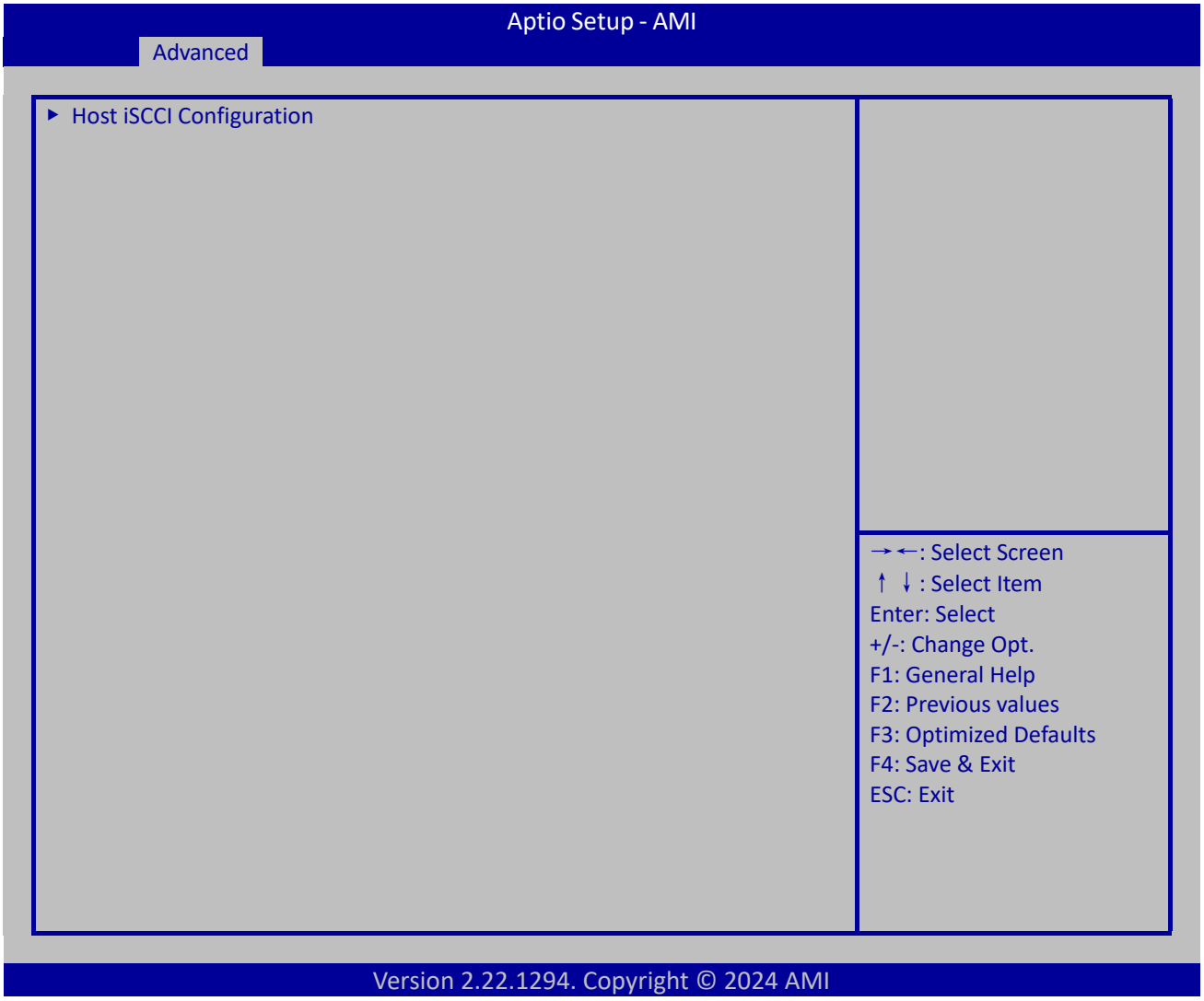
Advanced \ Tls Auth Configuration		
Menu Fields	**Settings**	**Comments**
Server CA Configuration	Selects sub-menu.	Press <Enter> to configure Server CA.
Client Cert Configuration		Client cert configuration is unsupported currently.

6.2.12 RAM Disk Configuration



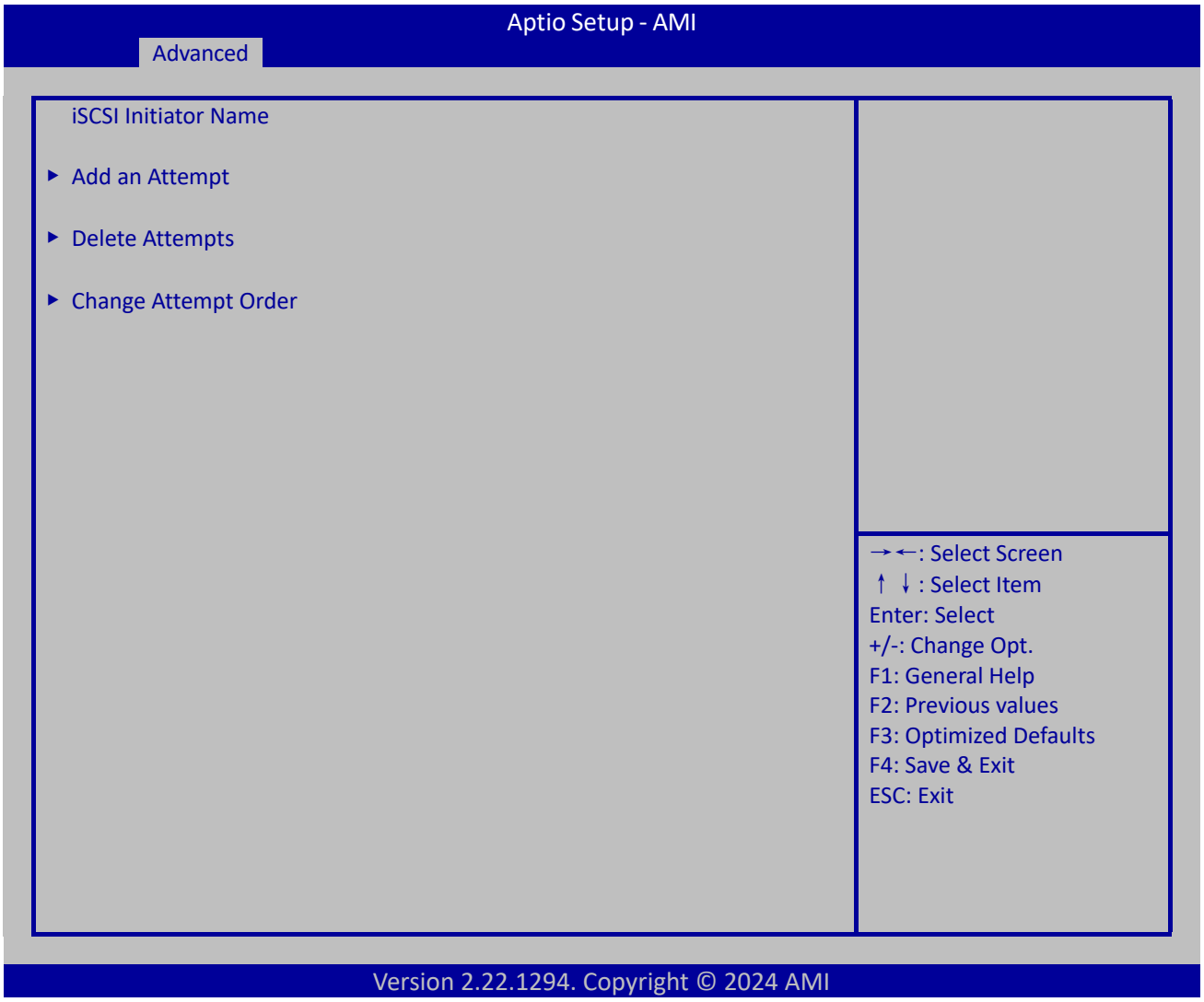
Advanced \ RAM Disk Configuration		
Menu Fields	**Settings**	**Comments**
Disk Memory Type:	**[Boot Service Data]** [Reserved]	Specifies type of memory to use from available memory pool in system to create a disk.
Create raw	Selects sub-menu.	Create a raw RAM disk.
Create from file	Selects sub-menu.	Create a RAM disk from a given file.
Remove selected RAM disk(s).		Remove selected RAM disk(s)

6.2.13 iSCSI Configuration



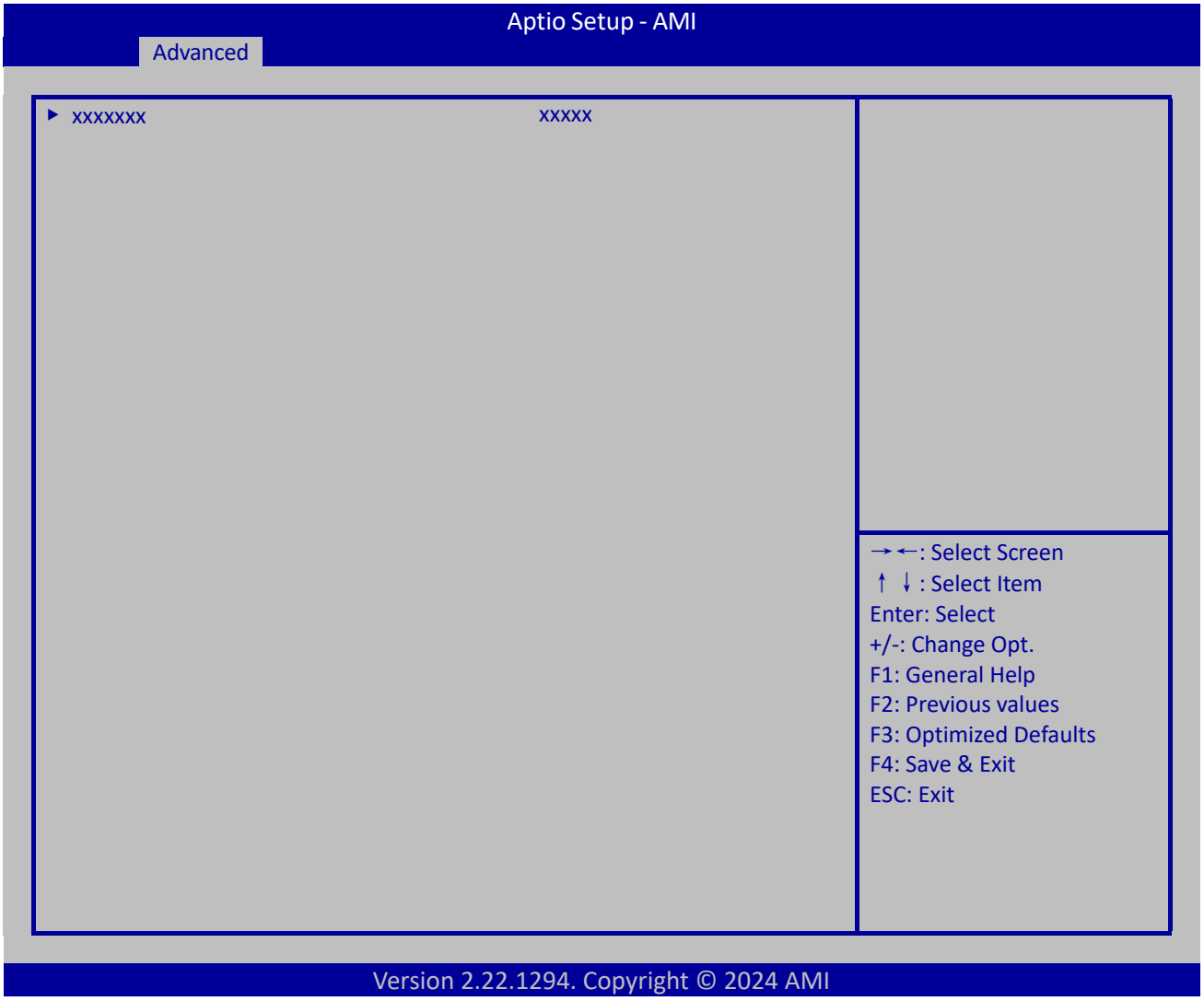
Advanced \ iSCSI Configuration		
Menu Fields	**Settings**	**Comments**
Host iSCCI Configuration	Selects sub-menu.	

6.2.13.1 Host iSCSI Configuration



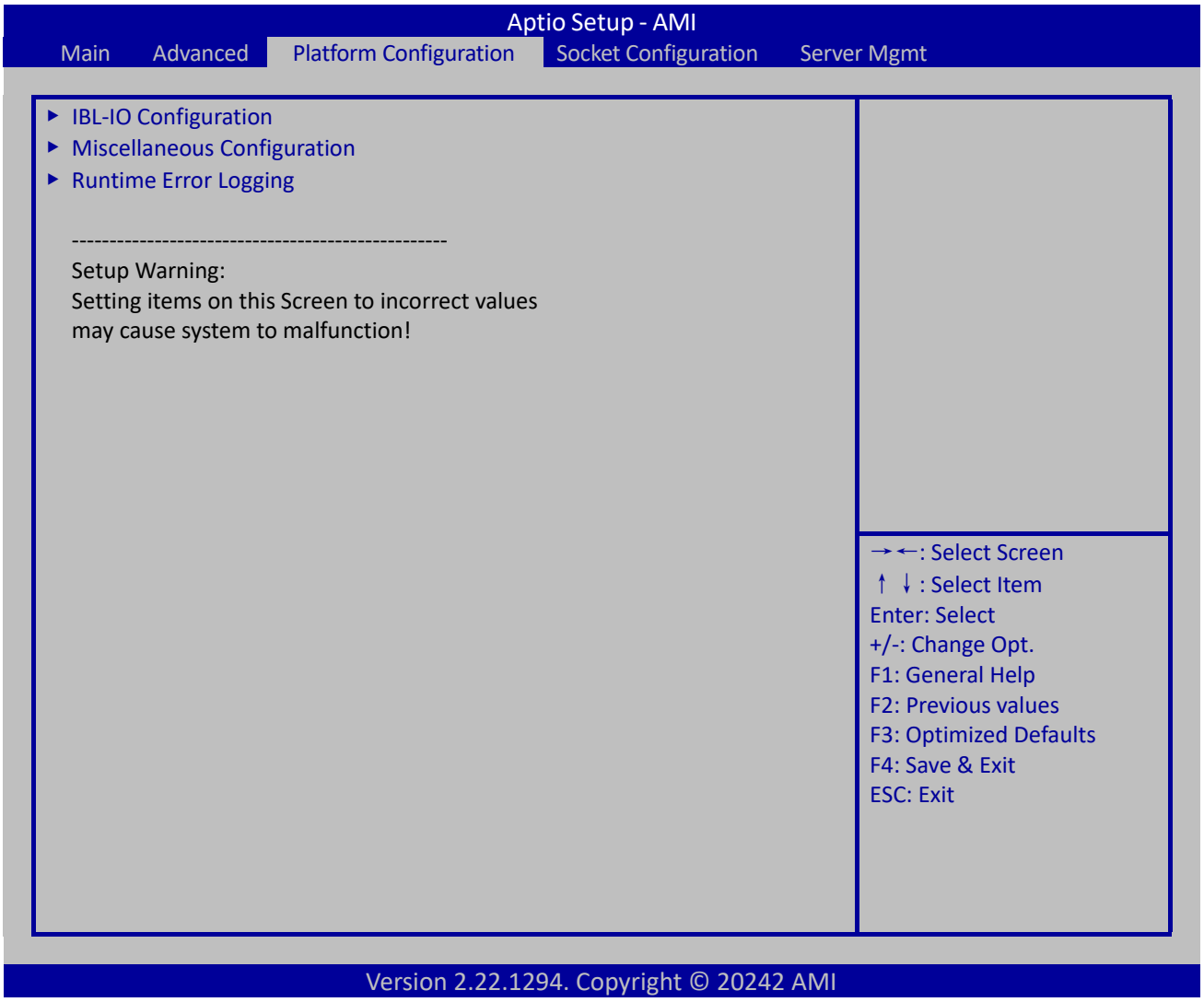
Advanced \ iSCSI Configuration \ Host iSCCI Configuration		
Menu Fields	**Settings**	**Comments**
iSCSI Initiator Name		The worldwide unique name of iSCSI Initiator. Only IQN format is accepted.Range is from 4 to 223
Add an Attempt	Selects sub-menu.	Add an Attempt
Delete Attempts		Delete one or more attempts
Change Attempt Order		Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the attempt order list.

6.2.14 Driver Health



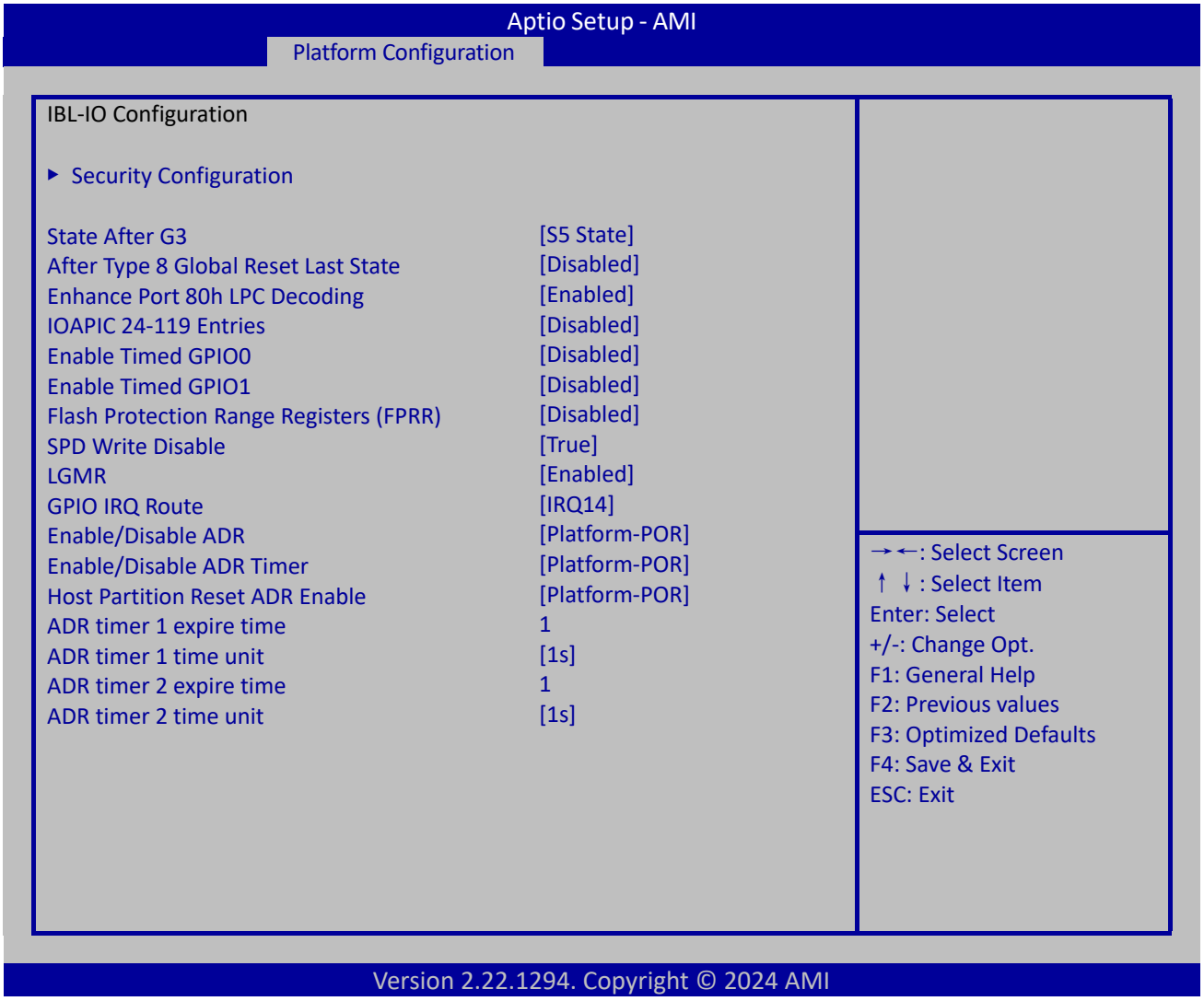
Advanced \ Driver Health			
Menu Fields		**Settings**	**Comments**
xxxxxxx	xxxxx	Selects sub-menu.	Provides Health Status for the Drivers/Controllers

6.3 PLATFORM CONFIGURATION



Platform Configuration		
Menu Fields	**Settings**	**Comments**
IBL-IO Configuration	Selects sub-menu.	
Miscellaneous Configuration	Selects sub-menu.	
Runtime Error Logging	Selects sub-menu.	

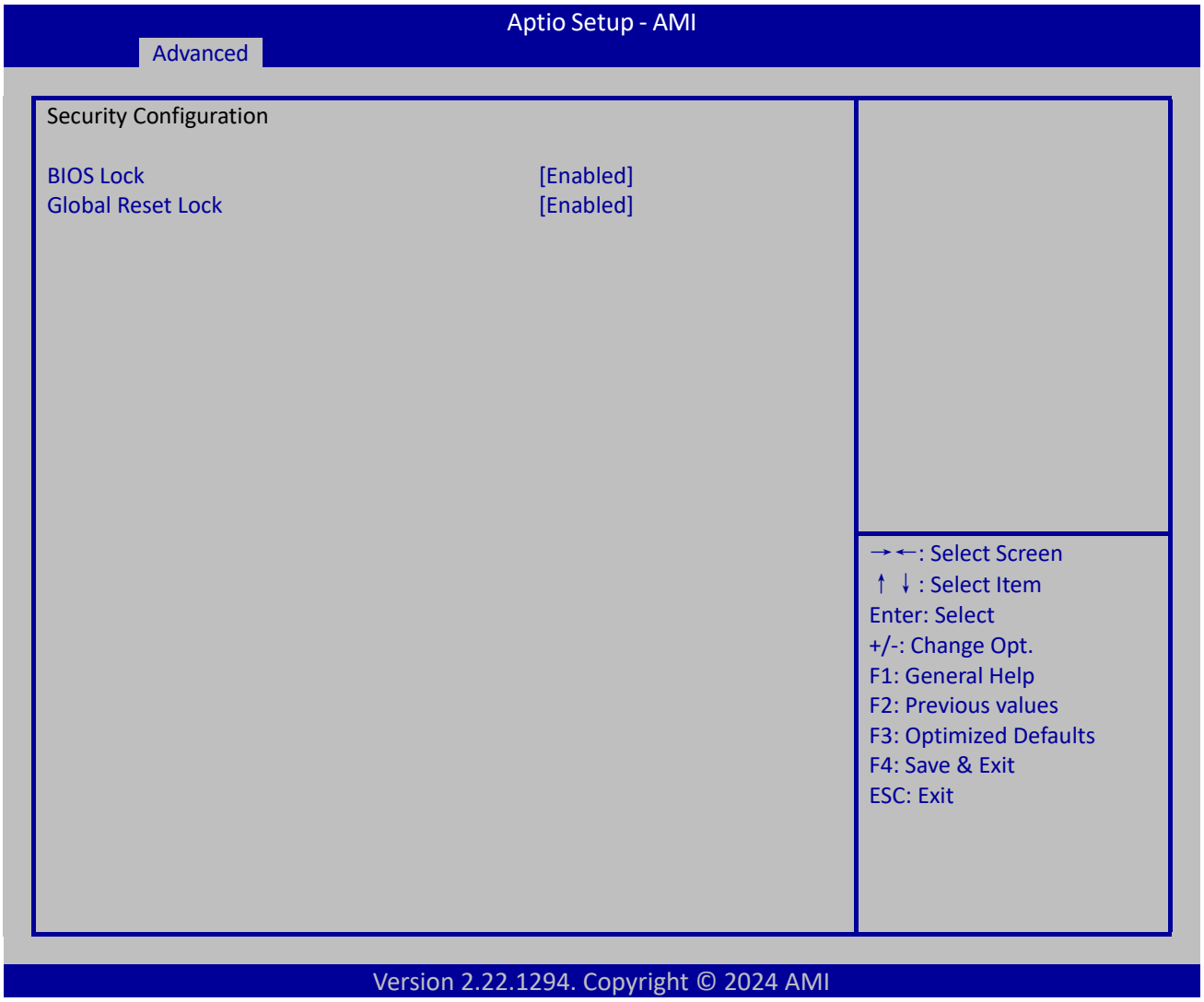
6.3.1 IBL-IO Configuration



Platform Configuration \ IBL-IO Configuration		
Menu Fields	**Settings**	**Comments**
Security Configuration	Selects sub-menu.	
State After G3	[S0 State] **[S5 State]** [Last State]	Specify what state to go to when power is re-applied after a power failure (G3 state).
After Type 8 Global Reset Last State	**[Disabled]** [Enabled]	Specify whether platform's previous state will be considered when determining whether to power-up after non-thermal and non-explicitly requested type 8 global resets.
Enhance Port 80h LPC Decoding	[Disabled] **[Enabled]**	Support the word/dword decoding of port 80h behind LPC
IOAPIC 24-119 Entries	**[Disabled]** [Enabled]	Enables/Disables IOAPIC 24-119 Entries. IRQ24-119 may be used by IBL devices. Disabling those interrupts may cause certain devices failure.
Enable Timed GPIO0	**[Disabled]** [Enabled]	Enable/Disable Timed GPIO0. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.

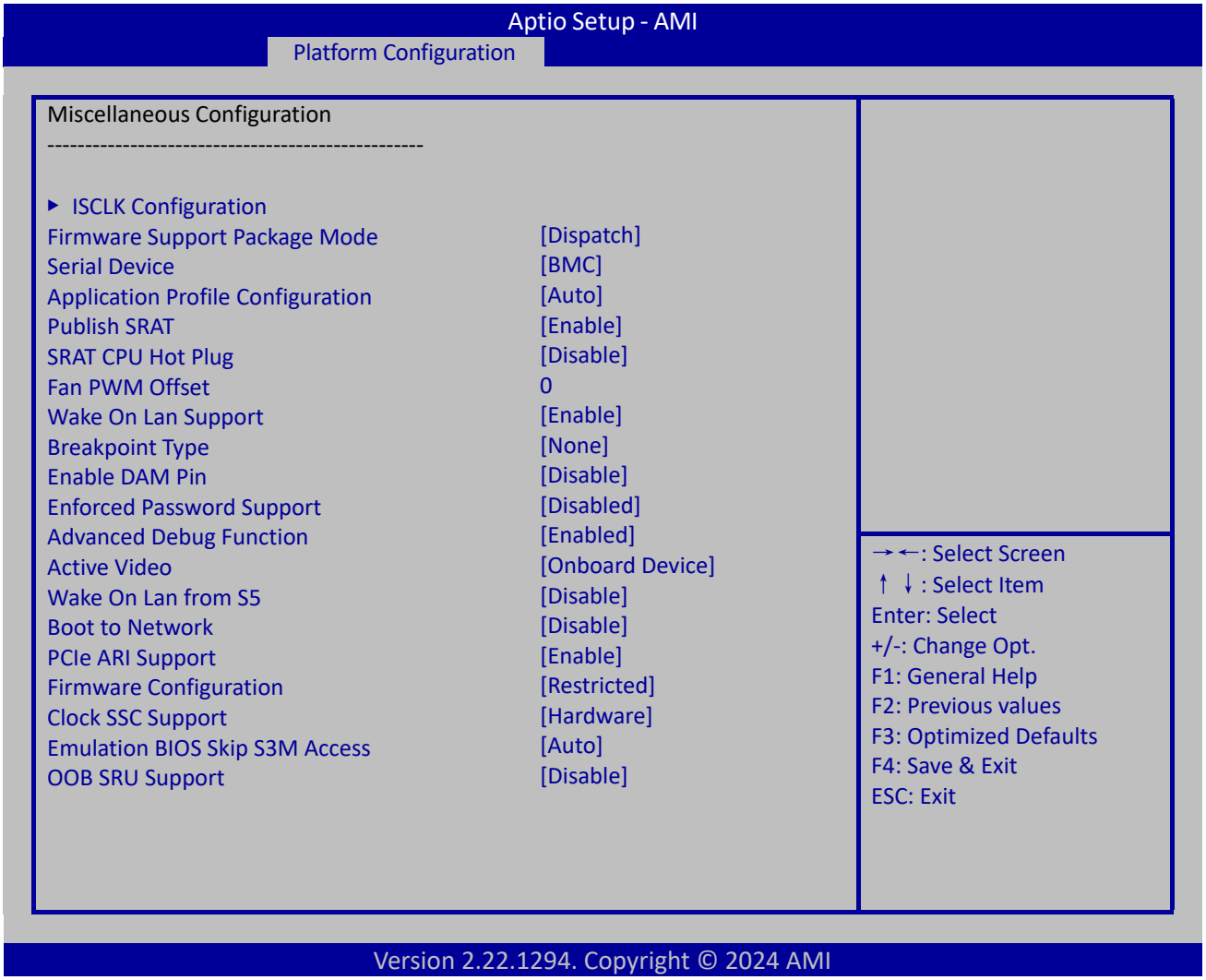
Platform Configuration \ IBL-IO Configuration		
Menu Fields	**Settings**	**Comments**
Enable Timed GPIO1	**[Disabled]** [Enabled]	Enable/Disable Timed GPIO1. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.
Flash Protection Range Registers (FPRR)	**[Disabled]** [Enabled]	Enable Flash Protection Range Registers
SPD Write Disable	**[True]** [False]	Enable/Disable setting SPD Write Disable
LGMR	**[Enabled]** [Disabled]	64KB memory block for LGMR (LPC Generic Memory Range) Decode
GPIO IRQ Route	**[IRQ14]** [IRQ15]	Route all GPIOs to one of the IRQ.
Enable/Disable ADR	**[Platform-POR]** [Enabled] [Disabled]	Enable or disable Automatic DIMM Refresh (ADR)
Enable/Disable ADR Timer	**[Platform-POR]** [Enabled] [Disabled]	Enable or disable ADR Timer.
Host Partition Reset ADR Enable	**[Platform-POR]** [Enabled] [Disabled]	Enables/Disables ADR on Host Partition Reset
ADR timer 1 expire time	**1**	Type desired ADR timer expire time, valid values - <1, 255>. Entered time is scaled by ADR timer time unit.
ADR timer 1 time unit	[1us] [10us] [100us] [1ms] [10ms] [100ms] **[1s]** [10s]	Select ADR timer time unit.
ADR timer 2 expire time	**1**	Type desired ADR timer expire time, valid values - <1, 255>. Entered time is scaled by ADR timer time unit.
ADR timer 2 time unit	[1us] [10us] [100us] [1ms] [10ms] [100ms] **[1s]** [10s]	Select ADR timer time unit.

6.3.1.1 Security Configuration



Platform Configuration \ IBL-IO Configuration \ Security Configuration		
Menu Fields	**Settings**	**Comments**
BIOS Lock	[Disabled] **[Enabled]**	Enable/Disable the IBL BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
Global Reset Lock	[Disabled] **[Enabled]**	Enable/Disable locking global host reset

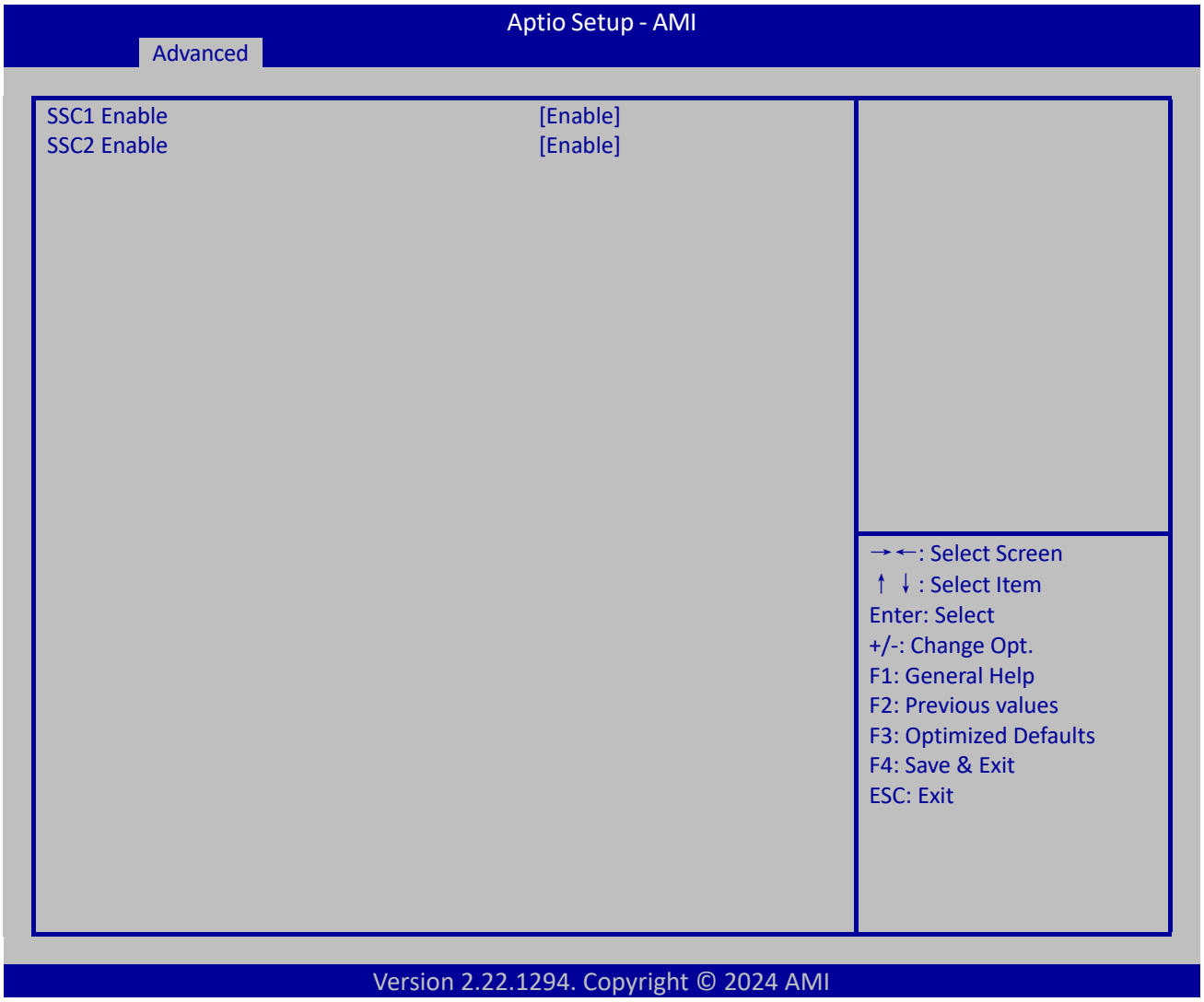
6.3.2 Miscellaneous Configuration



Platform Configuration \ Miscellaneous Configuration		
Menu Fields	**Settings**	**Comments**
ISCLK Configuration	Selects sub-menu.	
Firmware Support Package Mode	**[Dispatch]** [ARI]	Dispatch = Platform Boot with FSP Dispatch Mode, API = Platform Boot with FSP API Mode. After successfully switching this knob and resetting, the next boot up should be pure and the variables created in previous boot up will be deleted.
Serial Device	**[BMC]** [S3M]	Sets the Serial Device used to output bios serial log
Application Profile Configuration	**[Auto]** [General Computing] [Memory BandWidth] [Matrix Calculation] [Energy Efficiency] [Server Side Java] [OLTP] [Virtualization]	Application Profile Configuration provides a quick method of BIOS knob tuning accordingly to application. It's based on benchmark tests and may be not suitable to all workloads. You can still override the options.
Publish SRAT	[Disable]	Publish the SRAT ACPI table to the OS.

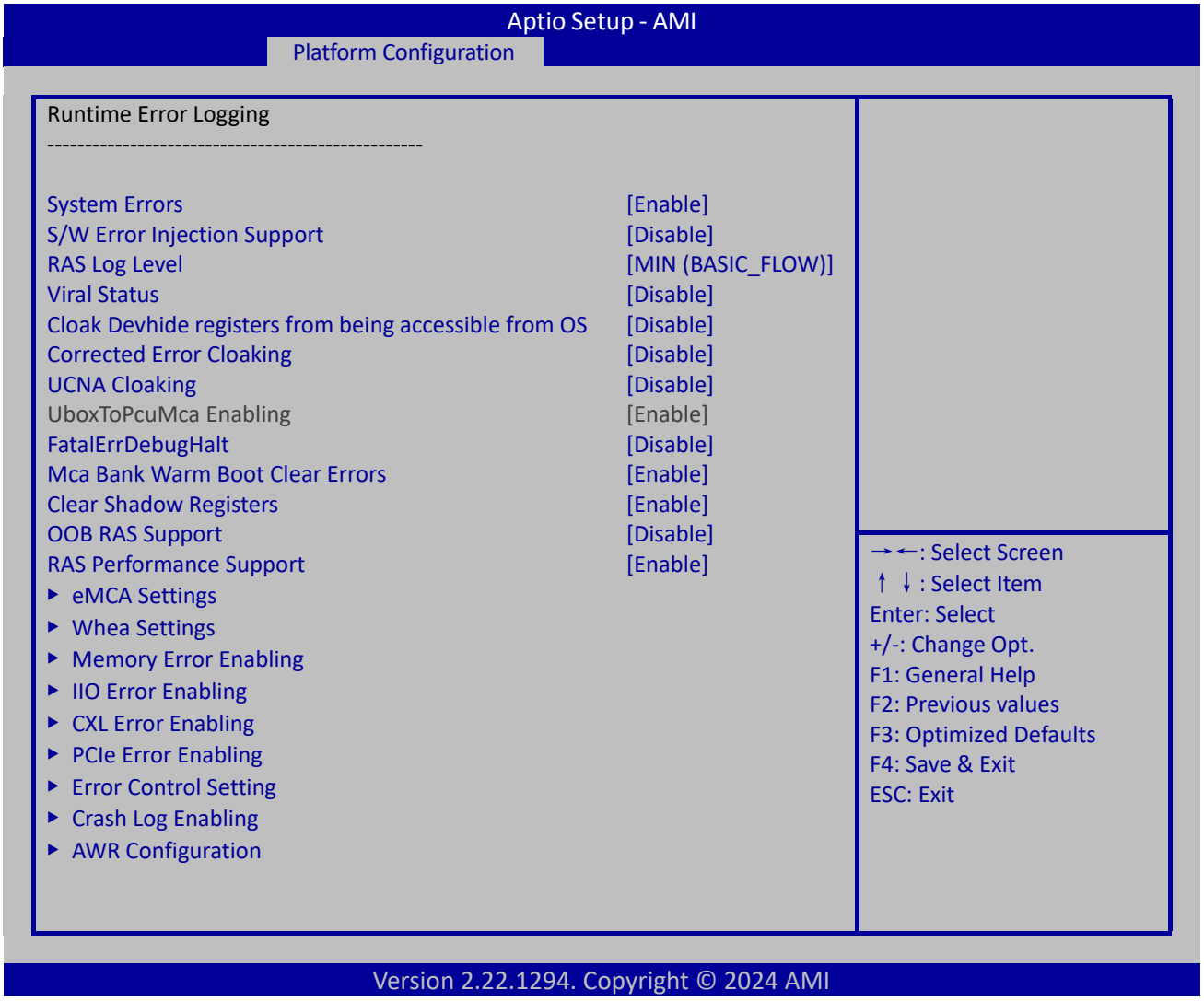
Platform Configuration \ Miscellaneous Configuration		
Menu Fields	**Settings**	**Comments**
	[Enable]	
SRAT CPU Hot Plug	**[Disable]** [Enable]	Set Processor Flag to Enabled for all processor entries in SRAT.
Fan PWM Offset	**0**	Valid Offset 0-100. This number is added to the calculated PWM value to increase Fan Speed
Wake On Lan Support	[Disable] **[Enable]**	Enable or Disable Wake On Lan Support
Breakpoint Type	**[None]** [After MRC] [After KTI RC] [After Resource Allocation] [After POST] [After Full Speed Setup] [Ready for IBIST]	Halt at specified points in BIOS
Enable DAM Pin	**[Disable]** [Enable]	Inform CPLD to control DAM hard strap pin by sending IPMI command to BMC.
Enforced Password Support	[Enabled] **[Disabled]**	Enables or Disables the Enforced Password support. Enabling it will allow the BIOS to send the Seed, Algorithm and password information to BMC.
Advanced Debug Function	[Disabled] **[Enabled]**	Advanced Debug Function (Dfx Knob)
Active Video	[Auto] **[Onboard Device]** [PCIE Device]	Select active Video type
Wake On Lan from S5	**[Disable]** [Enable]	Enables or Disables Wake on Lan from S5
Boot to Network	**[Disable]** [Enable]	Enables or Disables Boot to Network.
PCIe ARI Support	[Disable] **[Enable]**	Enable the PCIe Alternative Routing-ID Interpretation (ARI) support.
Firmware Configuration	[Ignore Policy Update] [Production] [Test] [Internal]DCU **[Restricted]** [Restricted SV]	Firmware Configuration options.
Clock SSC Support	[SSC Off] [SSC = -0.3%] [SSC = -0.5%] **[Hardware]**	Enable or disable the Clock Spread Spectrum support
Emulation BIOS Skip S3M Access	[Disable] [Enable] **[Auto]**	Emulation BIOS use it to skip S3M access. Enable: S3M is skipped; Disable: S3M is not skipped.
OOB SRU Support	**[Disabled]** [Enabled]	Enable/Disable OOB SMM Runtime Update feature. Enable: Use OOB Smm Runtime Update; Disable: Use In-band Smm Runtime Update.

6.3.2.1 ISCLK Configuration



Platform Configuration \ Miscellaneous Configuration \ ISCLK Configuration		
Menu Fields	**Settings**	**Comments**
SSC1 Enable	[Disable] **[Enable]**	Enables SSC for SSC PLL1
SSC2 Enable	[Disable] **[Enable]**	Enables SSC for SSC PLL2

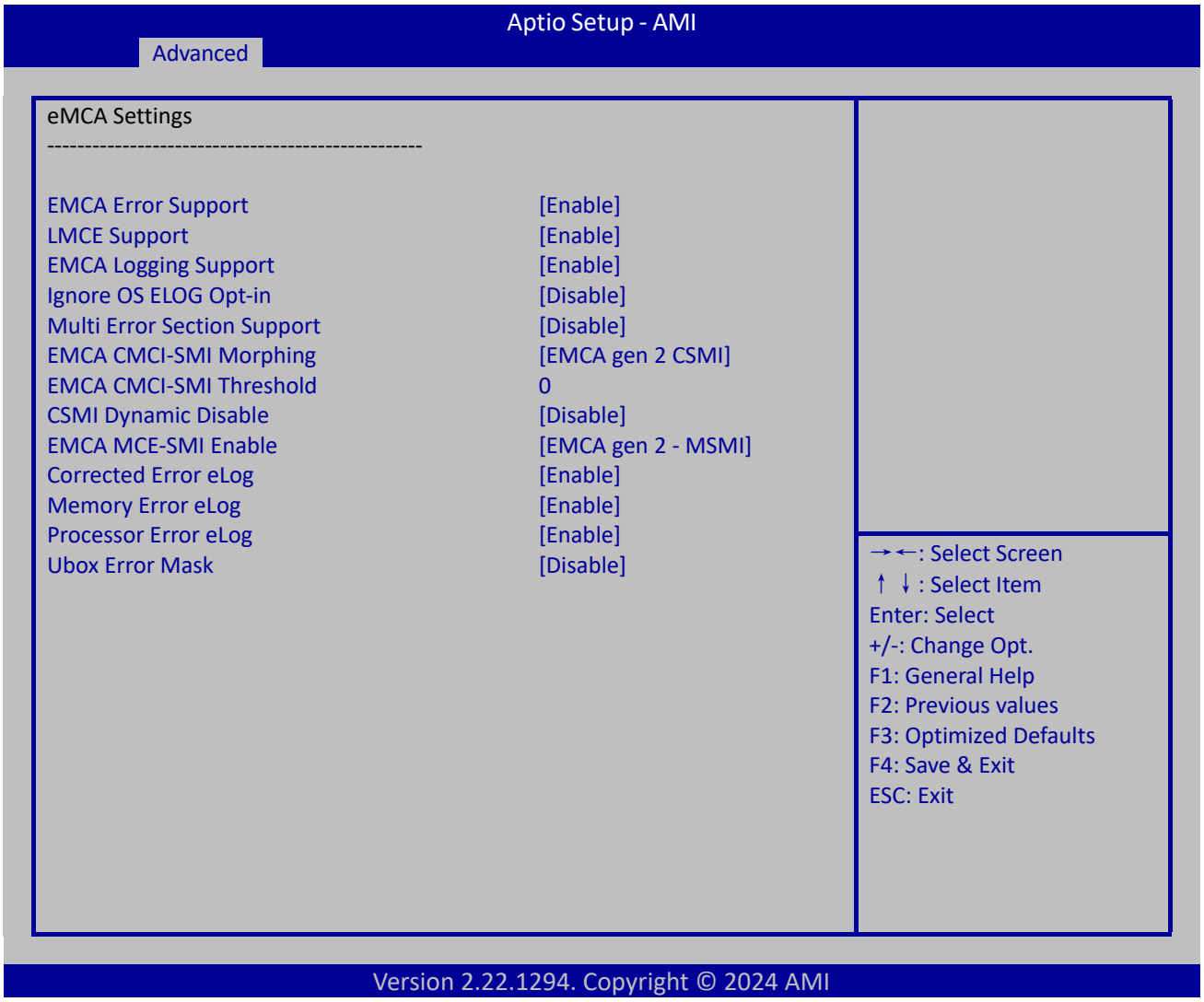
6.3.3 Runtime Error Logging



Platform Configuration \ Runtime Error Logging		
Menu Fields	**Settings**	**Comments**
System Errors	[Disable] **[Enable]**	System Error Enable/Disable setup options.
S/W Error Injection Support	**[Disable]** [Enable]	When Enabled S/W Error Injection is supported by unlocking MSR 0x790
RAS Log Level	[None] **[MIN (BASIC_FLOW)]** [MID (BASIC_FLOW, FUNC_FLOW)] [MAX (BASIC_FLOW, FUNC_FLOW, REG)]	RAS Log setup options.
Viral Status	**[Disable]** [Enable]	Enable/Disable Viral
Clear Viral Status	**[Disable]** [Enable]	Enable/Disable Clear Viral Status
Cloak Devhide registers from being accessible from OS	**[Disable]** [Enable]	Enable/Disable OS to access Devhide registers
Corrected Error Cloaking	**[Disable]** [Enable]	When enabled, Corrected errors are masked from OS/SW visibility.This option is valid only when EMCA is enabled

Platform Configuration \ Runtime Error Logging		
Menu Fields	**Settings**	**Comments**
UCNA Cloaking	**[Disable]** [Enable]	When enabled, UCNA errors are masked from OS/SW visibility.This option is valid only when EMCA is enabled
UboxToPcuMca Enabling	**[Enable]**	Enables or disables Ubox Local errors to cause MCA.
FatalErrDebugHalt	**[Disable]** [Enable]	DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjunction with ITP as thread will halt in Fatal error flow
Mca Bank Warm Boot Clear Errors	[Disable] **[Enable]**	Enable/Disable Mca Bank Warm Boot Clear Errors.
Clear Shadow Registers	[Disable] **[Enable]**	Enable/Disable clearing shadow registers.
OOB RAS Support	**[Disable]** [Enable]	Enable/Disable OOB RAS feature
RAS Performance Support	[Disable] **[Enable]**	Enable/Disable RAS Performance Support
eMCA Settings	Selects sub-menu.	
Whea Settings	Selects sub-menu.	
Memory Error Enabling	Selects sub-menu.	
IIO Error Enabling	Selects sub-menu.	
CXL Error Enabling	Selects sub-menu.	
PCIe Error Enabling	Selects sub-menu.	
Error Control Setting	Selects sub-menu.	
Crash Log Enabling	Selects sub-menu.	
AWR Configuration	Selects sub-menu.	

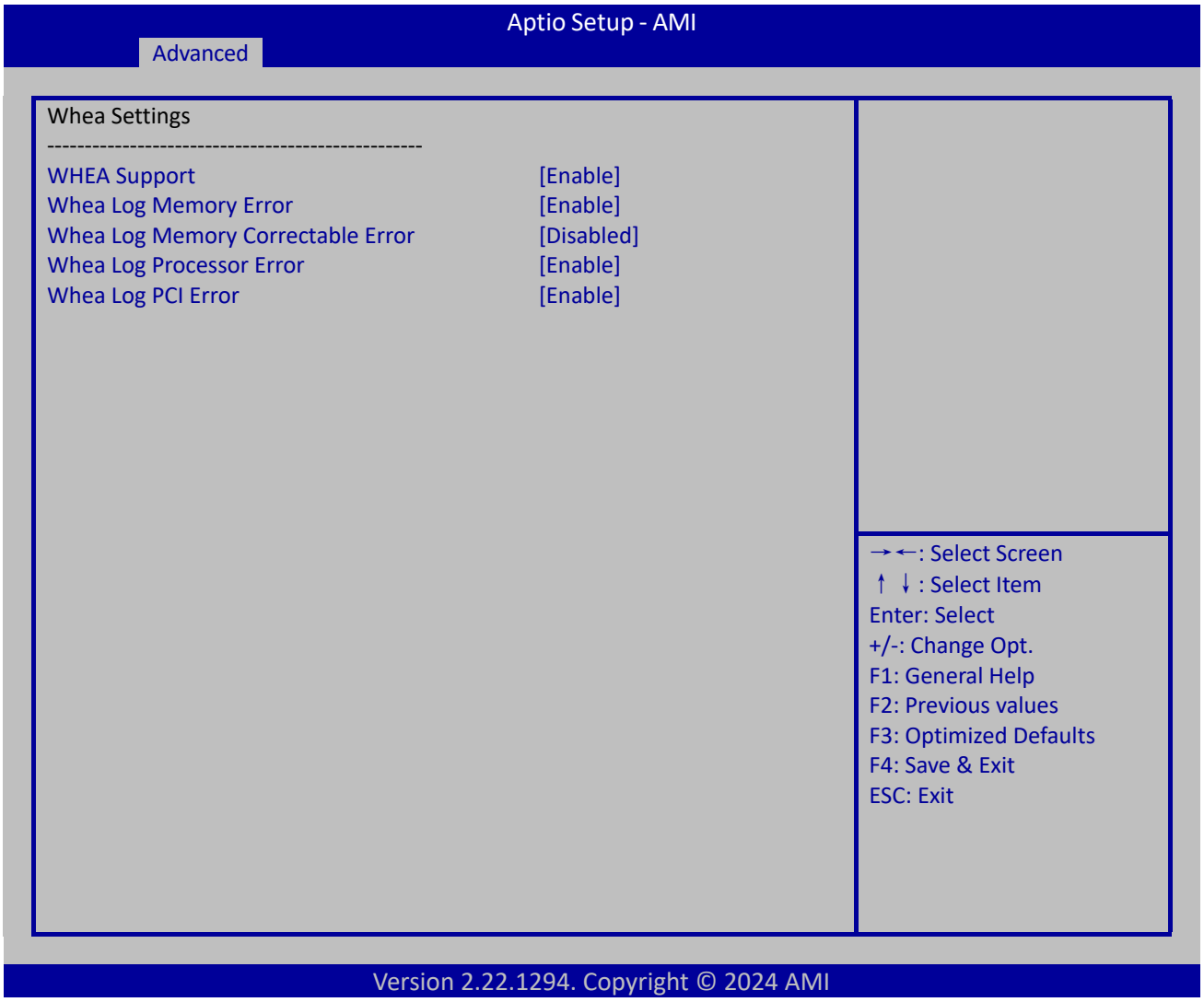
6.3.3.1 eMCA Settings



Platform Configuration \ Runtime Error Logging \ eMCA Settings		
Menu Fields	**Settings**	**Comments**
EMCA Error Support	[Disable] **[Enable]**	Enable/Disable EMCA Error support
LMCE Support	[Disable] **[Enable]**	Enable/Disable Local MCE firmware support
EMCA Logging Support	[Disable] **[Enable]**	Enable/Disable EMCA Logging
Ignore OS ELOG Opt-in	**[Disable]** [Enable]	Enable/Disable Ignore OS ELOG Opt-in and log
Multi Error Section Support	**[Disable]** [Enable]	Enable/Disable multi error section support
EMCA CMCI-SMI Morphing	[Disable] **[EMCA gen 2 CSMI]**	Enable/Disable EMCA CSMI
EMCA CMCI-SMI Threshold	**0**	Set the threshold of correctable error for signaling CMCI-CSMI
CSMI Dynamic Disable	**[Disable]** [Enable]	[Enable] - BIOS disables CSMI when error threshold reached.

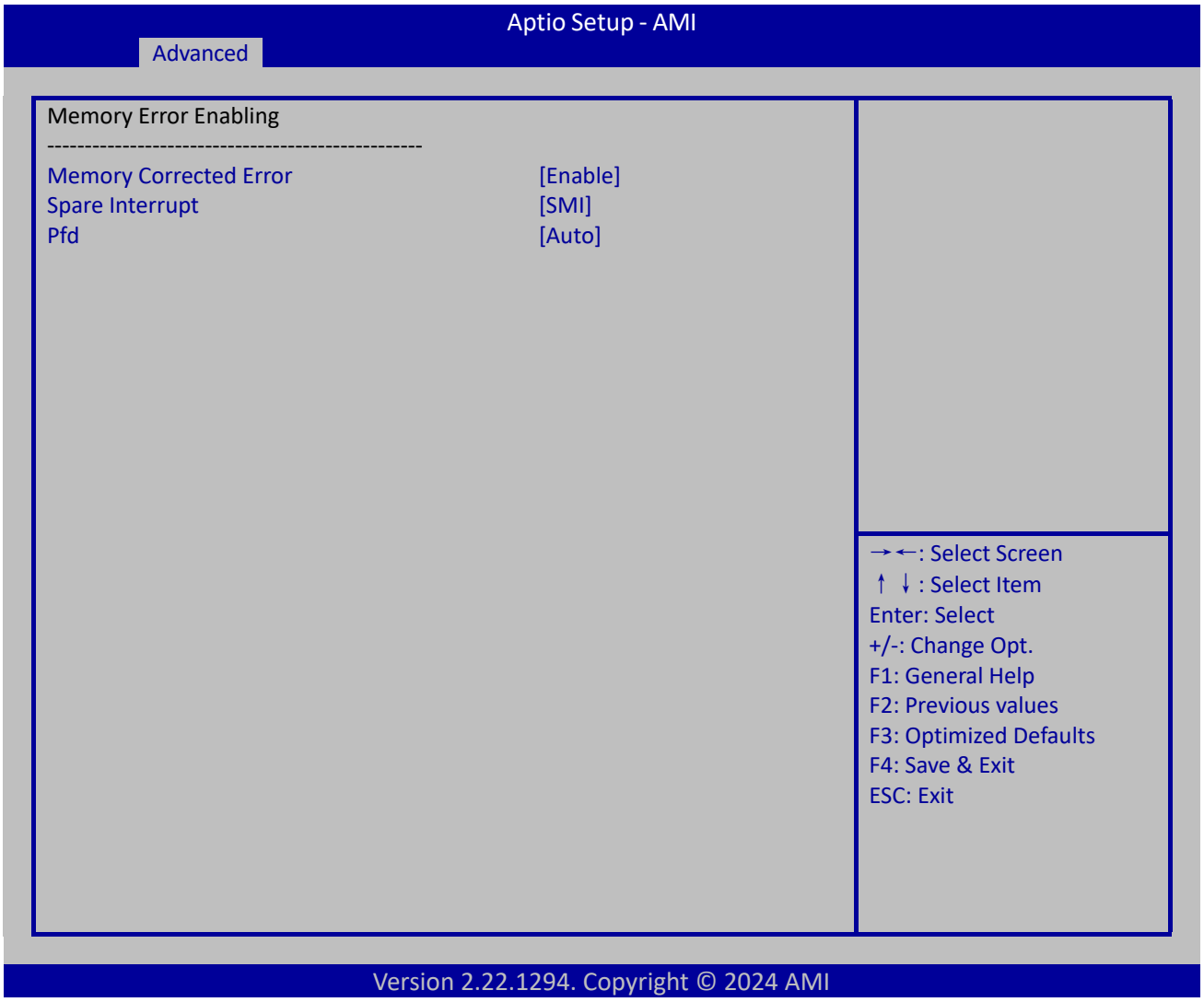
Platform Configuration \ Runtime Error Logging \ eMCA Settings		
Menu Fields	**Settings**	**Comments**
		[Disabled] - CSMI always on.
CSMI Dynamic Threshold	**14**	Set the threshold of CSMI Dynamic Disable. BIOS disables CSMI when error threshold reached.
EMCA MCE-SMI Enable	[Disable] **[EMCA gen 2 - MSMI]**	Enable/Disable EMCA Uncorrected SMI for gen2
Corrected Error eLog	[Disable] **[Enable]**	Enable/Disable Corrected Error eLog
Memory Error eLog	[Disable] **[Enable]**	Enable/Disable Memory Error eLog
Processor Error eLog	[Disable] **[Enable]**	Enable/Disable Processor Error eLog
Ubox Error Mask	**[Disable]** [Enable]	Mask SMI generation for Ubox Error.

6.3.3.2 Whea Settings



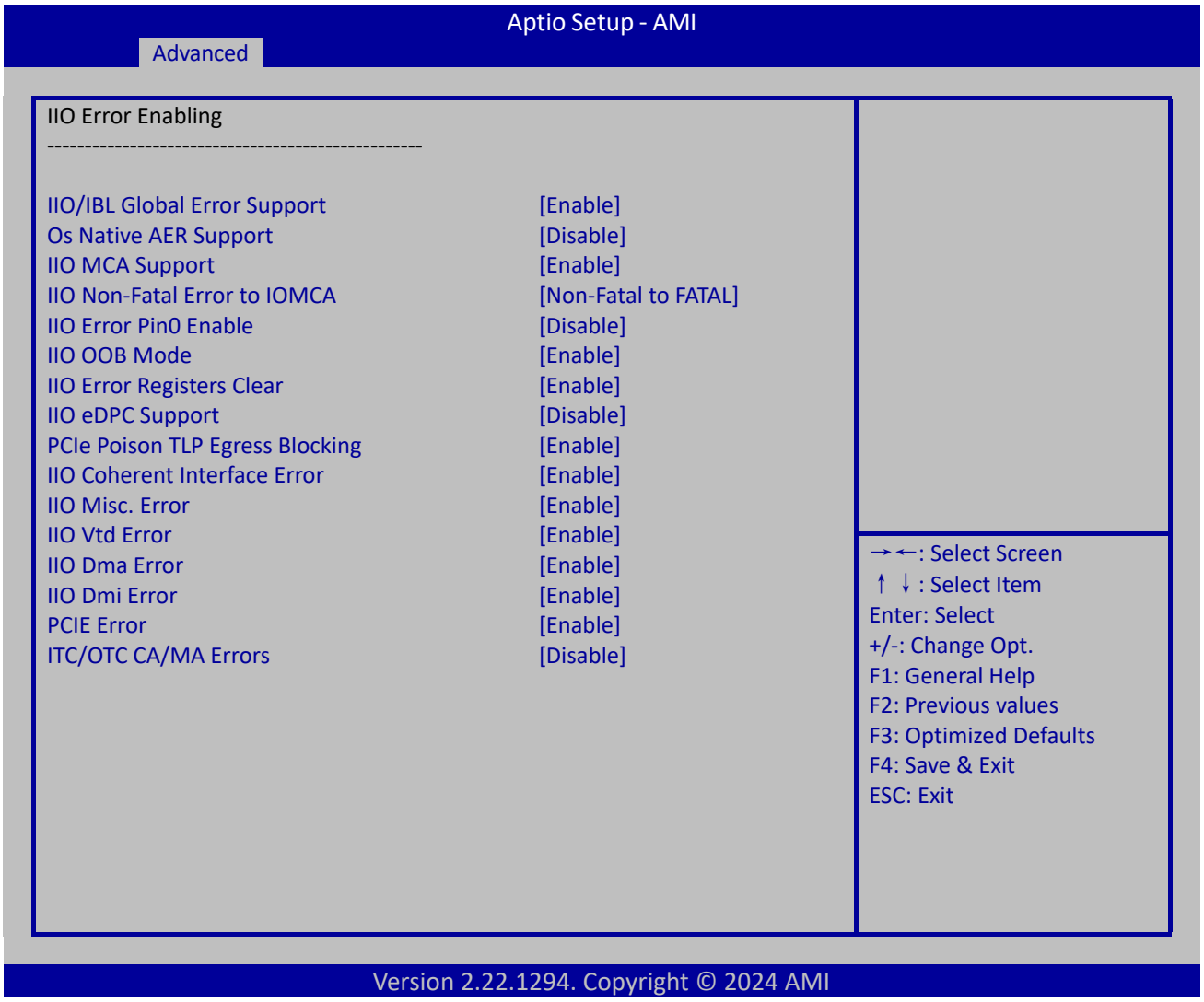
Platform Configuration \ Runtime Error Logging \ Whea Settings		
Menu Fields	**Settings**	**Comments**
WHEA Support	[Disable] **[Enable]**	Enable/Disable WHEA support
Whea Log Memory Error	[Disable] **[Enable]**	Enable/Disable Whea Log Memory Error
Whea Log Memory Correctable Error	**[Disabled]** [Disabled]	Enable/Disable Whea Log Memory Correctable Error
Whea Log Processor Error	[Disable] **[Enable]**	Enable/Disable Whea Log Processor Error
Whea Log PCI Error	[Disable] **[Enable]**	Enable/Disable Whea Log PCI Error

6.3.3.3 Memory Error Enabling



Platform Configuration \ Runtime Error Logging \ Memory Error Enabling		
Menu Fields	**Settings**	**Comments**
Memory Corrected Error	[Disable] **[Enable]**	Enable/Disable Memory Corrected Error
Spare Interrupt	[Disable] **[SMI]** [CMCI]	Spare Interrupt Selection. For Error Pin setting, please enable IIO Error Pin0 Enable.
Pfd	[Disable] [Enable] **[Auto]**	Pfd is to identify hard error out from errors. Auto indicates PFD is enabled dynamically based on system configuration.

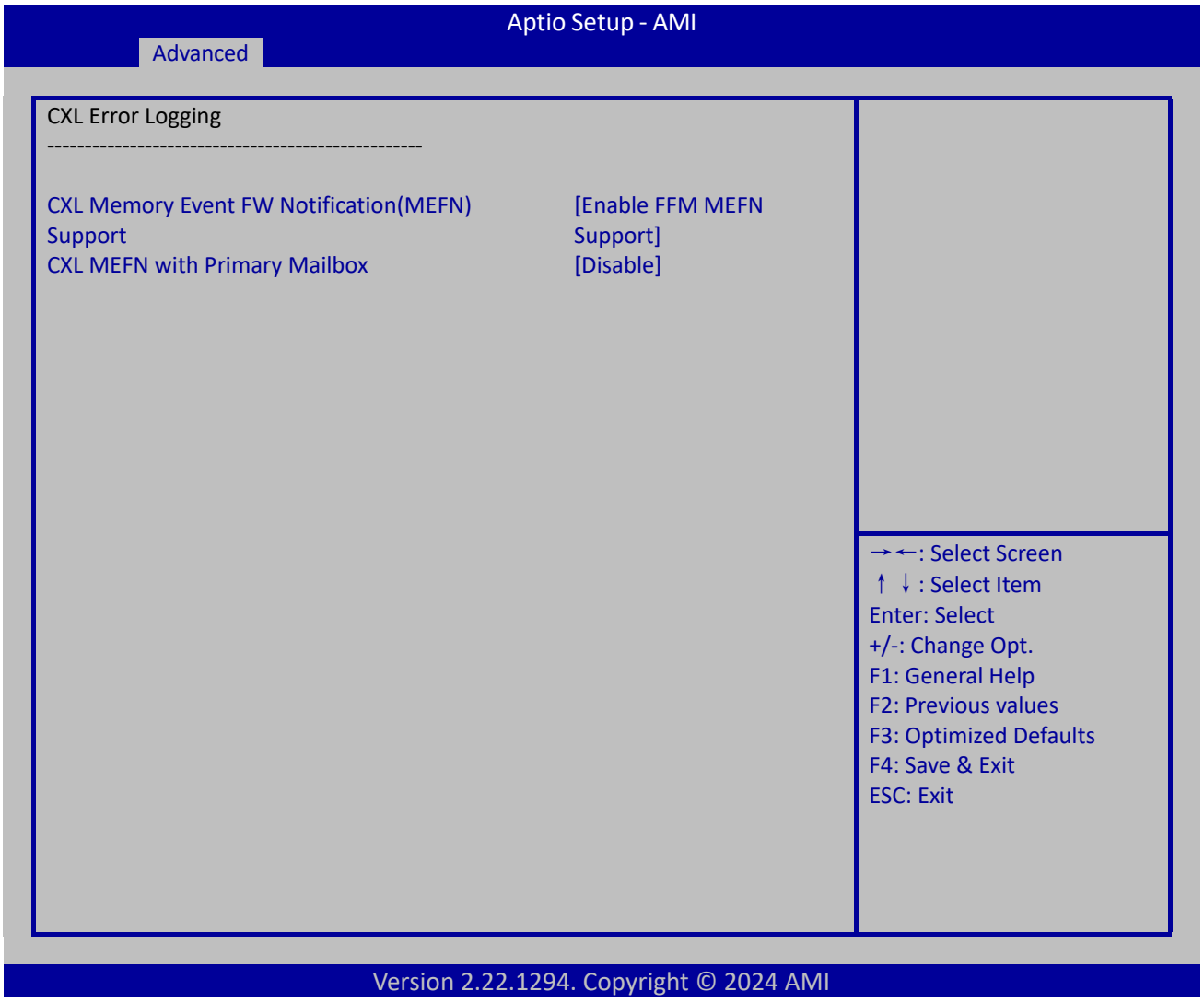
6.3.3.4 IIO Error Enabling



Platform Configuration \ Runtime Error Logging \ IIO Error Enabling		
Menu Fields	**Settings**	**Comments**
IIO/IBL Global Error Support	[Disable] **[Enable]**	Enable/Disable IIO/IBL Error Support.
Os Native AER Support	**[Disable]** [Enable]	Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability
IIO MCA Support	[Disable] **[Enable]**	Enable/Disable IIO MCA Support
IIO Non-Fatal Error to IOMCA	**[Non-Fatal to FATAL]** [Non-Fatal to SRAR] [Non-Fatal to UCNA] [Disable]	Enable/Disable IIO severity 1 error to MCA.
IIO Error Pin0 Enable	**[Disable]** [Enable]	Enable/Disable IIO Error Pin0
IIO OOB Mode	[Disable] **[Enable]**	Enable/Disable System Event Generation when Error Pin is enabled
IIO Error Registers Clear	[Disable]	Enable/Disable Clear IIO Error Registers

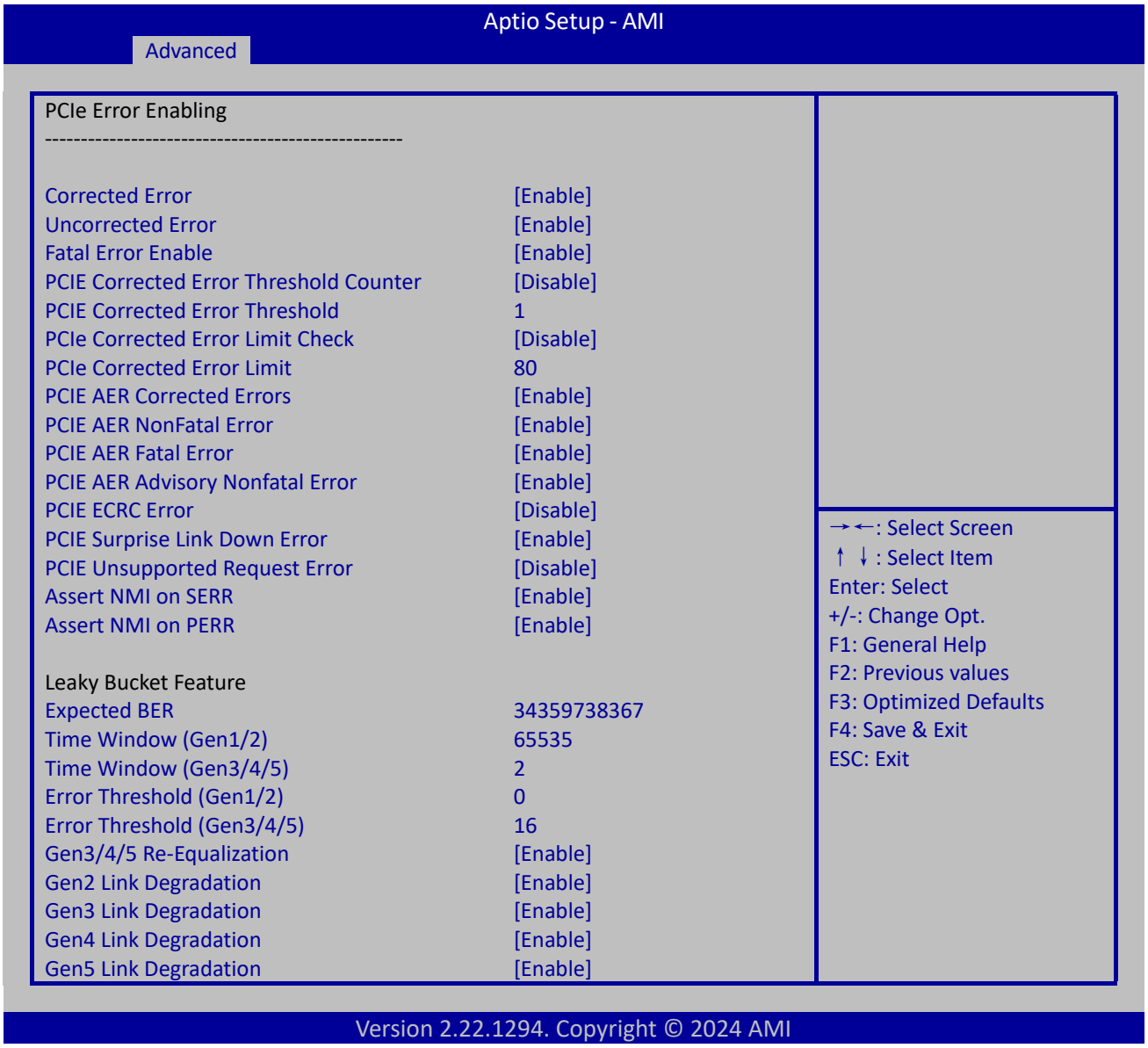
Platform Configuration \ Runtime Error Logging \ IIO Error Enabling		
Menu Fields	**Settings**	**Comments**
	[Enable]	
IIO eDPC Support	**[Disable]** [On Fatal Error] [On Fatal and Non-Fatal Errors]	Enable/Disable IIO eDPC Support
IIO eDPC Interrupt	**[Disable]** [Enable]	Enable/Disable IIO eDPC Interrupt
IIO eDPC ERR_COR Message	[Disable] **[Enable]**	Enable/Disable IIO eDPC ERR_COR Message
PCIe Poison TLP Egress Blocking	**[Enabled]** [Disabled]	Enable/Disable PCIe Poison TLP Egress Blocking
IIO Coherent Interface Error	[Disable] **[Enable]**	Enable/Disable IIO Coherent Interface Error
IIO Misc. Error	[Disable] **[Enable]**	Enable/Disable IIO Misc. Error
IIO Vtd Error	[Disable] **[Enable]**	Enable/Disable IIO Vtd Error
IIO Dma Error	[Disable] **[Enable]**	Enable/Disable IIO Dma Error
IIO Dmi Error	[Disable] **[Enable]**	Enable/Disable IIO Dmi Error
PCIE Error	[Disable] **[Enable]**	Enable/Disable PCIE Error
ITC/OTC CA/MA Errors	**[Disable]** [Enable]	Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC

6.3.3.5 CXL Error Enabling



Platform Configuration \ Runtime Error Logging \ CXL Error Enabling		
Menu Fields	**Settings**	**Comments**
CXL Memory Event FW Notification(MEFN) Support	[Disable MEFN Support] **[Enable FFM MEFN Support]** [Enable OSFM MEFN Support]	Enable/Disable CXL Memory Event FW Notification(MEFN) Support
CXL MEFN with Primary Mailbox	**[Disable]** [Enable]	Enable/Disable CXL MEFN with Primary Mailbox Only

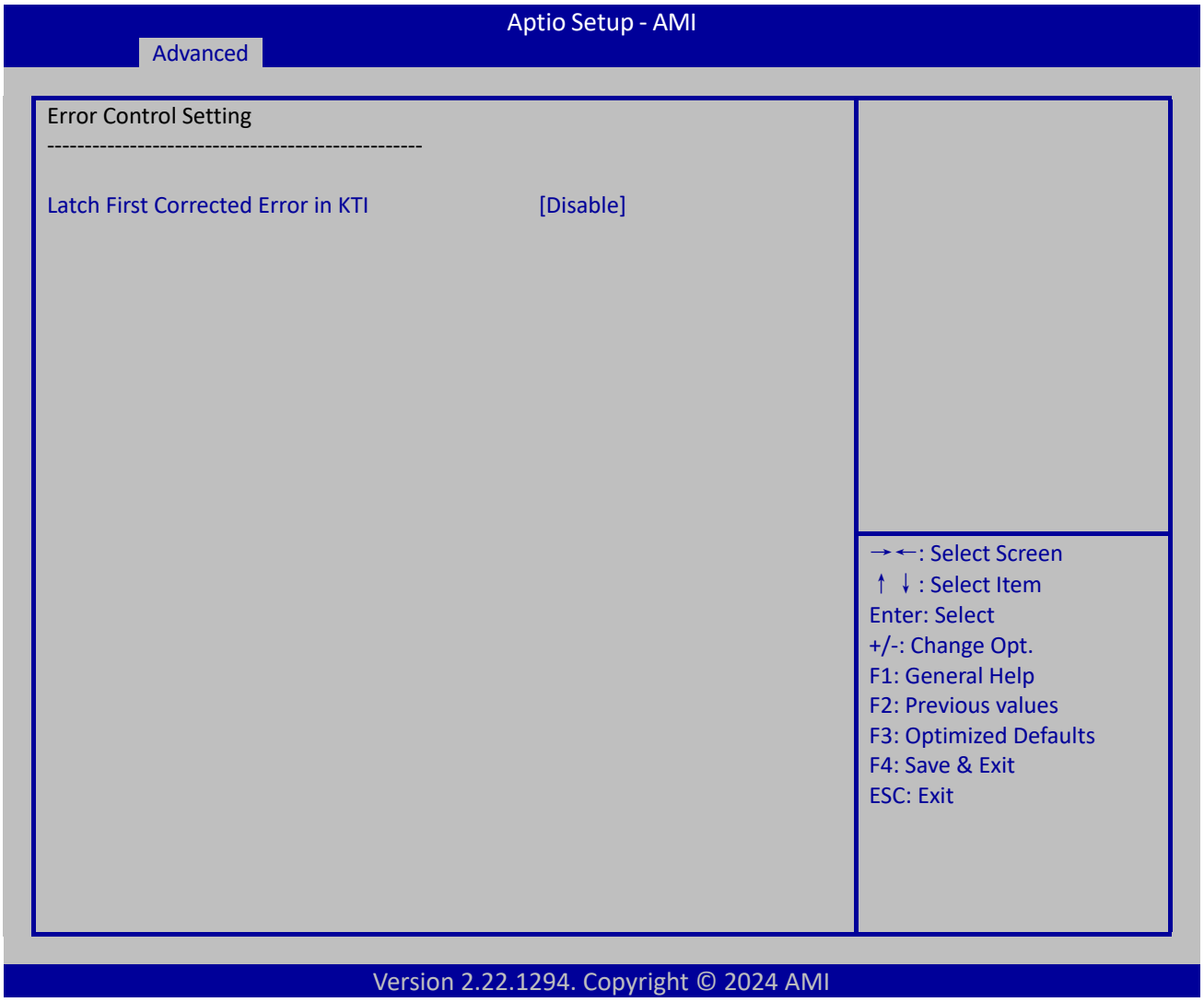
6.3.3.6 PCIe Error Enabling



Platform Configuration \ Runtime Error Logging \ PCIe Error Enabling		
Menu Fields	**Settings**	**Comments**
Corrected Error	[Disable] **[Enable]**	Enable & escalate Correctable Errors to error pins.
Uncorrected Error	[Disable] **[Enable]**	Enable & escalate Uncorrectable/Recoverable to error pins.
Fatal Error Enable	[Disable] **[Enable]**	Enable & escalate fatal errors to error pins.
PCIE Corrected Error Threshold Counter	**[Disable]** [Enable]	Enable/Disable PCIE Corrected Error Counter
PCIE Corrected Error Threshold	**1**	0x001 - 0x7fff
PCIe Corrected Error Limit Check	**[Disable]** [Enable]	Enable/Disable the feature to disable reporting PCIe corrected errors for a device if they exceed a given limit
PCIe Corrected Error Limit	**80**	Set the maximum number of corrected errors before corrected error reporting is disabled for a device

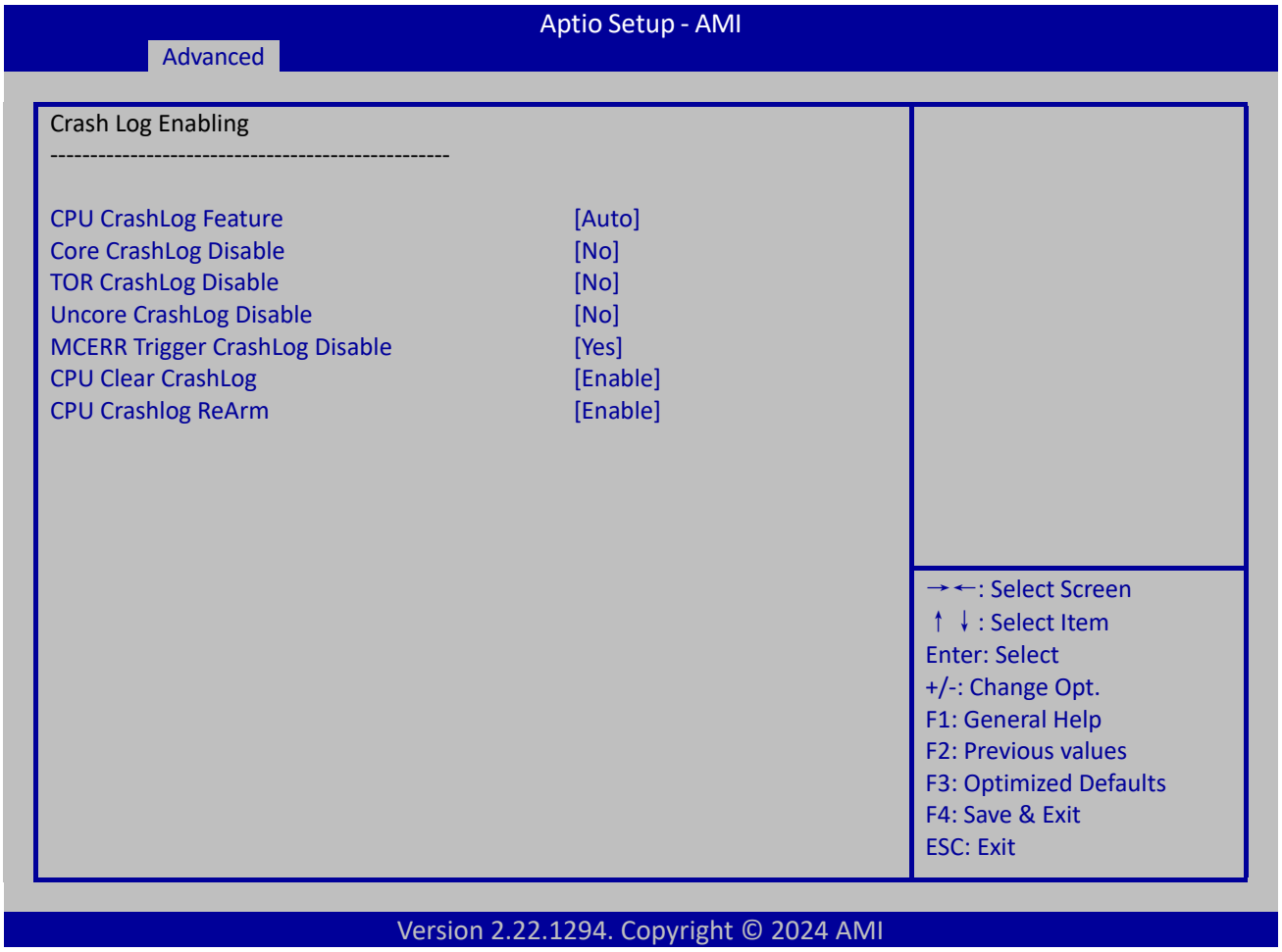
Platform Configuration \ Runtime Error Logging \ PCIe Error Enabling		
Menu Fields	**Settings**	**Comments**
PCIE AER Corrected Errors	[Disable] **[Enable]**	Enable/Disable PCIE AER Corrected Errors
PCIE AER NonFatal Error	[Disable] **[Enable]**	Enable/Disable PCIE AER NonFatal Error
PCIE AER Fatal Error	[Disable] **[Enable]**	Enable/Disable PCIE AER Fatal Error
PCIE AER Advisory Nonfatal Error	[Disable] **[Enable]**	Enable/Disable PCIE AER Advisory Nonfatal Error
PCIE ECRC Error	**[Disable]** [Enable]	Enable/Disable PCIE ECRC Error
PCIE Surprise Link Down Error	[Disable] **[Enable]**	Enable/Disable PCIE Surprise Link Down Error
PCIE Unsupported Request Error	**[Disable]** [Enable]	Enable/Disable PCIE Unsupported Request Error
Assert NMI on SERR	**[Enabled]** [Disabled]	On SERR, generate an NMI and log an error. Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.
Assert NMI on PERR	**[Enabled]** [Disabled]	On PERR, generate an NMI and log an error. Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.
Leaky Bucket Feature		
Expected BER	**34359738367**	Set the expected Bit Error Rate for all speeds.
Time Window (Gen1/2)	**65535**	Set the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.
Time Window (Gen3/4/5)	**2**	Set the error burst protection time window for Gen3, Gen4 and Gen5 speeds. A burst of errors within the window is counted as one.
Error Threshold (Gen1/2)	**0**	Set the error threshold for Gen1 and Gen2 speeds. An event is triggered when the error count exceeds the threshold.
Error Threshold (Gen3/4/5)	**16**	Set the error threshold for Gen3, Gen4 and Gen5 speeds. An event is triggered when the error count exceeds the threshold.
Gen3/4/5 Re-Equalization	[Disable] **[Enable]**	Enable or disable Gen3, Gen4 and Gen5 re-equalization. Applies only when operating at Gen3, Gen4 or Gen5 speeds. When an event is triggered, equalization is re-run.
Gen2 Link Degradation	[Disable] **[Enable]**	Enable or disable Gen2 link degradation. Applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.
Gen3 Link Degradation	[Disable] **[Enable]**	Enable or disable Gen3 link degradation. Applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.
Gen4 Link Degradation	[Disable] **[Enable]**	Enable or disable Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.
Gen5 Link Degradation	[Disable] **[Enable]**	Enable or disable Gen5 link degradation. Applies only when operating at Gen5 speeds. When an event is triggered, 32GT/s and higher modes are disabled.

6.3.3.7 Error Control Setting



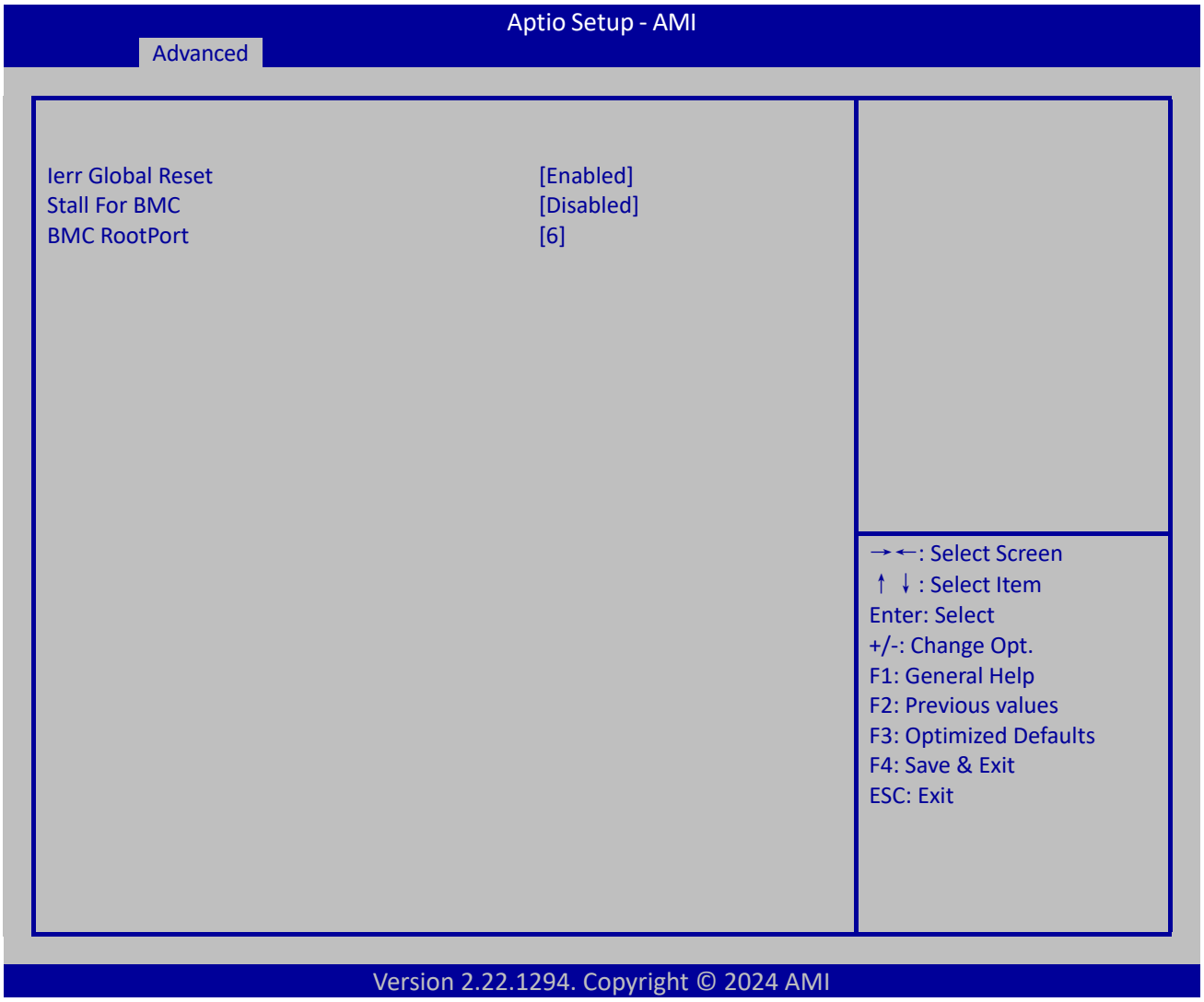
Platform Configuration \ Runtime Error Logging \ Error Control Setting		
Menu Fields	**Settings**	**Comments**
Latch First Corrected Error in KTI	**[Disable]** [Enable]	Enable or disable latch first corrected error in KTI.

6.3.3.8 Crash Log Enabling



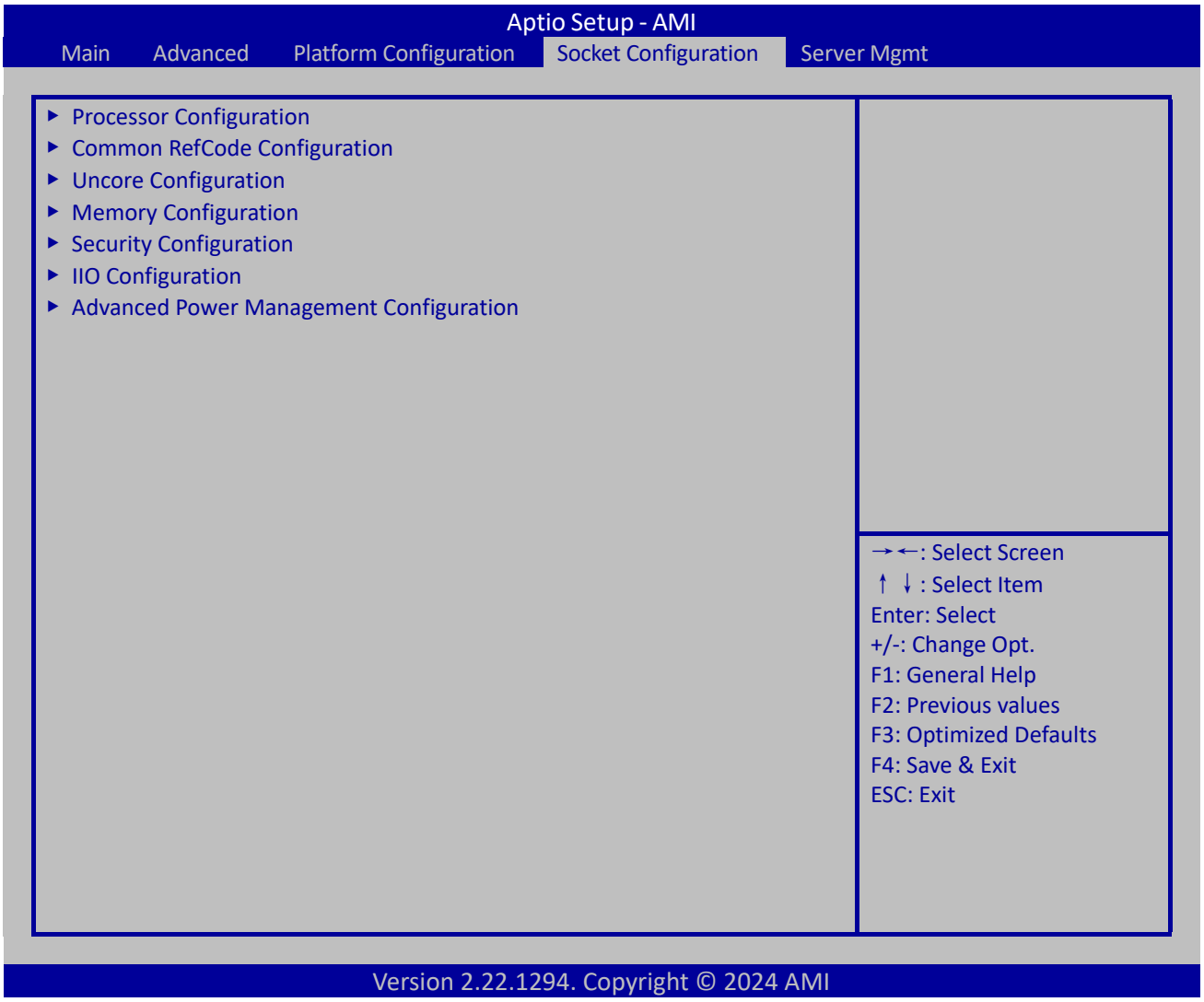
Platform Configuration \ Runtime Error Logging \ Crash Log Enabling		
Menu Fields	**Settings**	**Comments**
CPU CrashLog Feature	[Disable] [Enable] **[Auto]**	The feature helps collecting crash data from OOBMSM SSRAM
Core CrashLog Disable	**[No]** [Yes]	The feature helps to disable CPU Core crash log
TOR CrashLog Disable	**[No]** [Yes]	The feature helps to disable CPU TOR crash log
Uncore CrashLog Disable	**[No]** [Yes]	The feature helps to disable CPU Uncore crash log
MCERR Trigger CrashLog Disable	[No] **[Yes]**	The feature helps to disable MCERR to trigger crash log
CPU Clear CrashLog	[Disable] **[Enable]**	Option to clear CPU CrashLog after collection
CPU Crashlog ReArm	[Disable] **[Enable]**	Option to ReArm CPU CrashLog after collection

6.3.3.9 AWR Configuration



Platform Configuration \ Runtime Error Logging \ AWR Configuration		
Menu Fields	**Settings**	**Comments**
Ierr Global Reset	[Disabled] **[Enabled]**	Enables = when Ierr error present in last boot, do Global reset
Stall For BMC	**[Disabled]** [Enabled]	When enabled, system will enter spin loop during asynchronous warm reset allowing manual error collection
BMC RootPort	**[6]** [12]	RootPort that BMC is connected to

6.4 SOCKET CONFIGURATION



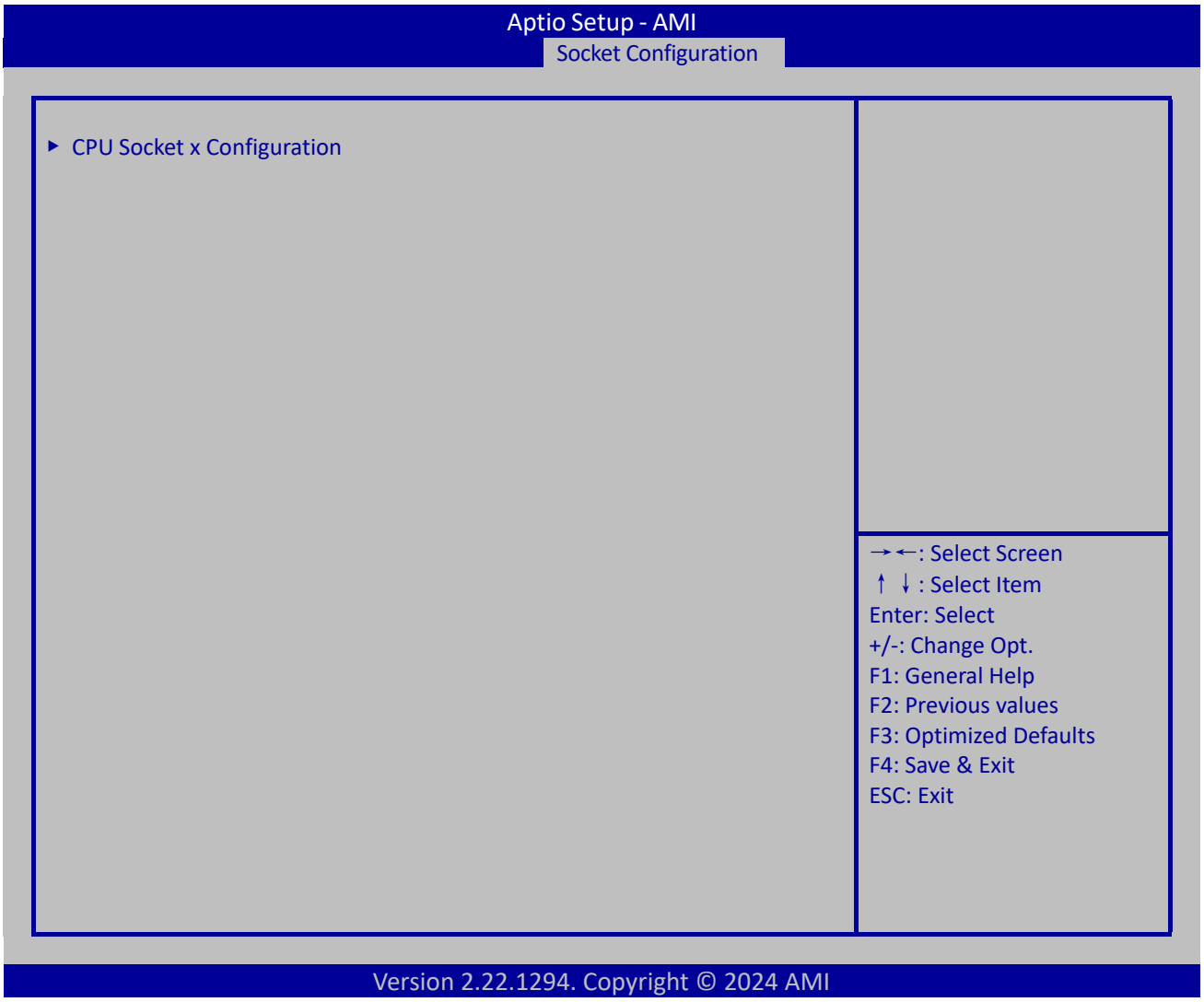
Socket Configuration		
Menu Fields	**Settings**	**Comments**
Processor Configuration	Selects sub-menu.	
Common RefCode Configuration	Selects sub-menu.	
Uncore Configuration	Selects sub-menu.	
Memory Configuration	Selects sub-menu.	
Security Configuration	Selects sub-menu.	
IIO Configuration	Selects sub-menu.	
Advanced Power Management Configuration	Selects sub-menu.	

6.4.1 Processor Configuration

Socket Configuration \ Processor Configuration		
Menu Fields	**Settings**	**Comments**
Per-Socket Configuration	Selects sub-menu.	
Processor BSP Revision	xxxx	
Processor Socket	Socket x	
Processor ID	xxxx	
Processor Frequency	x.xxxGHz	
Processor Max Ratio	xxH	
Processor Min Ratio	xxH	
Microcode Revision	xxxx	
L1 Cache RAM(Per Core)	xxxxKB	
L2 Cache RAM(Per Package)	xxxxKB	
L3 Cache RAM(Per Package)	xxxxKB	
Processor x Version	xxxx	
Enable LP [Global]	**[ALL LPs]** [Single LP]	Enable Logical Processor (Software Method to Enable/Disable Logical Processor threads)
Skip Flex Ratio Override	**[Disabled]** [Enabled]	Skip Flex Ratio overrides to use power-on default Flex Ratio values. In multi-socket systems, this will allow mixed flex ratio limits.
Check CPU BIST Result	[Disabled] **[Enabled]**	Disable failed BIST core when enabled, otherwise, ignore BIST result
3StrikeTimer	**[Enable]** [Disable]	Enable/disable the 3 strike counter by writing 0/1 to the MSR_DISABLE_SIGNALING_THREE_STRIKE_EVENT (MSR 0x01AB) BIT0
Fast String	[Disable] **[Enable]**	When enabled, enable fast strings for REP MOVS/STOS
Machine Check	[Disable] **[Enable]**	Enable or Disable the Machine Check
Hardware Prefetcher	**[Enable]** [Disable]	MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetch	**[Enable]** [Disable]	MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	[Disable] [Enable] **[Auto]**	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]). Auto will skip the register programming and keep the hardware default setting.
DCU IP Prefetcher	**[Enable]** [Disable]	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).
LLC Prefetch	**[Disable]** [Enable]	Enable/Disable LLC Prefetch on all threads
Homeless Prefetch	[Disable] [Enable] **[Auto]**	Enable/Disable Homeless Prefetch on all threads, Auto will skip the register programming and keep the hardware default setting.
FB Thread Slicing	**[Disable]** [Enable]	Enable/Disable FB (Fill Buffer) Thread Slicing per thread
AMP Prefetch	**[Enable]** [Disable]	Set to enable or disable MLC AMP prefetch (MSR 1A4h [5]).
Lowest APICID as BSP	**[Enable]** [Disable]	Enable - Try to select Processor with lowest APICID as BSP
APIC Physical Mode	**[Disable]** [Enable]	Enable/Disable the APIC physical destination mode

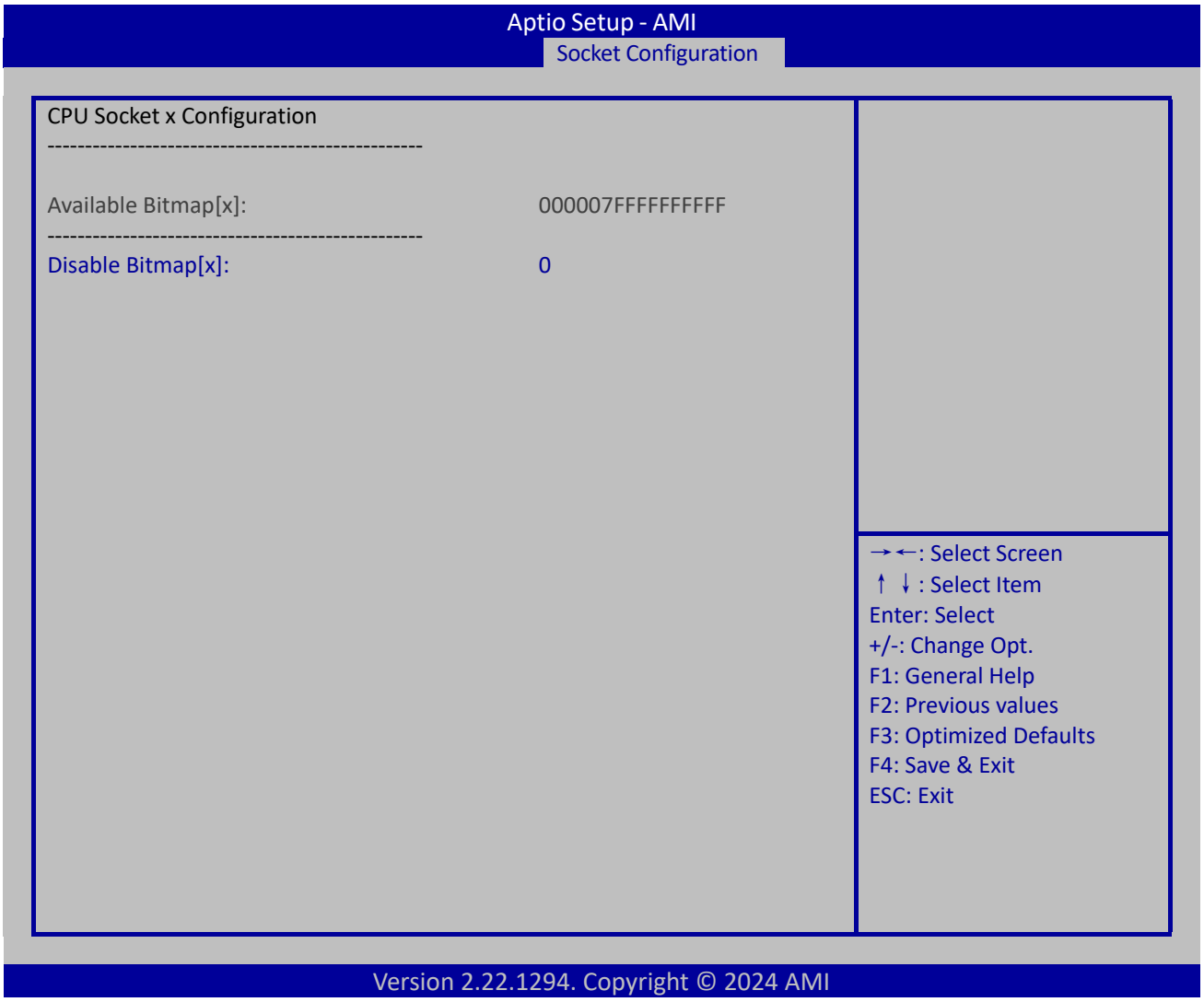
Socket Configuration \ Processor Configuration		
Menu Fields	**Settings**	**Comments**
DBP-F	[Enable] **[Disable]**	The DBP-F can be turned off by writing into the MSR 6Dh [2:3].
IIO LLC Ways Mask (Hex)	**0**	(SRF) 0: use hardware default, non-0 value will be written to MSR_IIO_LLC_WAYS, the maximum value is 0xFFF (GNR) 0: use hardware default, non-0 value will be written to MSR_IIO_LLC_WAYS, the maximum value is 0xFFFF
SMM Blocked and Delayed	**[Disable]** [Enable]	Enable/Disable SMM Blocked and Delayed
eSMM Save State	**[Disable]** [Enable]	Enable or Disable the eSMM Save State Feature
Smbus Error Recovery	[Disable] **[SMI]** [Error Pin]	Enable or Disable Smbus Error Recovery
Enable Intel(R) TXT	**[Disable]** [Enable]	Enables Intel(R) TXT.
VMX	[Disable] **[Enable]**	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	**[Disable]** [Enable]	Enables Safer Mode Extensions.
Lock Chipset	**[Enable]** [Disable]	Lock or Unlock chipset
BIOS ACM Error Reset	**[Disable]** [Enable]	When BIOS ACM error occurs, If enabled, it will disable TXT and Reset system (Restart system in non-TXT mode). If disabled, it will Ignore errors, and continue booting with no further BIOSACM being called
MSR Lock Control	[Disable] **[Enable]**	Enable - MSR 3Ah will be locked. Power Good reset is needed to remove lock bits.
PPIN Control	[Lock/Disable] **[Unlock/Enable]**	Unlock and Enable/Disable PPIN Control
AES-NI	[Disable] **[Enable]**	Enable/disable AES-NI support
Core Crash Data GPRs	**[Disabled]** [Enable]	Enabling this may expose personal or confidential information that may be held in the GPRs at the time of the Crash trigger
Processor trace	**[Disable]** [C0/C1 HWLS] [C2/C3 HWLS] [C0/C1 & C2/C3 (all) HWLS]	Enable/Disable processor trace feature from CPU MSR. Enabling this feature will immediately start trace collection.
Processor Trace OutPut Scheme	**[Single Range Output]** [ToPA Output]	Select Single Range Output scheme or ToPA table Output scheme
Processor trace memory allocation	**[4K]** [8K] [16K] [32K] [64K]	Select Processor trace memory region Size: from 4KB ~ 64KB
PSMI Configuration	Selects sub-menu.	

6.4.1.1 Per-Socket Configuration



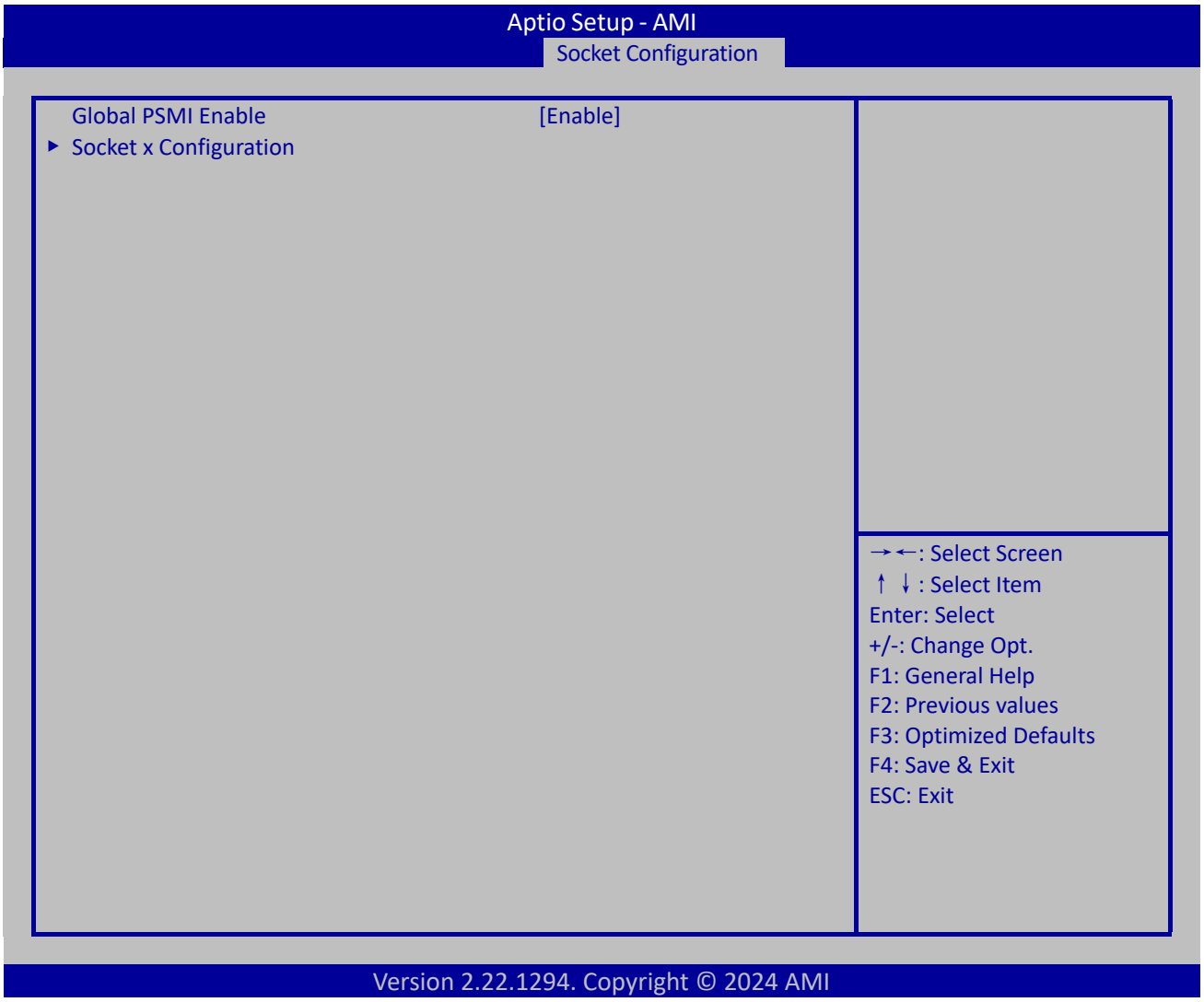
Socket Configuration \ Processor Configuration \ Per-Socket Configuration		
Menu Fields	**Settings**	**Comments**
CPU Socket x Configuration	Selects sub-menu.	

6.4.1.1.1 CPU Socket x Configuration



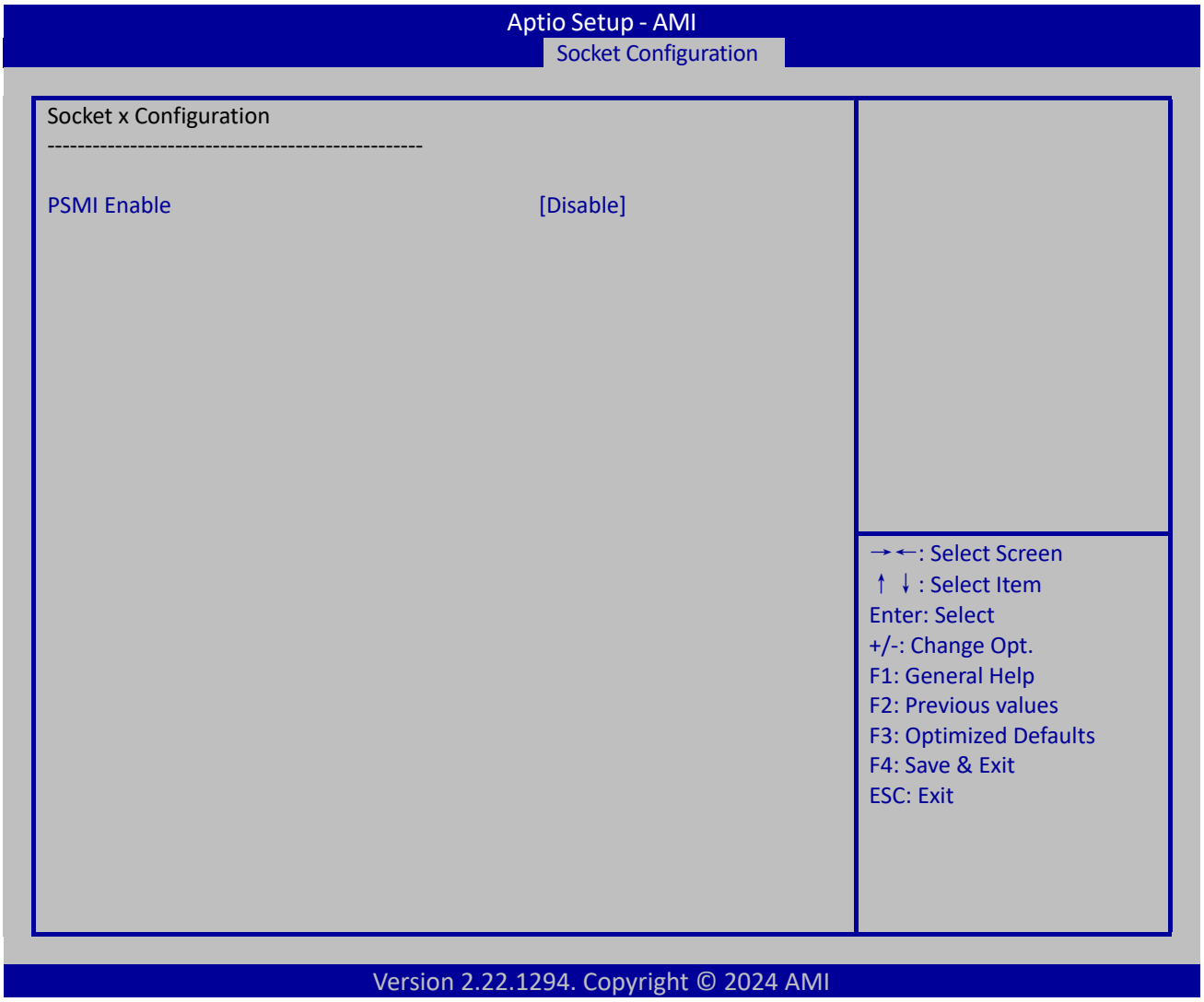
Socket Configuration \ Processor Configuration \ Per-Socket Configuration \ CPU Socket x Configuration		
Menu Fields	**Settings**	**Comments**
CPU Socket x Configuration		
Available Bitmap[x]:	000007FFFFFFFFFF	Displays the available Bitmap.
Disable Bitmap[x]:	**0**	Core Disable Bitmap(Hex) For every bit: set to Disable or clear to Enable NOTE: Any user core disable will force Static SST-PP. At least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

6.4.1.2 PSMI Configuration



Socket Configuration \ Processor Configuration \ PSMI Configuration		
Menu Fields	**Settings**	**Comments**
Global PSMI Enable	[Disable] **[Enable]** [Force setup]	Global PSMI Enable
CPU Socket x Configuration	Selects sub-menu.	

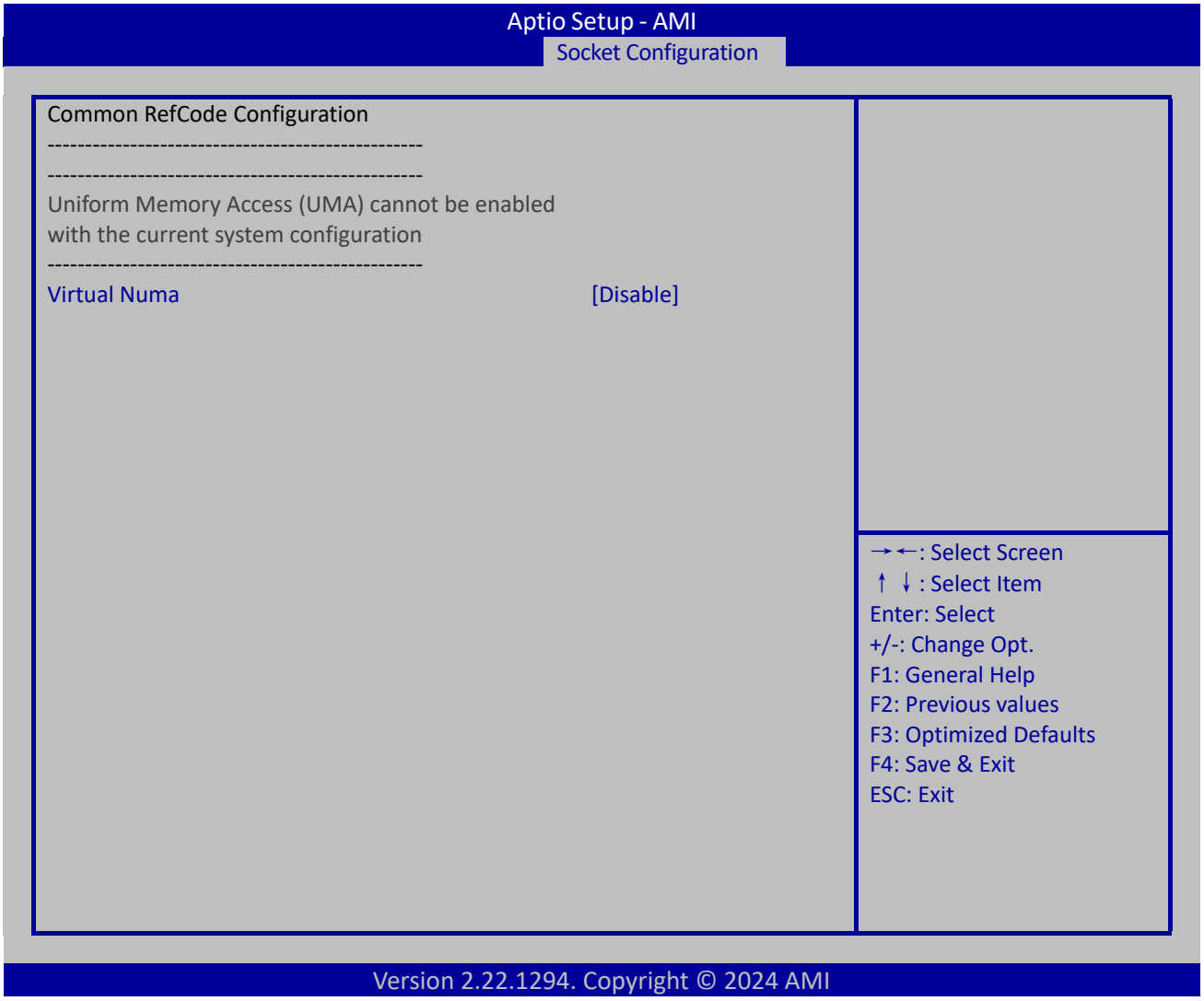
6.4.1.2.1 Socket x Configuration



Socket Configuration \ Processor Configuration \ PSMI Configuration \ Socket x Configuration		
Menu Fields	**Settings**	**Comments**
CPU Socket x Configuration		
PSMI Enable	**[Disable]** [Enable]	PSMI Enable
PSMI Handler Size	**[2M]** [4M] [8M]	PSMI Handler Size : 2MB - 8MB
PSMI Trace Region x	**[Disable]** [Enable]	PSMI Trace Region x
Buffer Size	**[16M]** [32M] [64M] [128M] [256M] [512M] [1G] [2G]	Buffer Size configurable and specified by 4-bit value(N) : 2^(23+N) bytes

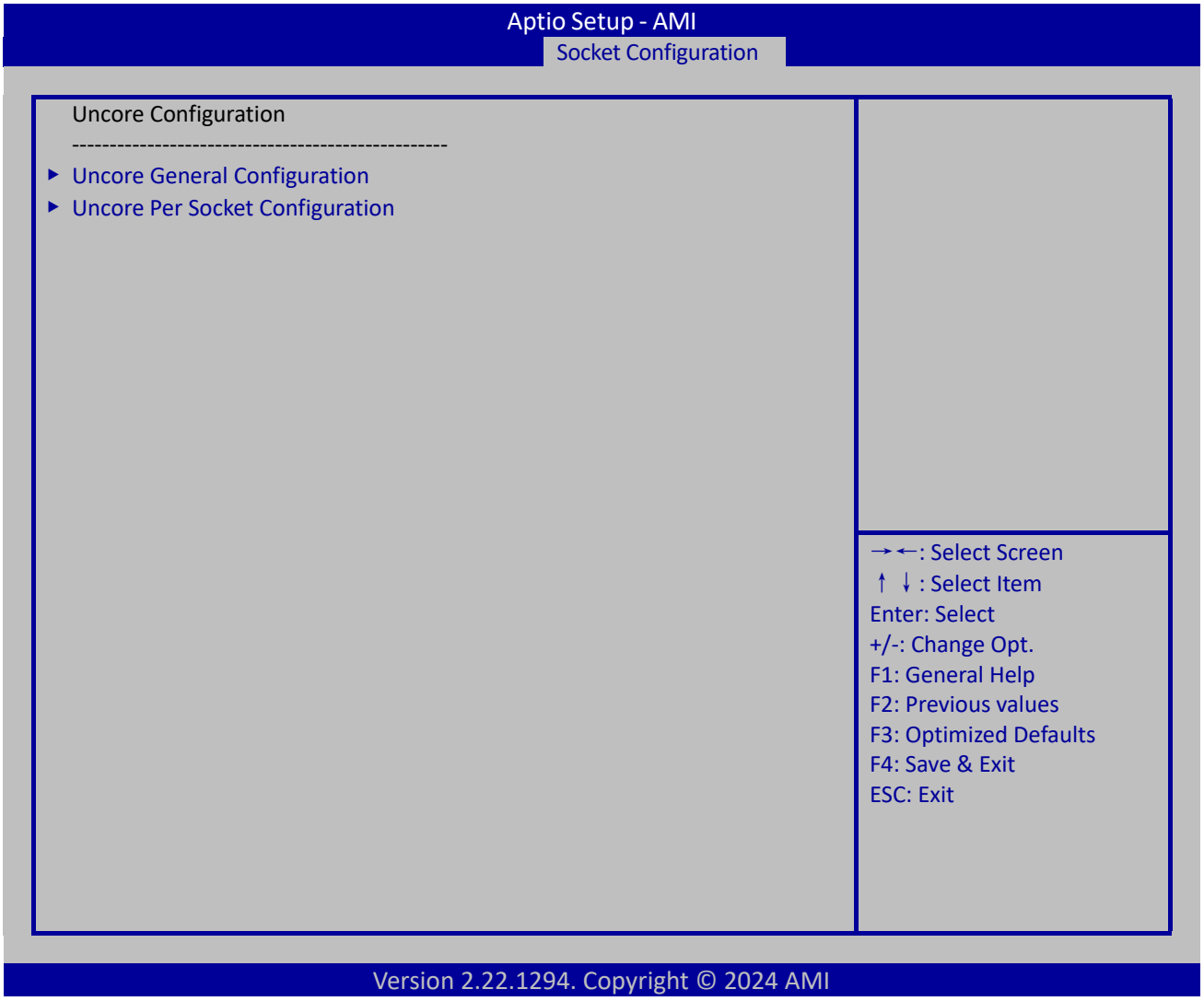
Socket Configuration \ Processor Configuration \ PSMI Configuration \ Socket x Configuration		
Menu Fields	**Settings**	**Comments**
	[4G] [8G] [16G] [32G] [64G] [128G] [256G]	
Cache Type	**[Any]** [Write Back]	Cache Type for buffer: Any, Write Back, Any with Range Register Compatibility, Write Back with Range Register Compatibility
Range Register Compatibility	**[Disable]** [Enable]	Enable to force the PSMI Trace memory to be naturally aligned

6.4.2 Common RefCode Configuration



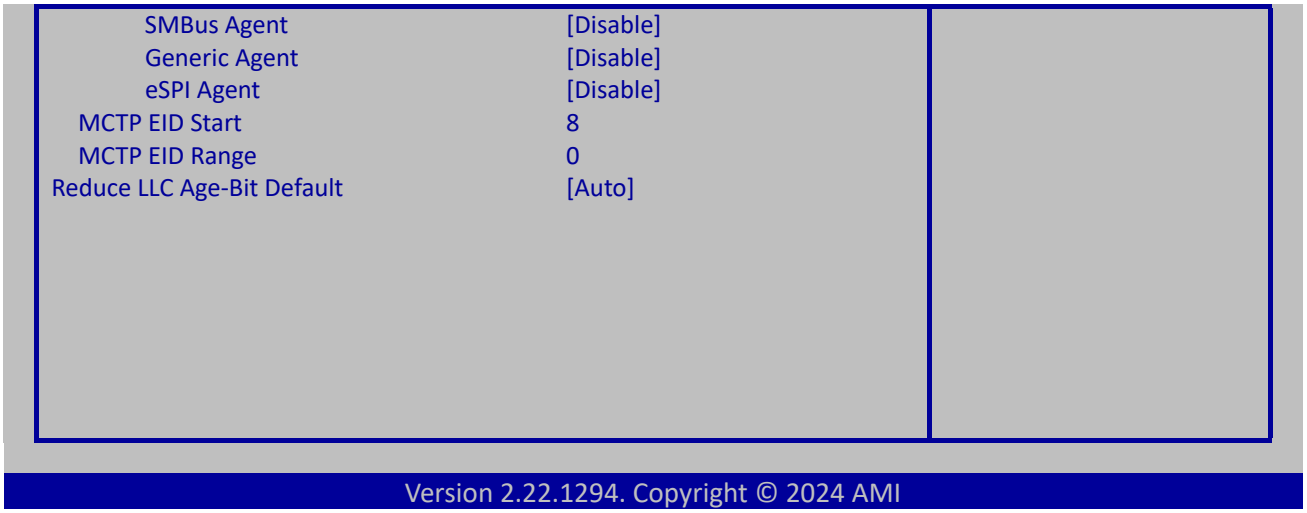
Socket Configuration \ Common RefCode Configuration		
Menu Fields	**Settings**	**Comments**
Virtual Numa	**[Disable]** [Enable]	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors.
Number of Virtual Numa Nodes	**0**	The number of virtual NUMA nodes per physical NUMA nodes. 0 means automatically set the number of virtual NUMA nodes based on system configuration. 1 equals disabling virtual NUMA.

6.4.3 Uncore Configuration



Socket Configuration \ Uncore Configuration		
Menu Fields	**Settings**	**Comments**
Uncore General Configuration	Selects sub-menu.	
Uncore Per Socket Configuration	Selects sub-menu.	

6.4.3.1 Uncore General Configuration



Socket Configuration \ Uncore Configuration \ Uncore General Configuration		
Menu Fields	**Settings**	**Comments**
Uncore Status	Selects sub-menu.	
Degrade Precedence	**[Topology Precedence]** [Feature Precedence]	Choose Topology Precedence to degrade features if system options are in conflict or choose Feature Precedence to degrade topology if system options are in conflict.
Link Frequency Select	[16.0GT/s] [20.0GT/s] [24.0GT/s] **[Auto]** [Use Per Link Setting]	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility.
Link L0p Enable	[Disable] [Enable] **[Auto]**	Enable - Set the c_l0p_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.
Link L1 Enable	[Disable] [Enable] **[Auto]**	Enable - Set the c_l1_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.
UPI Dynamic Link Width Reduction Support	[Disable] [Enable] **[Auto]**	Recover from hard failure on one or more UPI data lanes by dynamically resizing UPI link to 1/2 width, Auto - Auto decides based on Si Compatibility.
Directory Mode Enable	[Disable] [Enable] **[Auto]**	Directory Mode Enable, Auto - Auto decides based on Si Compatibility.
XPT Remote Prefetch	[Disable] [Enable] **[Auto]**	XPT Remote Prefetch
KTI Prefetch	[Disable] [Enable] **[Auto]**	KTI Prefetch, Auto - Auto decides based on Si Compatibility.
RdCur for XPT Prefetch	[Disable] [Enable] **[Auto]**	Enable - Set the suppress_mem_rd_prefetch_rdcur, Disable - Reset it, Auto - Auto decides based on Si Compatibility.
CPU SKU Type Mismatch check	[No] **[Yes]**	Yes or No to do CPU SKU Type Mismatch check

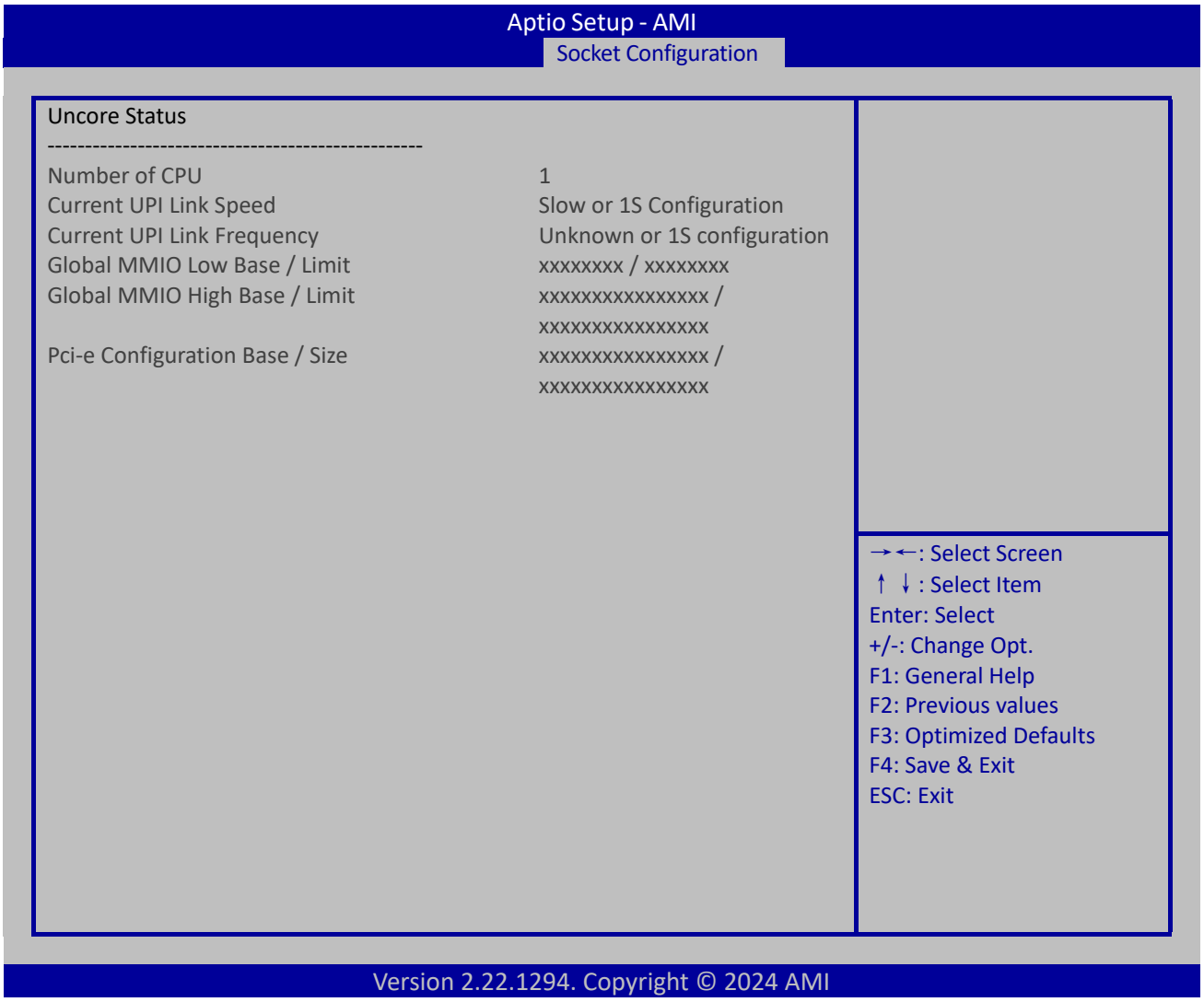
Socket Configuration \ Uncore Configuration \ Uncore General Configuration		
Menu Fields	**Settings**	**Comments**
Loctorem Thresholds Normal	[Disable] **[Auto]** [Low] [Medium] [High]	TOR Thresholds - Loctorem Thresholds Normal Setting, Auto - Auto decides based on Si Compatibility.
Loctorem Thresholds Empty	[Disable] **[Auto]** [Low] [Medium] [High]	TOR Thresholds - Loctorem Thresholds Empty Setting, Auto - Auto decides based on Si Compatibility.
UPI affinity	[Disable] [Enable] **[Auto]**	UPI affinity
IO Directory Cache (IODC)	[Disable] **[Auto]** [Enable for Remote InvItoM Hybrid Push] [Enable for Remote InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remote WCiLF]	IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores), Auto - Auto sets to WCiLF.
Legacy VGA Socket	**0**	Socket that claims the legacy VGA range; valid values are 0-3; 0 is default.
Distress QoS	**[Mode 0 - Disable the Distress QoS Feature]** [Mode 2 - M2M QoS Enable;CHA QoS Enable]	Distress QoS tuning recipes
On Demand In-band Provisioning Lock	[No] **[Yes]**	Enable/Disable On Demand In-band Provisioning Lock
S3m Telemetry update period	**1440**	S3m Telemetry update period in minutes. <65535> represent Disable
SplitLock	**[Disable]** [Enable] [Auto]	Enable - Enable the split lock. Disable - Disable the split lock. Auto - Auto decides based on Si Compatibility.
SNC	[Disable] [Enable] **[AUTO]**	Enable/Disable SNC mode. "Enable" means to enable SNC mode. When this is to "Disable", BIOS will enable UMA mode. Number of clusters is determined by BIOS based on detected SKU.
XPT Prefetch	[Disable] [Enable] **[Auto]**	XPT Prefetch, Auto - Auto decides based on Si Compatibility.
Legacy VGA Stack	**2**	Iio Device Instance that claims the legacy VGA range; valid values are 0-11.
PCIe Remote P2P Relaxed Ordering	**[Disable]** [Enable]	Relax P2P write ordering in hardware if software enforces ordering, or doesn't care. Default is DISABLE, so hardware will enforce P2P write ordering.
Uncore Debug Print Level	[Fatal] [Warning] [Summary] [Detail]	Uncore Debug message Print level setting. Fatal - Fatal message. Warning - Warning message. Summary - Simple message. Detail - Verbose. All - All message aboves

Socket Configuration \ Uncore Configuration \ Uncore General Configuration		
Menu Fields	**Settings**	**Comments**
	[All]	
Stale AtoS	[Disable] [Enable] **[Auto]**	Stale A to S Dir optimization, Auto - Auto decides based on Si Compatibility.
LLC dead line alloc	[Disable] **[Enable]** [Auto]	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC. Auto - Auto decides based on Si Compatibility.
Opportunistic-LLC-to-SF Migration	**[Disable]** [Enable] [Auto]	Control opportunistic-LLC-to-SF migration feature enable or disable, Auto - Auto decides based on Si Compatibility.
MBA BW Calibration Profiles	[Mid core BW shaping] [High core BW shaping] [Low core BW shaping] **[Auto]**	Choice of MBA BW throttling curve, Auto - Auto decides based on Si Compatibility.
PMM MBA BW downscale	**[1x]** [1/2x] [1/4x] [1/8x]	PMM BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling PMM BW throttling in a 2:1 ratio vs. DDR throttling.
CXL (Type3) MBA BW downscale	**[1x]** [1/2x] [1/4x] [1/8x]	CXL (Type3) BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling CXL (Type3) BW throttling in a 2:1 ratio vs. DDR throttling.
Remote Target MBA BW downscale	**[1x]** [1/2x] [1/4x] [1/8x]	Remote Target BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling Remote Target BW throttling in a 2:1 ratio vs. DDR throttling.
MMCFG Base	[1G] [1.5G] [1.75G] [2G] [2.25G] [3G] **[Auto]**	Select MMCFG Base, Auto - Auto decides based on Si Compatibility.
MMCFG Size	[64M] [128M] [256M] [512M] [1G] [2G] **[Auto]**	Select MMCFG Size, Auto - Auto decides based on Si Compatibility.
MMIO High Base	[248T] [120T] [88T] [60T] [30T] [56T] [40T] [32T] [24T] [16T]	Select MMIO High Base

Socket Configuration \ Uncore Configuration \ Uncore General Configuration		
Menu Fields	**Settings**	**Comments**
	[4T] [2T] [1T] [512G] [3584T] **[Auto]**	
MMIO High Granularity Size	[1G] [4G] [16G] [32G] [64G] [256G] [1024G] **[Auto]**	Selects the allocation size used to assign mmioh resources. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.
Limit CPU PA to 46 bits	**[Disable]** [Enable]	Limit CPU physical address to 46 bits to support older Hyper-v. If enabled, automatically disables TME-MT and limits the maximum MMIOH Base setup option to 60T
MCTP Bus Owner Selection	[CPU as Bus Owner] **[CPU as Bus Owner Proxy]**	Select the MCTP Bus Owner
Clock Modulation Enabled	[Disable] [Enable] **[Auto]**	Clock Modulation Enabled, Auto - Auto decides based on Si Compatibility.
Enable MMIO Downstream	**[Disable all PECI Agents]** [Enable all PECI Agents] [Use per-PECI Agent enable bit] [Auto]	PECI MMIO Downstream Access Configuration
Legacy Agent	**[Disable]** [Enable] [Auto]	Legacy PECI agent MMIO Downstream Access
SMBus Agent	**[Disable]** [Enable] [Auto]	SMBus PECI agent MMIO Downstream Access
Generic Agent	**[Disable]** [Enable] [Auto]	Generic PECI agent MMIO Downstream Access
eSPI Agent	**[Disable]** [Enable] [Auto]	ESPI PECI agent MMIO Downstream Access
PECI Trust Mode	[All PECI Agents untrusted] [All PECI Agents trusted"] **[Use per-PECI agent trust mode]** [Auto]	PECI Trust Mode Configuration
Legacy Agent	[Disable] **[Enable]** [Auto]	Legacy PECI agent in trust bit enable
SMBus Agent	**[Disable]** [Enable] [Auto]	SMBus PECI agent in trust bit enable
Generic Agent	**[Disable]** [Enable] [Auto]	Generic PECI agent in trust bit enable

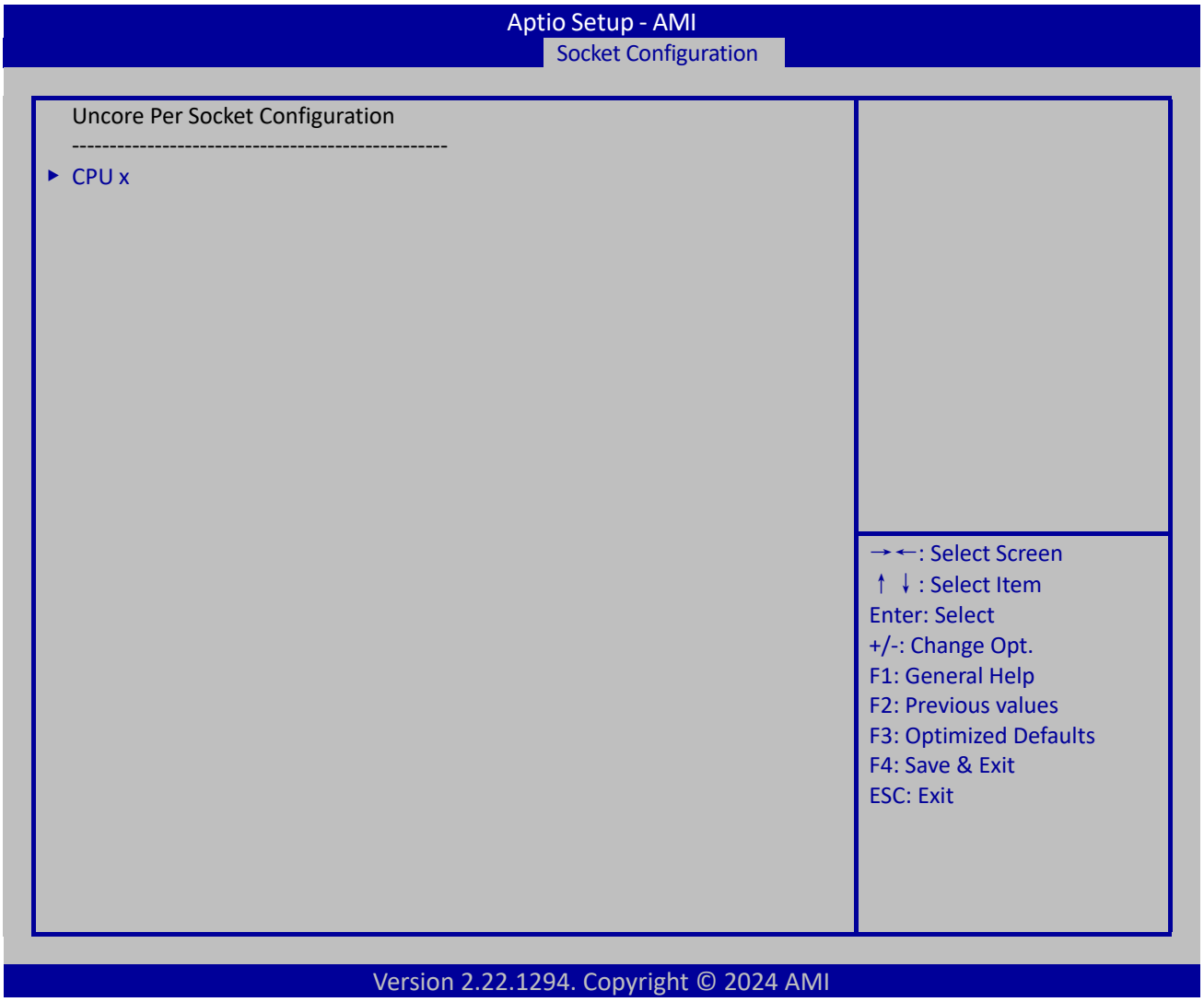
Socket Configuration \ Uncore Configuration \ Uncore General Configuration		
Menu Fields	**Settings**	**Comments**
eSPI Agent	**[Disable]** [Enable] [Auto]	ESPI PECI agent in trust bit enable
MCTP EID Start	**8**	Controls the start value used for the MCTP EID
MCTP EID Range	**0**	Controls the range value used for the MCTP EID
SLF Enable	[Disable] [Enable] **[Auto]**	Send B2P command for Pcode SLF Enable programming, enable by default for supported CPU Type

6.4.3.1.1 Uncore Status



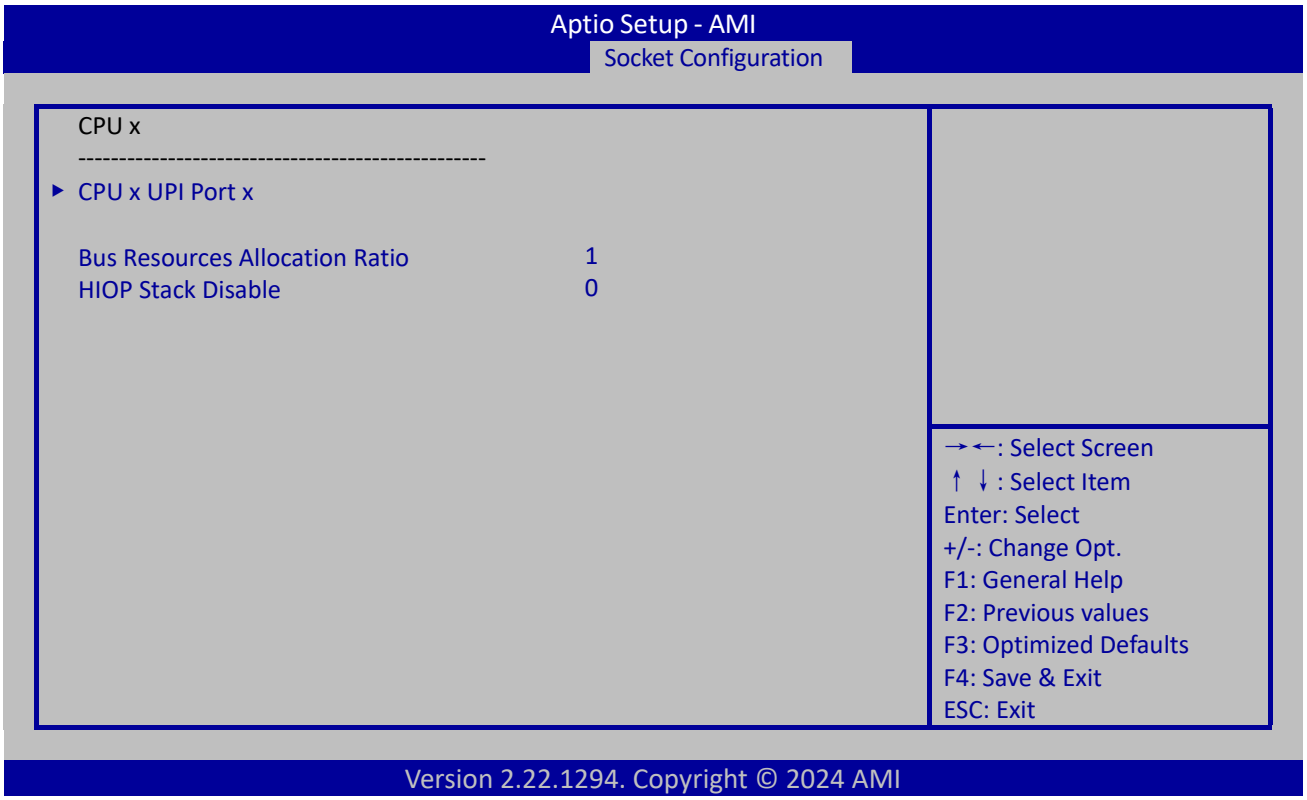
Socket Configuration \ Uncore Configuration \ Uncore General Configuration \ Uncore Status		
Menu Fields	**Settings**	**Comments**
Number of CPU	1	Displays the CPU counts
Current UPI Link Speed	Slow or 1S Configuration	Displays the current UPI link speed
Current UPI Link Frequency	Unknown or 1S configuration	Displays the current UPI link frequency
Global MMIO Low Base / Limit	xxxxxxxx / xxxxxxxx	Displays the global MMIO low base / limit
Global MMIO High Base / Limit	xxxxxxxxxxxxxxxx / xxxxxxxxxxxxxxxx	Displays the global MMIO high base / limit
Pci-e Configuration Base / Size	xxxxxxxxxxxxxxxx / xxxxxxxxxxxxxxxx	Displays the Pci-e configuration base / size

6.4.3.2 Uncore Per Socket Configuration



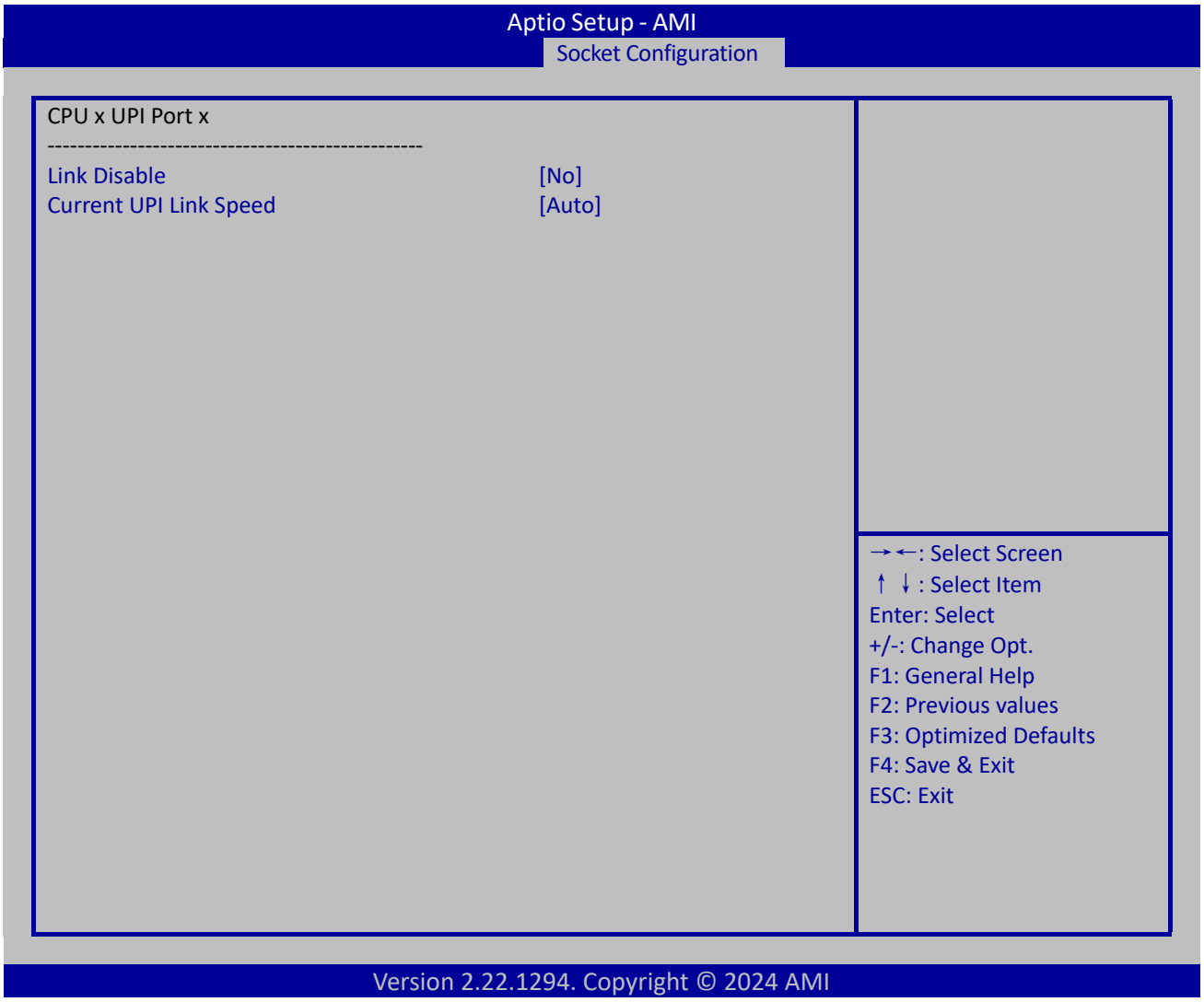
Socket Configuration \ Uncore Configuration \ Uncore Per Socket Configuration		
Menu Fields	**Settings**	**Comments**
CPU x	Selects sub-menu.	

6.4.3.2.1 CPU x



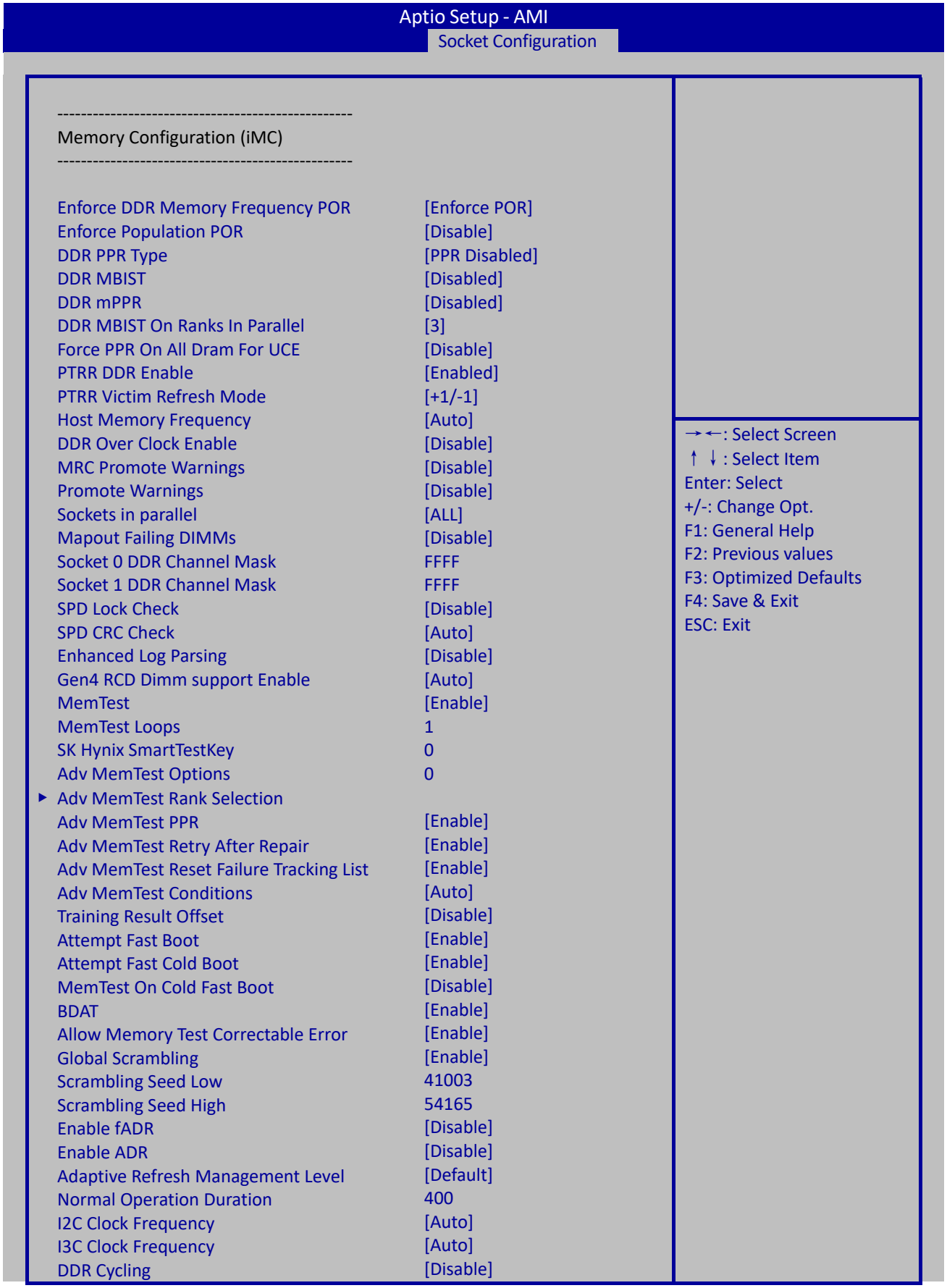
Socket Configuration \ Uncore Configuration \ Uncore Per Socket Configuration \ CPU x		
Menu Fields	**Settings**	**Comments**
CPU x		
CPU x UPI Port x	Selects sub-menu.	
Bus Resources Allocation Ratio	1	Bus resources allocation ratio, range 0 to 8
HIOP Stack Disable	0	Enables/Disables given HIOP STACK. Default is AUTO no stack is disabled. 1 - The stacks indicated by the bit locations are disabled. 0 - The stacks indicated by the bit locations are not modified. The stack order is abstracted so each bit 0 = stack 0 ... bit n = stack n. For PE numbering convention bits are incrementally mapped from bit0 to instances HC(0->n), {TIP(0->n), ETH(0->n)}*, then PE(0->n) and PE(a->x). The bit setting for each stack expect ETH, can be overridden by BIOS based on CPU-knob compatibility. TIP and ETH only if available in system .

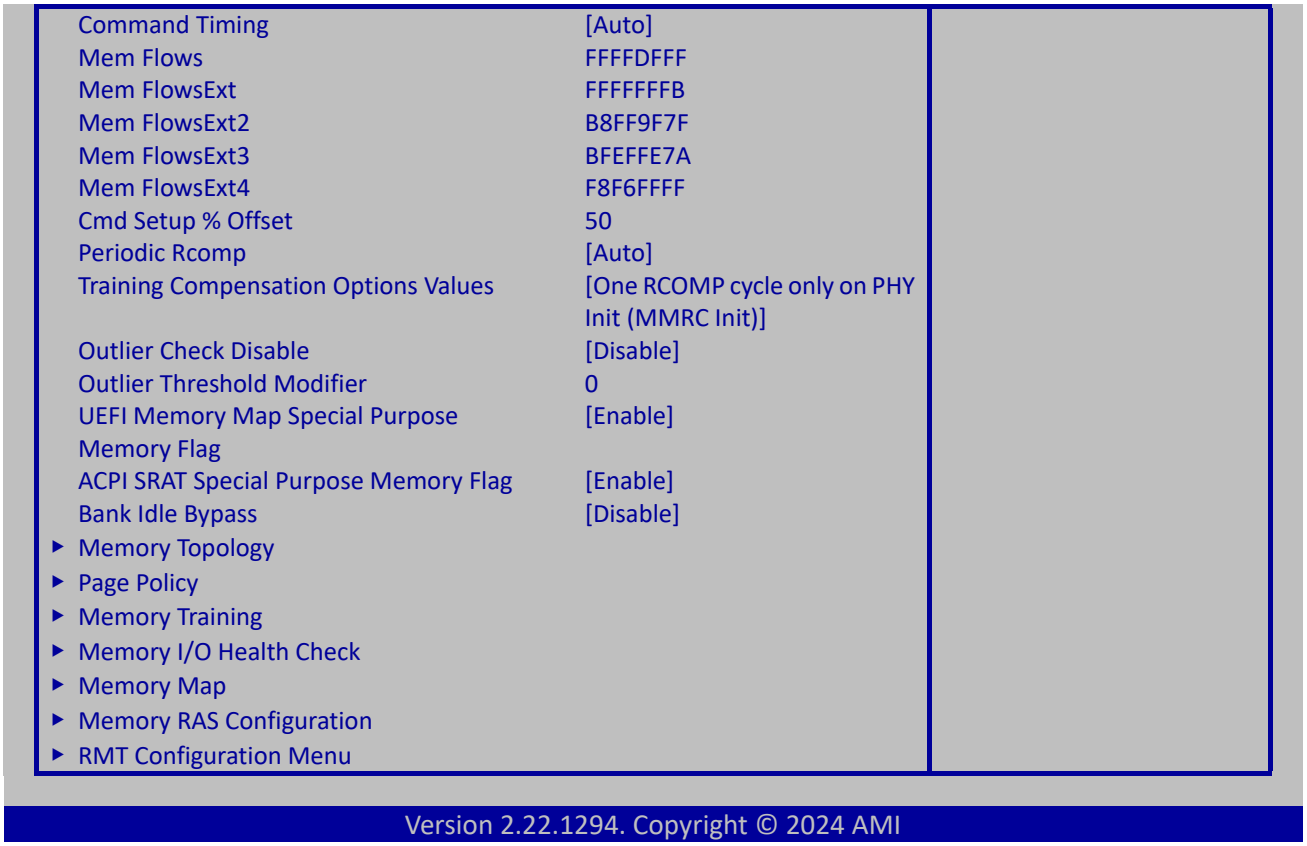
6.4.3.2.1.1 CPU x UPI Port x



Socket Configuration \ Uncore Configuration \ Uncore Per Socket Configuration \ CPU x \ CPU x UPI Port x		
Menu Fields	**Settings**	**Comments**
Link Disable	**[No]** [Yes]	Disable a single UPI port. No: Not disable; Yes: Disable
Current UPI Link Speed	[16.0GT/s] [20.0GT/s] [24.0GT/s] **[Auto]**	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility.

6.4.4 Memory Configuration





Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
Enforce DDR Memory Frequency POR	**[Enforce POR]** [Enforce Stretch Goals] [Disabled]	Enforces Plan Of Record restrictions for DDR frequency programming.
Enforce Population POR	**[Disable]** [Enable]	Enable Memory Population POR Enforcement.
DDR PPR Type	**[PPR Disabled]** [Hard PPR] [Soft PPR]	Selects DDR Post Package Repair Type - Hard / Soft / Disabled.
DDR MBIST	**[Disabled]** [Enabled]	Enable / Disable DDR MBIST (Memory Built-In Self-Test)
DDR mPPR	**[Disabled]** [Enabled]	Enable / Disable DDR mPPR (Memory Built-In Self-Test Post Package Repair)
DDR MBIST On Ranks In Parallel	[1] [2] **[3]**	It provides flexibility in case that the vendor Idd values could dictate DDR MBIST execution concurrency. 1 - 1 rank at a time. 2 - 2 ranks at a time. 3 - 3 ranks at a time.
Force PPR On All Dram For UCE	**[Disable]** [Enable]	Enable/Disable force PPR on all dram for UCE.
PTRR DDR Enable	[Disabled] **[Enabled]**	Enable / Disable support for PTRR in DDR
PTRR Victim Refresh Mode	**[+1/-1]** [+1/-1/+2/-2]	Select between +1/-1 or +1/-1/+2/ and -2 victim refresh mode
Host Memory Frequency	**[Auto]** [4800] [5200] [5600]	Maximum Host DDR Memory Frequency Selections in MT/s. If the "AUTO" option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. If Enforce POR is

Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
	[6000] [6400] [7200]	disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Note: For MCR, DDR DRAM frequency is half of Host frequency
DDR Over Clock Enable	**[Disable]** [Enable]	Determines if enable DDR Over Clock
MRC Promote Warnings	**[Disable]** [Enable]	Determines if MRC warnings are promoted to system level
Promote Warnings	**[Disable]** [Enable]	Determines if warnings are promoted to system level
Sockets in parallel	**[ALL]** [1] [2] [4]	ALL - All sockets operate in parallel. 1 - At any time only one socket is executing. 2 - At any time only two sockets are executing. 4 - At any time only four sockets are executing
Mapout Failing DIMMs	**[Disable]** [Enable]	When a rank would be mapped out, instead disable the full DIMM
Socket 0 DDR Channel Mask	**FFFF**	Enable (1) or disable (0) DDR memory channels. One bit corresponding to one channel per socket.
Socket 1 DDR Channel Mask	**FFFF**	Enable (1) or disable (0) DDR memory channels. One bit corresponding to one channel per socket.
SPD Lock Check	**[Disable]** [Enable]	Enables or disables SPD lock status check
SPD CRC Check	**[Auto]** [Disable] [Enable]	Enable/Disable SPD CRC Check. Auto = dynamically selected.
Enhanced Log Parsing	**[Disable]** [Enable]	Enables additional output in debug log for easier machine parsing
Gen4 RCD Dimm support Enable	**[Auto]** [Disable] [Enable]	Determines if Gen4 RCD Type Dimm supported in plaform
MemTest	[Disable] **[Enable]**	Enable - Enables memory test during normal boot. Disable - Disables this feature.
MemTest Loops	**1**	Number of memory test loops during normal boot, set to 0 to run memtest infinitely
SK Hynix SmartTestKey	**0**	Confidential key to be used in SK Hynix Smart Test
Adv MemTest Options	**0**	This option is a bit mask[19:0]: All 0 = disabled: bit-0=XMATS8, bit-1=XMATS16, bit-2=Reserved, bit-3=Reserved, bit-4=WCMATS8, bit-5=WCMCH8, bit-6=Reserved, bit-7=MARCHCM64, bit-8=Reserved, bit-9=Reserved, bit-10=Reserved, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3, bit-16=SK-HYNIX, bit-17=SAMSUNG, bit-18=MICRON-RMW, bit-19=SCRAM_X2
Adv MemTest Rank Selection	Selects sub-menu.	
Adv MemTest PPR	[Disable] **[Enable]**	This option enable/disable ppr flow for MemTest
Adv MemTest Retry After Repair	[Disable] **[Enable]**	Enable/disable Retry of the current Adv MemTest step after a PPR repair is done.
Adv MemTest Reset Failure Tracking List	[Disable] **[Enable]**	Enable/disable Reset of the Row Failure Tracking List after each Adv MemTest option. Useful for testing performance of multiple options.

Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
Adv MemTest Conditions	[Disable] **[Auto]** [Manual]	Auto = set test conditions based on test type; Manual = specify global test conditions; Disable = Do not apply test conditions.
Adv MemTest PMIC VDD Level	**1100**	Specify PMIC VDD and VDDQ level in units of mV.
Adv MemTest tWR	**48**	Specify tWR timing between 48 to 96 in units of tCK.
Adv MemTest tREFI	**3900**	Specify tREFI (refresh rate) timing between 1850 to 7800 in nsec.
Adv MemTest Pause	**64**	Specify a pause delay between 0 to 256000 in units of usec. This is a time period where refresh is disabled between write and read sequences.
Training Result Offset	**[Disable]** [Enable]	Enable/Disable training results offset. When enabled, offsets will be applied to the trained results. If enabled during cold fast boot, the offset will be applied on every cold fast boot, cumulatively.
Offset RecEnDelay	**100**	How much to offset RecEnDelay final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105 (Range -32 to +32)
Offset TxDq	**100**	How much to offset TxDq final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset RxDq	**100**	How much to offset RxDq final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset TxVref	**100**	How much to offset TxVref final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset RxVref	**100**	How much to offset RxVref final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset RxSampler	**100**	How much to offset RxSampler final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset CmdAll	**100**	How much to offset CmdAll final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset CmdVref	**100**	How much to offset CmdVref final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset CtlAll	**100**	How much to offset CtlAll final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Offset CtlVref	**100**	How much to offset CtlVref final memory training results. +ve starts at 0 --> for an offset of +7, enter 7; -ve starts at 100 --> for an offset of -5, enter 105
Attempt Fast Boot	[Disable] **[Enable]**	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature.
Attempt Fast Cold Boot	[Disable] **[Enable]**	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature.

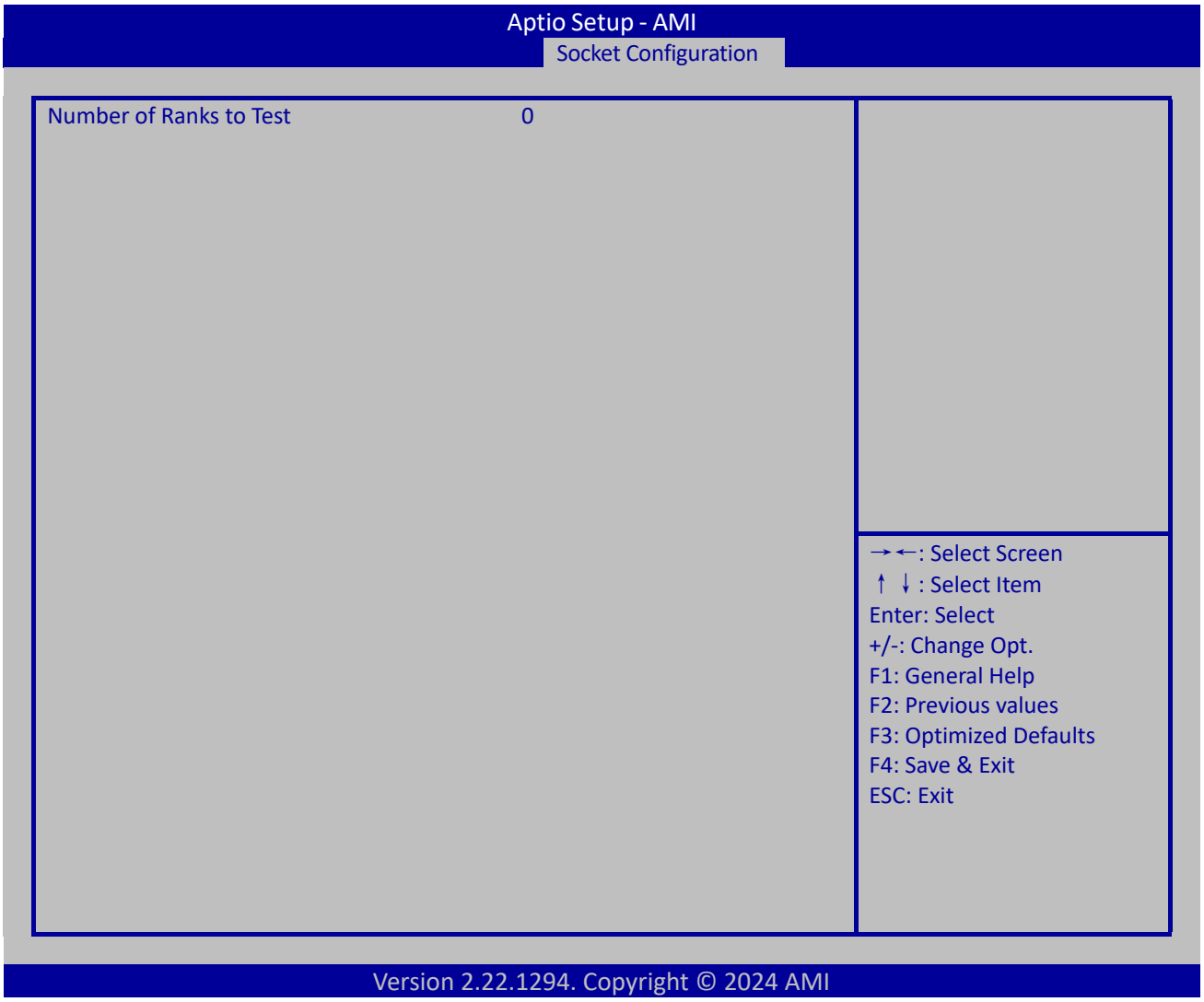
Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
MemTest On Cold Fast Boot	**[Disable]** [Enable]	Enable - Enables memory test during cold fast boot. Disable - Disables this feature.
BDAT	[Disable] **[Enable]**	Enable Disables publishing BDAT ACPI Table
Allow Memory Test Correctable Error	[Disable] **[Enable]**	Enable - Logs error and allows correctable errors during memory test(DIMM Rank not removed). Disable - Logs error and removes DIMM Rank.
Global Scrambling	[Disable] **[Enable]**	Enable - Enables global data scrambling. Disable - Disables global data scrambling
Scrambling Seed Low	**41003**	Low 32 bits of the scrambling seed
Scrambling Seed High	**54165**	High 32 bits of the scrambling seed
Enable fADR	**[Disable]** [Enable]	Enable/Disable fADR capability in the platform
fADR Configuration	Selects sub-menu.	
Enable ADR	**[Disable]** [Enable]	Enables the detecting and enabling of ADR This is not available if fADR is enabled since fADR requires ADR to be enabled
ADR Data Save Mode	[Batterybacked DIMMs] **[CXL Type 3 / GPF]**	Data Save Mode for ADR
Check PlatformDetectADR	**[Disable]** [Enable]	Use the PlatformDetectADR function as a recovery indicator
Adaptive Refresh Management Level	**[Default]** [Level A] [Level B] [Level C]	Selects Adaptive Refresh Management(ARFM) Level when refresh management(RFM) is required. 0:Default - RAAIMT, RAAMMT, RAADEC; 1:Level A - RAAIMT-A, RAAMMT-A, RAADEC-A; 2:Level B - RAAIMT-B, RAAMMT-B, RAADEC-B; 3:Level C - RAAIMT-C, RAAMMT-C, RAADEC-C
Normal Operation Duration	**400**	Set normal operation duration interval (0 - 65535)
I2C Clock Frequency	**[Auto]** [400 kHz in I2C mode] [700 kHz in I2C mode] [1 MHz in I2C mode]	Sets DDR5 I2C Clock Frequencies For SPD Access.
I3C Clock Frequency	**[Auto]** [4 MHz in I3C mode] [6 MHz in I3C mode] [8 MHz in I3C mode] [9 MHz in I3C mode] [10 MHz in I3C mode]	Sets DDR5 I3C Clock Frequencies For SPD Access.
DDR Cycling	**[Disable]** [Enable]	When enabled, MRC will train the memory and then power cycle over and over to stress MRC
Command Timing	**[Auto]** [1N] [2N]	Selects the desired memory controller command timing
Mem Flows	**FFFFDFFF**	Enable(1)/Disable(0) multi steps with BitMask - HOST_XOVER_CALIBRATION-BIT0; SENSE_AMP-BIT1; EARLY_CMD_CLK-BIT2; RECEIVE_ENABLE-BIT3; READ_DQ_DQS_COARSE-BIT4; WR_LVL_EXT-BIT5; WR_LVL_INT-BIT6; WR_DQ_DQS_COARSE-BIT7; PUBLISH_ACT_DIMM_MANIFEST-BIT8; MEM_LATE-BIT9; ENFORCE_POPULATION_POR-BIT10; INIT_STRUCTURES_LATE-BIT11; WR_VREF-BIT12; ROUND_TRIP_LATENCY_OPTIMIZATION-BIT13;

Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
		DETECT_DIMM_CONFIG-BIT14; POST_FRONTSIDE_COMMAND-BIT15; POST_BACKSIDE_COMMAND-BIT16; INIT_CLOCKS-BIT17; RCD_DCA_DFE_TAP1-BIT18; MDQS_RECEIVE_ENABLE-BIT19; BUFFER_DRAM_WRITE_LEVELING-BIT20; RCD_DCA_TIMING_SIMPLE-BIT21; UNLOCK_MEMORY_AFTER_RAM_TRAINING-BIT22; NA-BIT23; CHECK_STATUS_TRAINING-BIT24; MEM_INIT-BIT25; READ_DQ_SWIZZLE_DISCOVERY-BIT26; NORMAL_MODE_SWITCH-BIT27; CMD_VREF_CENTERING-BIT28; LRDIMM_WR_VREF_CENTERING-BIT29; ADVANCED_MEM_TEST-BIT30; CONFIGURE_VDD-BIT31
Mem FlowsExt	**FFFFFFFB**	Enable(1)/Disable(0) multi steps with BitMask - TX_DQ_XTALK_CAL-BIT0; SAVE_RESTORE_CTE-BIT1; CMD_NORMALIZATION-BIT2; POWER_ON_MEM-BIT3; CONFIGURE_RANK_SIZE-BIT4; LRDIMM_BCOM-BIT5; CHECK_POR_COMPATIBILITY-BIT6; INIT_DDRIO_INTERFACE_EARLY-BIT7; EARLY_INIT_THERMAL_THROTTLING-BIT8; INIT_THERMAL_THROTTLING-BIT9; POST_TRAINING_INIT-BIT10; EARLY_MC_CONFIG-BIT11; LATE_MC_CONFIG-BIT12; SSA_RMT-BIT13; INIT_MEM_TRAINING-BIT14; GATHER_SPD_DATA-BIT15; INIT_DDRIO_INTERFACE_LATE-BIT16; RCD_QCA-BIT17; DDR_TRAINING-BIT18; CHECK_UGB_ADC_VOLTAGE-BIT19; HMRC_SCAD_EXIT-BIT20; INIT_MEM_MAP-BIT21; NA-BIT22; HOST_RCOMP_STATIC_LEG-BIT23; QCA_COMPLEX_MULTI_VREF_TRAINING-BIT24; PRE_TRAINING_INIT-BIT25; CS_AND_RCD_DCS_TIMING-BIT26; RCD_QCS_TIMING-BIT27; RCD_DCA_VREF_COMPLEX_PATTERN-BIT28; RCD_DCA_TIMING_COMPLEX_PATTERN-BIT29; INIT_CMI_CREDIT-BIT30; SET_RAS_CONFIG-BIT31
Mem FlowsExt2	**B8FF9F7F**	Enable(1)/Disable(0) multi steps with BitMask - WRITE_DQDQS_PRE_DFE_2D_CENTERING-BIT0; WRITE_DQDQS_POST_DFE_2D_CENTERING-BIT1; RCD_DCA_DCK_DUTY_CYCLE_TRAINING-BIT2; RCD_DCA_DFE-BIT3; READ_DQDQS_PRE_DFE_2D_CENTERING-BIT4; READ_DQDQS_POST_DFE_2D_CENTERING-BIT5; TX_PERIODIC_RETRAIN-BIT6; CA_SLEW_RATE-BIT7; RCD_DCA_TCO-BIT8; DISABLE_UNFUSED_CHANNELS-BIT9; TURNAROUND_OPTIMIZATION-BIT10; READ_DQ_DQS_DFE-BIT11; WRITE_DQ_DQS_DFE-BIT12; DQ_SLEW_RATE-BIT13; OFFSET_TRAINING_RESULTS-BIT14; READ_DQ_DQS_DUTY_CYCLE_ADJUSTER-BIT15; WRITE_DQ_DQS_TCO_Training-BIT16;

Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
		PBA_ENUMERATE-BIT17; DB_DFE_DDR5-BIT18; WRITE_DQDQS_ODT_LATENCY-BIT19; POST_PACKAGE_REPAIR_FLOW-BIT20; TRAINING_FOR_ML_DATA-BIT21; EARLY_MCR_EARLY_SWIZZLE_DISCOVERY-BIT22; MCR_PSEUDO_CHANNEL_PHASE-BIT23; READ_DQ_DQS_XTALK_CANCELLATION_TRAINING-BIT24; LDO_TRAINING-BIT25; RX_JITTER_CANCELLATION_TRAINING-BIT26; RCD_DCA_VREF_SIMPLE_PATTERN-BIT27; MDQS_READ_DELAY_TRAINING-BIT28; BUFFER_WRITE_DELAY-BIT29; CTE_DRAM_INIT-BIT30; PDA_ENUMERATE-BIT31
Mem FlowsExt3	**BFEFFE7A**	Enable(1)/Disable(0) multi steps with BitMask - RCD_DCS_DFE_TRAINING-BIT0; LRDIMM_BACKSIDE_TX_PER_TXN-BIT1; PATTERN_CHECKOUT-BIT2; RX_PER_BIT_DESKEW-BIT3; CA_TIMING_SIMPLE_PATTERN-BIT4; CA_VREF_COMPLEX_PATTERN-BIT5; BUILD_UNUSED_MC_BITMASK-BIT6; TRAINING_RESULT_CHECK-BIT7; RCD_DCS_VREF_TRAINING-BIT8; RD_DQDQS_POST_DFE_LATE-BIT9; DISPLAY_TRAINING_RESULTS-BIT10; MDLL_LDO_CALIBRATION_STEP-BIT11; LDO_DESKEW_CALIBRATION_COMP_STEP-BIT12; LDO_DESKEW_CALIBRATION_DATA_STEP-BIT13; RX_DQS_OFFSET_CALIBRATION_STEP-BIT14; DRAM_INIT-BIT15; CA_TIMING_COMPLEX_PATTERN-BIT16; CC_CLK_RX_OFFSET_CALIBRATION_STEP-BIT17; CHECK_DDRIO_POWER_STATUS-BIT18; RX_VREF_ODT_INIT-BIT19; CPCGC_DQ_SWIZZLE_DISCOVERY-BIT20; RX_DQ_DATA_CALIBRATION_STEP-BIT21; SET_DDRIO_POWER_SAVINGS-BIT22; WRITE_DQS_EQ-BIT23; RX_DQ_COMP_CALIBRATION_STEP-BIT24; INIT_RX_DQS_COMP_RETRAIN-BIT25; LATE_RX_DQS_COMP_RETRAIN-BIT26; ENABLE_RX_RETRAIN-BIT27; RX_DQ_CTLE-BIT28; DDR_MBIST_MPPR-BIT29; RCD_TAP1_COARSE_VREF_CENTERING-BIT30; ENABLE_HOST_REFRESH-BIT31
Mem FlowsExt4	**F8F6FFFF**	Enable(1)/Disable(0) multi steps with BitMask - MDQS_PER_BIT_READ_DELAY-BIT0; PRINT_PERFORMANCE_SETTINGS-BIT1; PRINT_ALL_STAT-BIT2; DIMM_INFO-BIT3; DDR_RESET_LOOP-BIT4; MCR_DATA_CONFIG-BIT5; MEM_SWEEP_TESTER-BIT6; POST_PACKAGE_REPAIR_MAIN-BIT7; RCSIM_CACHE_DDRIO-BIT8; SETUP_SV_LAND_SCRAMBLER-BIT9; SWITCH_TO_CPGC_OUT_OF_ORDER_MODE-BIT10; CTLE_OFFSET_CORRECTION-BIT11;

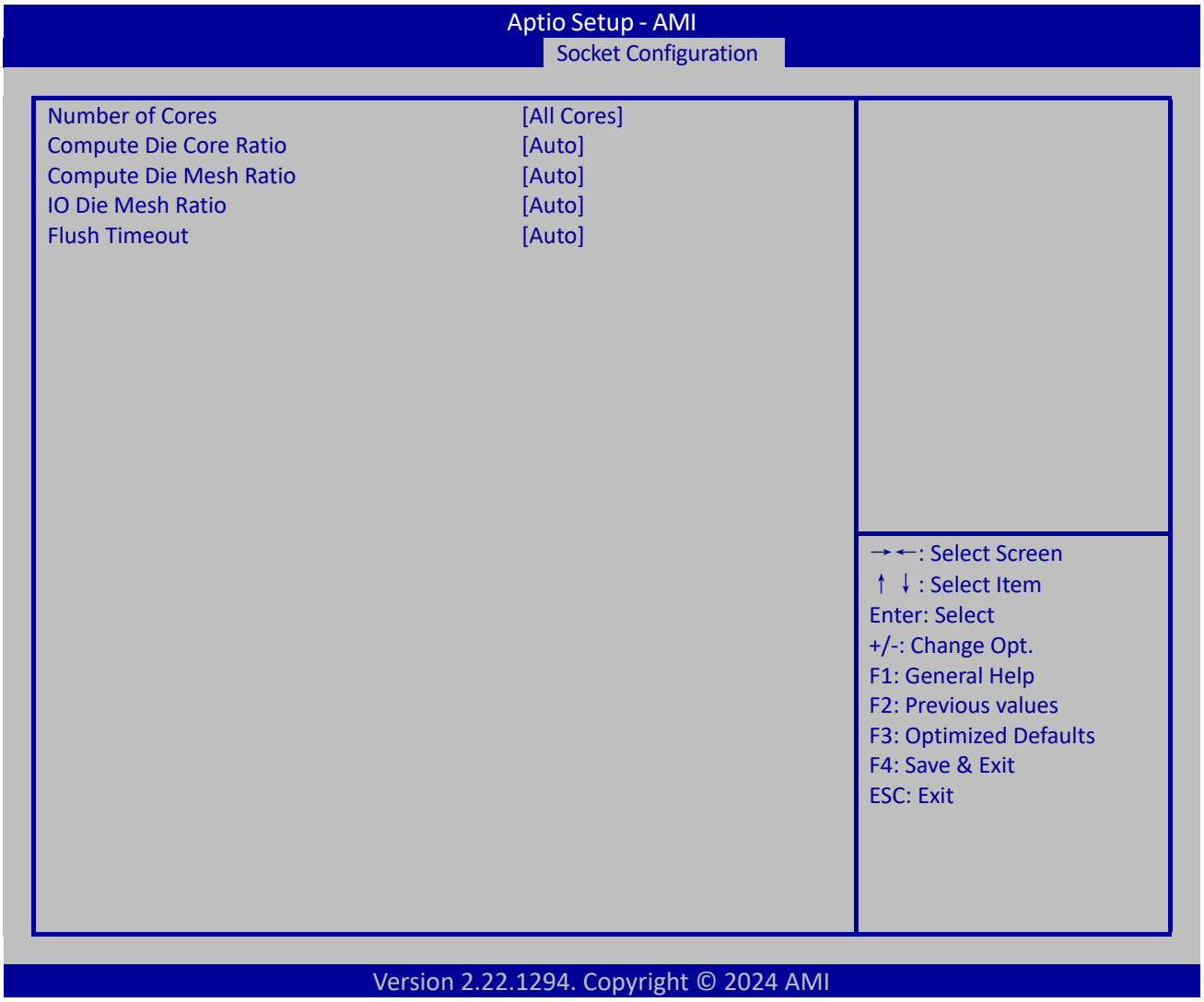
Socket Configuration \ Memory Configuration		
Menu Fields	**Settings**	**Comments**
		RANK_MARGIN_TOOL-BIT12; BOOT_HEALTH_TEST-BIT13; WRITE_DQ_DQS_DFE_EARLY-BIT14; QCSQCA_TRAINING_PREREQ-BIT15; CMD_NORM_EARLY-BIT16; RAS_CHECK_DIMM_RANKS-BIT17; INIT_MC_SERVICE-BIT18; MDQ_PER_BIT_WRITE_DELAY_TRAINING-BIT19; NBIAS_BASED_ANALOG_SETTINGS_ADJUST-BIT20; NBIAS_BASED_RX_DQS_DELAY_ADJUST-BIT21; SENSE_AMP_OPTIMIZATION_TRAINING-BIT22; CTE_CPGD_CADB_TEST-BIT23; DB_DUTYCYCLE_TRAINING-BIT24;MR4_DDR_2XREFRESH-BIT25;MR4_DDR_THROTTLING-BIT26;READ_DQ_DQS_DFE_LATE-BIT27;CA_SCRAMBLE-BIT28;RCD_DCA_TIMING_COMPLEX_AFTER_DFE-BIT29; RCD_DCA_VREF_COMPLEX_LAST-BIT30; RCD_DCA_TIMING_COMPLEX_LAST-BIT31
Cmd Setup % Offset	**50**	Cmd setup / hold percent offset for late cmd training result. The possible values are from 0 to 100
Periodic Rcomp	[Disable] [Enable] **[Auto]**	Anto(2)/Enable(1)/Disable(0) Memory Periodic Rcomp cycles
Training Compensation Options Values	**[One RCOMP cycle only on PHY Init (MMRC Init)]** [One RCOMP cycle after every JEDEC Init] [One RCOMP cycle right before every training step]	Options for issuing a Compensation cycle (RCOMP) at specific points in training
Outlier Check Disable	[Enable] **[Disable]**	Enable(0)/Disable(1) Vendor Specific DIMM Outlier Check And Mapout. Enable means to do the Check and Mapout.
Outlier Threshold Modifier	**0**	How much to modify the base outlier threshold (i.e. -17), to modify -1, enter 101 (threshold will be -18), to modify +1, enter 1 (threshold will be -16)
UEFI Memory Map Special Purpose Memory Flag	**[Enable]** [Disable]	Allow or disallow the SP Memory Flag to be set in the UEFI Memory Map and in the ACPI SRAT table
ACPI SRAT Special Purpose Memory Flag	**[Enable]** [Disable]	Allow or disallow the ACPI SRAT SP Memory Flag to be set when UEFI Memory Map Special Purpose Flag is enabled
Memory Topology	Selects sub-menu.	
Page Policy	Selects sub-menu.	
Memory Training	Selects sub-menu.	
Memory I/O Health Check	Selects sub-menu.	
Memory Map	Selects sub-menu.	
Memory RAS Configuration	Selects sub-menu.	
RMT Configuration Menu	Selects sub-menu.	

6.4.4.1 Adv MemTest Rank Selection



Socket Configuration \ Memory Configuration \ Adv MemTest Rank Selection		
Menu Fields	**Settings**	**Comments**
Number of Ranks to Test	**0**	Select how many Ranks will be tested by AdvMemTest. Maximum of 8 Ranks are allowed. Value of 0 will test all present Ranks in the system.

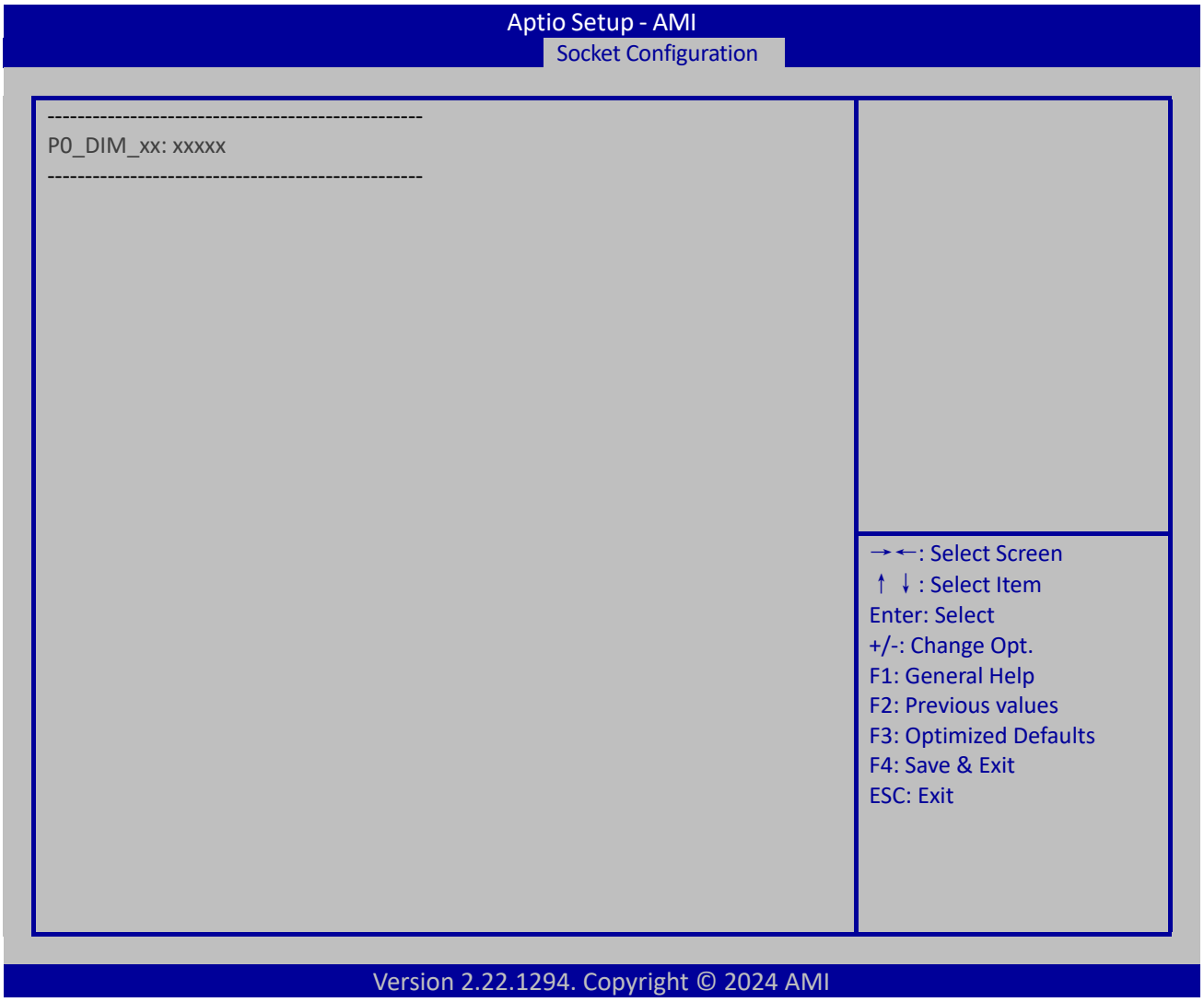
6.4.4.2 fADR Configuration



Socket Configuration \ Memory Configuration \ Adv MemTest Rank Selection		
Menu Fields	**Settings**	**Comments**
Number of Cores	[1 Core] [4 Cores] **[Auto]**	Number of cores to be used to flush CPU Cache
Compute Die Core Ratio	**[Auto]** [Manual]	Compute Die Core Ratio to be used during an ADR event: Auto - Compute Die Core Ratio set to Core/IA P1 ratio; Manual - Compute Die Core Ratio set to user requested value
Compute Die Core Ratio Value	**FF**	Compute Die Core Ratio to be used during an ADR event
Compute Die Mesh Ratio	**[Auto]** [Manual]	Compute Die Mesh Ratio to be used during an ADR event: Auto - Compute Die Mesh Ratio set to Mesh/CLM P1 ratio; Manual - Compute Die Mesh Ratio set to user requested value
Compute Die Mesh Ratio Value	**FF**	Compute Die Mesh Ratio to be used during an ADR event
IO Die Mesh Ratio	**[Auto]** [Manual]	IO Die Mesh Ratio to be used during an ADR event: Auto - Compute Die Mesh Ratio set to Mesh/CLM P1 ratio; Manual - Compute Die Mesh Ratio set to user requested value

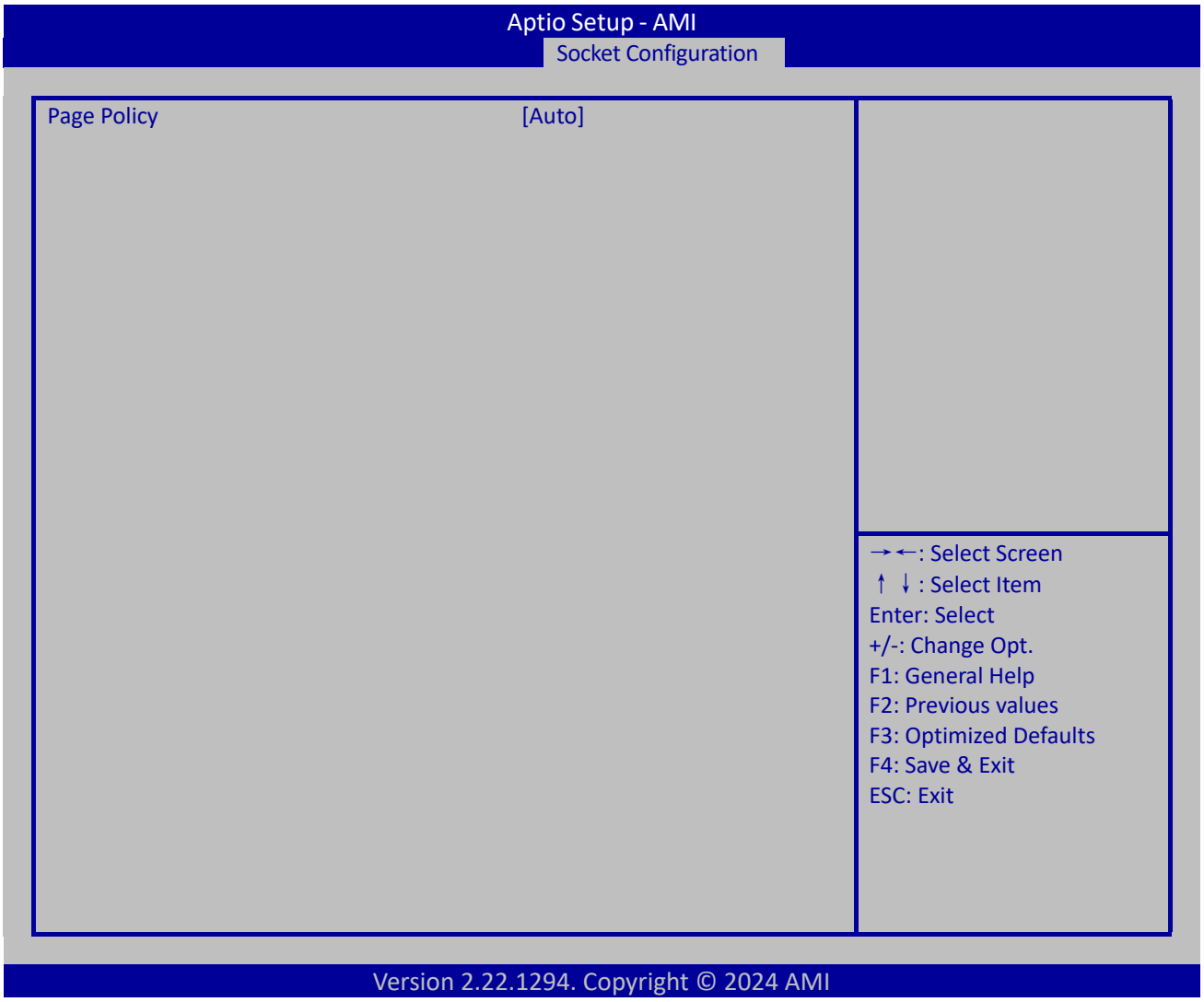
Socket Configuration \ Memory Configuration \ Adv MemTest Rank Selection		
Menu Fields	**Settings**	**Comments**
IO Die Mesh Ratio Value	**FF**	IO Die Mesh Ratio to be used during an ADR event
Flush Timeout	**[Auto]** [Manual]	Flush Timeout value to be used during an ADR event: Auto - Flush Timeout scales to the number of enabled sockets (i.e. 1 socket - 1 sec, 2 sockets 2 sec, 4 sockets - 4 secs); Manual - Flush Timeout set to user requested value
Flush Timeout Value	**FFF**	Specifies flush timeout value in 1sec units (0 value disables timeout)

6.4.4.3 Memory Topology



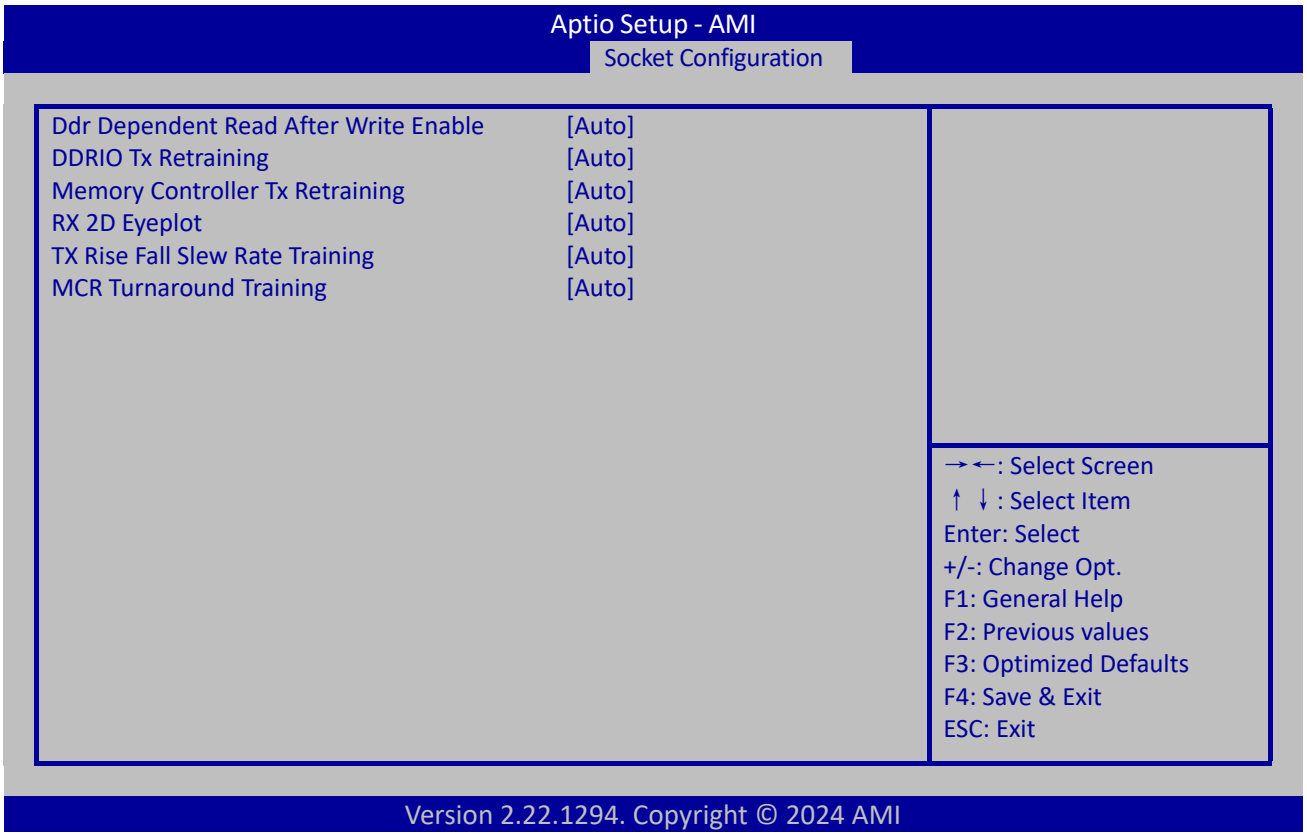
Socket Configuration \ Memory Configuration \ Memory Topology		
Menu Fields	**Settings**	**Comments**
P0_DIM_xx:	xxxxx	Displays the memory information.

6.4.4.4 Page Policy



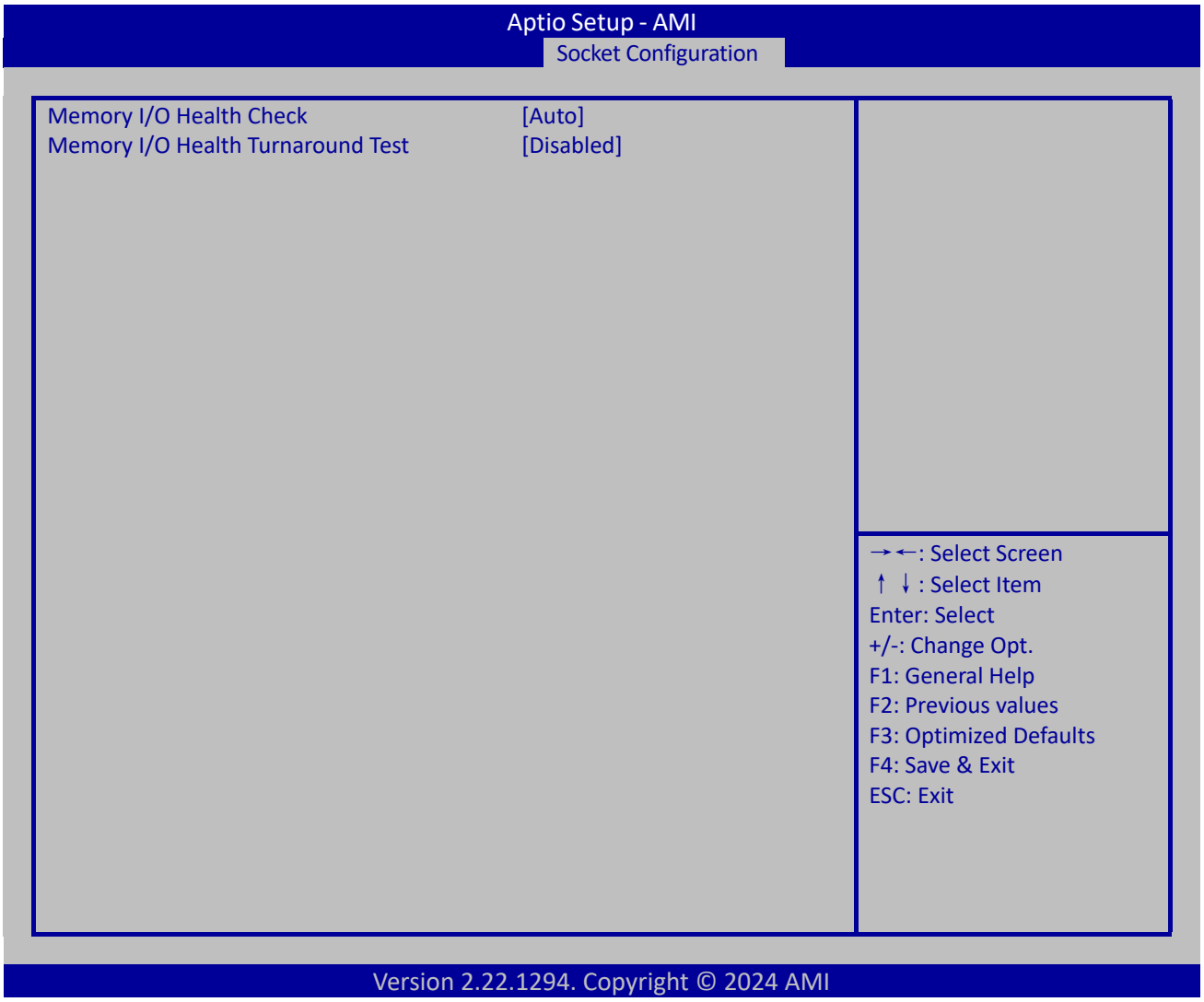
Socket Configuration \ Memory Configuration \ Page Policy		
Menu Fields	**Settings**	**Comments**
Page Policy	**[Auto]** [Closed] [Adaptive]	Select DRAM Page Policy

6.4.4.5 Memory Training



Socket Configuration \ Memory Configuration \ Memory Training		
Menu Fields	**Settings**	**Comments**
Ddr Dependent Read After Write Enable	[Disable] [Enable] **[Auto]**	Enable/Disable Ddr Dependent Read after writes
DDRIO Tx Retraining	[Disable] [Enable] **[Auto]**	Enable/Disable DDRIO Txrt_en retraining bit
Memory Controller Tx Retraining	[Disable] [Enable] **[Auto]**	Enable/Disable MC pdc_dqs_en register bit
RX 2D Eyeplot	[Disable] [Enable] **[Auto]**	Enable/Disable RX 2D Eyeplot bit
TX Rise Fall Slew Rate Training	[Disable] [Enable] **[Auto]**	Enable/Disable TX Rise Fall Slew Rate Training. Auto = dynamically selected. Enable or Disable will control TXRFSR regardless of frequency
MCR Turnaround Training	[Disable] [Enable] **[Auto]**	Enable/Disable MCR Turnaround Training

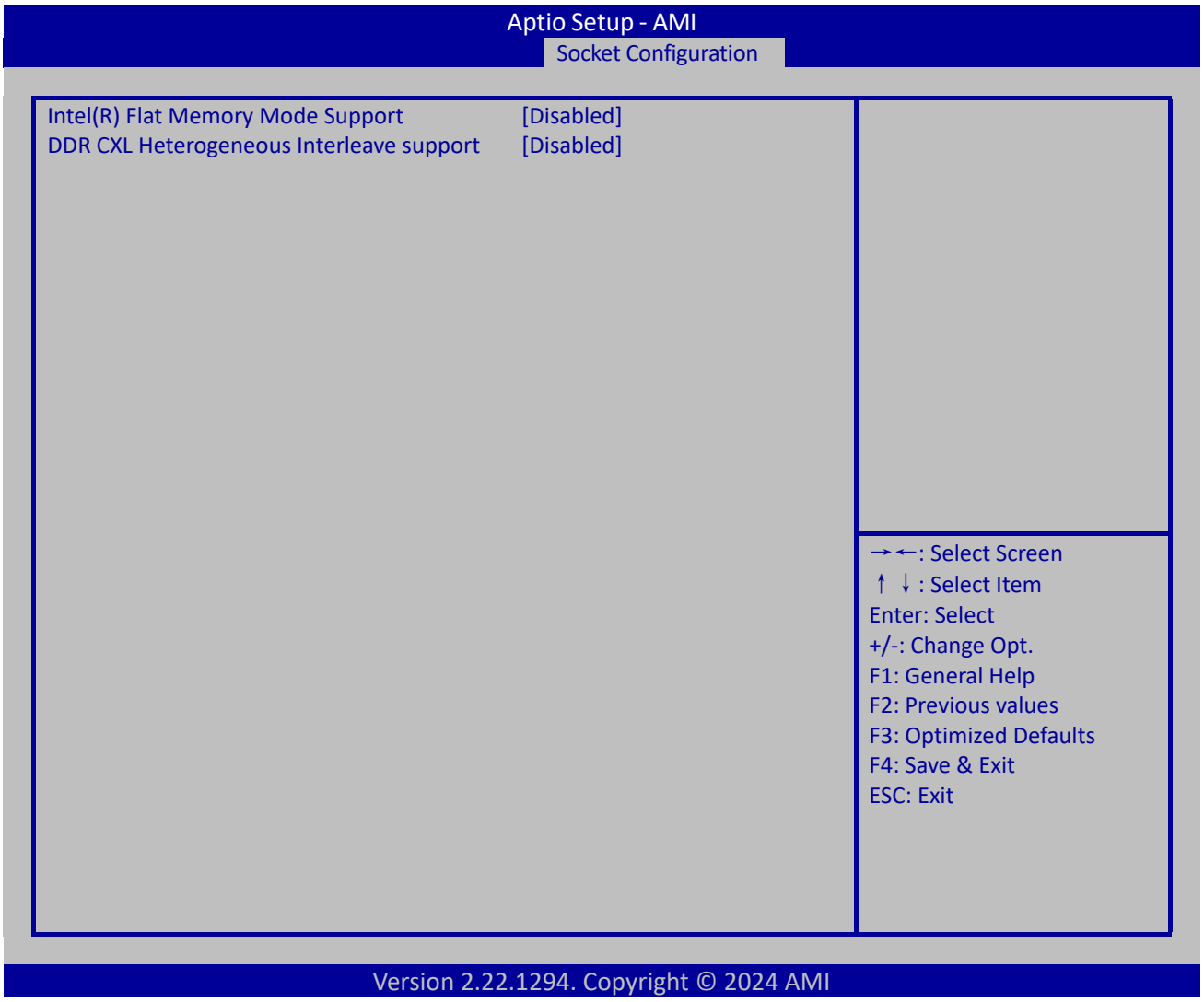
6.4.4.6 Memory I/O Health Check



Socket Configuration \ Memory Configuration \ Memory I/O Health Check		
Menu Fields	**Settings**	**Comments**
Memory I/O Health Check	**[Auto]** [Manual] [Disable]	Select option Auto for default values. Manual for new values. Disable for disabling feature
Memory I/O Health Turnaround Test	**[Disabled]** [Enabled]	Select option Disable for disabling feature. Enable for enabling feature
Reboot On Critical Failure	[Disable] **[Enable]**	Reboot System on Critical failure to do Memory Training
Memory I/O Health Check Critical Retries	**1**	Set the number of reboots/retrains for when I/O Health Check encounters a critical error. Valid range is 0-7
Memory I/O Health Check Loop Count	**0**	(0-AUTO) CPGC Test Loop Count for Memory IO Health Test
Telemetry Offsets		
TxDqDelay Left Edge	**5**	Offset for TxDqDelay Left Edge
TxDqDelay Right Edge	**5**	Offset for TxDqDelay Right Edge

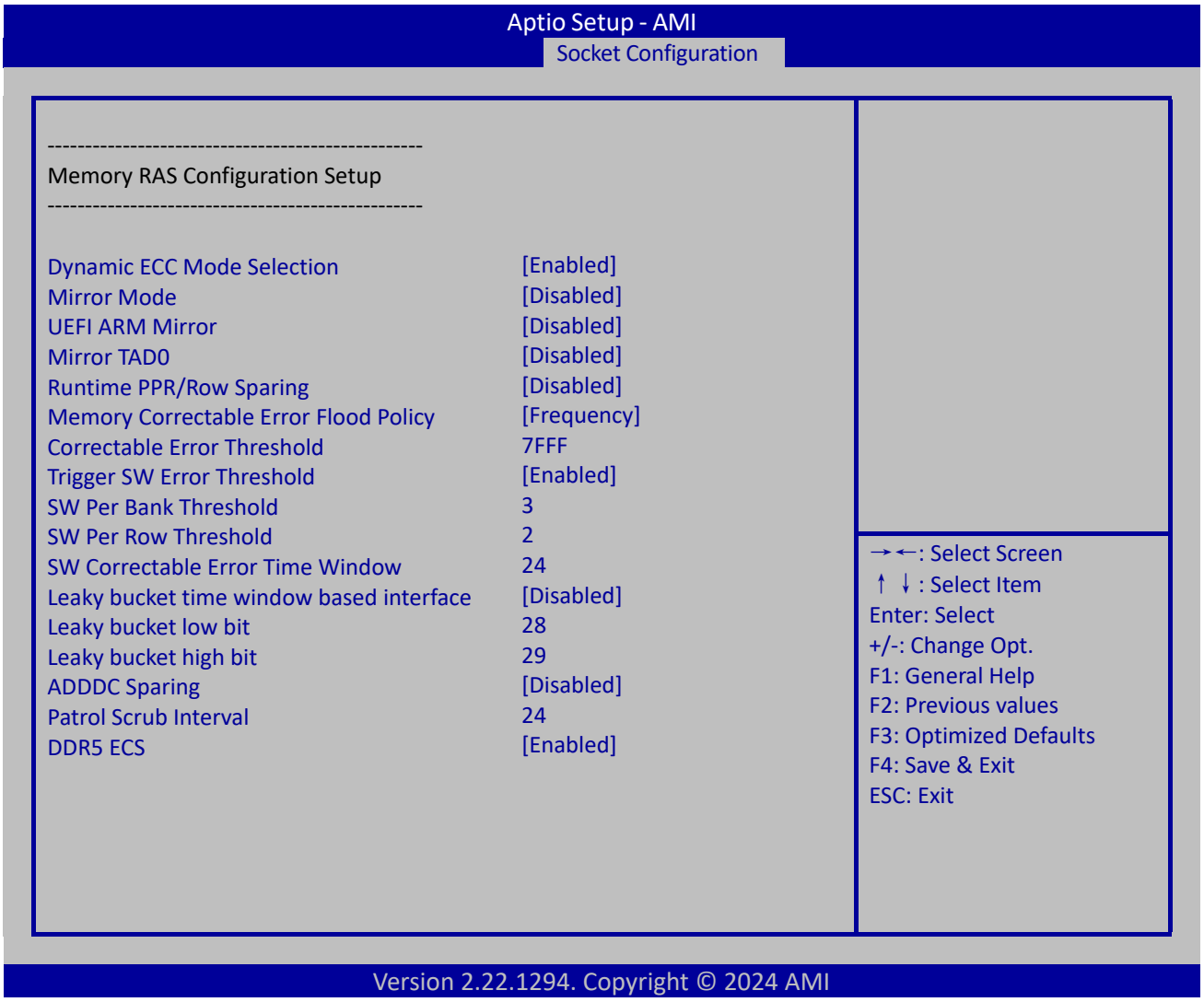
Socket Configuration \ Memory Configuration \ Memory I/O Health Check		
Menu Fields	**Settings**	**Comments**
TxVref Left Edge	**5**	Offset for TxVref Left Edge
TxVref Right Edge	**5**	Offset for TxVref Right Edge
RxDqsDelay Left Edge	**5**	Offset for RxDqsDelay Left Edge
RxDqsDelay Right Edge	**5**	Offset for RxDqsDelay Right Edge
RxVref Left Edge	**5**	Offset for RxVref Left Edge
RxVref Right Edge	**5**	Offset for RxVref Right Edge
Critical Offsets		
TxDqDelay Left Edge	**3**	Offset for TxDqDelay Left Edge
TxDqDelay Right Edge	**3**	Offset for TxDqDelay Right Edge
TxVref Left Edge	**4**	Offset for TxVref Left Edge
TxVref Right Edge	**3**	Offset for TxVref Right Edge
RxDqsDelay Left Edge	**3**	Offset for RxDqsDelay Left Edge
RxDqsDelay Right Edge	**3**	Offset for RxDqsDelay Right Edge
RxVref Left Edge	**4**	Offset for RxVref Left Edge
RxVref Right Edge	**4**	Offset for RxVref Right Edge

6.4.4.7 Memory Map



Socket Configuration \ Memory Configuration \ Memory Map		
Menu Fields	**Settings**	**Comments**
Intel(R) Flat Memory Mode Support	**[Disabled]** [Enabled]	Enable or disable Intel(R) Flat Memory Mode support
DDR CXL Heterogeneous Interleave support	[Enabled] **[Disabled]**	Enables DDR CXL Heterogeneous Interleave support

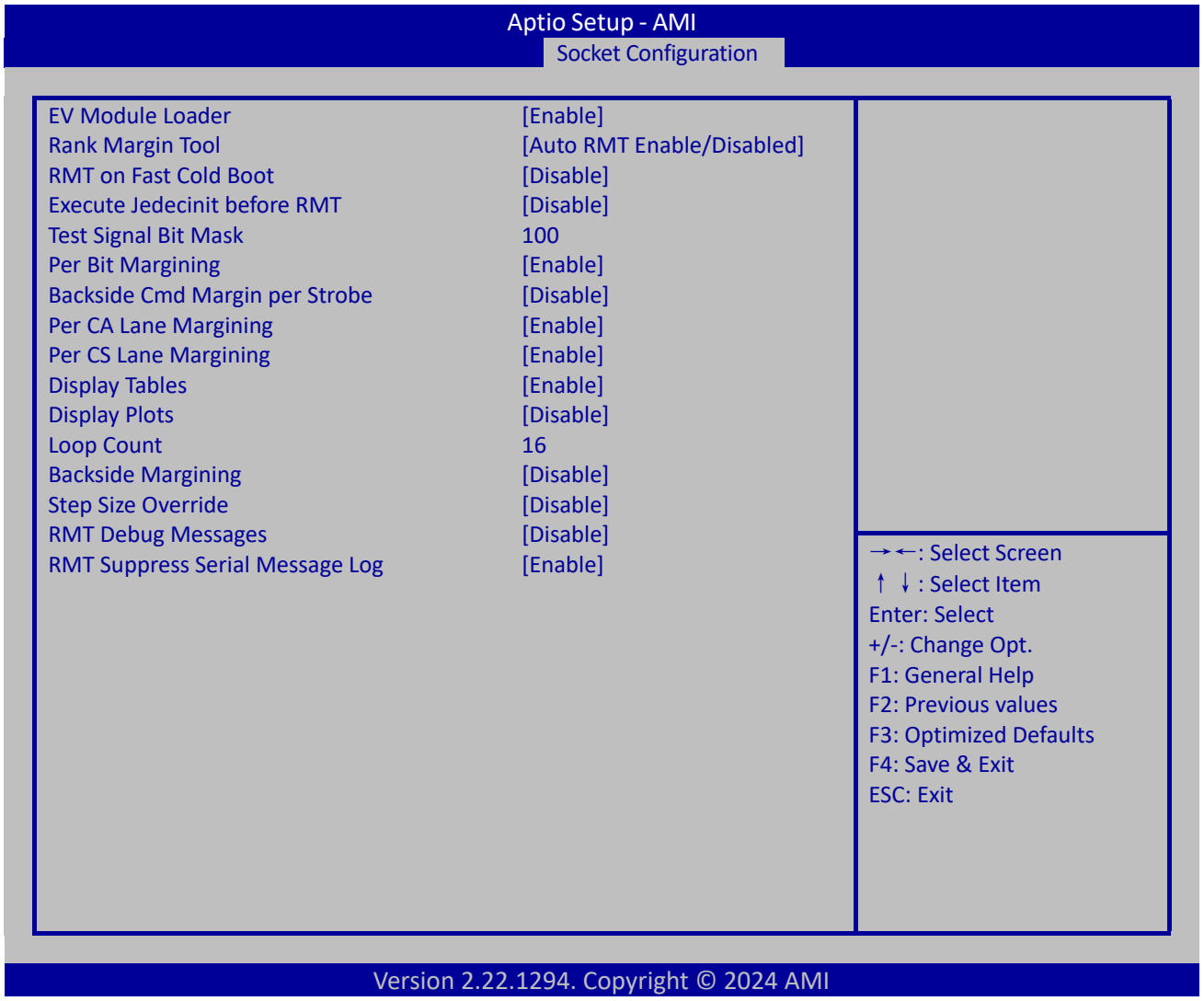
6.4.4.8 Memory RAS Configuration



Socket Configuration \ Memory Configuration \ Memory RAS Configuration		
Menu Fields	**Settings**	**Comments**
Dynamic ECC Mode Selection	[Disabled] **[Enabled]**	Enable/Disable Dynamic ECC Mode Selection
Mirror Mode	**[Disabled]** [Full Mirror Mode]	Full Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable XPT Prefetch.
UEFI ARM Mirror	**[Disabled]** [Enabled]	Imitate behavior of UEFI based Address Range Mirror with setup option
Mirror TAD0	[Enabled] **[Disabled]**	Enable Mirror on entire memory for TAD0
ARM Mirror percentage	**2500**	Enter the percentage to be mirrored in basis points. Mirror options are 10%, 15%, 20%,

Socket Configuration \ Memory Configuration \ Memory RAS Configuration		
Menu Fields	**Settings**	**Comments**
		25%, 30%, 35%, 40%. 25% is represented 2500. Any other number entered will be rounded to nearest greater number, for ex. number > 2000 and <=2500 will be rounded to 2500. And Any number > 4000, will be rounded to 4000
Runtime PPR/Row Sparing	**[Disabled]** [Enabled]	Enable/Disable Runtime PPR / Row Sparing. This feature is disabled for GNR-A and GNRD-A Steppings
Memory Correctable Error Flood Policy	[Disable] [Once] **[Frequency]**	[Disabled] Don't deal with Memory CE flood. [Once] Only First Memory CE will trigger SMI, and BIOS will disable silicon SMI. [Frequency] Disable SMI when Memory CE reach threshold within time limits.
Correctable Error Threshold	**7FFF**	Correctable Error Threshold (0x01 - 0x7fff) used for sparing, and leaky bucket
Trigger SW Error Threshold	[Disabled] **[Enabled]**	Enable or Disable Sparing trigger SW Error Match Threshold
SW Per Bank Threshold	**3**	SW Per Bank Correctable Error Threshold (1 - 0x7FFF) used for bank level error
SW Per Row Threshold	**2**	SW Per Row Correctable Error Threshold (1 - 0x7FFF) used for row level error
SW Correctable Error Time Window	**24**	Sw Correctable Error time window based interface in Hour (0 - 24)
Leaky bucket time window based interface	**[Disabled]** [Enabled]	Enable/Disable leaky bucket time window based interface
Leaky bucket time window based interface Hour	**24**	Leaky bucket time window based interface Hour" (0 - 24)
Leaky bucket time window based interface Minute	**0**	Leaky bucket time window based interface Minute" (0 - 60)
Leaky bucket low bit	**28**	Leaky bucket low bit" (0x1 - 0x29)
Leaky bucket high bit	**29**	Leaky bucket high bit" (0x1 - 0x29)
ADDDC Sparing	**[Disabled]** [Enabled]	Enable/Disable ADDDC Sparing (ADDDC will be disabled if Mirroring is enabled)
Enable ADDDC Error Injection	[Disabled] **[Enabled]**	Enable/Disable ADDDC error injection. This requires to force the interleave granularity to 64B for B/L step parts
Patrol Scrub Interval	**24**	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto!
DDR5 ECS	[Disabled] **[Enabled]** [Enable ECS with Result Collection]	Disable: Disable ECS/Result collection. Enable: Enable ECS without Result Collection. Enable ECS with Result Collection: Enable ECS/Result Collection.

6.4.4.9 RMT Configuration Menu

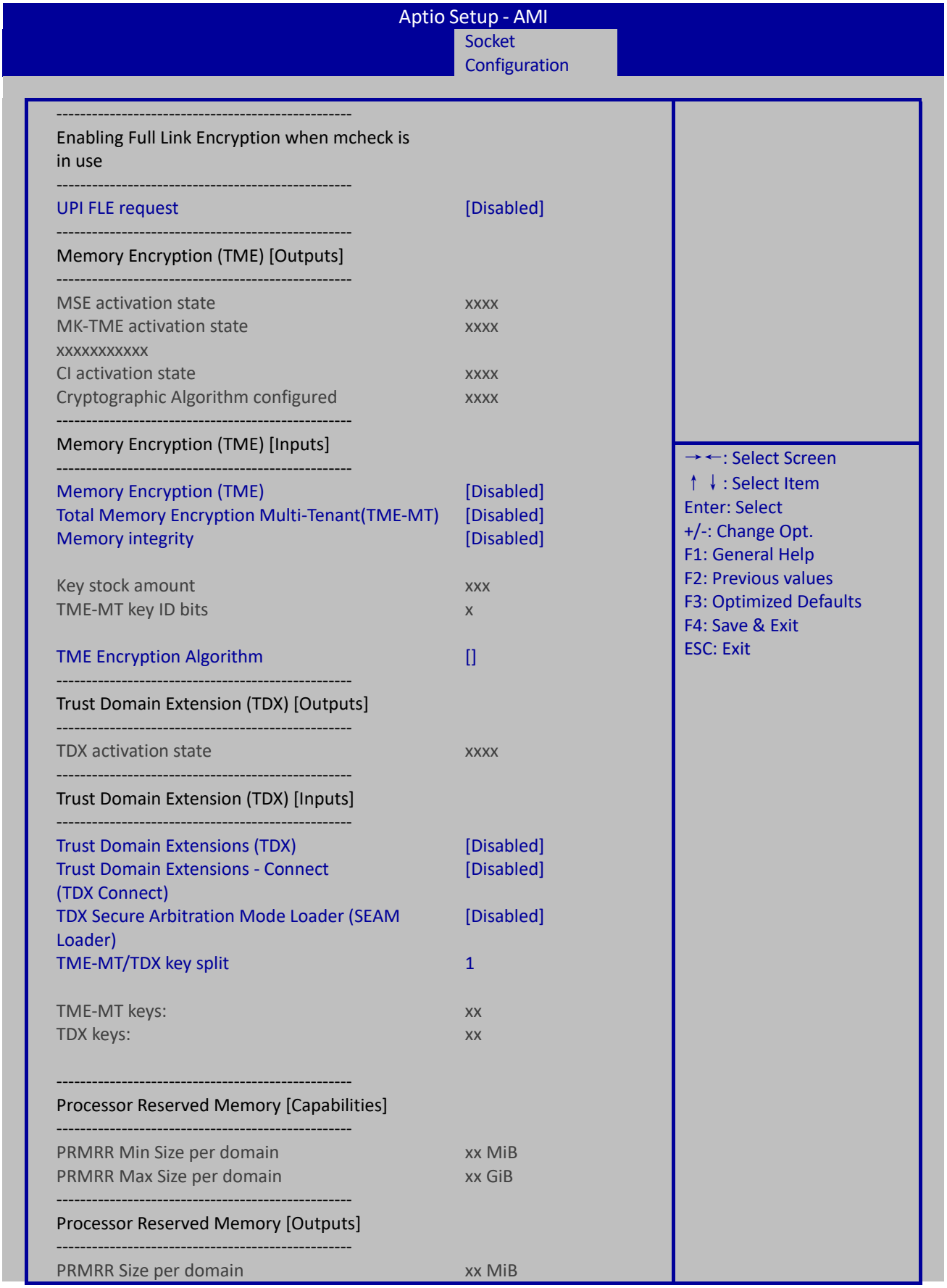


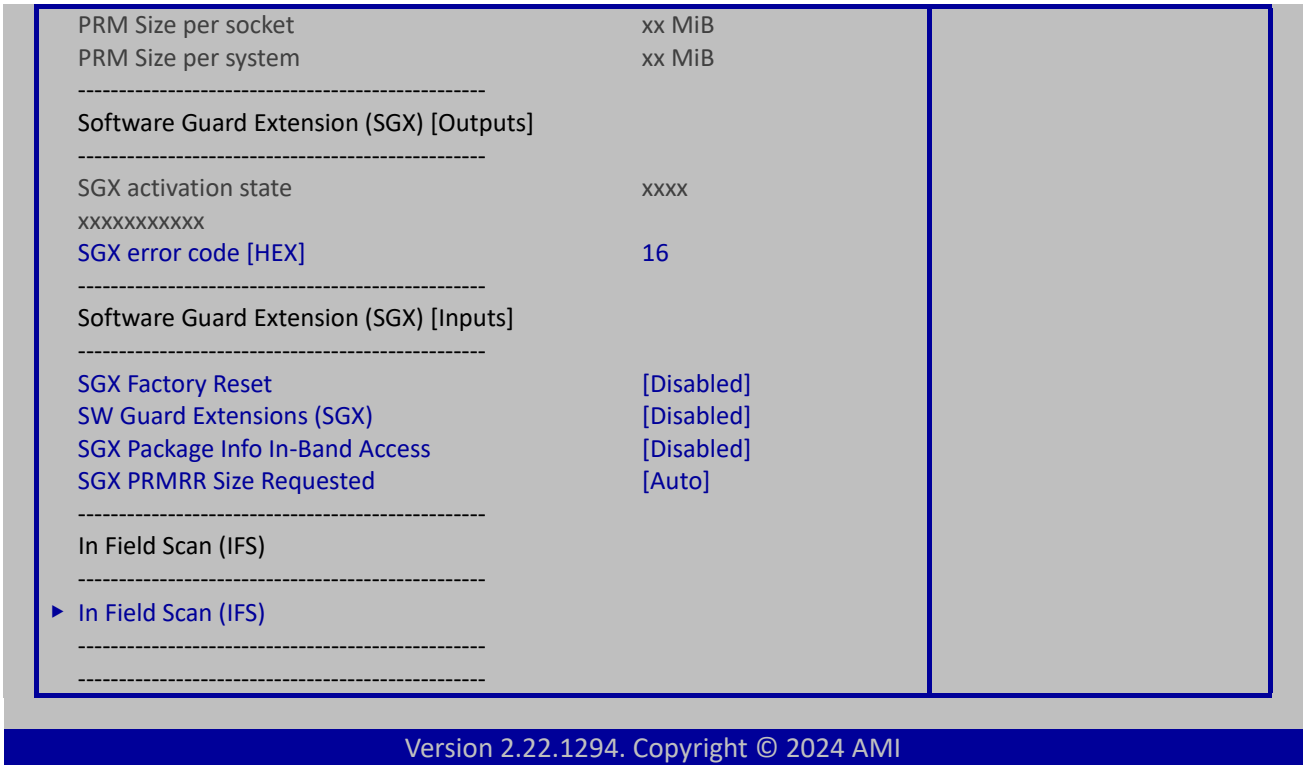
Socket Configuration \ Memory Configuration \ RMT Configuration Menu		
Menu Fields	**Settings**	**Comments**
EV Module Loader	**[Enable]** [Disable]	Enables loading the EV test module
Rank Margin Tool	[Normal RMT & Turnaround RMT Disabled] [Normal RMT Enabled] [Turnaround RMT Enabled] [Normal RMT & Turnaround RMT Enabled] **[Auto RMT Enable/Disabled]**	Enables/disables two types of RMT independently
RMT on Fast Cold Boot	[Enable] **[Disable]**	Enable/Disable the Rank Margin Tool on a Fast Cold Boot
Execute Jedecinit before RMT	[Enable] **[Disable]**	Execute Jedecinit before Rank Margin Tool. NOTE: JedecInit is always executed when RMTBacksideMargining is enabled
Test Signal Bit Mask	**100**	1 means skipping test. Frontside[RxDqsDelay:bit0,TxDqDelay:bit1,

Socket Configuration \ Memory Configuration \ RMT Configuration Menu		
Menu Fields	**Settings**	**Comments**
		RxSamplerEvenOdd (RxSamplerEven/RxSamplerOdd/RxVref):bit2, TxVref:bit3, DbDfeVrefGroup:bit4,DcaDelay:bit5, RcdDcaVref:bit6,DcsDelay:bit7,DcaDfeVref:bit8, DcaSamplerEvenOdd:bit9,CaDelay:bit10, CsDelay:bit11,UdimmCaVref:bit12, UdimmCsVref:bit13]; Backside[RxDqsDelay:bit16, TxDqDelay:bit17,RxVref:bit18, TxVref:bit19, QcaDelay:bit21,DramCaVref:bit22,QcsDelay:bit23, DramCsVref:bit24,BcomDelay:bit26,BcomVref:bit27].
Per Bit Margining	**[Enable]** [Disable]	Enable Per Bit Margining
Backside Cmd Margin per Strobe	[Enable] **[Disable]**	Enable Backside Cmd Margin per Strobe
Per CA Lane Margining	**[Enable]** [Disable]	Enable Per CA Lane Margining
Per CS Lane Margining	**[Enable]** [Disable]	Enable Per CS Lane Margining
Display Tables	**[Enable]** [Disable]	Enable displaying results as tables
Display Plots	[Enable] **[Disable]**	Enable the display of per-bit results as plots
Loop Count	**16**	Exponential loop count for single rank test
Backside Margining	[Enable] **[Disable]**	Enable margin test on the register or buffer backside
Step Size Override	[Enable] **[Disable]**	Enable overriding the default step sizes
RxDqs	**[1]** [2] [4] [8]	Step size of RxDqs. Auto: 1. Supported values: 1,2,4,8
RxVref	**[1]** [2] [4] [8]	Step size of RxVref. Auto: 1. Supported values: 1,2,4,8
TxDq	**[1]** [2] [4] [8]	Step size of TxDqs. Auto: 1. Supported values: 1,2,4,8
TxVref	**[1]** [2] [4] [8]	Step size of TxVref. Auto: 1. Supported values: 1,2,4,8
CmdAll	**[1]** [2] [4] [8]	Step size of CmdAll. Auto: 1. Supported values: 1,2,4,8
CmdVref	**[1]** [2] [4] [8]	Step size of CmdVref. Auto: 1. Supported values: 1,2,4,8
CtlAll	**[1]** [2]	Step size of CtlAll. Auto: 1. Supported values: 1,2,4,8

Socket Configuration \ Memory Configuration \ RMT Configuration Menu		
Menu Fields	**Settings**	**Comments**
	[4] [8]	
RMT Debug Messages	[Enable] **[Disable]**	Enables the RMT debug messages
RMT Suppress Serial Message Log	**[Enable]** [Disable]	Suppress the serial message to only output error message when running RMT

6.4.5 Security Configuration

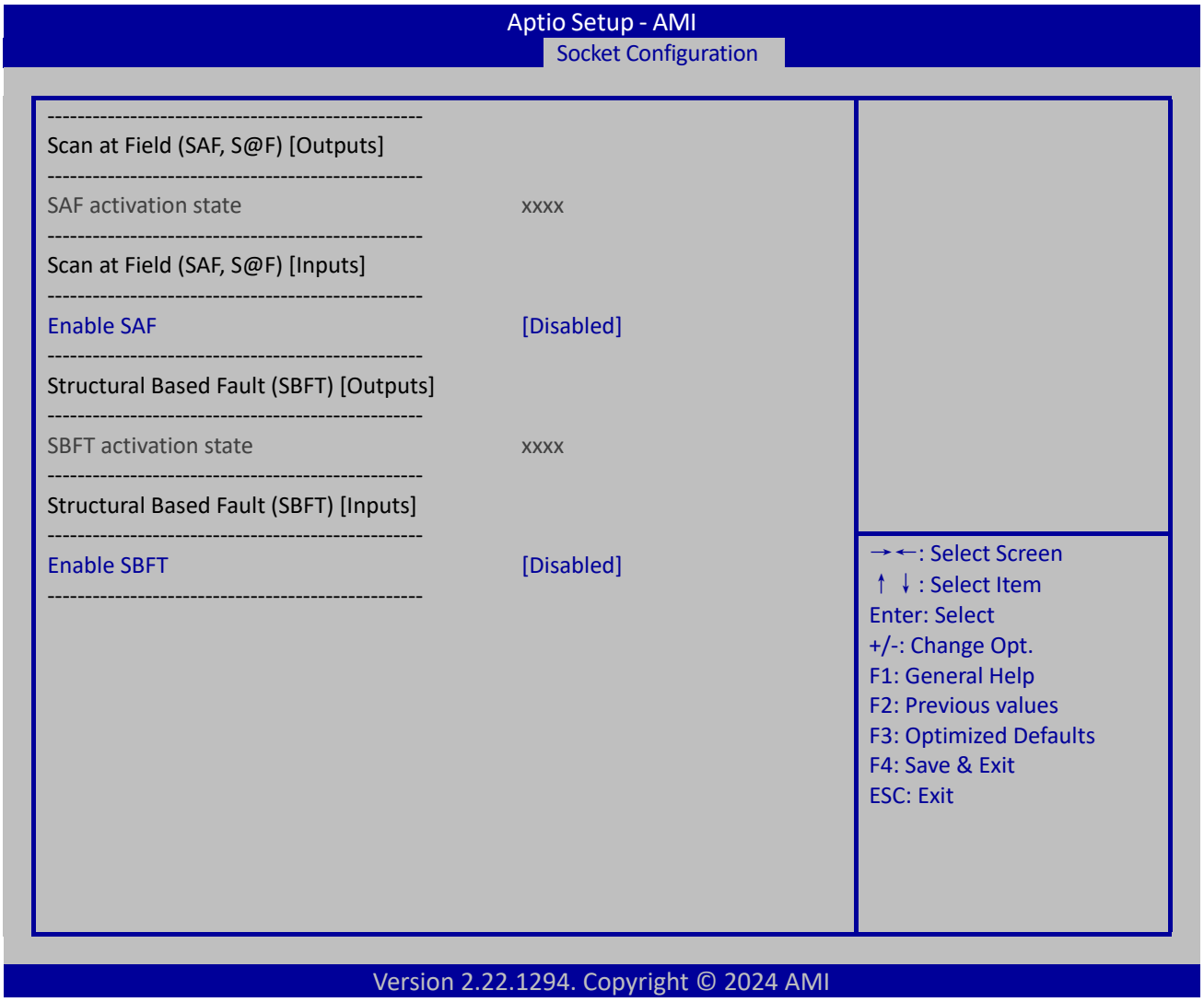




Socket Configuration \ Security Configuration		
Menu Fields	**Settings**	**Comments**
Enabling Full Link Encryption when mcheck is in use		
UPI FLE request	**[Disabled]** [Enabled]	UPI FLE if requested will be enabled whenever mcheck will be launched (when SGX, SAF, TDX or other technologies are enabled)
Memory Encryption (TME) [Outputs]		
MSE activation state	xxxx	Indicates if Memory Security Engine is active/inactive in current boot.
MK-TME activation state	xxxx	Indicates if Multi Key Total Memory Encryption is active/inactive in current boot.
xxxxxxxxxxx		Displays the TME or MSE status.
CI activation state	xxxx	Indicates if cryptographic integrity was activated. If crypto integrity is disabled, logical integrity was activated
Cryptographic Algorithm configured	xxxx	Indicates what cryptografic algorithm is configured in current boot.
Memory Encryption (TME) [Inputs]		
Memory Encryption (TME)	**[Disabled]** [Enabled]	Enable/Disable Memory Encryption (TME)
Total Memory Encryption Multi-Tenant (TME-MT)	**[Disabled]** [Enabled]	Enable/Disable Total Memory Encryption - Multi-Tenant (TME-MT). Can be enabled only if Socket Configuration -> Processor Configuration -> Limit CPU PA to 46 bits = Disable
Memory integrity	**[Disabled]** [Enabled]	Enable/Disable memory Integrity
Key stock amount	xxx	Total number of keys that can be used by TME-MT.
TME-MT key ID bits	x	Total number of bits that can be used by TME-MT.

Socket Configuration \ Security Configuration		
Menu Fields	**Settings**	**Comments**
TME Encryption Algorithm	[AES-XTS-128] **[AES-XTS-256]**	Choose Encryption Algorithm to be used for Total Memory Encryption (TME) ***NOTE: This item options will be changed based on different CPU.***
Trust Domain Extension (TDX) [Outputs]		
TDX activation state	xxxx	Indicates if TDX is active/inactive in current boot.
Trust Domain Extension (TDX) [Inputs]		
Trust Domain Extensions (TDX)	**[Disabled]** [Enabled]	Enable/Disable Trust Domain Extensions (TDX)
Trust Domain Extensions - Connect (TDX Connect)	**[Disabled]** [Enabled]	Enable/Disable Trust Domain Extensions - Connect (TDX Connect)
TDX Secure Arbitration Mode Loader (SEAM Loader)	**[Disabled]** [Enabled]	Enable/Disable TDX Secure Arbitration Mode Loader (SEAM Loader)
TME-MT/TDX key split	**1**	Designate number of bits for TDX usage. The rest will be used by TME-MT.
TME-MT keys:	xx	Current (KMK) Number of keys designated for TME-MT usage. Reboot need to recalculate keys after change MMIO Base and/or Size
TDX keys:	xx	Current (KTD) Number of keys designated for TDX usage. Reboot need to recalculate keys after change MMIO Base and/or Size
Processor Reserved Memory [Capabilities]		
PRMRR Min Size per domain	xx MiB	Current PRMRR minimum size per domain. Reboot to update.
PRMRR Max Size per domain	xx GiB	Current PRMRR maximum size per domain. Reboot to update.
Processor Reserved Memory [Outputs]		
PRMRR Size per domain	xx MiB	PRMRR size per domain. Reboot or change any security technology PRMRR size to update.
PRM Size per socket	xx MiB	Sum of domain PRM sizes in a socket. Reboot or change any security technology PRMRR size to update.
PRM Size per system	xx MiB	Sum of socket PRM sizes in system. Reboot or change any security technology PRMRR size to update.
Software Guard Extension (SGX) [Outputs]		
SGX activation state	xxxx	Indicates if SGX is active/inactive in current boot.
xxxxxxxxxxx		Displays the SGX status.
SGX error code [HEX]	**16**	Shows hexadecimal SGX internal error code
Software Guard Extension (SGX) [Inputs]		
SGX Factory Reset	**[Disabled]** [Enabled]	Perform SGX Factory Reset, on subsequent boot: delete all registration data, if SGX enabled will force Initial Platform Establishment flow.
SW Guard Extensions (SGX)	**[Disabled]** [Enabled]	Enable/Disable Software Guard Extensions (SGX)
SGX Package Info In-Band Access	**[Disabled]** [Enabled]	Enable/Disable Software Guard Extensions (SGX) Package Info In-Band Access
SGX PRMRR Size Requested	**[Auto]**	SGX PRMRR Size per domain
In Field Scan (IFS)	Selects sub-menu.	

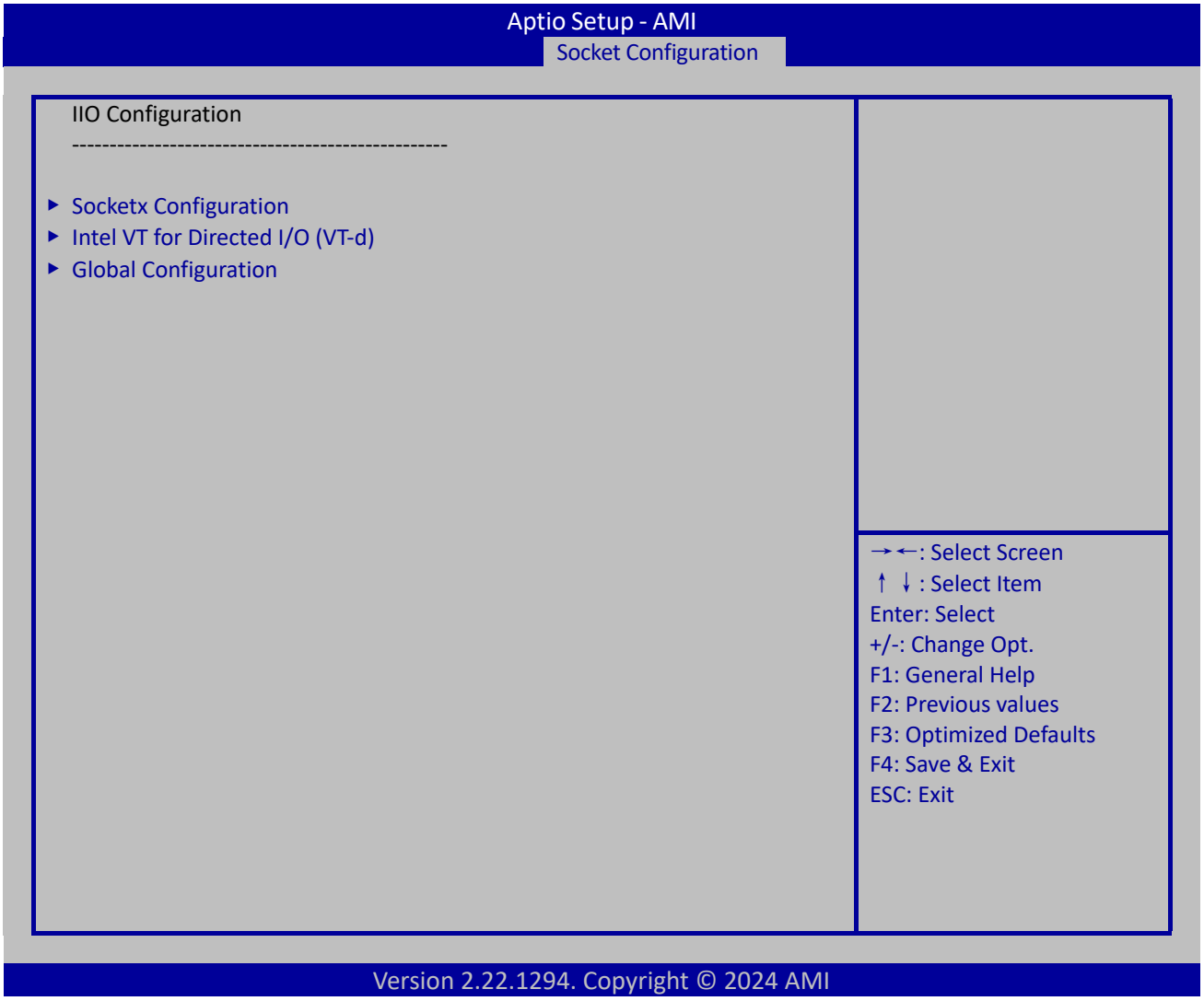
6.4.5.1 In Field Scan (IFS)



Socket Configuration \ Security Configuration \ In Field Scan (IFS)		
Menu Fields	**Settings**	**Comments**
Scan at Field (SAF, S@F) [Outputs]		
SAF activation state	xxxx	Indicates if SAF is enabled/disabled in current boot.
Scan at Field (SAF, S@F) [Inputs]		
Enable SAF	**[Disabled]** [Enabled]	Enable/Disable Scan At Field (SAF)
SAF PRMRR Size Requested	**[128M]** [256M]	Set SAF size region inside of PRM - just a constituent that may not be equal to the total PRM size ***NOTE: This item options will be changed based on different CPU.***
Structural Based Fault (SBFT) [Outputs]		
SBFT activation state	xxxx	Indicates if SBFT was enabled/disabled in current boot.
Structural Based Fault (SBFT) [Inputs]		
Enable SBFT	**[Disabled]**	Enable/Disable Structural Based Fault Test (SBFT) Support.

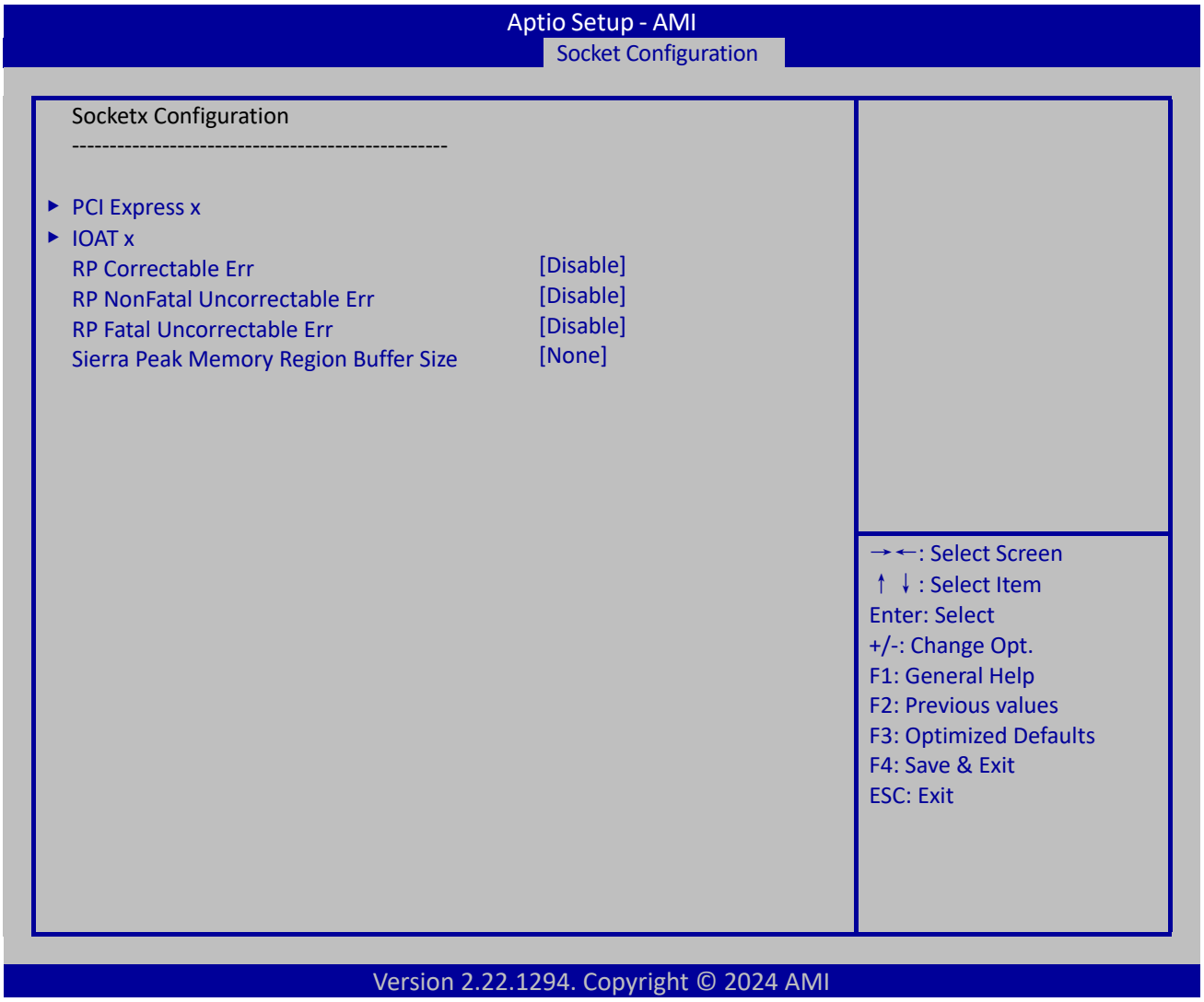
Socket Configuration \ Security Configuration \ In Field Scan (IFS)		
Menu Fields	**Settings**	**Comments**
	[Enable SBFT and SGX] [Enabled]	To enable/disable feature please go to Processor DFX menu.
SBFT PRMRR Size Requested	**[256M]** [512M]	Set SBFT size region inside of PRM - just a constituent that may not be equal to the total PRM size ***NOTE: This item options will be changed based on different CPU.***

6.4.6 IIO Configuration



Socket Configuration \ IIO Configuration		
Menu Fields	**Settings**	**Comments**
Socketx Configuration	Selects sub-menu.	
Intel VT for Directed I/O (VT-d)	Selects sub-menu.	
Global Configuration	Selects sub-menu.	

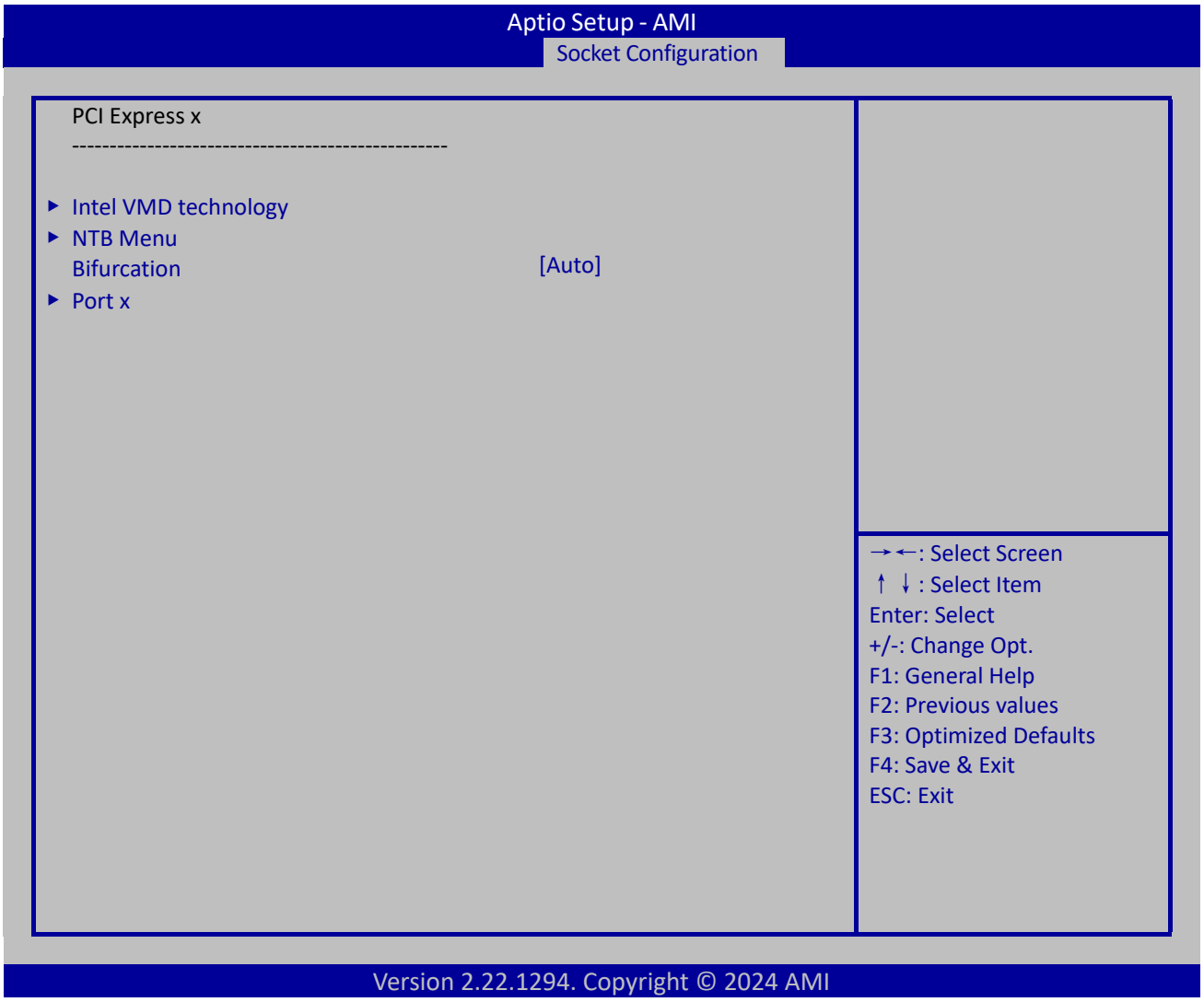
6.4.6.1 Socketx Configuration



Socket Configuration \ IIO Configuration \ Socketx Configuration		
Menu Fields	**Settings**	**Comments**
Socketx Configuration		
PCI Express x	Selects sub-menu.	
IOAT x	Selects sub-menu.	
RP Correctable Err	**[Disable]** [Enable]	Applies to root ports only. Enable interrupt on correctable errors
RP NonFatal Uncorrectable Err	**[Disable]** [Enable]	Applies to root ports only. Enable interrupt on a non-fatal error
RP Fatal Uncorrectable Err	**[Disable]** [Enable]	Applies to root ports only. Enable interrupt on fatal errors.
Sierra Peak Memory Region Buffer Size	**[None]** [1MB] [8MB] [64MB] [128MB] [256MB]	Select size of memory buffer for each single Sierra Peak instance

Socket Configuration \ IIO Configuration \ Socketx Configuration		
Menu Fields	**Settings**	**Comments**
	[512MB] [1GB] [2GB] [4GB] [8GB]	

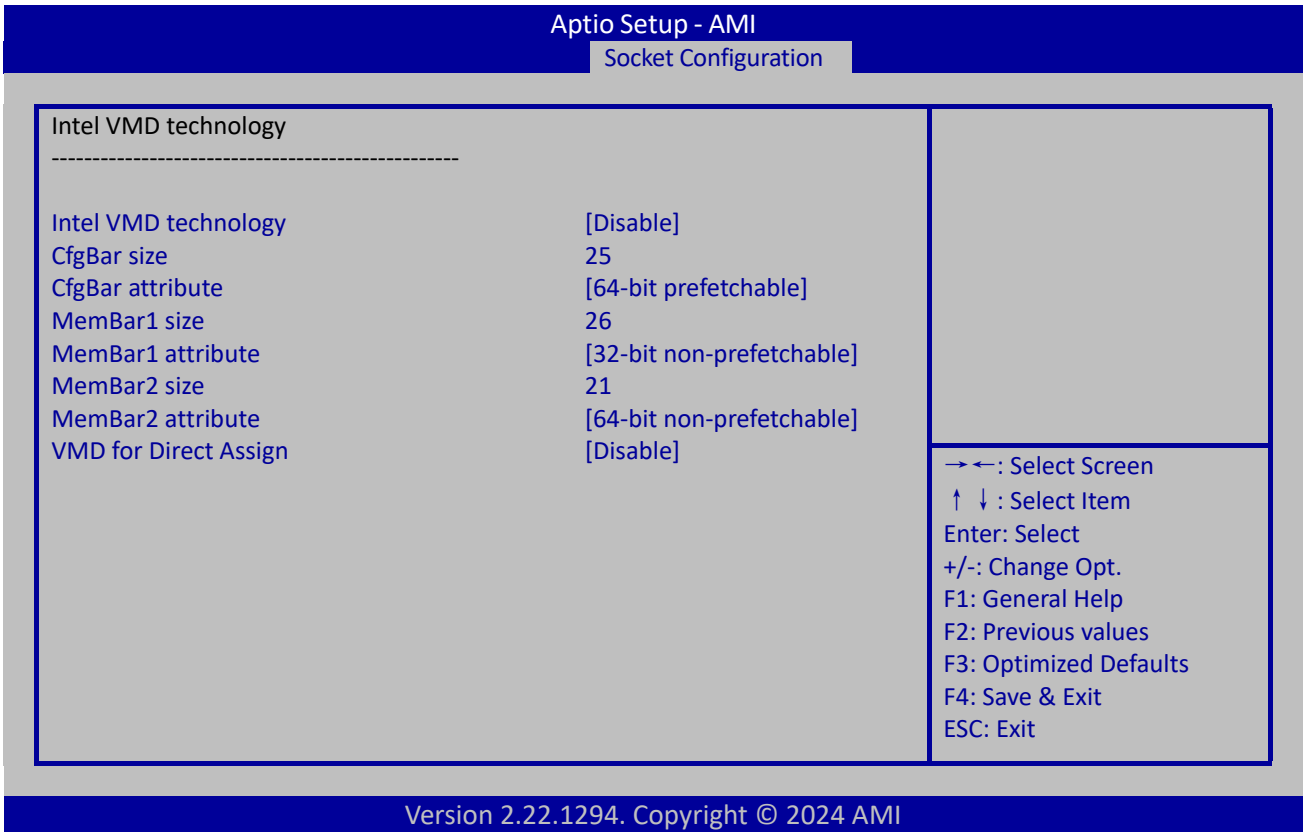
6.4.6.1.1 PCI Express x



Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x		
Menu Fields	**Settings**	**Comments**
PCI Express x		
Intel VMD technology	Selects sub-menu.	
NTB Menu	Selects sub-menu.	
Bifurcation	**[Auto]** [x4x4x4x4] [x4x4x_x8] [x_x8x4x4] [x_x8x_x8] [x_x_x_x16] [x2x2x4x_x8] [x4x2x2x_x8] [x_x8x2x2x4] [x2x2x4x4x8] [x4x2x2x4x4] [x4x4x2x2x4] [x2x2x2x2x_x8]	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.

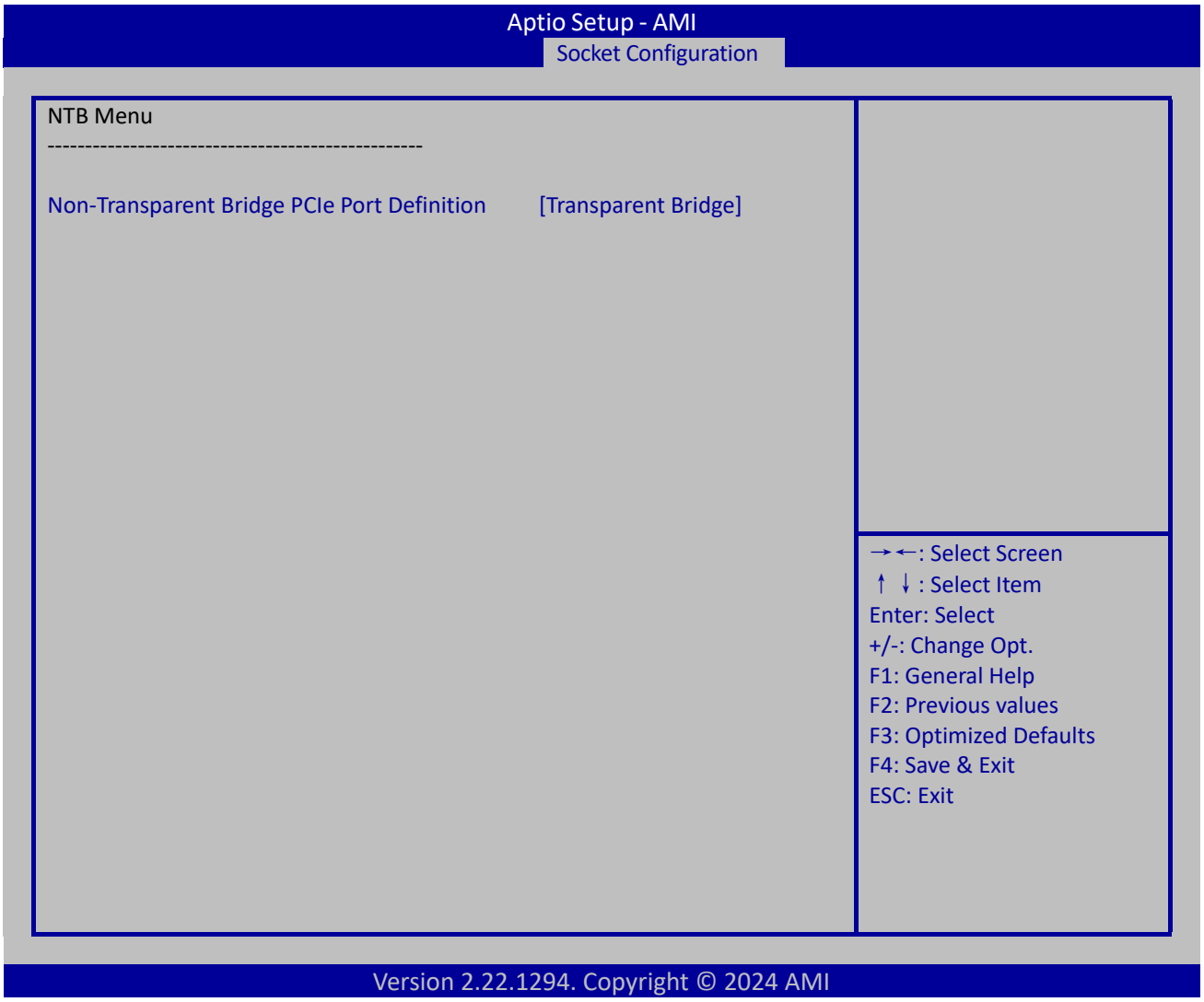
Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x		
Menu Fields	**Settings**	**Comments**
	[x2x2x2x2x4x4] [x2x2x4x2x2x4] [x4x2x2x2x2x4] [x2x2x2x2x2x2x4] [x_x8x4x2x2] [x4x4x4x2x2] [x_x8x2x2x2x2] [x2x2x4x4x2x2] [x4x2x2x4x2x2] [x4x4x2x2x2x2] [x2x2x2x2x4x2x2] [x2x2x4x2x2x2x2] [x4x2x2x2x2x2x2] [x2x2x2x2x2x2x2x2]	
Port x	Selects sub-menu.	

6.4.6.1.1.1 Intel VMD technology



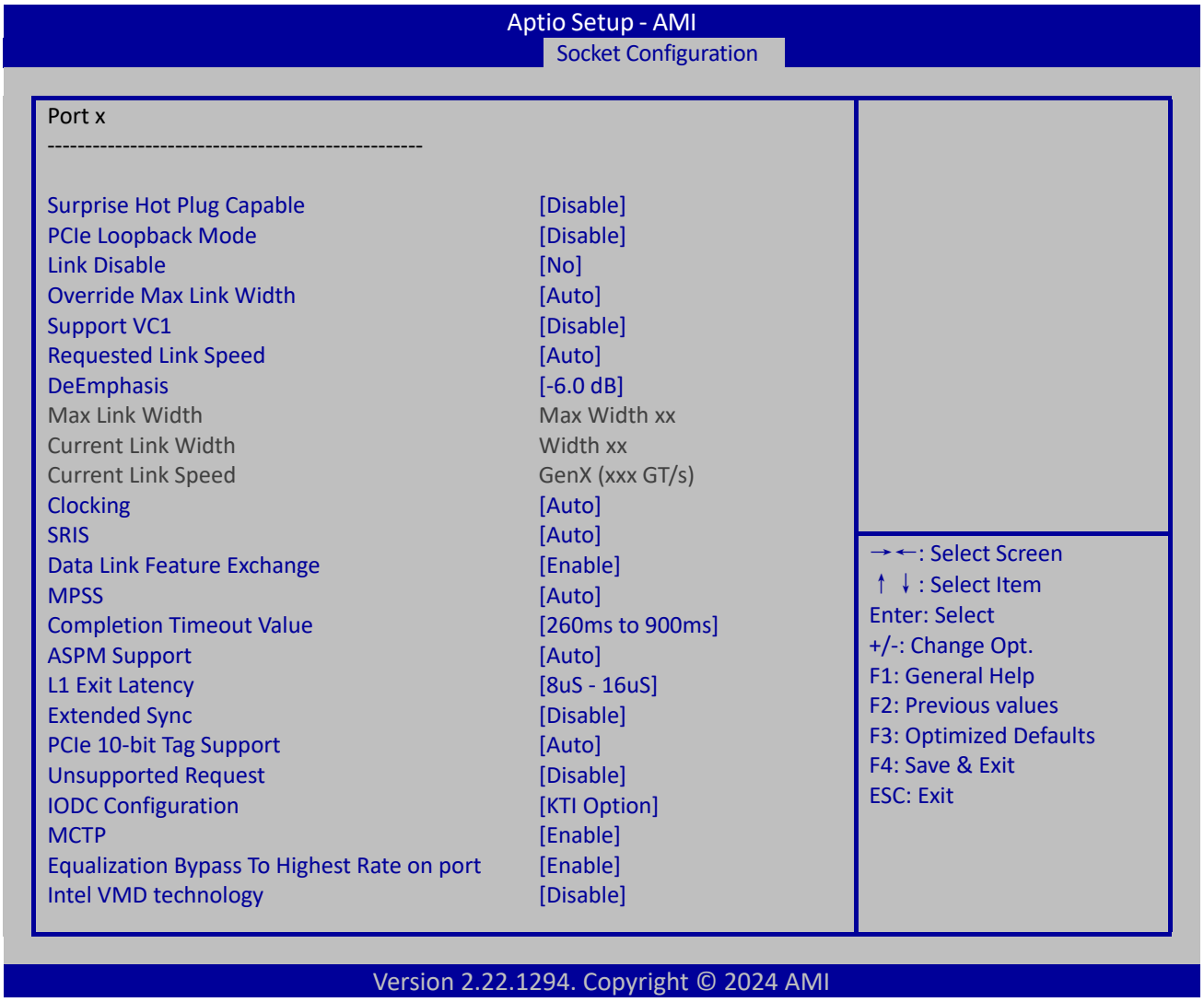
Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x \ Intel VMD technology		
Menu Fields	**Settings**	**Comments**
Intel VMD technology	**[Disable]** [Enable]	Enable/Disable VMD in this IIO Domain.
CfgBar size	**25**	Setup VMD Config BAR size (in bits Min=20, Max=27), ex: 20bits=1MB, 27bits=128MB
CfgBar attribute	[32-bit non-prefetchable] [64-bit non-prefetchable] **[64-bit prefetchable]**	Set up VMD Config BAR attribute, like 64-bit or prefetchable
MemBar1 size	**26**	Setup VMD Memory BAR1 size (in bits Min=20), ex: 20bits=1MB, 22bits=4MB, 26bits=64MB
MemBar1 attribute	**[32-bit non-prefetchable]** [64-bit non-prefetchable] [64-bit prefetchable]	Set up VMD Memory BAR1 attribute, like 64-bit or prefetchable
MemBar2 size	**21**	Setup VMD Memory BAR2 size (in bits Min=20), ex: 20bits=1MB, 22bits=4MB, 26bits=64MB
MemBar2 attribute	[32-bit non-prefetchable] **[64-bit non-prefetchable]** [64-bit prefetchable]	Set up VMD Memory BAR2 attribute, like 64-bit or prefetchable
VMD for Direct Assign	**[Disable]** [Enable]	Enable/Disable VMD for Direct Assign

6.4.6.1.1.2 NTB Menu



Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x \ NTB Menu		
Menu Fields	**Settings**	**Comments**
Non-Transparent Bridge PCIe Port Definition	**[Transparent Bridge]** [NTB to NTB]	[EMBAR1XBASE, EMBAR2XBASE] Configures port as TB or NTB-NTB
NTB BARs 23, 45 enable	**[Disable]** [Enable]	Enables NTB bars 23, 45 and lets setting their sizes
NTB IMBAR23/EMBAR23 size	**22**	NTB IMBAR23/EMBAR23 size. Value <12 or >29 (47 for BIOS supporting > 4G PCI) disables BAR.
NTB IMBAR45/EMBAR45 size	**22**	NTB IMBAR45/EMBAR45 size. Value <12 or >29 (47 for BIOS supporting > 4G PCI) disables BAR.
Crosslink control Override	**[DSD/USP]** [USD/DSP]	Configure NTB port as DSP/USP, USD/DSP, or use external pin

6.4.6.1.1.3 Port x

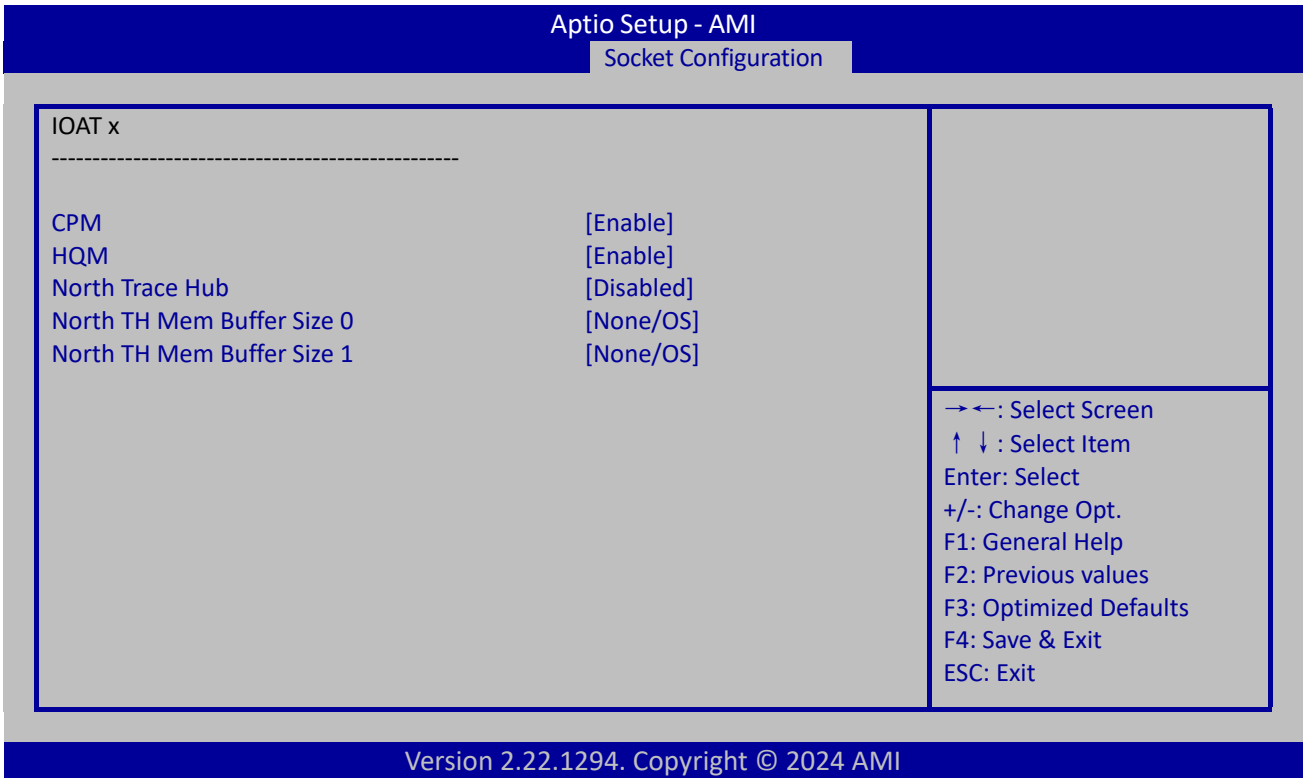


Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x \ Port x		
Menu Fields	**Settings**	**Comments**
Port x		
Surprise Hot Plug Capable	[Disable] [Enable]	This option specifies if the link is considered Surprise Hot Plug capable. ***NOTE: This item default setting based on project design which port support hotplug.***
PCIe Loopback Mode	**[Disable]** [Enable]	Enable/Disable loopback support for this PCIe port.
Link Disable	**[No]** [Yes]	This option disables the link so that the no training occurs but the CFG space is still active.
Override Max Link Width	**[Auto]** [x1] [x2] [x4] [x8] [x16]	Override the max link width that was set by bifurcation
Support VC1	**[Disable]**	Enable/Disable PCIe Port VC1 support.

Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x \ Port x		
Menu Fields	**Settings**	**Comments**
	[Enable]	x2 ports share the same VC1 channel
Requested Link Speed	**[Auto]** [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)] [Gen 4 (16 GT/s)] [Gen 5 (32 GT/s)]	Choose Link Speed for this PCIe port
DeEmphasis	**[-6.0 dB]** [-3.5 dB]	DeEmphasis control (LNKCON2[6]) for this PCIe port.
Max Link Width	Max Width xx	Displays the max link width for this PCIe port.
Current Link Width	Width xx	Displays the current link width for this PCIe port.
Current Link Speed	GenX (xxx GT/s)	Displays the current link speed for this PCIe port.
Clocking	[Distinct] [Common] **[Auto]**	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.
SRIS	[Disable] [Enable] **[Auto]**	Enable or Disable SRIS. 'Auto' keeps board default.
Data Link Feature Exchange	[Disable] **[Enable]**	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
MPSS	[128B] [256B] [512B] **[Auto]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
Completion Timeout Value	[50us to 50ms] [50us to 100us] [1ms to 10ms] [16ms to 55ms] [65ms to 210ms] **[260ms to 900ms]** [1s to 3.5s] [Disable]	Enable / disable the PCIe Completion Timeout in Device Control2 register.
ASPM Support	[Disable] **[Auto]**	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.
L1 Exit Latency	[<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] **[8uS - 16uS]** [16uS - 32uS] [32uS - 64uS] [>64uS]	The length of time this port requires to complete transition from L1 to L0
Extended Sync	**[Disable]** [Enable]	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
PCIe 10-bit Tag Support	[Disable] **[Auto]** [Force Enable]	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag

Socket Configuration \ IIO Configuration \ Socketx Configuration \ PCI Express x \ Port x		
Menu Fields	**Settings**	**Comments**
		Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.
Unsupported Request	**[Disable]** [Enable]	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
IODC Configuration	**[KTI Option]** [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remote WViLF]	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)
MCTP	[Disable] **[Enable]**	Enable/Disable MCTP
Equalization Bypass To Highest Rate on port	[Disable] **[Enable]**	Equalization Bypass To Highest Rate Support Enable/Disable
Intel VMD technology	**[Disable]** [Enable]	Enable/Disable Intel Volume Management Device Technology on specific root port

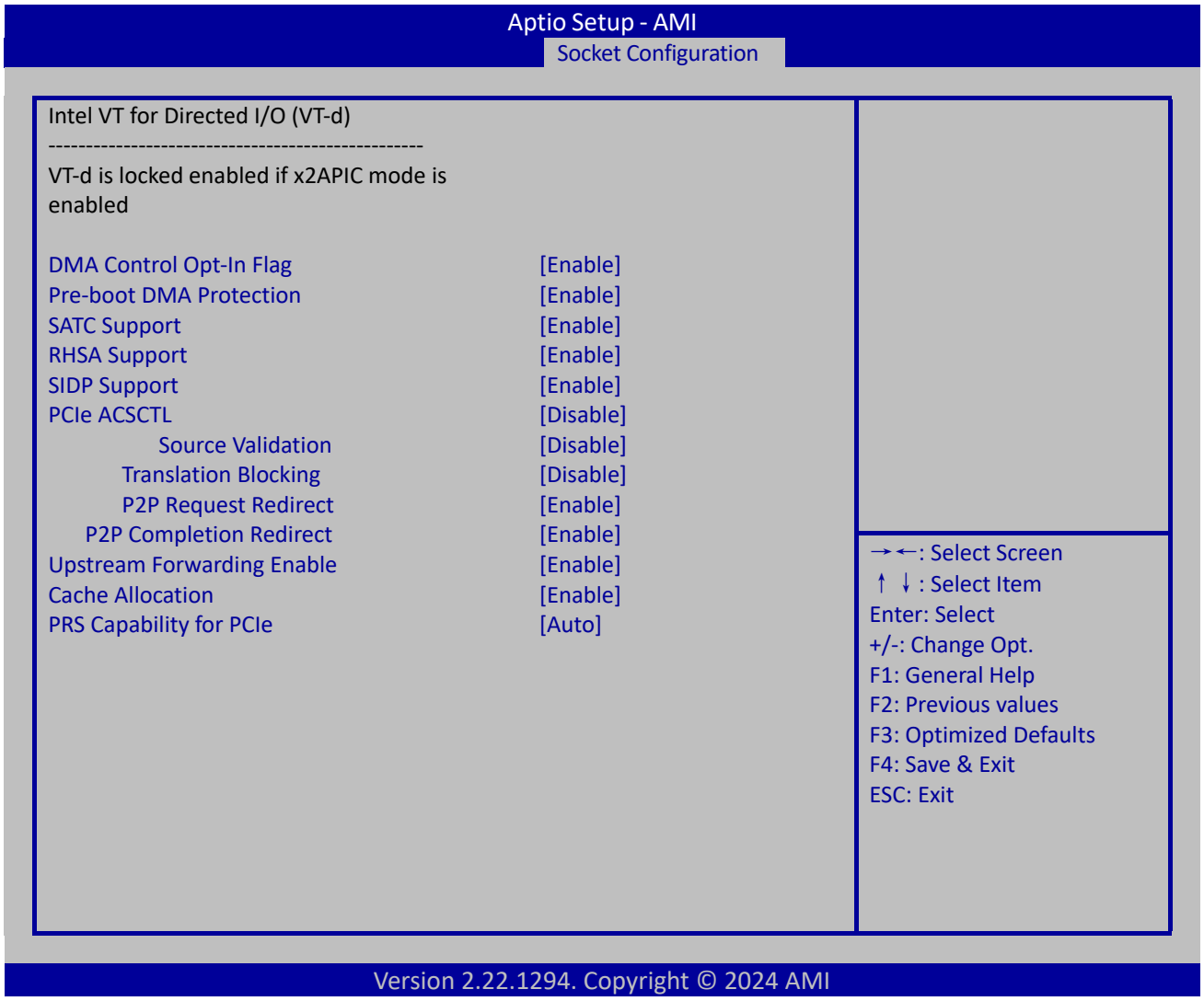
6.4.6.1.2 IOAT x



Socket Configuration \ IIO Configuration \ Socketx Configuration \ IOAT x		
Menu Fields	**Settings**	**Comments**
IOAT x		
CPM	[Disable] **[Enable]**	Select CPM Enable/Disable
HQM	[Disable] **[Enable]**	Select HQM Enable/Disable
North Trace Hub	**[Disabled]** [Enabled]	Enable/Disable CPU Trace Hub. Note: DMA protection (VTd) should be disabled.
North TH Mem Buffer Size 0	**[None/OS]** [1MB] [8MB] [64MB] [128MB] [256MB] [512MB] [1G] [2G] [4G] [8G]	Select size of memory region 0 buffer. Choose None/OS if OS-supported memory or trace forwarding is desired.
North TH Mem Buffer Size 1	**[None/OS]** [1MB] [8MB] [64MB] [128MB] [256MB] [512MB]	Select size of memory region 1 buffer. Choose None/OS if OS-supported memory or trace forwarding is desired.

Socket Configuration \ IIO Configuration \ Socketx Configuration \ IOAT x		
Menu Fields	**Settings**	**Comments**
	[1G] [2G] [4G] [8G]	

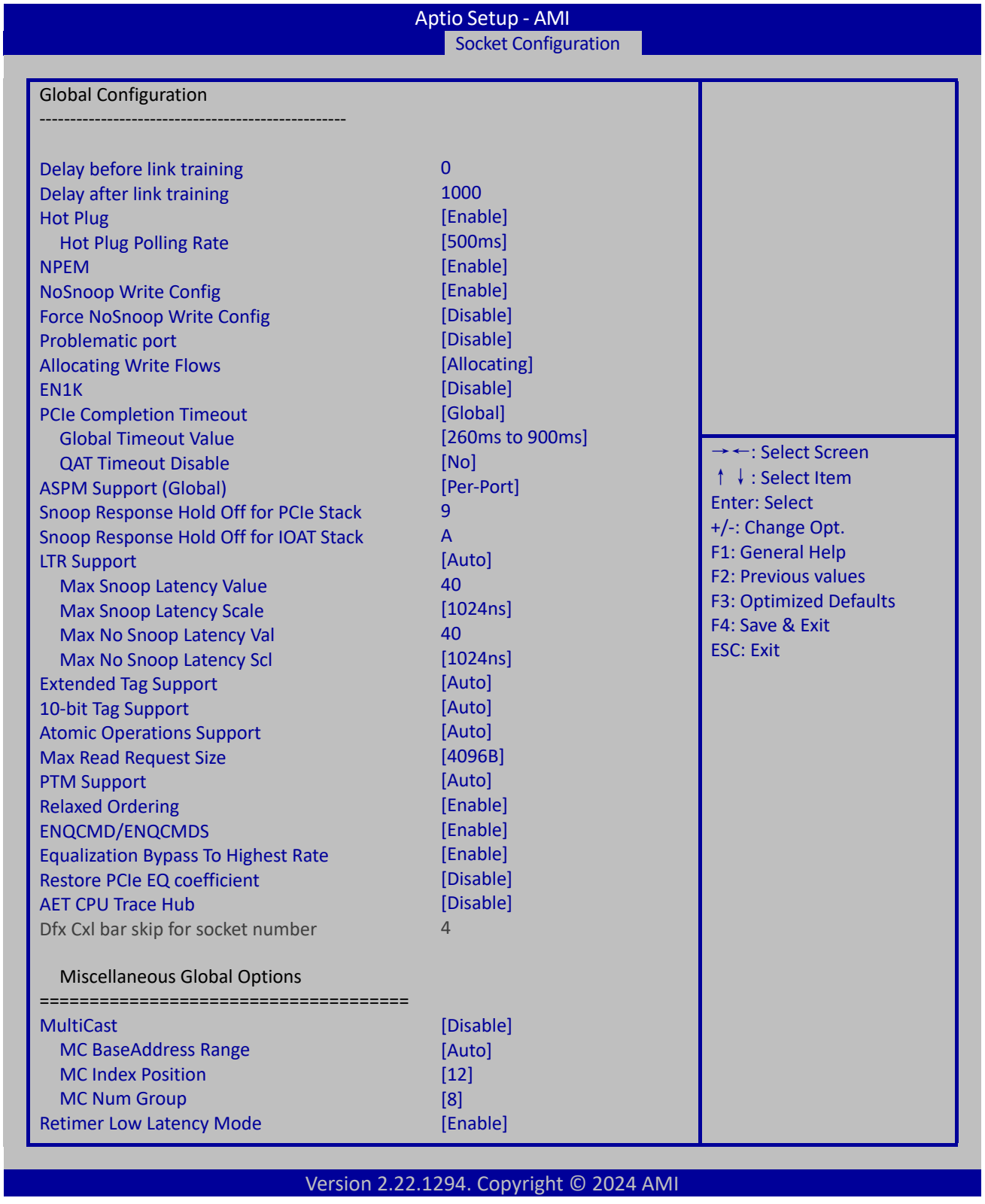
6.4.6.2 Intel VT for Directed I/O (VT-d)



Socket Configuration \ IIO Configuration \ Intel VT for Directed I/O (VT-d)		
Menu Fields	**Settings**	**Comments**
DMA Control Opt-In Flag	**[Enable]** [Disable]	Enable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR in ACPI to request OS to enable DMA protection. Not compatible with Direct Device Assignment (DDA).
Pre-boot DMA Protection	[Disable] **[Enable]**	Enable DMA Protection in Pre-boot environment.
SATC Support	**[Enable]** [Disable]	Enable/Disable SATC support.
RHSA Support	**[Enable]** [Disable]	Enable/Disable RHSA support.
SIDP Support	**[Enable]** [Disable]	Enable/Disable SIDP support.
PCIe ACSCTL	**[Disable]** [Enable]	Enable/Disable overwrite of PCI Access Control Services Control register in PCI root ports.
Source Validation	**[Disabled]** [Enabled]	When set, the component validates the Bus Number from the Requester ID of upstream

Socket Configuration \ IIO Configuration \ Intel VT for Directed I/O (VT-d)		
Menu Fields	**Settings**	**Comments**
		Requests against the secondary/subordinate Bus Numbers.
Translation Blocking	**[Disabled]** [Enabled]	When set, the component blocks all upstream Memory Requests whose Address Translation (AT) field is not set to the default value.
P2P Request Redirect	[Disabled] **[Enabled]**	This bit determines when the component redirects peer-to-peer Requests upstream.
P2P Completion Redirect	[Disabled] **[Enabled]**	Determines when the component redirects peer-to-peer Completions upstream, applicable only to Read Completions whose Relaxed Ordering Attribute is clear.
Upstream Forwarding Enable	[Disabled] **[Enabled]**	When set, the component forwards upstream any Request or Completion TLPs it receives that were redirected upstream by a component lower in the hierarchy.
Cache Allocation	**[Enable]** [Disable]	Enable cache allocation. This knob is independent of VT-d support.
PRS Capability for PCIe	[Disabled] [Enabled] **[Auto]**	Enable/Disable support for page request services capability on discrete PCIe devices. Enabling should only be to test vehicle for PCIe cards supporting PRS, and it might lead to platform hang.

6.4.6.3 Global Configuration



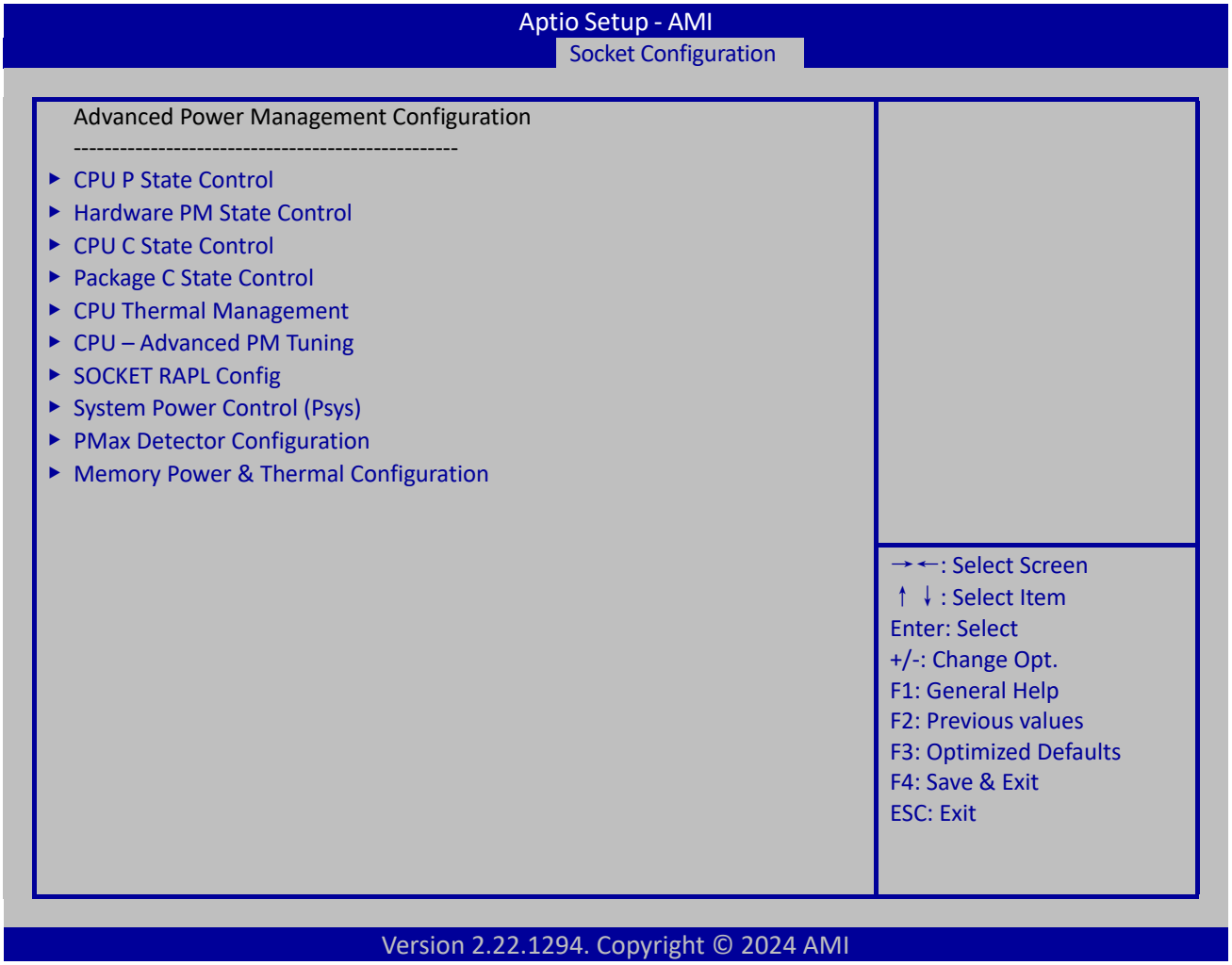
Socket Configuration \ IIO Configuration \ Global Configuration		
Menu Fields	**Settings**	**Comments**
Global Configuration		

Socket Configuration \ IIO Configuration \ Global Configuration		
Menu Fields	**Settings**	**Comments**
Delay before link training	**0**	Custom delay before PCIe link training on IIO ports (in millisecond).
Delay after link training	**1000**	This knob defines the time that System Firmware preserve for PCIe devices to train link and initialize for Configuration Request, after System Firmware started link training on PCIe Root Port. Default 1000 ms conforms to PCIe specification requirement. Using lower value (min is 500 ms), although usually works, does not follow the specification. Larger value may be used to work around problematic devices.
Hot Plug	[Disable] **[Enable]**	Enable/Disable PCIe Hot Plug globally
Hot Plug Polling Rate	[Auto] **[500ms]** [1s]	The rate that PCIe root ports should poll for a hot plugged device. 'Auto' keeps silicon registers default.
NPEM	[Disable] **[Enable]**	Enable/Disable NPEM globally
NoSnoop Write Config	[Disable] **[Enable]**	NoSnoop Write Configuration
Force NoSnoop Write Config	**[Disable]** [Enable]	Force NoSnoop Write Configuration
Problematic port	**[Disable]** [NP-NP Problematic] [P-P Problematic]	Selects whether problematic port lock flows need to be enabled in the system. Selection allows for P-P or NP-NP lock flows or neither.
Allocating Write Flows	[Non-Allocating] **[Allocating]**	Selects Vc0/VCp writes selection for all CPU PCIe ports as either allocating or non-allocating. Auto enables POR setting
EN1K	**[Disable]** [Enable]	Enables 1K granularity for I/O space decode in each of the virtual P2P bridges corresponding to root ports, and DMI ports
PCIe Completion Timeout	[Per-Port] **[Global]**	The policy to configure the PCIe Completion Timeout in DevCtl2 register. 'Global' will use Global Timeout Value for all PCIe devices in the system. 'Per-Port' will use Global Timeout Value for RCiEP while Root Port hierarchy timeout is configured with port knob.
Global Timeout Value	[50us to 50ms] [50us to 100us] [1ms to 10ms] [16ms to 55ms] [65ms to 210ms] **[260ms to 900ms]** [1s to 3.5s] [Disable]	Completion Timeout to program in DevCtl2 register in RCiEP devices and in Root Port hierarchy if 'Global' policy was selected above.
QAT Timeout Disable	**[No]** [Yes]	Option to disable Completion Timeout in QAT accelerators to avoid its expiration possible in systems with many sockets. Expiration may lead to BSOD.
ASPM Support (Global)	[Disable] **[Per-Port]**	This option can disable ASPM support for all PCIe root ports.
Snoop Response Hold Off for PCIe Stack	**9**	Sets Snoop Response Hold Off value, 256 cycles as Default

Socket Configuration \ IIO Configuration \ Global Configuration		
Menu Fields	**Settings**	**Comments**
Snoop Response Hold Off for IOAT Stack	**A**	Sets Snoop Response Hold Off value, 256 cycles as Default
LTR Support	[Disable] **[Auto]**	This option can disable Latency Tolerance Reporting support in all PCIe root ports. 'Auto' keeps hardware default.
Max Snoop Latency Value	**40**	The value of platform limit for max snoop latency to set in LTR Extended Capability register. Unit defined by Scale knob below.
Max Snoop Latency Scale	[1ns] [32ns] **[1024ns]** [32768ns] [1048576ns] [33554432ns]	The the scale of the value of platform limit for max snoop latency to set in appropriate LTR Extended Capability register.
Max No Snoop Latency Val	**40**	The value of platform limit for max no snoop latency to set in LTR Extended Capability register. Unit defined by Scale knob below.
Max No Snoop Latency Scl	[1ns] [32ns] **[1024ns]** [32768ns] [1048576ns] [33554432ns]	The the scale of the value of platform limit for max no snoop latency to set in appropriate LTR Extended Capability register.
Extended Tag Support	[Disable] **[Auto]**	This option can disable 8-bit Tag support in all PCIe root ports. 'Auto' keeps hardware default.
10-bit Tag Support	[Disable] **[Auto]**	This option can disable 10-bit Tag Requester (not Completer) support in all PCIe Root Ports. 'Auto' keeps hardware default. 10-bit Tag Completer support is required in all gen4 and newer devices per PCIe specification. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Ports, however OS can reconfigure and enable it.
Atomic Operations Support	[Disable] **[Auto]**	This option can disable Atomic Operation Routing support in all PCIe root ports and block Atomic Operation Requester in PCI hierarchy. 'Auto' keeps hardware default.
Max Read Request Size	[AUTO] [128B] [256B] [512B] [1024B] [2048B] **[4096B]**	This option can set Max Read Request Size in PCI hierarchy. 'Default' keeps hardware default.
PTM Support	[Disable] **[Auto]**	This option can disable Precision Time Management support in PCI hierarchy. 'Auto' keeps hardware default.
Relaxed Ordering	[Disable] **[Enable]**	Relaxed Ordering Enable/Disable
ENQCMD/ENQCMDS	[Disable] **[Enable]**	Enqueue requests support Enable/Disable
Equalization Bypass To Highest Rate	[Disable] **[Enable]**	Equalization Bypass To Highest Rate Support Enable/Disable

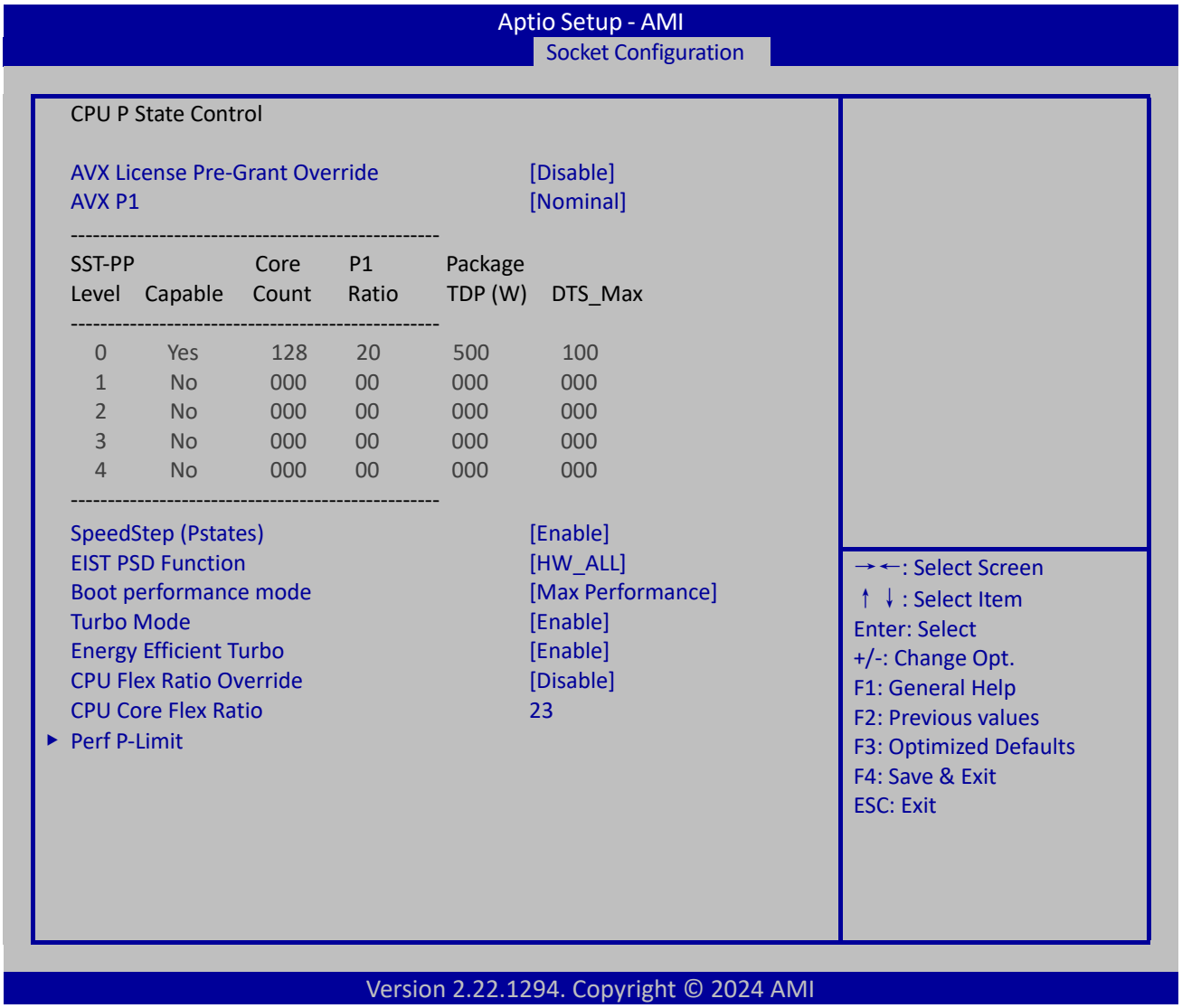
Socket Configuration \ IIO Configuration \ Global Configuration		
Menu Fields	**Settings**	**Comments**
Restore PCIe EQ coefficient	**[Disable]** [Enable]	Enable/Disable PCIe EQ coefficient restoring
AET CPU Trace Hub	**[Disable]** [Enable]	Enable/Disable CPU Trace Hub for AET event tracing
Dfx Cxl bar skip for socket number	4	CXL BAR will be skipped in PEI for multi-socket config
Miscellaneous Global Options		
MultiCast	**[Disable]** [Enable]	Enable MultiCast (for validation use)
MC BaseAddress Range	**[Auto]** [Below_4G]	Allocate memory for MultiCast test purpose
MC Index Position	**[12]** [20]	MC_Index_Position value
MC Num Group	[1] **[8]** [32] [64]	MC_Num_Group value
Retimer Low Latency Mode	[Disable] **[Enable]** [16GT/s Only] [32GT/s Only]	Enable 16GT/s and 32GT/s HW autonomous re-timer low latency mode

6.4.7 Advanced Power Management Configuration



Socket Configuration \ Advanced Power Management Configuration		
Menu Fields	**Settings**	**Comments**
CPU P State Control	Selects sub-menu.	
Hardware PM State Control	Selects sub-menu.	
CPU C State Control	Selects sub-menu.	
Package C State Control	Selects sub-menu.	
CPU Thermal Management	Selects sub-menu.	
CPU – Advanced PM Tuning	Selects sub-menu.	
SOCKET RAPL Config	Selects sub-menu.	
System Power Control (Psys)	Selects sub-menu.	
PMax Detector Configuration	Selects sub-menu.	
Memory Power & Thermal Configuration	Selects sub-menu.	

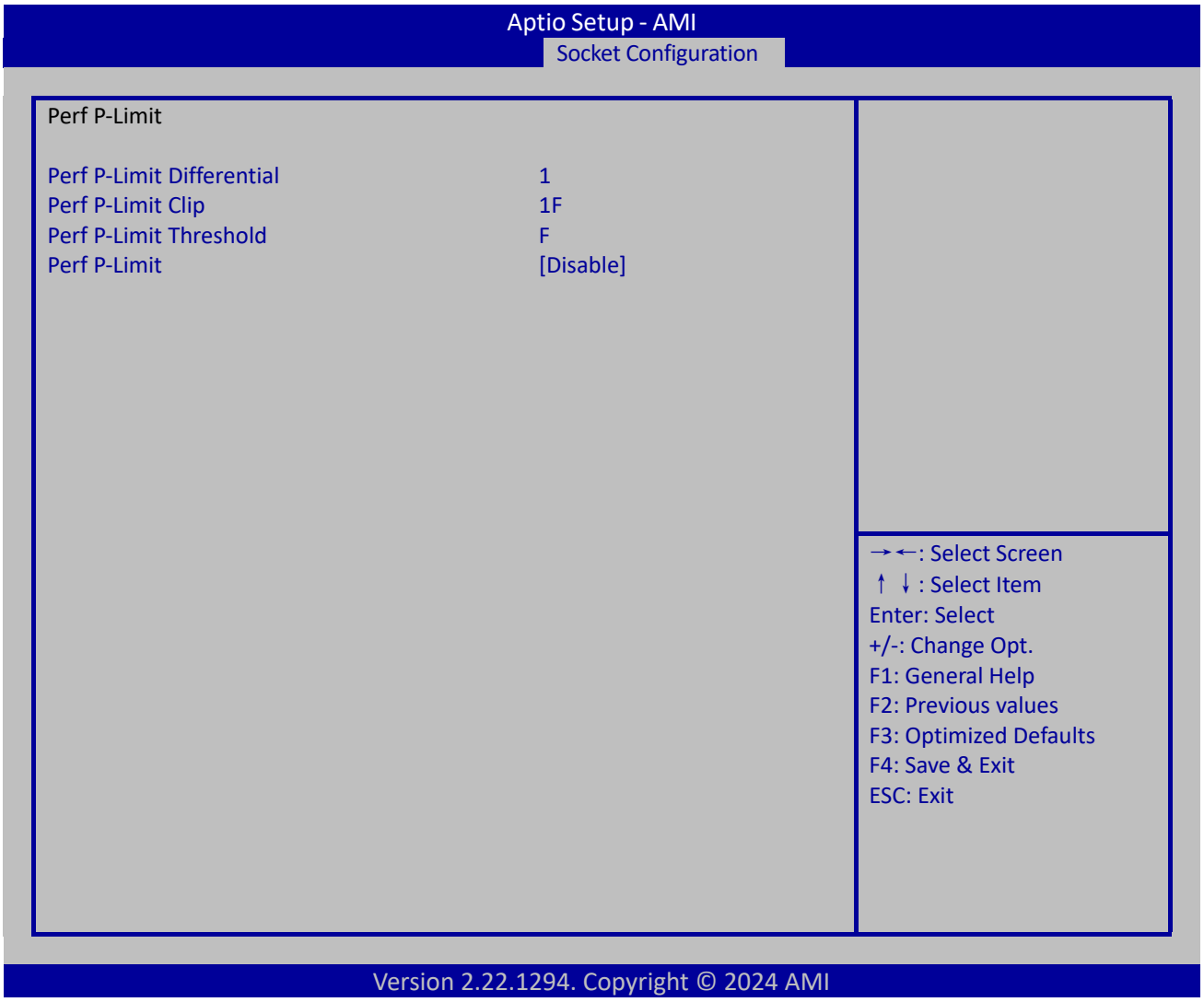
6.4.7.1 CPU P State Control



Socket Configuration \ Advanced Power Management Configuration \ CPU P State Control		
Menu Fields	**Settings**	**Comments**
AVX License Pre-Grant Override	**[Disable]** [Enabled]	Enables AVX ICCP pre-grant level override.
AVX ICCP pre-grant level	**[128 Heavy]** [256 Light] [256 Heavy] [512 Light] [512 Heavy] [AMX]	Pre-grants an AVX level to the core. Base frequency is not updated
AVX P1	**[Nominal]** [Level 1] [Level 2]	AVX P1 level selection NOTE: Dynamic SST-PP and SST-BF will be disabled when Avx P1 Level is not in Nominal.
SST-PP Level / Capable / Core Count / P1 Ratio / Package TDP (W) / DTS_Max		
x / x / xxx / xx / xxx / xxx		Displays the SST-PP information.
SpeedStep (Pstates)	[Disable]	Enable/Disable EIST (P-States)

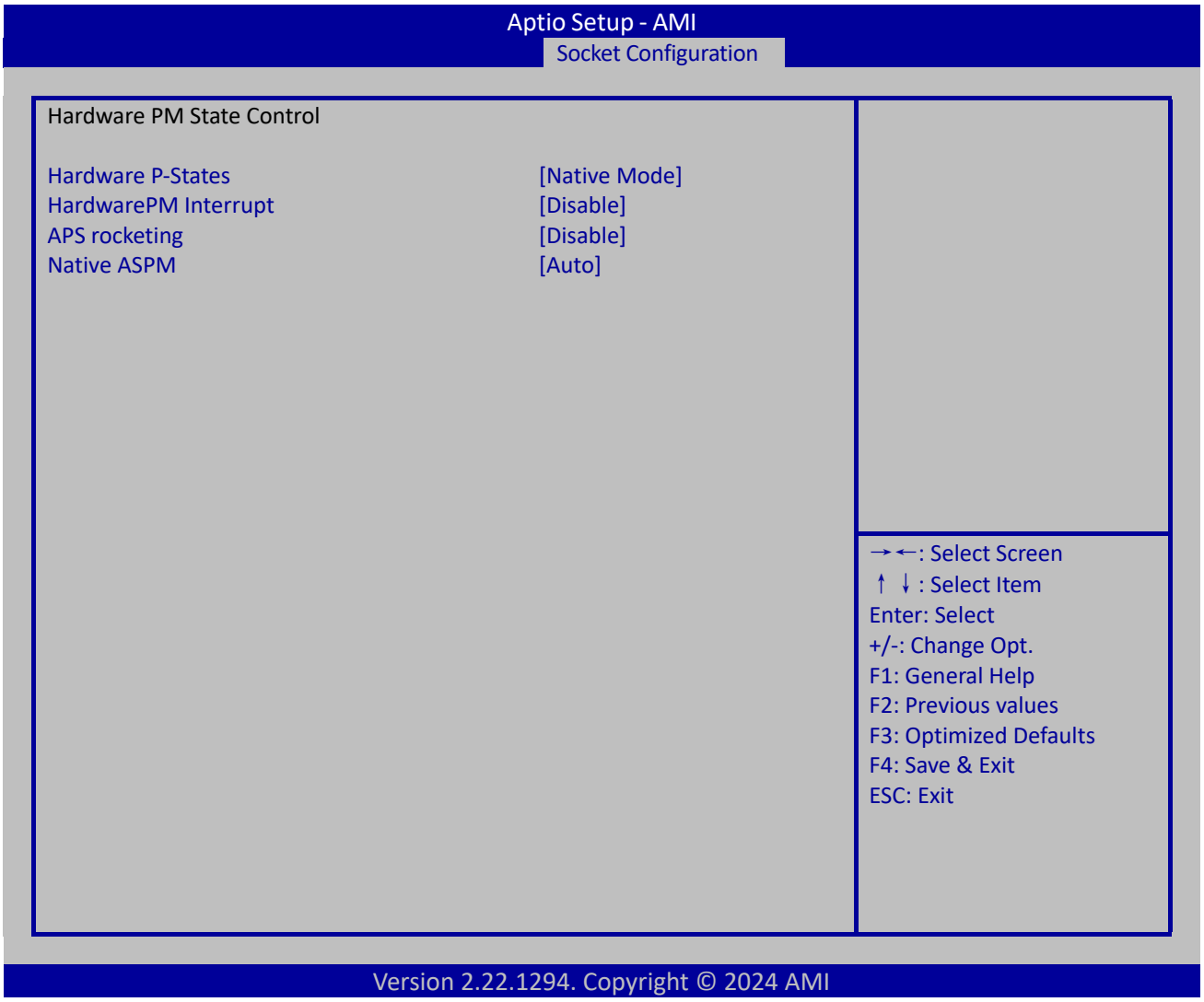
Socket Configuration \ Advanced Power Management Configuration \ CPU P State Control		
Menu Fields	**Settings**	**Comments**
	[Enable]	
EIST PSD Function	**[HW_ALL]** [SW_ALL]	Choose HW_ALL/SW_ALL in _PSD return
Boot performance mode	**[Max Performance]** [Max Efficiency]	Select the performance state that the BIOS will set before OS hand off.
Turbo Mode	[Disable] **[Enable]**	Enable/Disable processor Turbo Mode
Energy Efficient Turbo	**[Enable]** [Disable]	Enable/Disable Energy Efficient Turbo. Enable: MSR 0x1FC Bit[19] = 0 Disable: MSR 0x1FC Bit[19] = 1.
CPU Flex Ratio Override	**[Disable]** [Enabled]	Enable/Disable CPU Flex Ratio Programming NOTE: Dynamic SST-PP and SST-BF will be disabled when CPU Flex Ratio Override is enabled.
CPU Core Flex Ratio	**23**	Non-Turbo Mode Processor Core Ratio Multiplier
Perf P-Limit	Selects sub-menu.	

6.4.7.1.1 Perf P-Limit



Socket Configuration \ Advanced Power Management Configuration \ CPU P State Control \ Perf P-Limit		
Menu Fields	**Settings**	**Comments**
Perf P-Limit Differential	**1**	Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.
Perf P-Limit Clip	**1F**	Maximum value the floor is allowed to be set to for perf P-limit.
Perf P-Limit Threshold	**F**	Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.
Perf P-Limit	**[Disable]** [Enable]	Enable/Disable Performance P-Limit

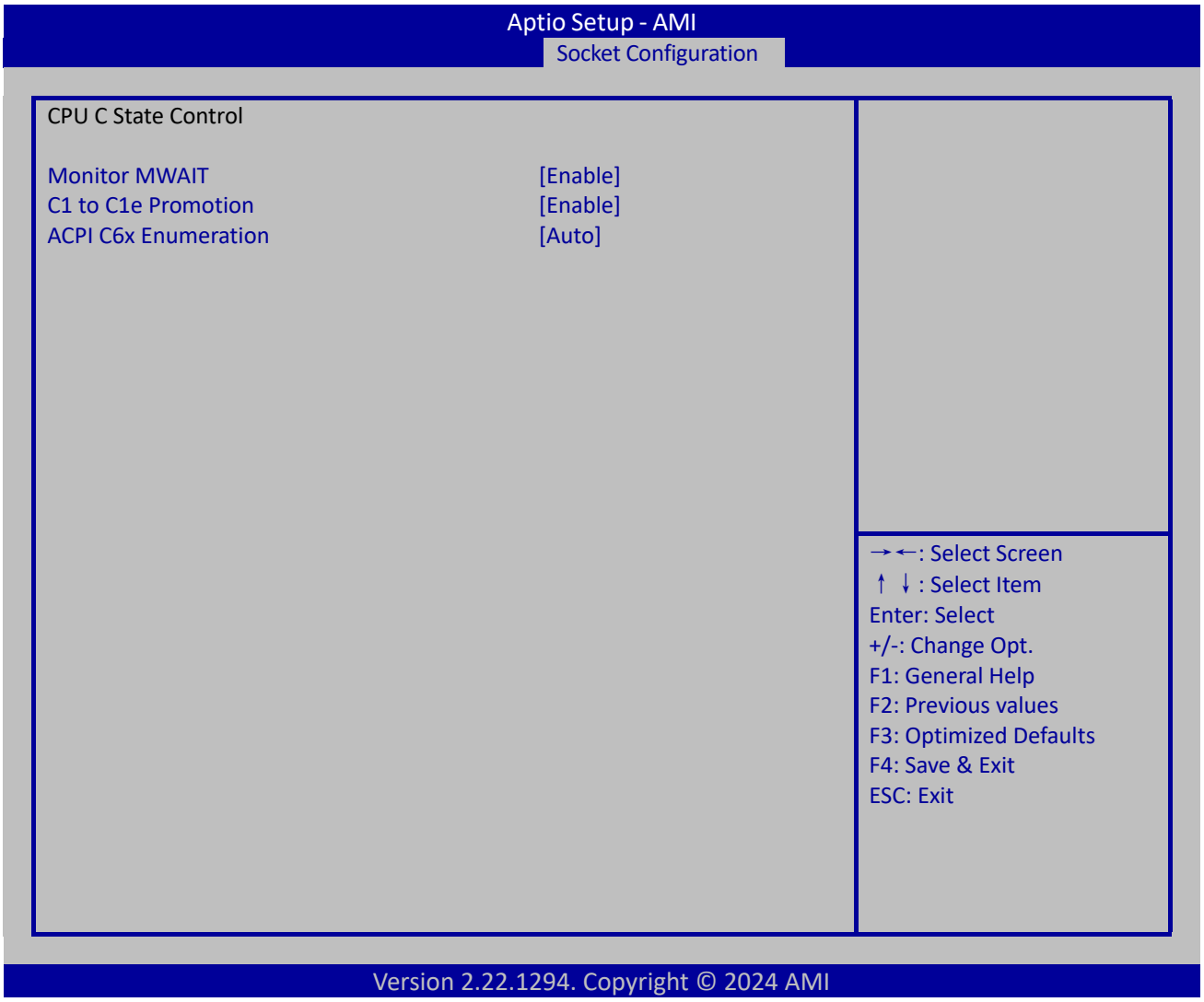
6.4.7.2 Hardware PM State Control



Socket Configuration \ Advanced Power Management Configuration \ Hardware PM State Control		
Menu Fields	**Settings**	**Comments**
Hardware P-States	[Disable] **[Native Mode]** [Out of Band Mode] [Native Mode with No Legacy Support]	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States) Native Mode:Hardware chooses a P-state based on OS guidance Out of Band Mode:Hardware autonomously chooses a P-state (no OS guidance) NOTE: When HWP is 'Disable' or 'OOB', Dynamic SST-PP will be disabled. SST-BF can only be enabled when HWP mode is 'Native Mode with No Legacy Support'."
HardwarePM Interrupt	**[Disable]** [Enable]	Enable/Disable Hardware PM Interrupt
EPP profile	[Performance] **[Balance Performance]** [Balance Power] [Power]	Choose an HWPM Profile (EPP)

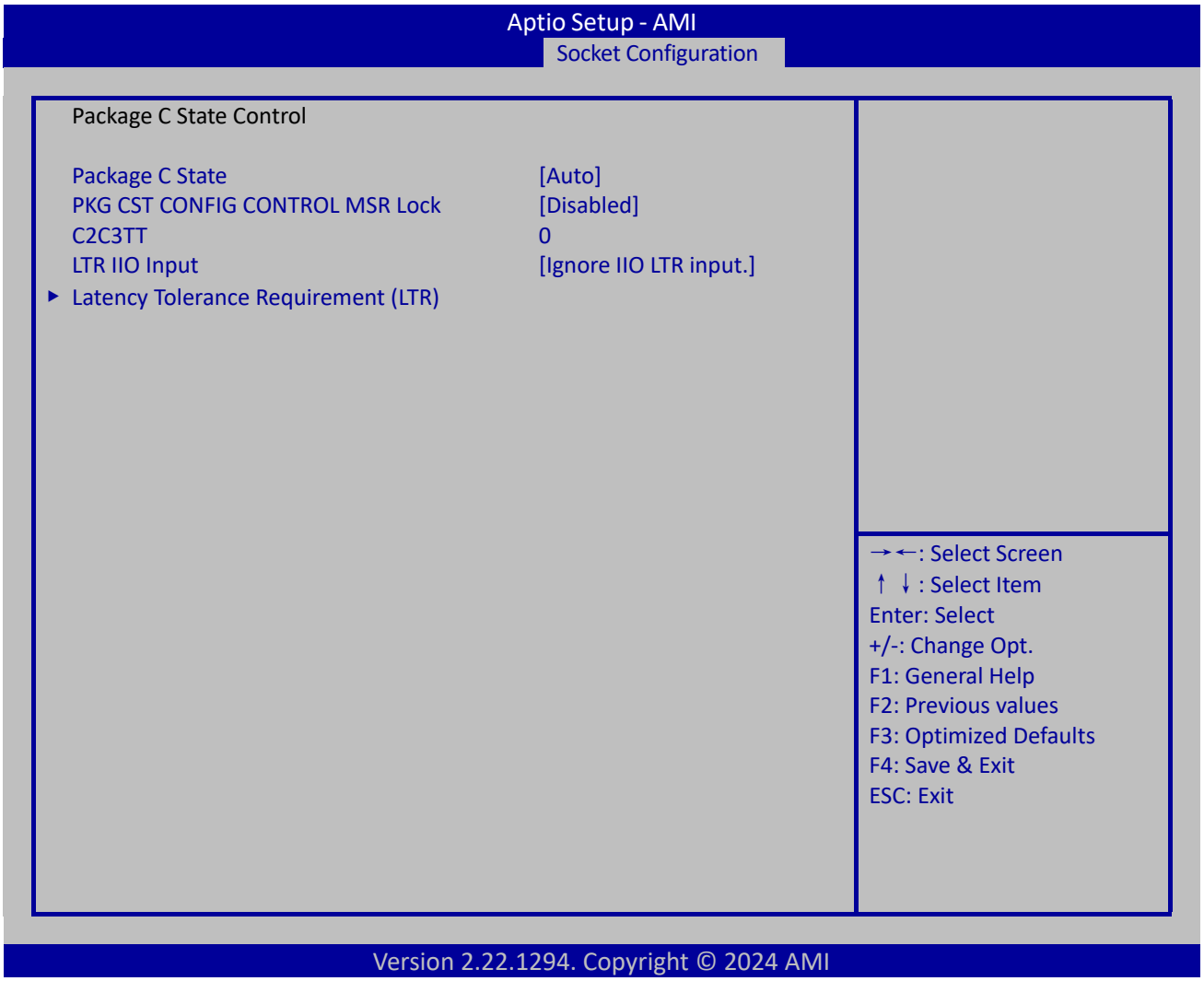
Socket Configuration \ Advanced Power Management Configuration \ Hardware PM State Control		
Menu Fields	**Settings**	**Comments**
APS rocketing	[Enable] **[Disable]**	Enable/Disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up
Native ASPM	**[Auto]** [Enabled] [Disabled]	Enabled - OS Controlled ASPM, Disabled - ASPM Off, AUTO - BIOS Controlled ASPM

6.4.7.3 CPU C State Control



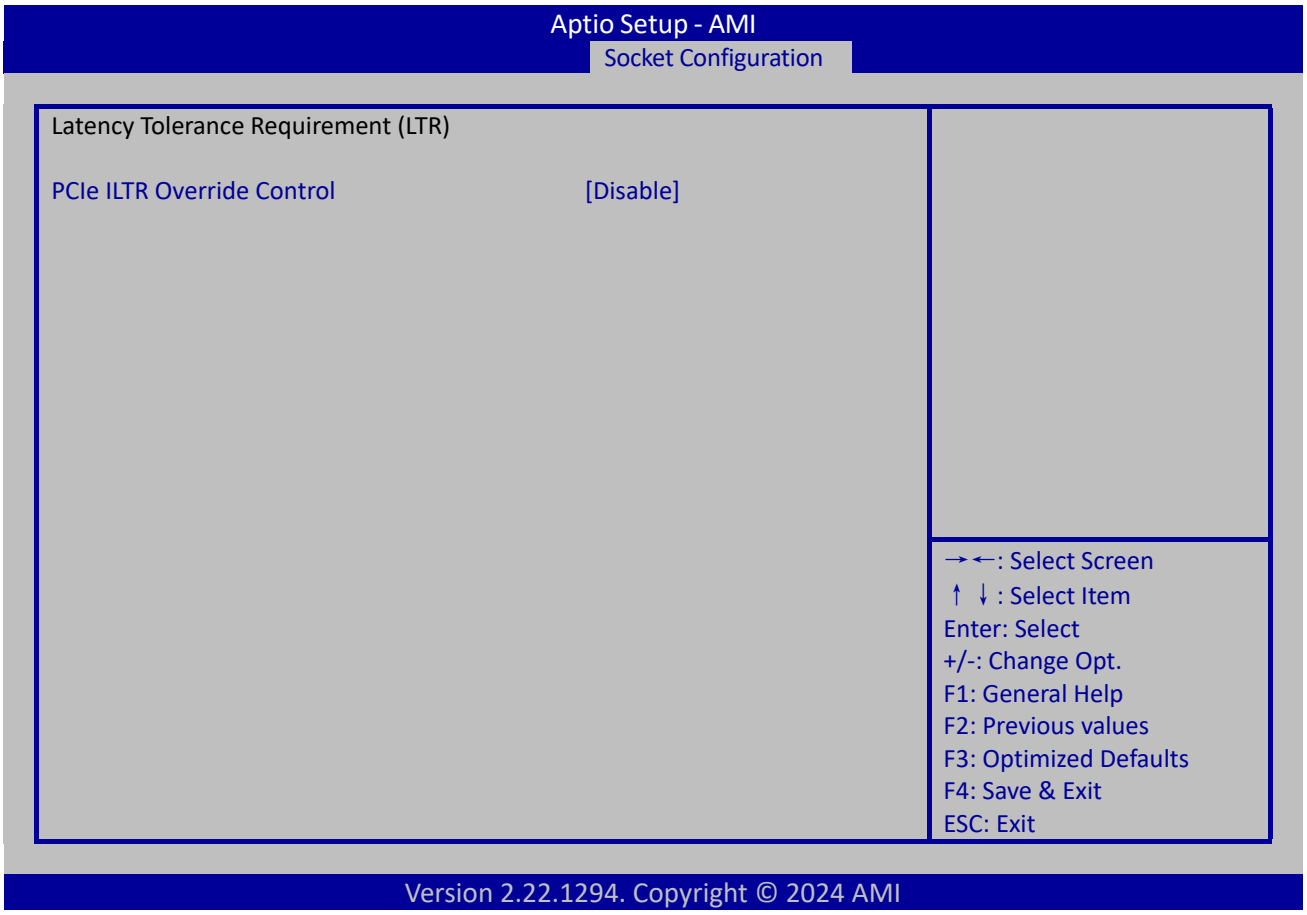
Socket Configuration \ Advanced Power Management Configuration \ CPU C State Control		
Menu Fields	**Settings**	**Comments**
Monitor MWAIT	[Disable] **[Enable]**	Allows Monitor and MWAIT instructions.
C1 to C1e Promotion	[Disable] **[Enable]**	CPU will promote C1 request to C1e state.
ACPI C6x Enumeration	[Disable] [C6S as ACPI C2] [C6S as ACPI C3] [C6S-P as ACPI C2] [C6S-P as ACPI C3] **[Auto]**	AUTO: Maps to C6S-P as ACPI C2 Disable: Don't enumerate any C6S state in ACPI C6S as ACPI C2/C3: Enumerate C6S as ACPI C2/C3 state. PkgC6 is not allowed C6S-P as ACPI C2/C3: Enumerate C6S-P as ACPI C2/C3 state. PkgC6 is allowed.

6.4.7.4 Package C State Control



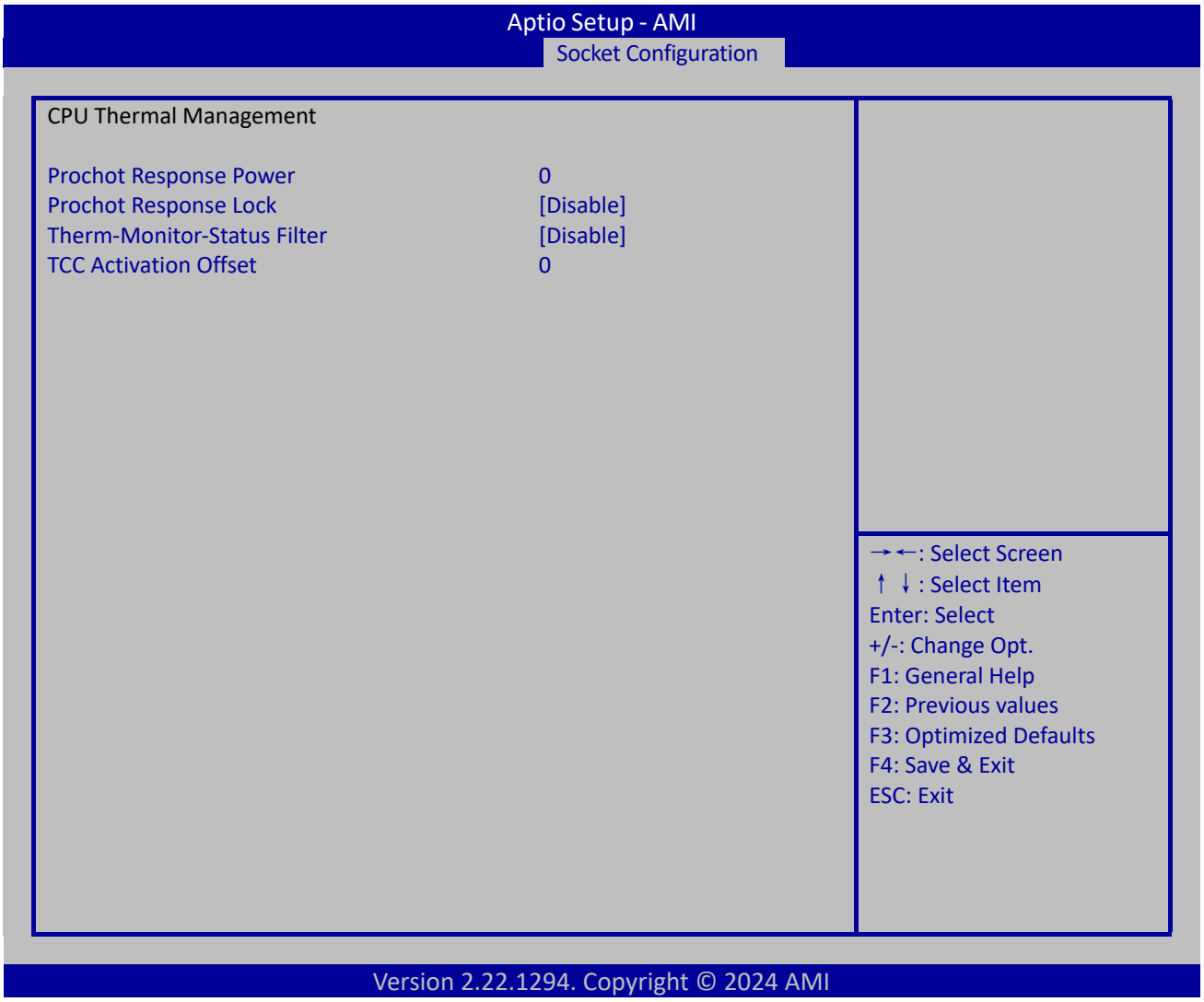
Socket Configuration \ Advanced Power Management Configuration \ Package C State Control		
Menu Fields	**Settings**	**Comments**
Package C State	[C0/C1 state] [C2 state] [C6(non Retention) state] [No Limit] **[Auto]**	Package C State limit, the state Auto maps is program specific.
PKG CST CONFIG CONTROL MSR Lock	**[Disabled]** [Enabled]	Enable - MSR E2h will be locked. Power Good reset is needed to remove lock bits.
C2C3TT	**0**	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = C2C3TT CSR Bit[11:0].
LTR IIO Input	[Take IIO LTR input] **[Ignore IIO LTR input]**	Take IIO LTR input: MSR 1FCh Bit[35] = 0 Ignore IIO LTR input: MSR 1FCh Bit[35] = 1.
Latency Tolerance Requirement (LTR)	Selects sub-menu.	

6.4.7.4.1 Latency Tolerance Requirement (LTR)



Socket Configuration \ Advanced Power Management Configuration \ Package C State Control \ Latency Tolerance Requirement (LTR)		
Menu Fields	**Settings**	**Comments**
PCIe ILTR Override Control	**[Disable]** [Enable]	Allows manual overrides for PCIE_ILTR_OVRD
Snoop Latency Override Valid	**[Disable]** [Enable]	Snoop Latency override Control
Force Snoop Latency Override	**[Disable]** [Enable]	Control to ignore PCIe ILTR, and force the Snoop Latency value
Snoop Latency Multiplier	**0**	Override Value is multiplied by this field to yield a time value
Snoop Latency Value	**0**	Latency requirement for Snoop requests
Non-Snoop Latency Override Valid	**[Disable]** [Enable]	Non-Snoop Latency override Control
Force Non-Snoop Latency Override	**[Disable]** [Enable]	Control to ignore PCIe ILTR, and force the Non-Snoop Latency value
Non-Snoop Latency Multiplier	**0**	Override Value is multiplied by this field to yield a time value
Non-Snoop Latency Value	**0**	Latency requirement for Non-Snoop requests

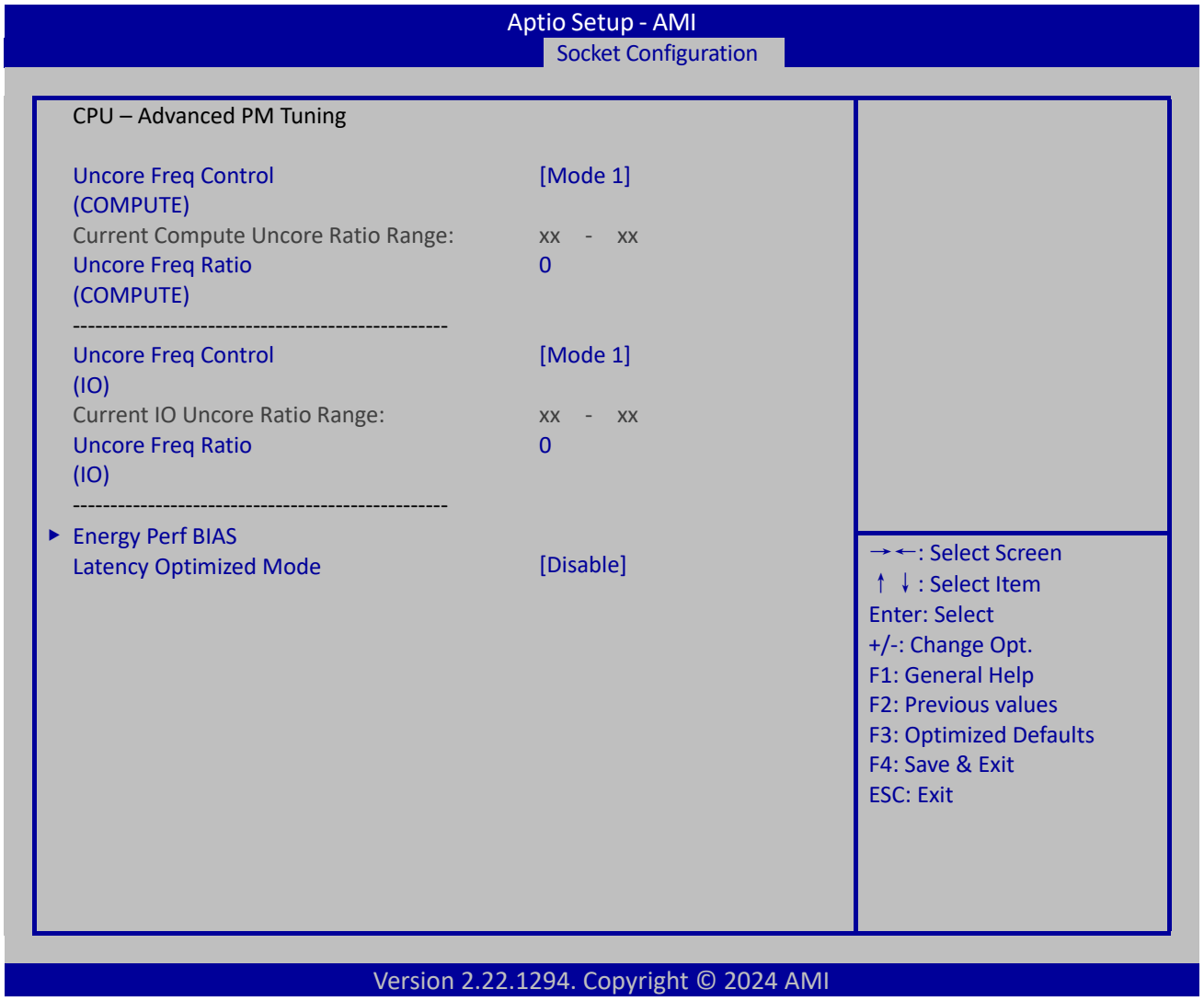
6.4.7.5 CPU Thermal Management



Socket Configuration \ Advanced Power Management Configuration \ CPU Thermal Management		
Menu Fields	**Settings**	**Comments**
Prochot Response Power	**0**	System will be below this power limit when xxPROCHOT is asserted. Unit = 0.125 W. The PROCHOT response power physical bounds are set inside the CPU. User is expected to run appropriate workload to determine the valid range of power consumption. Default value = TDP.
Prochot Response Lock	**[Disable]** [Enable]	Lock the Prochot settings until next reset.
Therm-Monitor-Status Filter	**[Disable]** [Enable]	Enable Filter based therm_monitor_status (IA32_THERM_STATUS[0]) reporting
Therm-Monitor-Status Filter Time Window	[0.07] [0.1] [0.24] [0.4] **[1.1]** [2.2]	Time window(Seconds) for the filter.

Socket Configuration \ Advanced Power Management Configuration \ CPU Thermal Management		
Menu Fields	**Settings**	**Comments**
	[4.64] [9.29] [18.8] [37.7] [75.5] [151] [302]	
TCC Activation Offset	**0**	

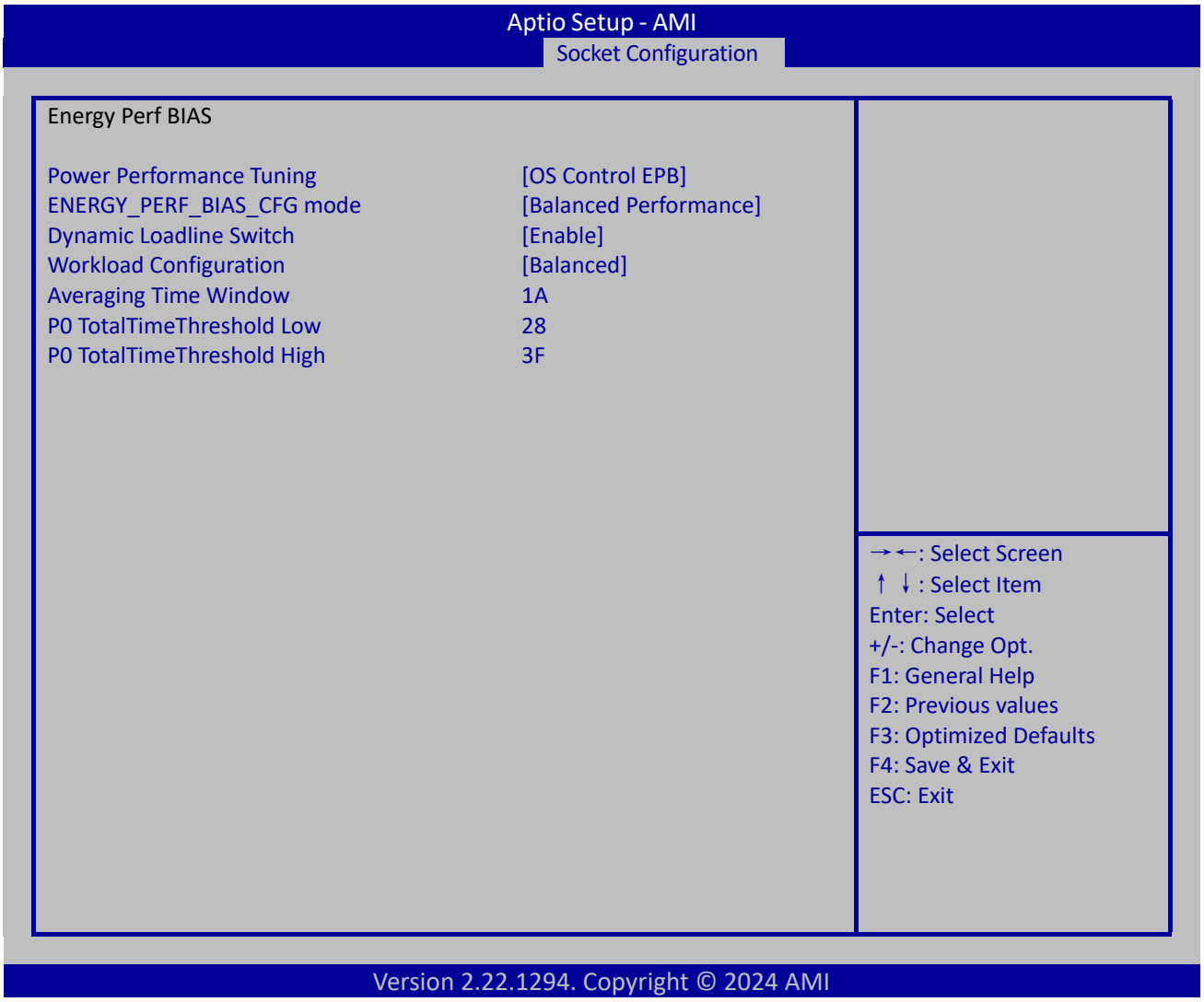
6.4.7.6 CPU – Advanced PM Tuning



Socket Configuration \ Advanced Power Management Configuration \ CPU – Advanced PM Tuning		
Menu Fields	**Settings**	**Comments**
Uncore Freq Control (COMPUTE)	[Mode 0] **[Mode 1]**	Mode 0: Power Limited Ordered Throttling Mode 1: Power Limited Proportional Throttling
Current Compute Uncore Ratio Range:	xx - xx	Displays the current compute Uncore ratio range.
Uncore Freq Ratio (COMPUTE)	**0**	0: Set dynamic Uncore frequency range from max and min fused values. Otherwise Uncore will run at a constant frequency ratio, the UFS algorithm will be disabled, but physical limits may still reduce frequency. NOTE: The user input will be clipped to the range accordingly during boot.
Uncore Freq Control (IO)	[Mode 0] **[Mode 1]**	Mode 0: Power Limited Ordered Throttling Mode 1: Power Limited Proportional Throttling
Current IO Uncore Ratio Range:	xx - xx	Displays the current IO Uncore ratio range.

Socket Configuration \ Advanced Power Management Configuration \ CPU – Advanced PM Tuning		
Menu Fields	**Settings**	**Comments**
Uncore Freq Ratio (IO)	**0**	0: Set dynamic Uncore frequency range from max and min fused values. Otherwise Uncore will run at a constant frequency ratio, the UFS algorithm will be disabled, but physical limits may still reduce frequency. NOTE: The user input will be clipped to the range accordingly during boot.
Energy Perf BIAS	Selects sub-menu.	
Latency Optimized Mode	**[Disable]** [Enabled]	Enable/Disable Latency Optimized Mode (Perf).

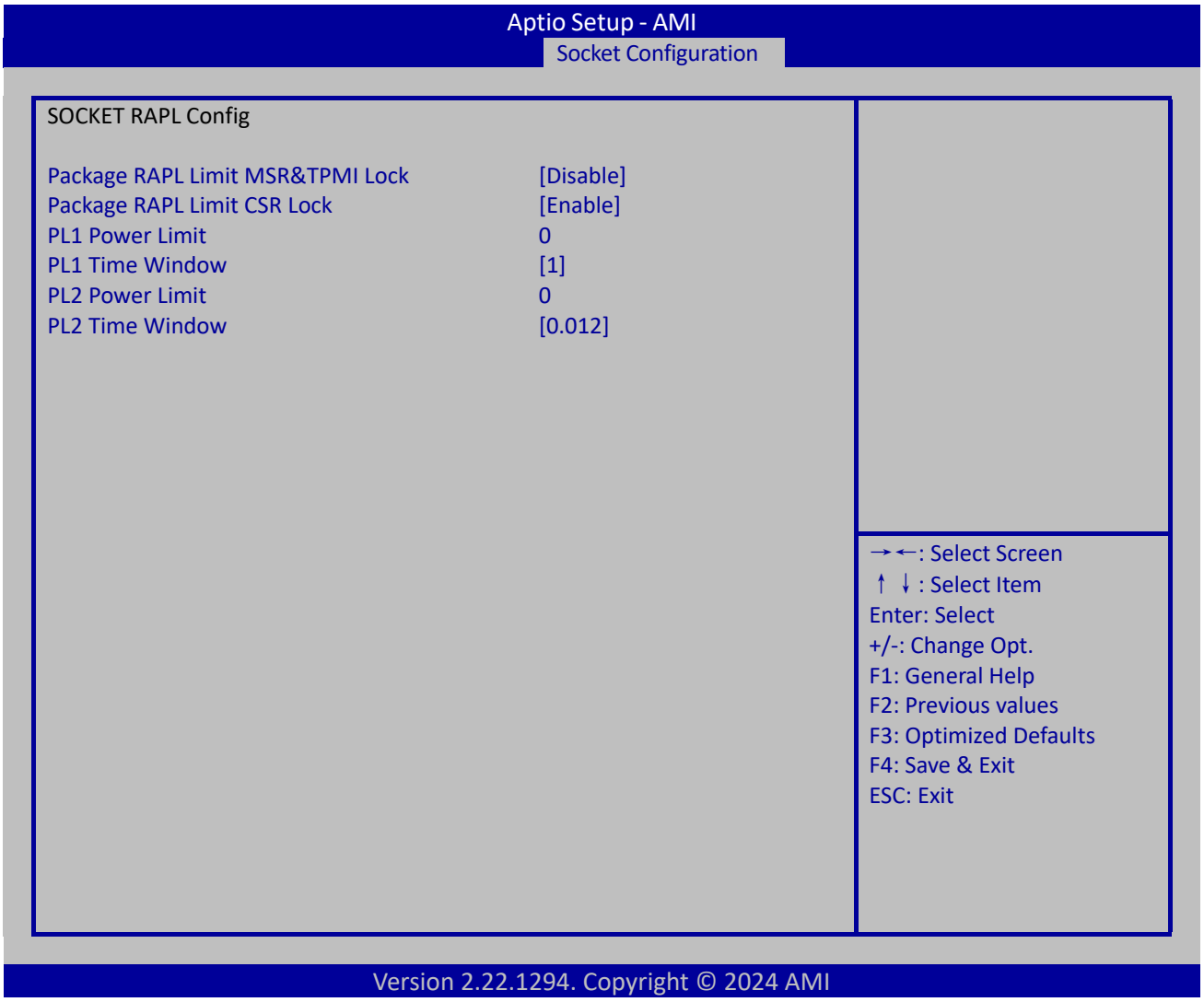
6.4.7.6.1 Energy Perf BIAS



Socket Configuration \ Advanced Power Management Configuration \ CPU – Advanced PM Tuning \ Energy Perf BIAS		
Menu Fields	**Settings**	**Comments**
Power Performance Tuning	**[OS Controls EPB]** [BIOS Controls EPB] [PECI Controls EPB]	Options decide who Controls EPB. In OS mode: IA32_ENERGY_PERF_BIAS is used In BIOS mode: ENERGY_PERF_BIAS_CONFIG is used In PECI mode: PCS53 is used
ENERGY_PERF_BIAS_CFG mode	[Performance] **[Balance Performance]** [Balance Power] [Power]	Use input from ENERGY_PERF_BIAS_CONFIG mode selection. PERF/Balanced Perf/Balanced Power/Power
Dynamic Loadline Switch	[Disable] **[Enable]**	Dynamic Loadline Switch control. MSR 0x1FC[Bit33]
Workload Configuration	**[Balanced]** [I/O sensitive]	This allows optimization for the workload characterization. The two options for selection
Averaging Time Window	**1A**	This is used to control the effective window of the average for C0 an P0 time

Socket Configuration \ Advanced Power Management Configuration \ CPU – Advanced PM Tuning \ Energy Perf BIAS		
Menu Fields	**Settings**	**Comments**
P0 TotalTimeThreshold Low	**28**	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than this threshold
P0 TotalTimeThreshold High	**3F**	The HW switching mechanism ENABLES the performance setting (0) when the total P0 time is greater than this threshold

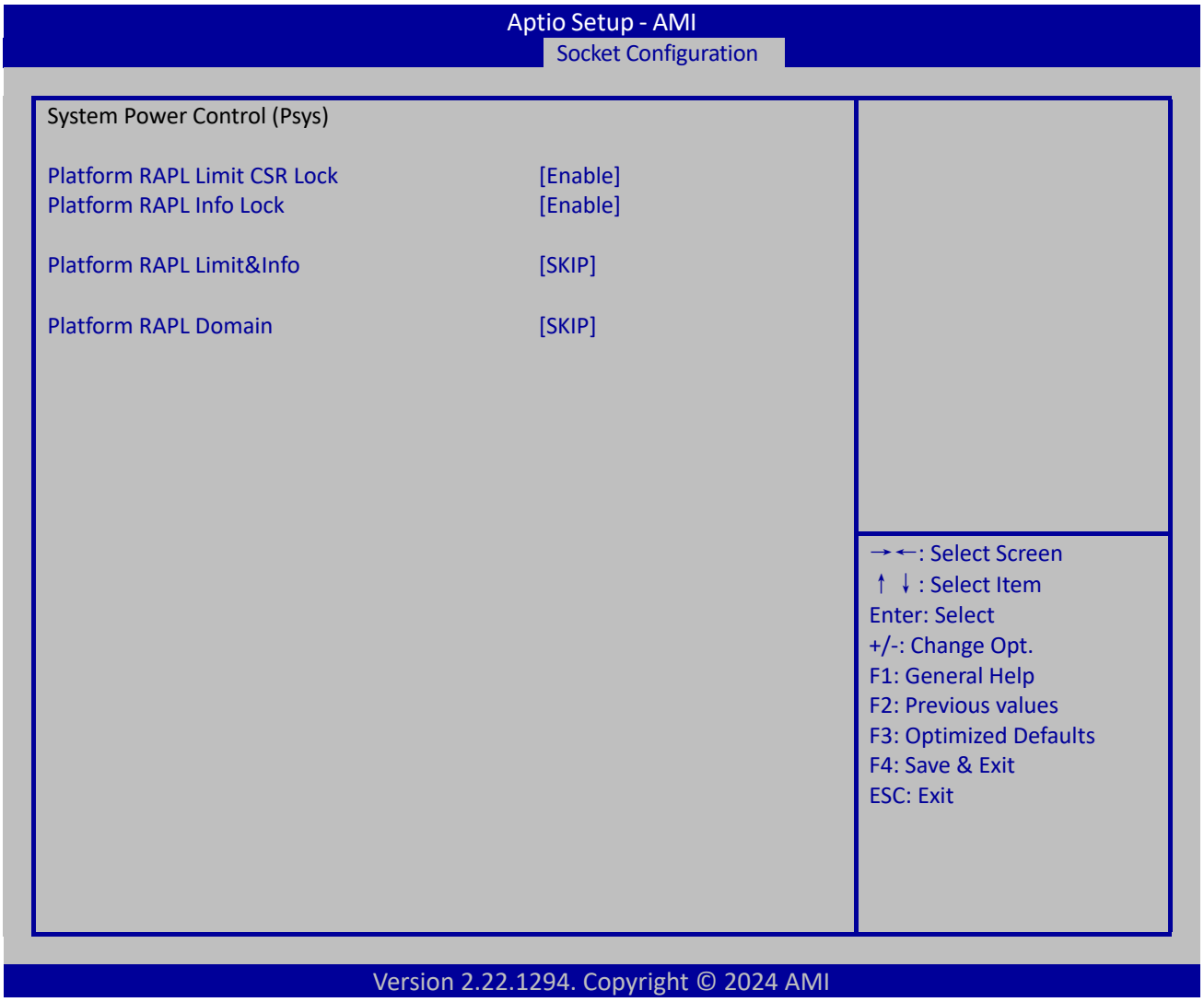
6.4.7.7 SOCKET RAPL Config



Socket Configuration \ Advanced Power Management Configuration \ SOCKET RAPL Config		
Menu Fields	**Settings**	**Comments**
Package RAPL Limit MSR&TPMI Lock	**[Disable]** [Enable]	Enable/Disable locking of Package RAPL Limit MSR&TPMI and a reset will be required to unlock the register.
Package RAPL Limit CSR Lock	[Disable] **[Enable]**	Enable/Disable locking of Package RAPL Limit CSR and a reset will be required to unlock the register.
PL1 Power Limit	**0**	PL1 Power Limit in Watts. The value may vary from 0 to Fused TDP Value. If the value is 0, the Fused TDP value will be programmed. A value greater than Fused TDP value will not be programmed.
PL1 Time Window	**[1]** [1.25] [1.5] [1.75] [2] [2.5] [3]	PL1 value in seconds. The value may vary from 1 to 5. Indicates the time window over which TDP value should be maintained.

Socket Configuration \ Advanced Power Management Configuration \ SOCKET RAPL Config		
Menu Fields	**Settings**	**Comments**
	[3.5] [4] [5]	
PL2 Power Limit	**0**	PL2 Power Limit in Watts. The value may vary from 0 to 120% Fused TDP Value. If the value is 0, BIOS programs 120% * Fused TDP value.
PL2 Time Window	**[0.012]** [0.014] [0.016] [0.02] [0.023] [0.027] [0.031] [0.039]	PL2 value in seconds. The value may vary from 0.012 to 0.039. Indicates the time window over which TDP value should be maintained.

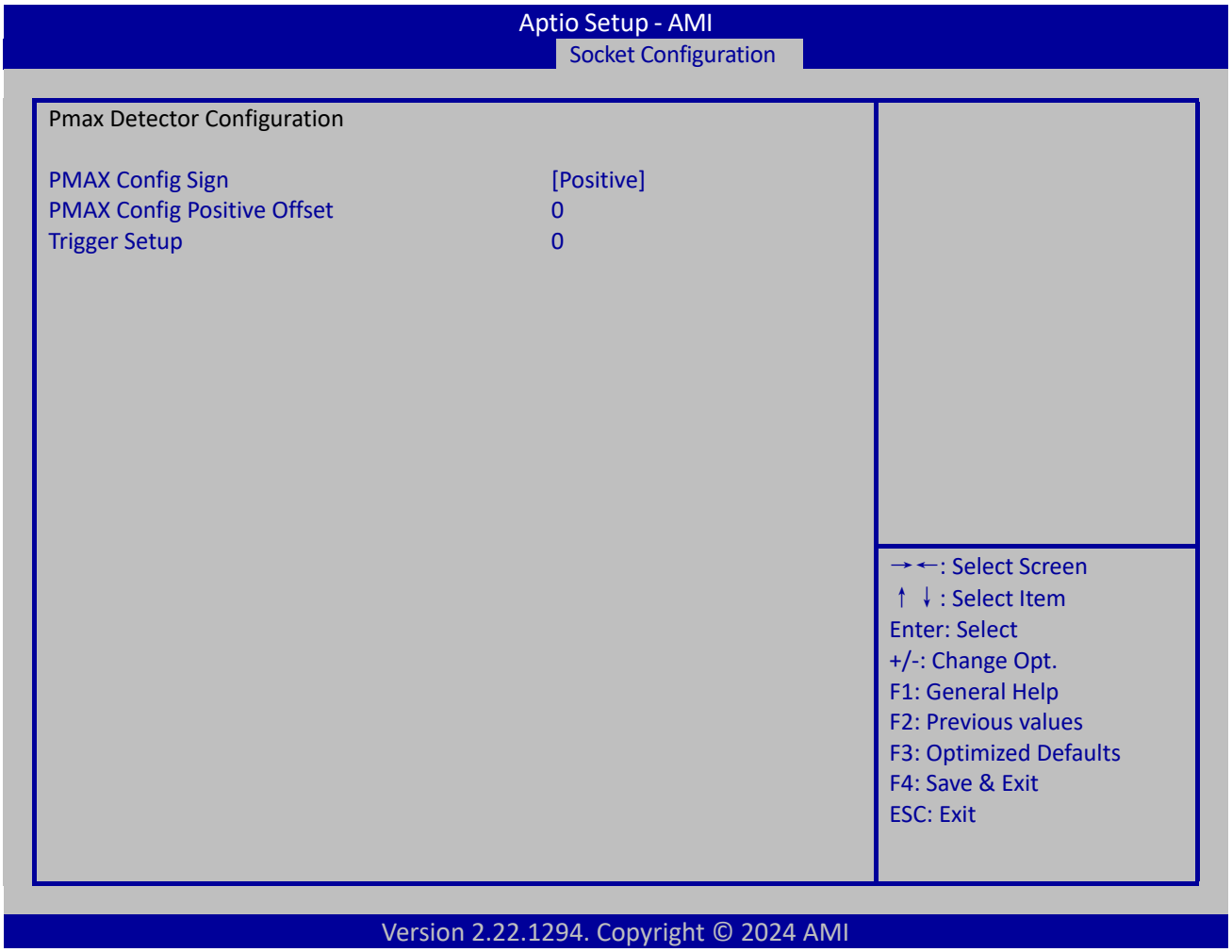
6.4.7.8 System Power Control (Psys)



Socket Configuration \ Advanced Power Management Configuration \ System Power Control (Psys)		
Menu Fields	**Settings**	**Comments**
Platform RAPL Limit CSR Lock	[Disable] **[Enable]**	Enable/Disable locking of Platform Power Limit CSR and a reset will be required to unlock the register.
Platform RAPL Info Lock	[Disable] **[Enable]**	Enable/Disable locking of Platform Power Info registers and a reset will be required to unlock the register.
Platform RAPL Limit&Info	**[SKIP]** [Beechnut City 1x PSU Config 1] [Beechnut City 1x PSU Config 2] [Beechnut City 2x PSU Config 1] [Beechnut City 2x PSU Config 2] [Beechnut City 3x PSU Config 1] [Manual]	Configure Platform RAPL Limit and Info by Platform Power Limit and Info CSR. SKIP: Use hardware default Manual: External customer to input manually Other options: Predefined board configures (PSU Config 1: 1600W PSU, PSU Config 2: 2130W PSU)
PPL1 Limit	[Disable] **[Enable]**	Enable/Disable PPL1 by Platform Power Limit CSR.
PPL1 Power Limit	**0**	PPL1 Power Limit in Watts.
PPL1 Time Window	**[1]**	PPL1 value in seconds.

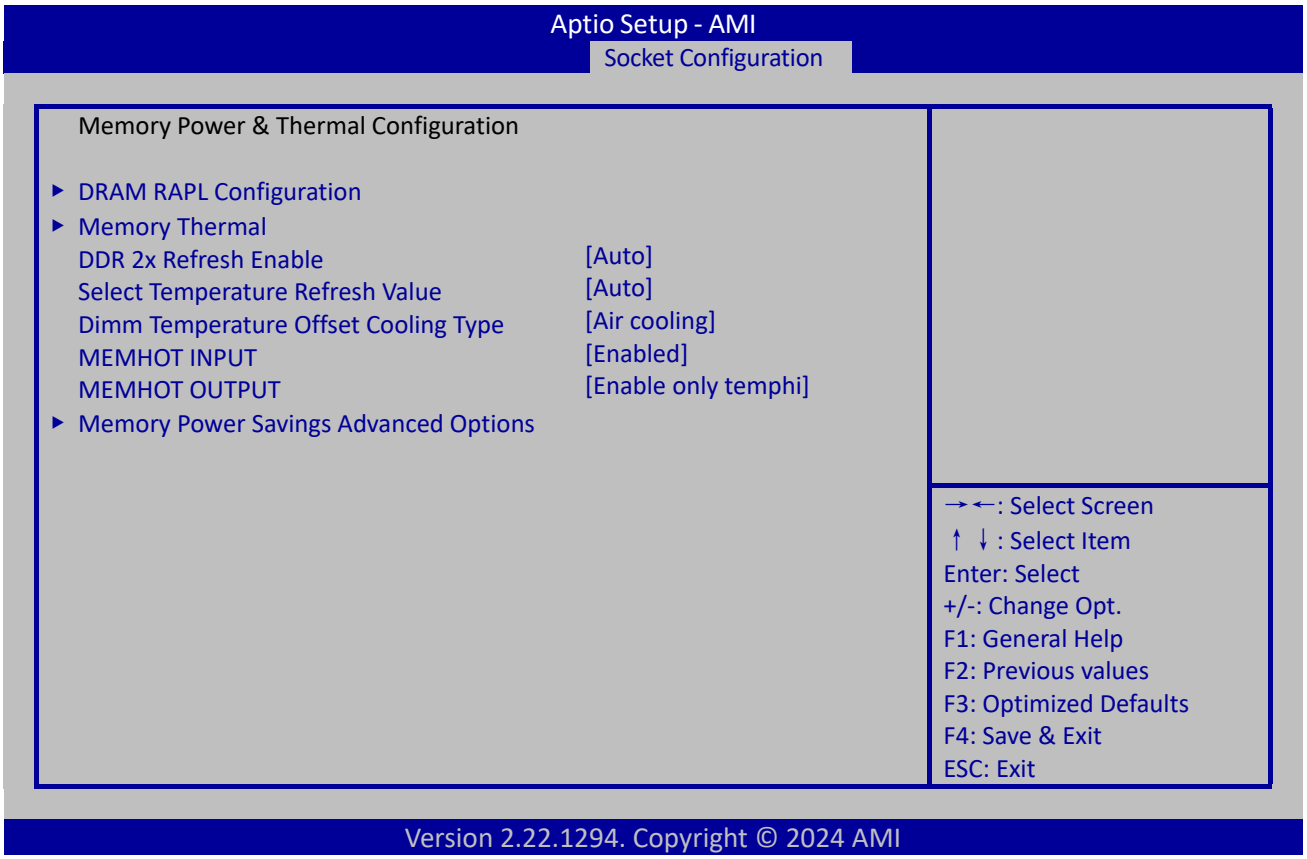
Socket Configuration \ Advanced Power Management Configuration \ System Power Control (Psys)		
Menu Fields	**Settings**	**Comments**
	[1.25] [1.5] [1.75] [2] [2.5] [3] [3.5] [4] [5]	
PPL2 Limit	[Disable] **[Enable]**	Enable/Disable PPL2 by Platform Power Limit CSR.
PPL2 Power Limit	**0**	PPL2 Power Limit in Watts.
PPL2 Time Window	**[0.012]** [0.014] [0.016] [0.02] [0.023] [0.027] [0.031] [0.039]	PPL2 value in seconds.
PPL Minimal Power Limit	**0**	Override the Minimal PPL power limit.
PPL1 Maximum Power Limit	**16383**	Override the Minimal PPL1 power limit.
PPL2 Maximum Power Limit	**16383**	Override the Minimal PPL2 power limit.
Maximum Time Window	**[1]** [1.25] [1.5] [1.75] [2] [2.5] [3] [3.5] [4] [5]	Override the Maximum PPL Time Window.
Platform RAPL Domain	**[SKIP]** [BEECHNUTCITY Domain Config 1] [BEECHNUTCITY Domain Config 2] [Manual]	Configure Psys socket primary and secondary by B2P mailbox PSYS_CONFIG. SKIP: Use hardware default Manual: External customer to input manually BEECHNUTCITY Domain Config 1: Even socket is primary and odd socket is secondary BEECHNUTCITY Domain Config 2: Even socket is secondary and odd socket is primary
Socket x is primary	**[Disabled]** [Enabled]	Set the socket x as primary which connected with Psys sensor.

6.4.7.9 Pmax Detector Configuration



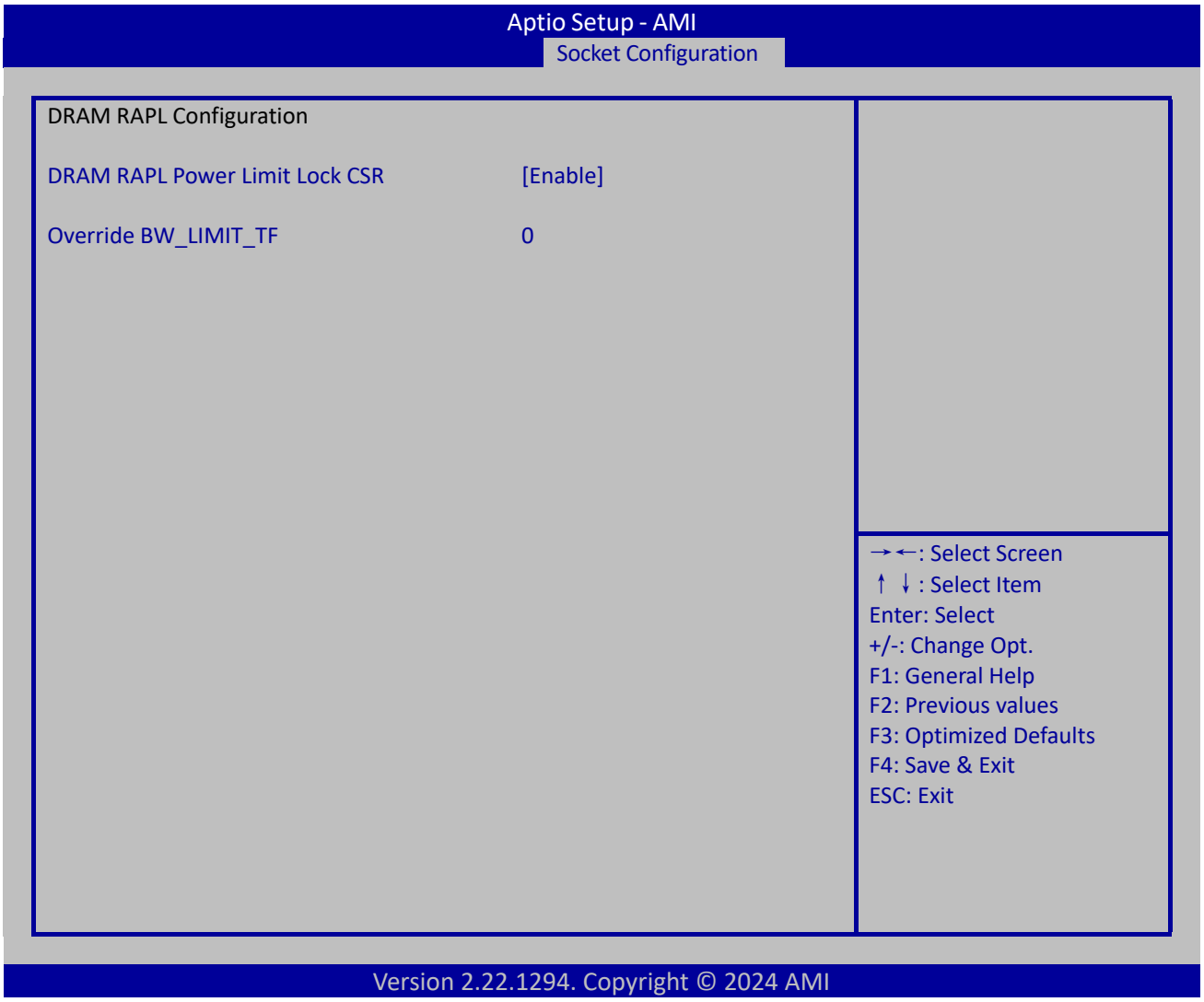
Socket Configuration \ Advanced Power Management Configuration \ Pmax Detector Configuration		
Menu Fields	**Settings**	**Comments**
PMAX Config Sign	**[Positive]** [Negative]	Negative: Detector will trip on higher power consumption. Positive: Detector will trip on lower power consumption.
PMAX Config Positive Offset	**0**	Input decimal correction factor to program. Valid input values are 0 to 63. Will be positive based on PMAX Config Sign value.
PMAX Config Negative Offset	**0**	Input decimal correction factor to program. Valid input values are 0 to 6. Will be negative based on PMAX Config Sign value.
Trigger Setup	**0**	Possible selection options [0], [1], [2] [0] = Interaction disabled (default) [1] = Enable external trigger mode [2] = Enable internal trigger observability

6.4.7.10 Memory Power & Thermal Configuration



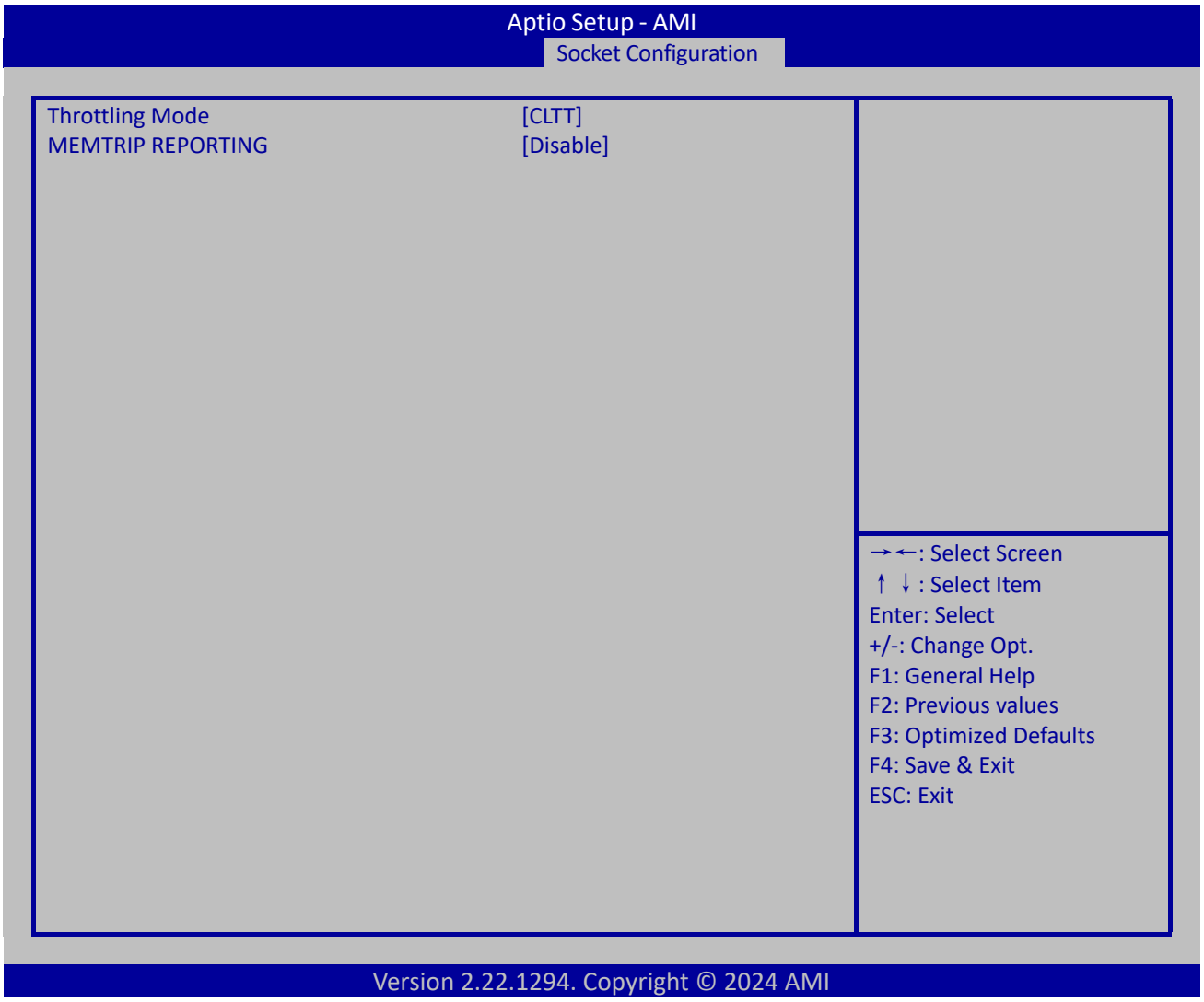
Socket Configuration \ Advanced Power Management Configuration \ Memory Power & Thermal Configuration		
Menu Fields	**Settings**	**Comments**
DRAM RAPL Configuration	Selects sub-menu.	
Memory Thermal	Selects sub-menu.	
DDR 2x Refresh Enable	**[Auto]** [Disable] [Enable]	Enable/Disable 2x Refresh. Auto = dynamically selected.
Select Temperature Refresh Value	**[Auto]** [Manual]	Option to manually enter Temperature refresh value. Select Manual to enter value, Auto for default
Dimm Temperature Offset Cooling Type	**[Air cooling]** [Liquid cooling (tube)] [Immersion cooling]	DIMM cooling type to define temperature Offset value.
MEMHOT INPUT	[Disabled] **[Enabled]**	Configure Memhot input
MEMHOT OUTPUT	[Disabled] **[Enable only temphi]** [Enable only temphi & mid] [Enable only temphi, mid and low]	Configure Memhot output
Memory Power Savings Advanced Options	Selects sub-menu.	

6.4.7.10.1 DRAM RAPL Configuration



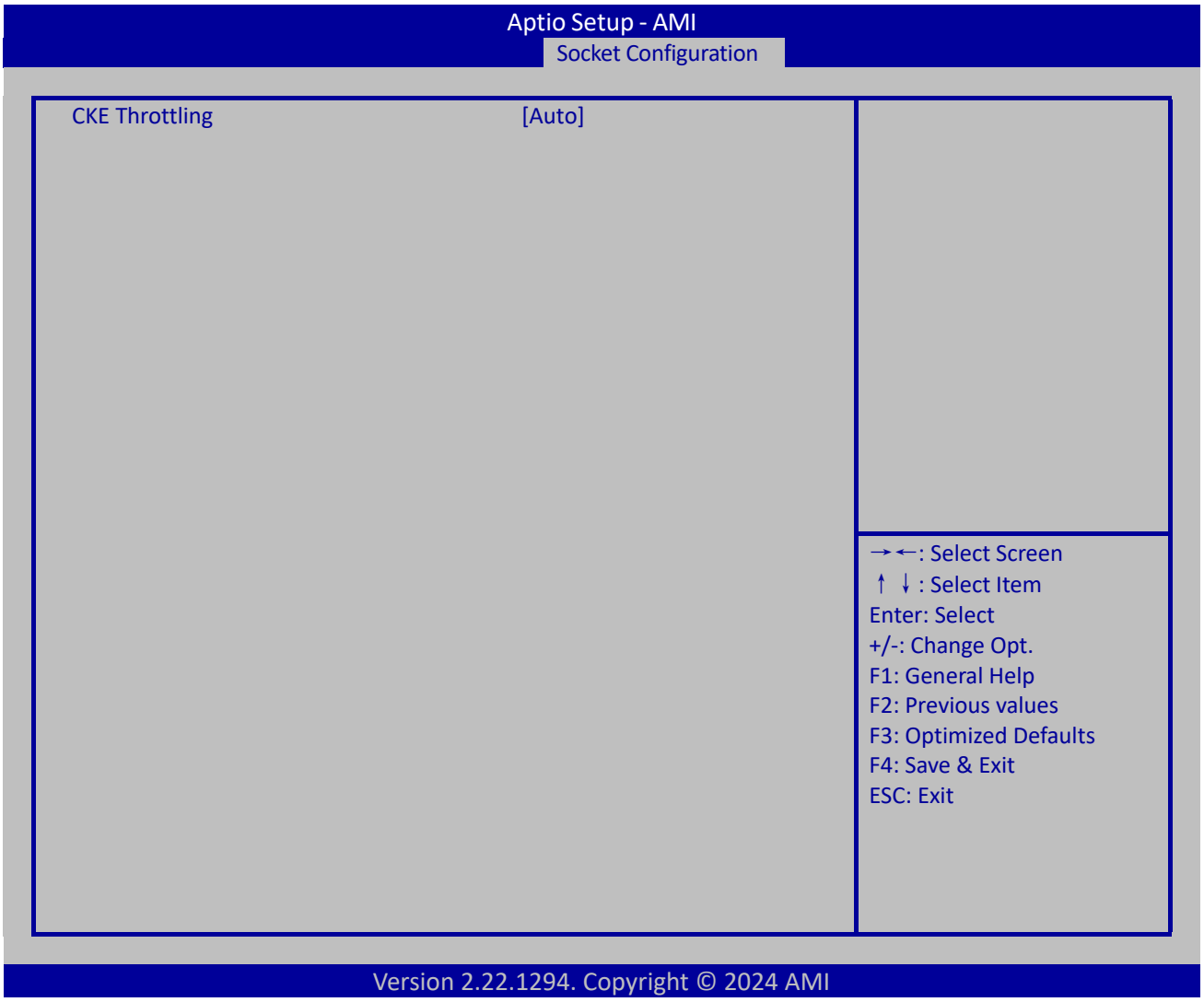
Socket Configuration \ Advanced Power Management Configuration \ Memory Power & Thermal Configuration \ DRAM RAPL Configuration		
Menu Fields	**Settings**	**Comments**
DRAM RAPL Power Limit Lock CSR	[Disable] **[Enable]**	This Option allows unlock/lock DRAM_PLANE_POWER_LIMIT.pp_pwr_lim_lock. Enable – Lock Disable - Unlock
Override BW_LIMIT_TF	**0**	Allows custom tuning of BW_LIMIT_TF

6.4.7.10.2 Memory Thermal



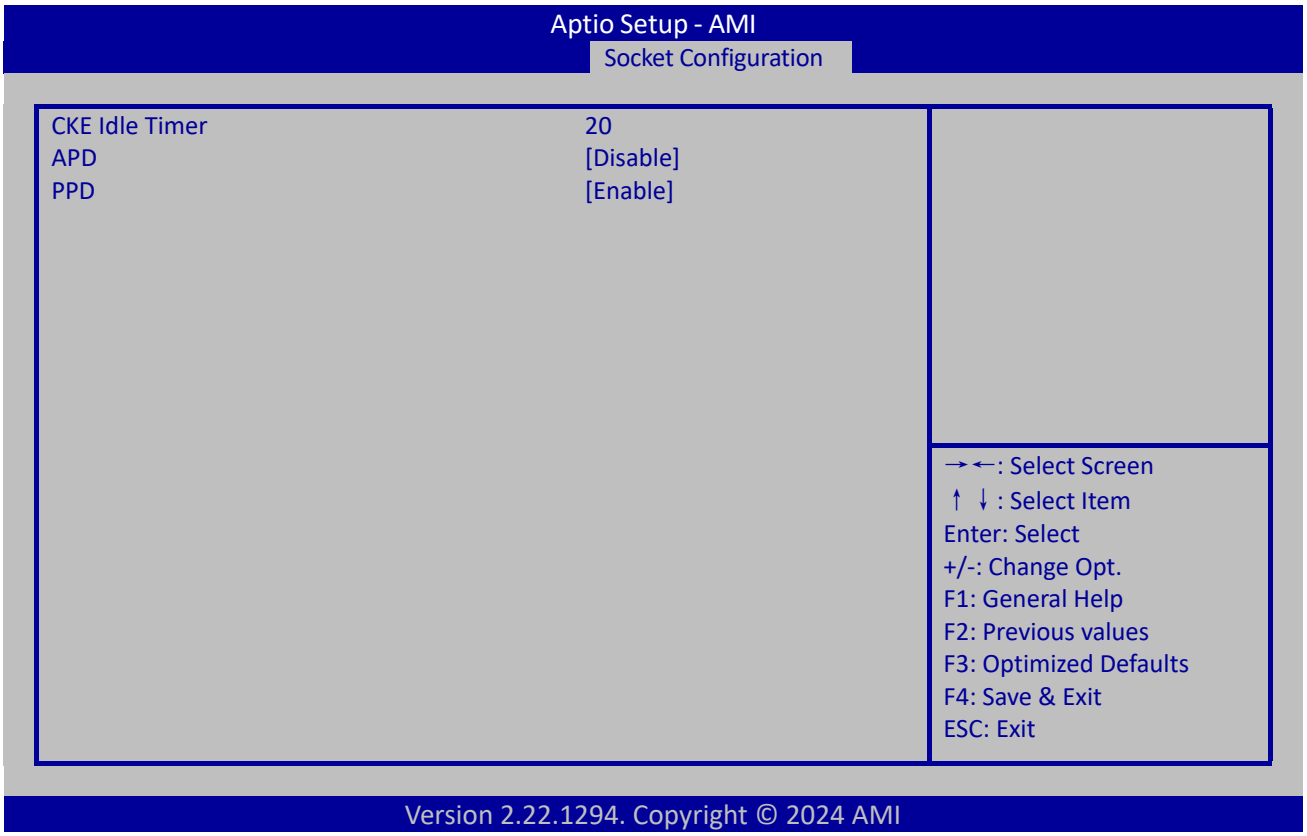
Socket Configuration \ Advanced Power Management Configuration \ Memory Power & Thermal Configuration \ Memory Thermal		
Menu Fields	**Settings**	**Comments**
Throttling Mode	[Disable] **[CLTT]** [CLTT with PECI]	Configure Thermal Throttling Mode.
MEMTRIP REPORTING	**[Disable]** [Enable]	Disable - Processor will ignore all Mem Trip tree. Enable - Processor will include all Mem Trip tree.

6.4.7.10.3 Memory Power Savings Advanced Options



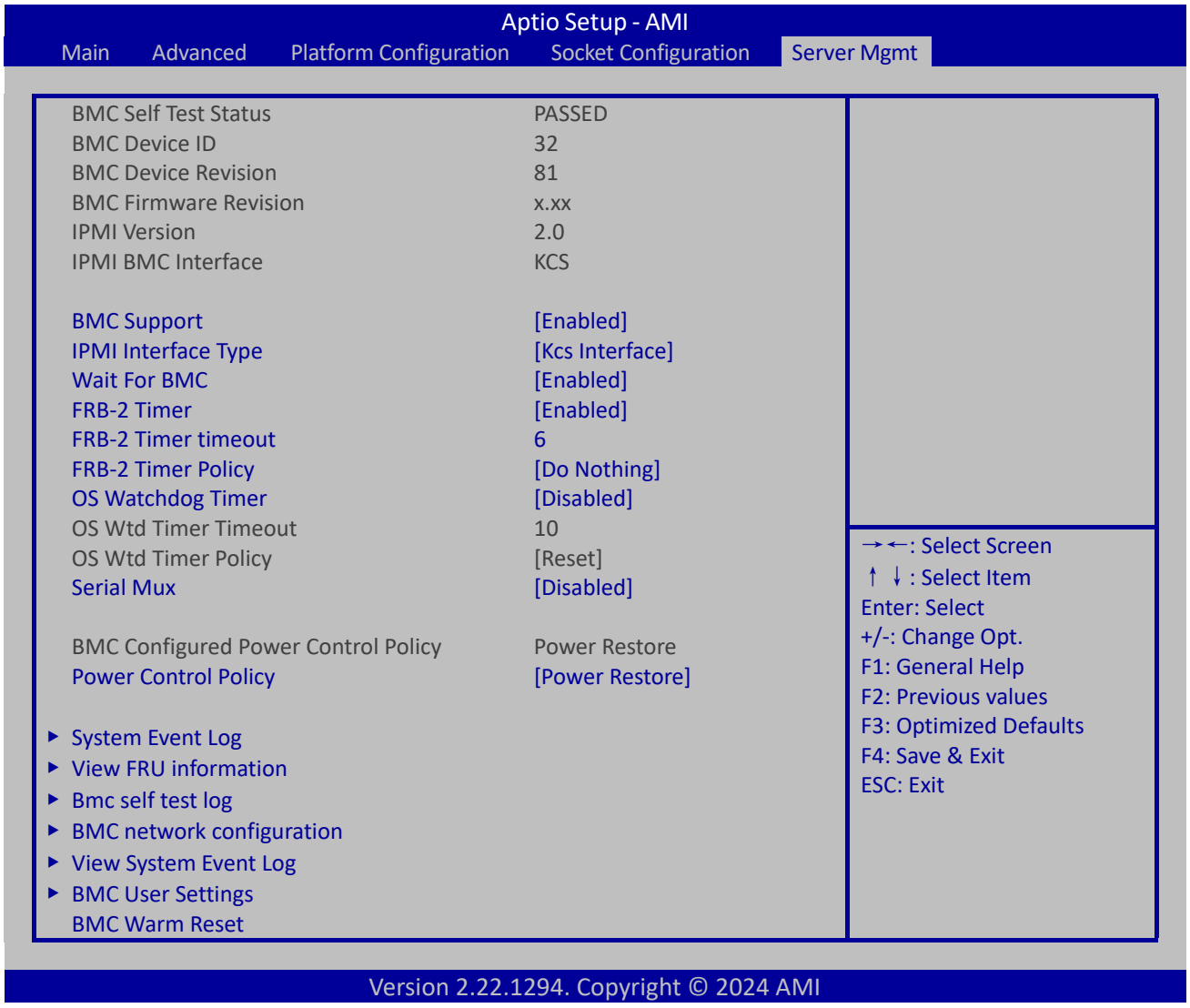
Socket Configuration \ Advanced Power Management Configuration \ Memory Power & Thermal Configuration \ Memory Power Savings Advanced Options		
Menu Fields	**Settings**	**Comments**
CKE Throttling	**[Auto]** [Manual]	Configures CKE Throttling
CKE Feature	Selects sub-menu.	

6.4.7.10.3.1 CKE Feature



Socket Configuration \ Advanced Power Management Configuration \ Memory Power & Thermal Configuration \ Memory Power Savings Advanced Options \ CKE Feature		
Menu Fields	**Settings**	**Comments**
CKE Idle Timer	**20**	CKE Idle Timer in ns.
APD	**[Disable]** [Enable]	Active Power-Down mode On/Off
PPD	[Disable] **[Enable]**	Pre-charge Power-Down mode On/Off

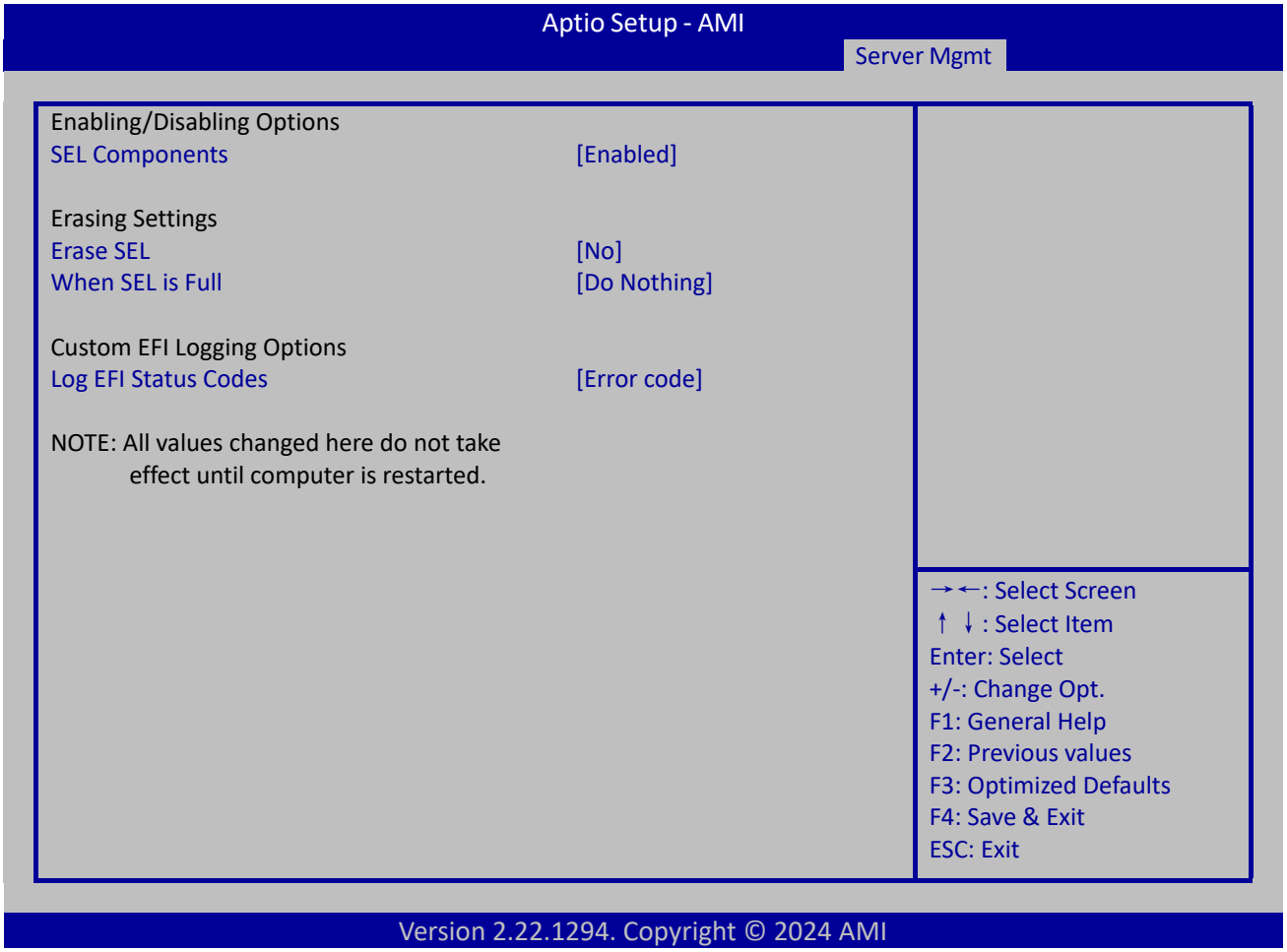
6.5 SERVER MGMT



Server Mgmt		
Menu Fields	**Settings**	**Comments**
BMC Self Test Status	PASSED	Displays the BMC Self Test Status.
BMC Device ID	32	Displays the BMC Device ID.
BMC Device Revision	81	Displays the BMC Device Revision.
BMC Firmware Revision	x.xx	Displays the BMC version.
IPMI Version	2.0	Displays the IPMI version.
IPMI BMC Interface	KCS	Displays the type of interface to communicate BMC from HOST.
BMC Support	**[Enabled]** [Disabled]	Enable/Disable interfaces to communicate with BMC
IPMI Interface Type	**[Kcs Interface]** [Bt 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

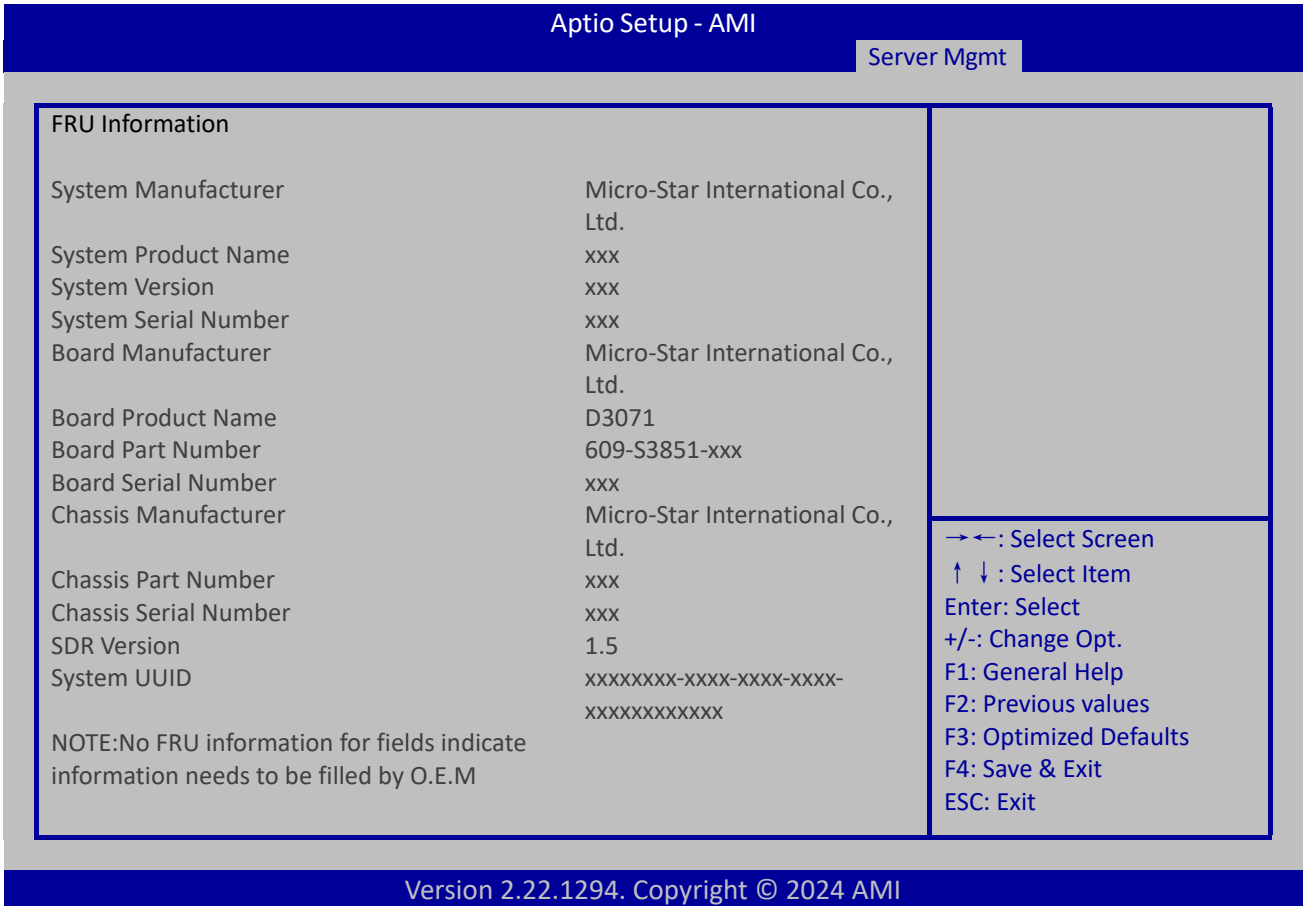
Server Mgmt		
Menu Fields	**Settings**	**Comments**
		during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.
FRB-2 Timer	**[Enabled]** [Disabled]	Enable or Disable FRB-2 timer(POST timer)
FRB-2 Timer timeout	**6**	Enter value Between 1 to 30 min for FRB-2 Timer Expiration
FRB-2 Timer Policy	**[Do Nothing]** [Reset] [Power Down] [Power Cycle]	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.
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 successfully loaded or follows the OS Boot Watchdog Timer policy.
OS Wtd Timer Timeout	**10**	Enter the 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.
BMC Configured Power Control Policy	Power Restore	Displays the current BMC power restore policy status.
Power Control Policy	[Do Not PowerUp] [Last Power State] **[Power Restore]**	Configure how the system should respond if AC Power is lost,Reset not required as selected Power policy will be set in BMC when policy is saved
System Event Log	Selects sub-menu.	
View FRU information	Selects sub-menu.	
Bmc self test log	Selects sub-menu.	
BMC network configuration	Selects sub-menu.	
View System Event Log	Selects sub-menu.	
BMC User Settings	Selects sub-menu.	
BMC Warm Reset		Press <Enter> to do Warm Reset BMC.

6.5.1 System Event Log



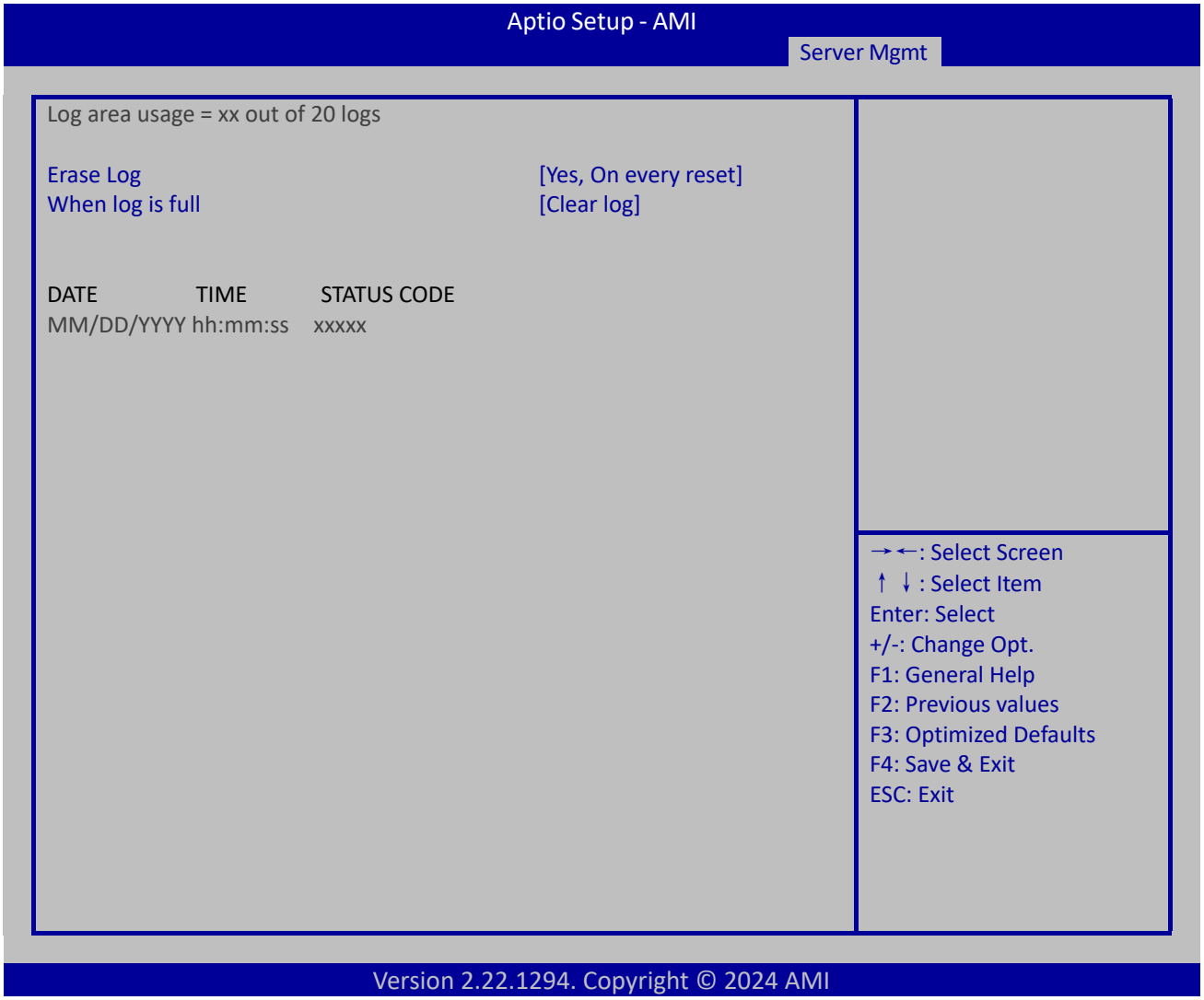
Server Mgmt \ System Event Log		
Menu Fields	**Settings**	**Comments**
Enabling/Disabling Options		
SEL Components	[Disabled] **[Enabled]**	Change this to enable or disable event logging for error/progress codes during boot.
Erasing Settings		
Erase SEL	**[No]** [Yes, On next reset] [Yes, On every reset]	Choose options for erasing SEL.
When SEL is Full	**[Do Nothing]** [Erase Immediately] [Delete Oldest Record]	Choose options for reactions to a full SEL.
Custom EFI Logging Options		
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.

6.5.2 View FRU information



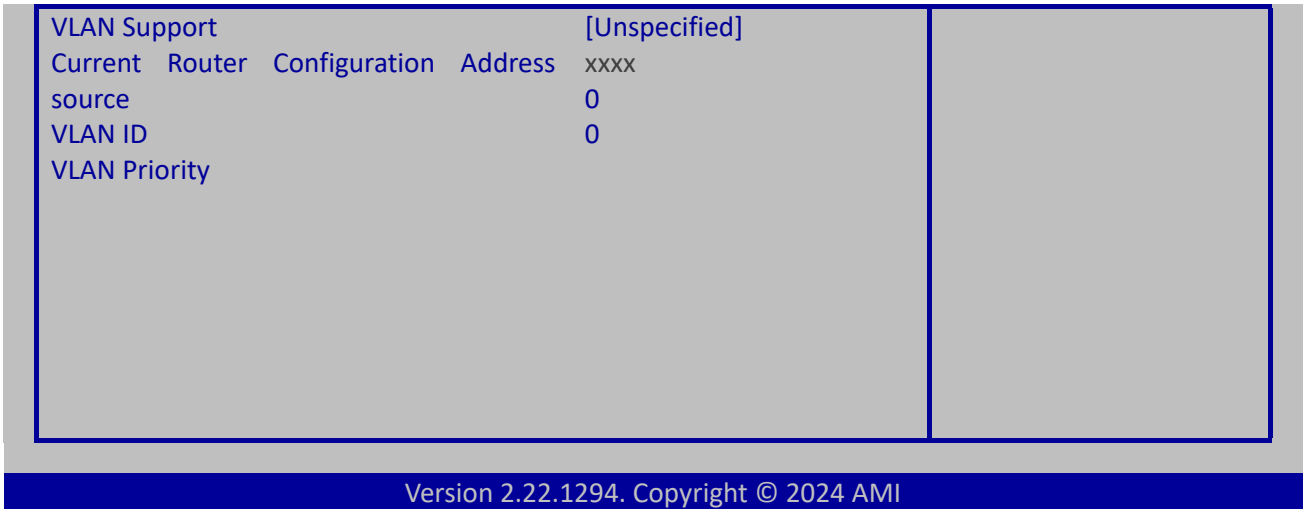
Server Mgmt \ View FRU information		
Menu Fields	**Settings**	**Comments**
FRU Information		
System Manufacturer	Micro-Star International Co., Ltd.	Displays the FRU System Manufacturer.
System Product Name	xxx	Displays the FRU System Product Name.
System Version	xxx	Displays the FRU System Version.
System Serial Number	xxx	Displays the FRU System Serial Number.
Board Manufacturer	Micro-Star International Co., Ltd.	Displays the FRU Board Manufacturer.
Board Product Name	D3071	Displays the FRU Board Product Name.
Board Part Number	609-S3851-xxx	Displays the FRU Board Part Number.
Board Serial Number	xxx	Displays the FRU Board Serial Number.
Chassis Manufacturer	Micro-Star International Co., Ltd.	Displays the FRU Chassis Manufacturer.
Chassis Part Number	xxx	Displays the FRU Chassis Part Number.
Chassis Serial Number	xxx	Displays the FRU Chassis Serial Number.
SDR Version	1.5	Displays the Version of Sensor Data Records.
System UUID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Displays the System Unique ID.

6.5.3 Bmc self test log



Server Mgmt \ Bmc self test log		
Menu Fields	**Settings**	**Comments**
Log area usage = xx out of 20 logs		Displays the log area usage
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
DATE TIME STATUS CODE		
MM/DD/YYYY hh:mm:ss xxxxx		Logs the report returned by BMC self test command

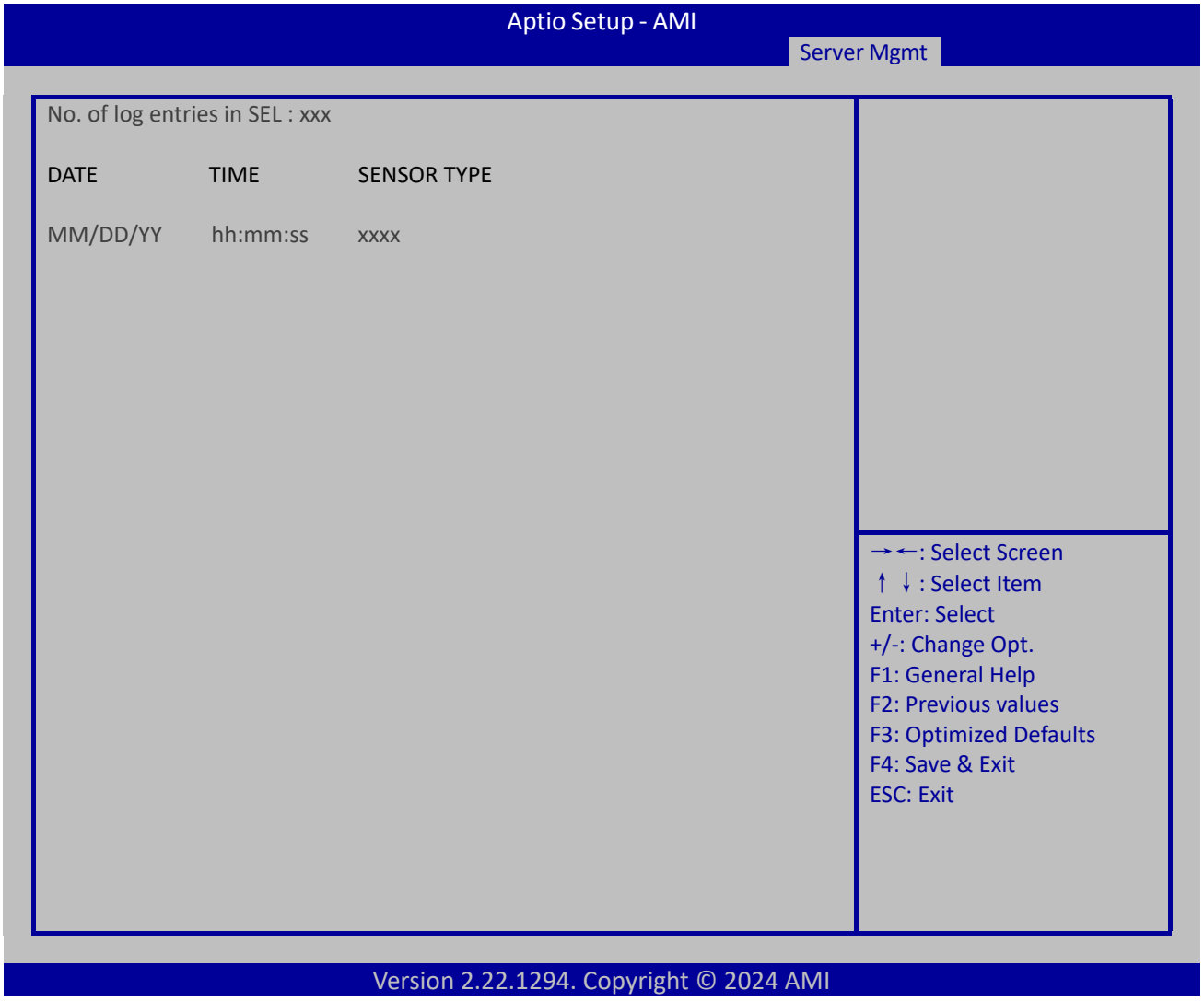
6.5.4 BMC network configuration



Server Mgmt \ BMC network configuration		
Menu Fields	**Settings**	**Comments**
BMC network configuration		
Configure IPv4 support		
Lan channel x		
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 any BMC network parameters during BIOS phase
Current Configuration Address source	xxxxxxxx	Current LAN Configuration statically or dynamically(by BIOS or BMC). Unspecified for not Configured address space
Station IP address	**...**	Enter station IP address
Subnet mask	**...**	Enter subnet mask
Station MAC address	xx-xx-xx-xx-xx-xx	
Router IP address	**0.0.0.0**	Enter router IP address
Router MAC address	**00-00-00-00-00-00**	Enter router MAC address
Configure IPv6 support		
Lan channel x		
IPv6 Support	**[Enabled]** [Disabled]	Enable or Disable LANx IPv6 Support
Configuration Address source	**[Unspecified]** [Static] [DynamicBmcDhcp]	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Current Configuration Address source	xxxxxxxx	Current IPv6 LAN Configuration statically or dynamically by BMC). Unspecified for not Configured address space
Station IPv6 address	**:::::::**	Enter station IPv6 address
Prefix Length	**0**	Change the prefix length
IPv6 address status	Disabled	Status of station IPv6 address to BMC.
IPv6 DHCP Algorithm	DHCPv6	Providing the DHCP method used like DHCPv6 or StateLess Address Auto Configuration(SLAAC).

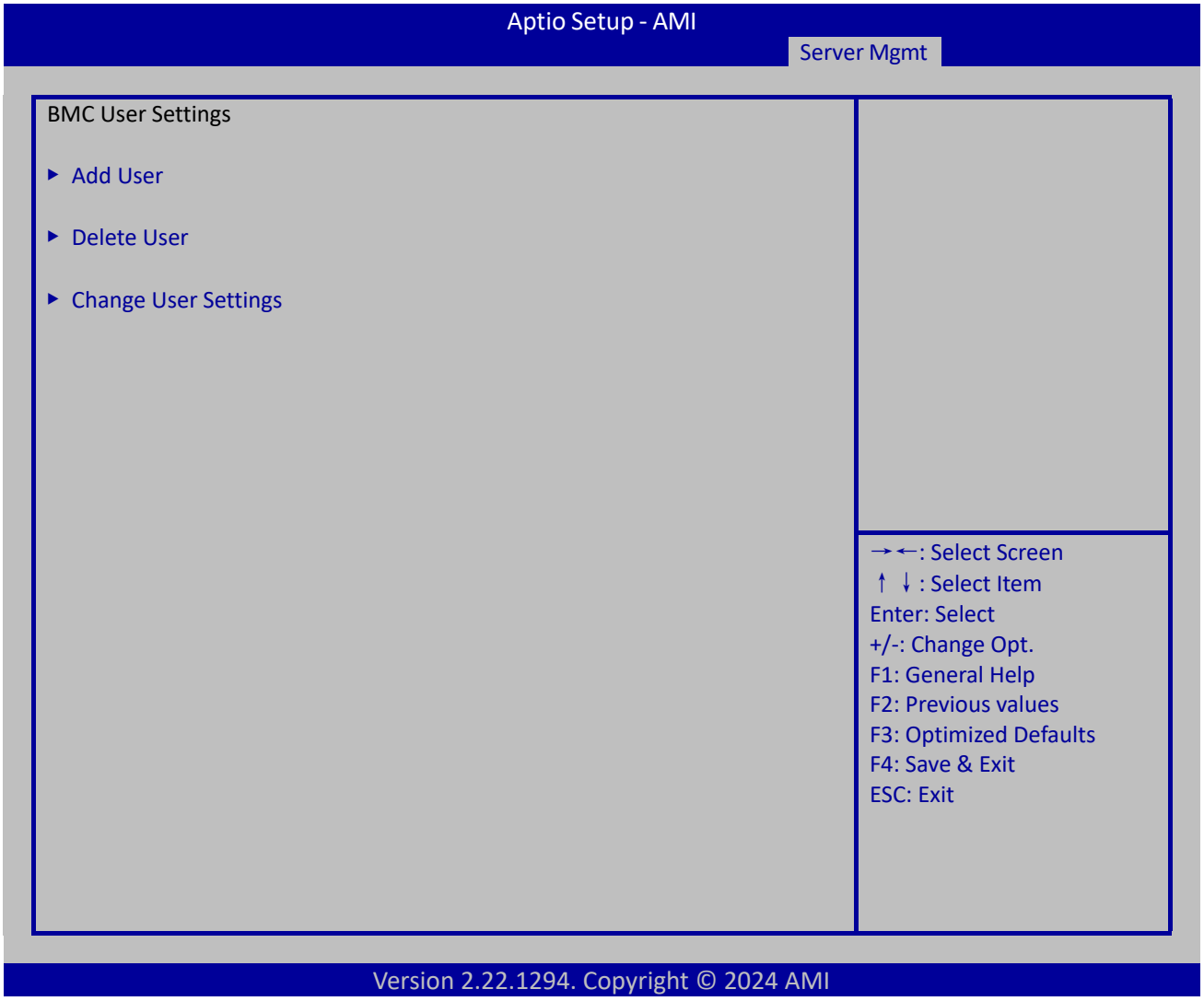
Server Mgmt \ BMC network configuration		
Menu Fields	**Settings**	**Comments**
Configuration Router LanX Address source	**[Unspecified]** [Static] [DynamicBmcDhcp]	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Current Router Configuration Address source	xxxxxxxx	Current IPv6 Router LAN Configuration statically or dynamically by BMC). Unspecified for not Configured address space
IPv6 Router1 IP Address	**:::::::**	Change the IPv6 Router1 IP Address
IPv6 Router1 Prefix Length LanX	**0**	Change the IPv6 Router Prefix Length
IPv6 Router1 Prefix Value LanX	**:::::::**	Change the IPv6 Router Prefix Value
Configure VLAN support		
Lan channel x		
VLAN Support	[Enabled] [Disabled] **[Unspecified]**	Enable VLAN Support to specify the 802.1q VLAN ID
Current Router Configuration Address source	xxxx	Current VLAN Configuration Enabled or Disabled(by BIOS or BMC). Unspecified for not Configured address space
VLAN ID	**0**	VLAN ID Range is from 1-4094. VLAN ID 0 & 4095 are reserved VLAN ID's.
VLAN Priority	**0**	Value ranges from 0 to 7. 7 is the highest priority for VLAN.

6.5.5 View System Event Log



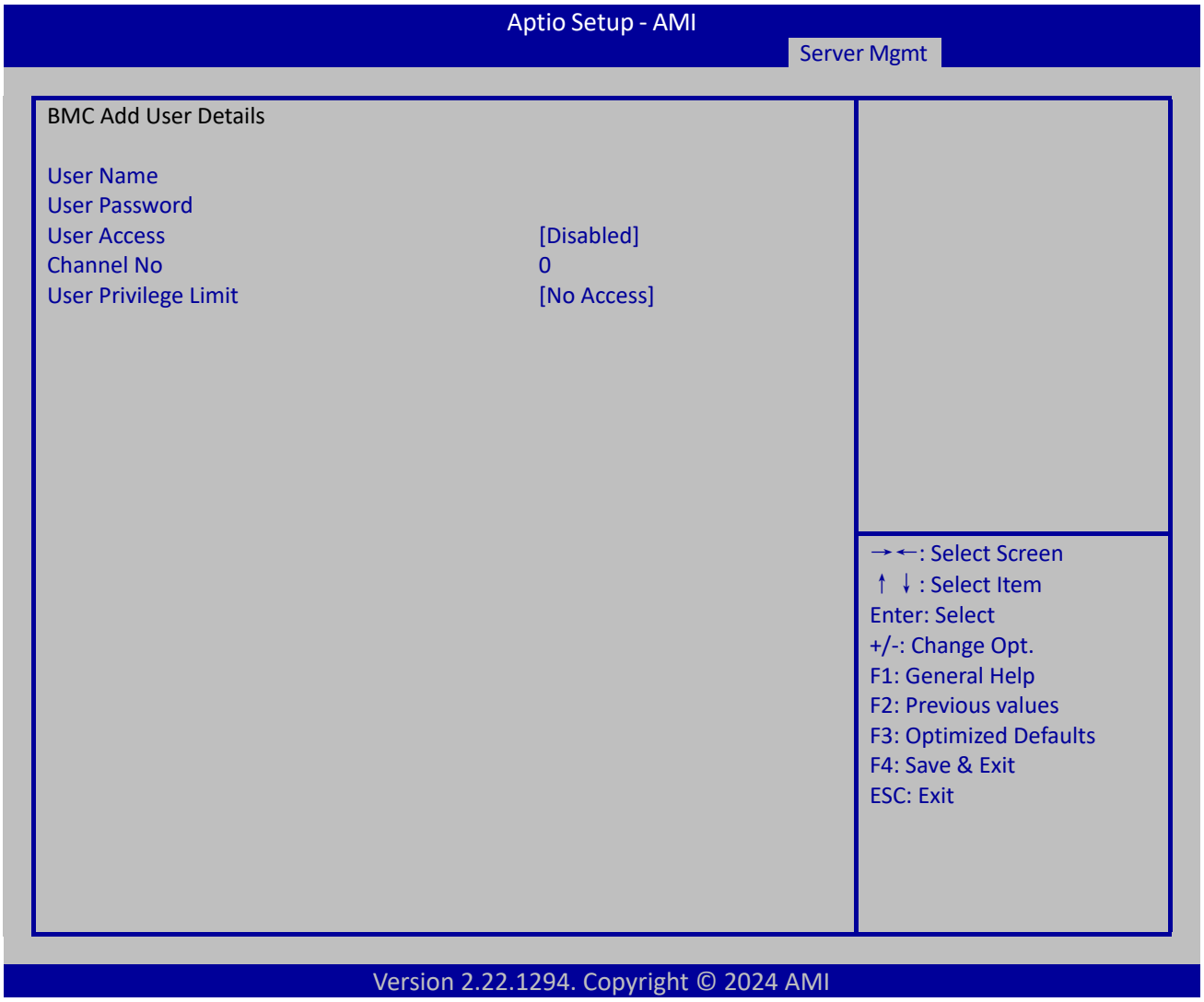
Server Mgmt \ View System Event Log		
Menu Fields	**Settings**	**Comments**
No. of log entries in SEL : xxx		Displays the number of log entries in SEL.
MM/DD/YY hh:mm:ss xxxx		HEX: xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx Generator ID: Sensor Number: Event Description: Record Type Assertion/Deassertion Event

6.5.6 BMC User Settings



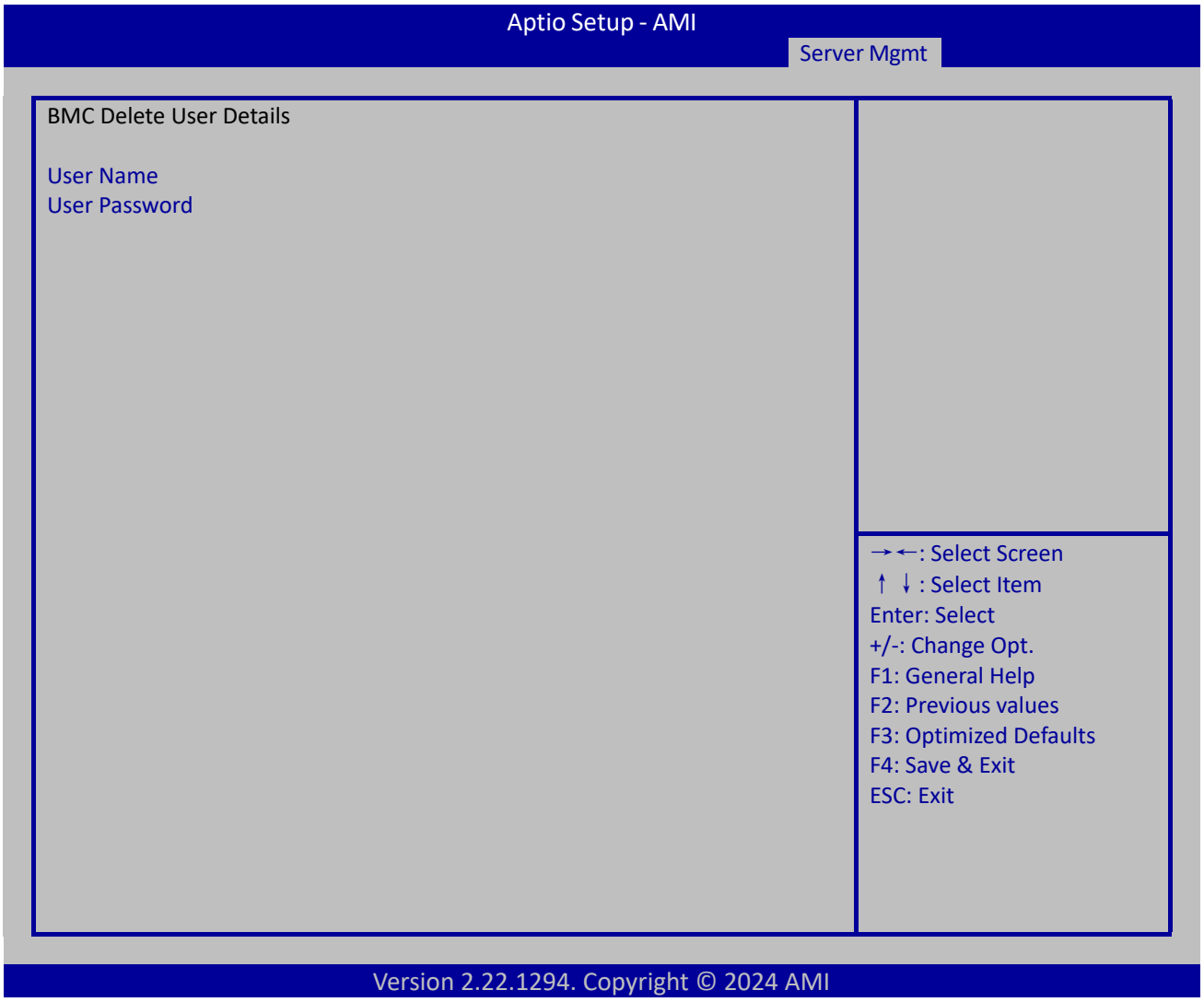
Server Mgmt \ BMC User Settings		
Menu Fields	**Settings**	**Comments**
BMC User Settings		
Add User	Selects sub-menu.	
Delete User	Selects sub-menu.	
Change User Settings	Selects sub-menu.	

6.5.6.1 Add User



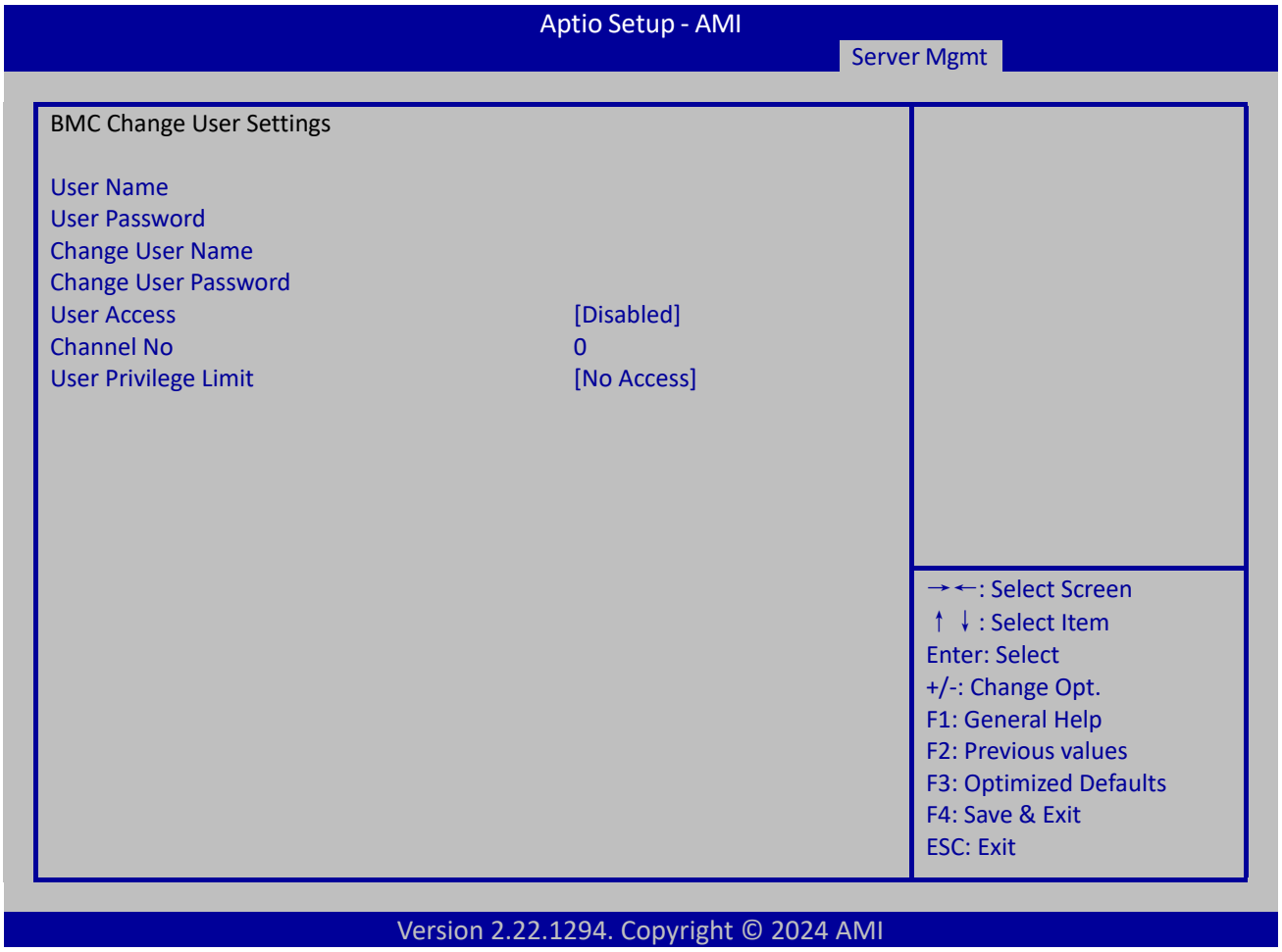
Server Mgmt \ BMC User Settings \ Add User		
Menu Fields	**Settings**	**Comments**
BMC Add User Details		
User Name		Enter BMC User Name
User Password		Enter BMC User Password
User Access	[Enabled] **[Disabled]**	Enable/Disable the BMC User's Access.
Channel No	**0**	Enter BMC Channel Number
User Privilege Limit	**[No Access]** [Callback] [User] [Operator] [Administrator]	Enter BMC User Privilege Limit for Selected Channel

6.5.6.2 Delete User



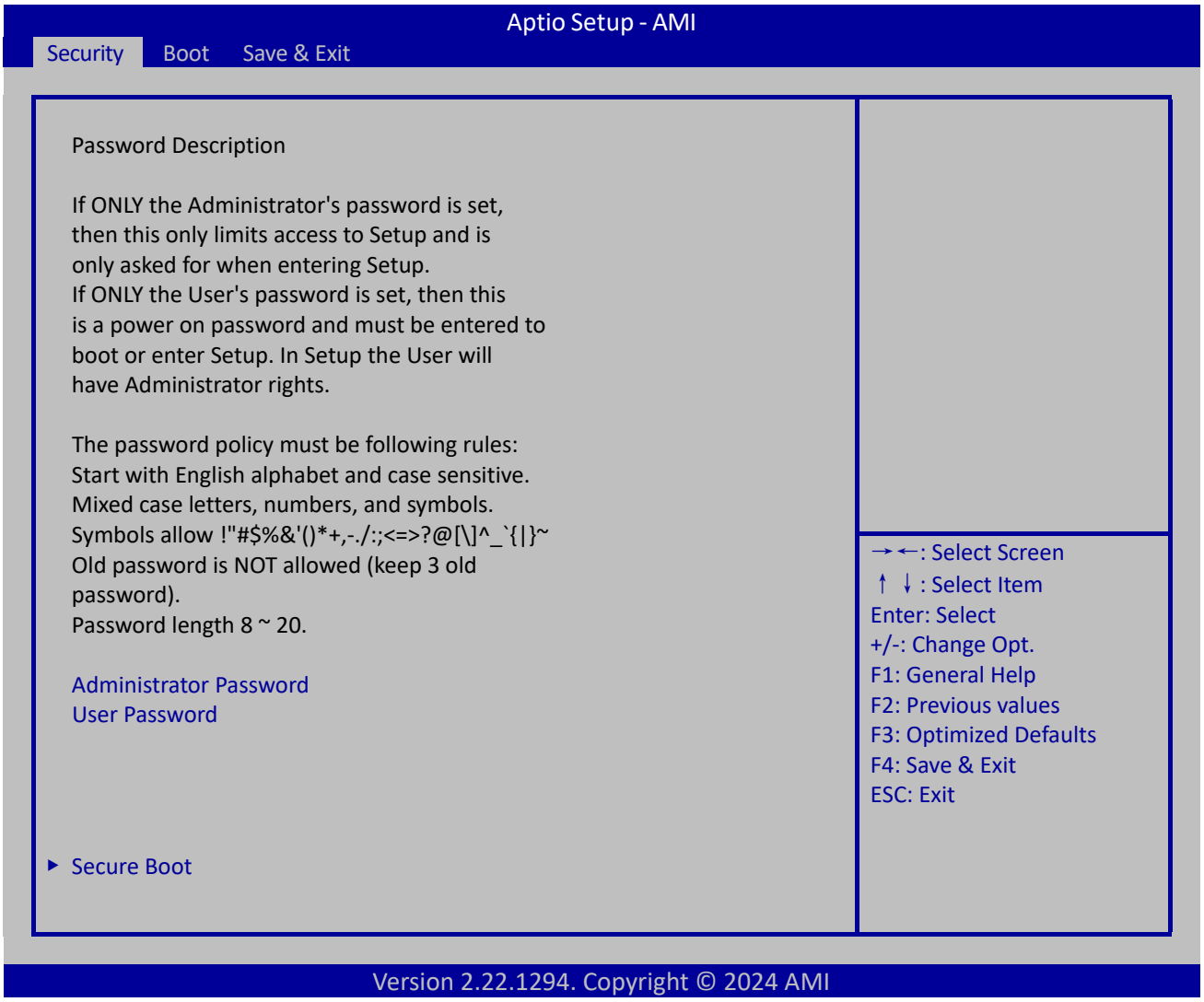
Server Mgmt \ BMC User Settings \ Delete User		
Menu Fields	**Settings**	**Comments**
BMC Delete User Details		
User Name		Enter BMC User Name
User Password		Enter BMC User Password

6.5.6.3 Change User Settings



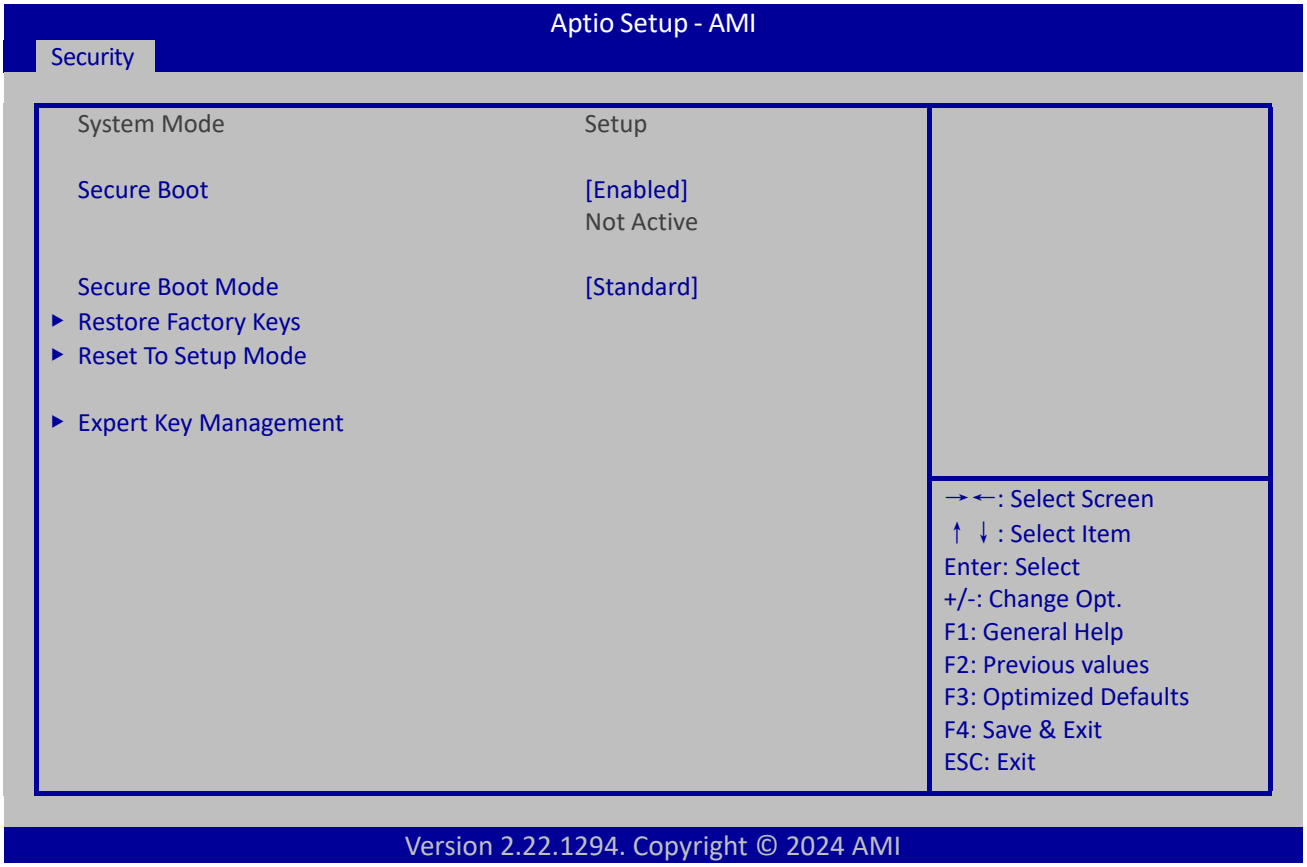
Server Mgmt \ BMC User Settings \ Change User Settings		
Menu Fields	**Settings**	**Comments**
BMC Change User Settings		
User Name		Enter BMC User Name
User Password		Enter BMC User Password
Change User Name		Enter New User Name
Change User Password		Enter New Password to change.
User Access	[Enabled] **[Disabled]**	Enable/Disable the BMC User's Access.
Channel No	**0**	Enter BMC Channel Number
User Privilege Limit	**[No Access]** [Callback] [User] [Operator] [Administrator] [OEM Proprietary]	Enter BMC User Privilege Limit for Selected Channel

6.6 SECURITY



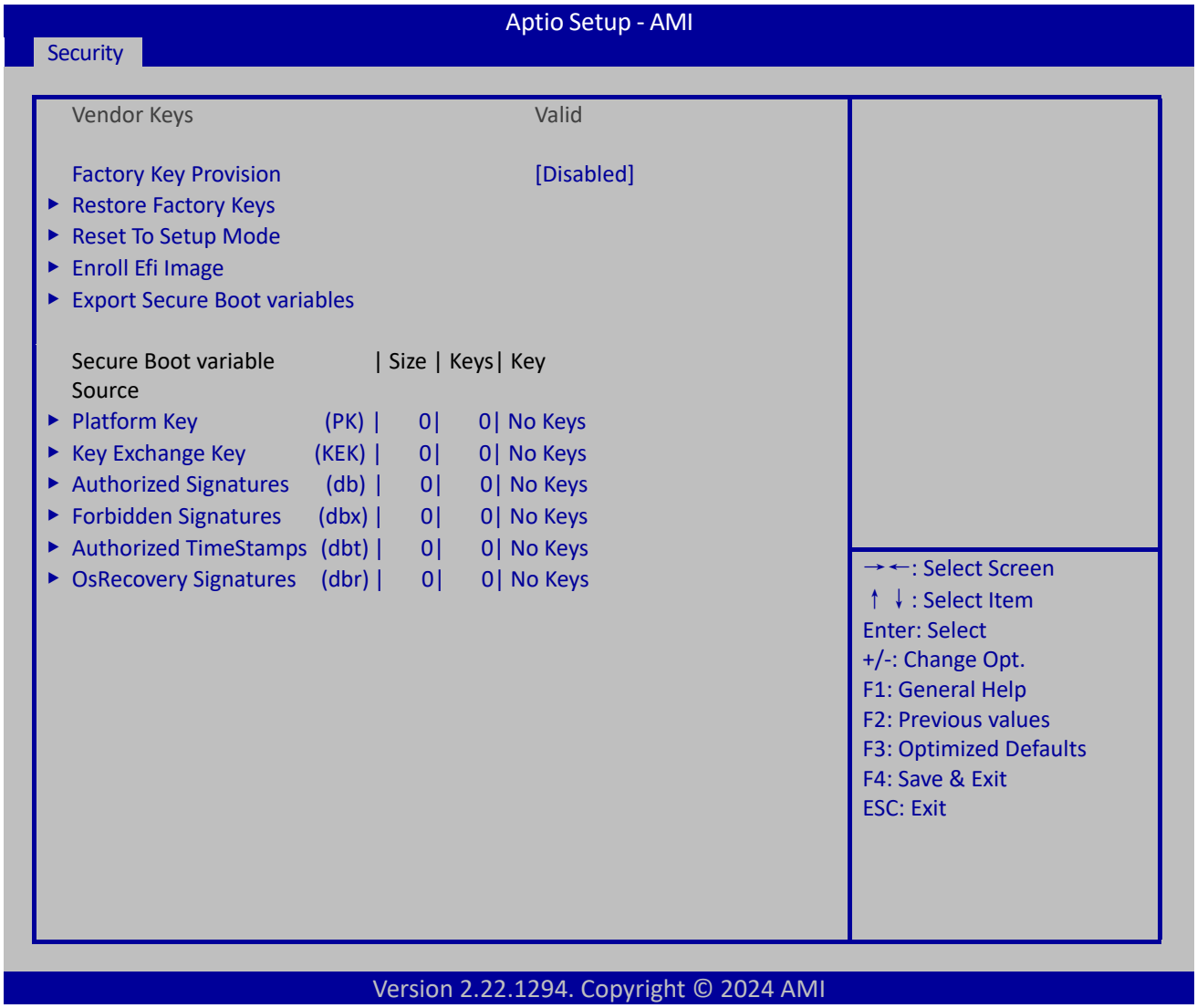
Security		
Menu Fields	**Settings**	**Comments**
Administrator Password		Set Administrator Password
User Password		Set User Password
Secure Boot	Selects sub-menu.	

6.6.1 Secure Boot



Security \ Secure Boot		
Menu Fields	**Settings**	**Comments**
System Mode	Setup	Displays the system mode.
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 requires platform reset
	Not Active	Displays the current active status of secure boot.
Secure Boot Mode	**[Standard]** [Custom]	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Expert Key Management	Selects sub-menu.	

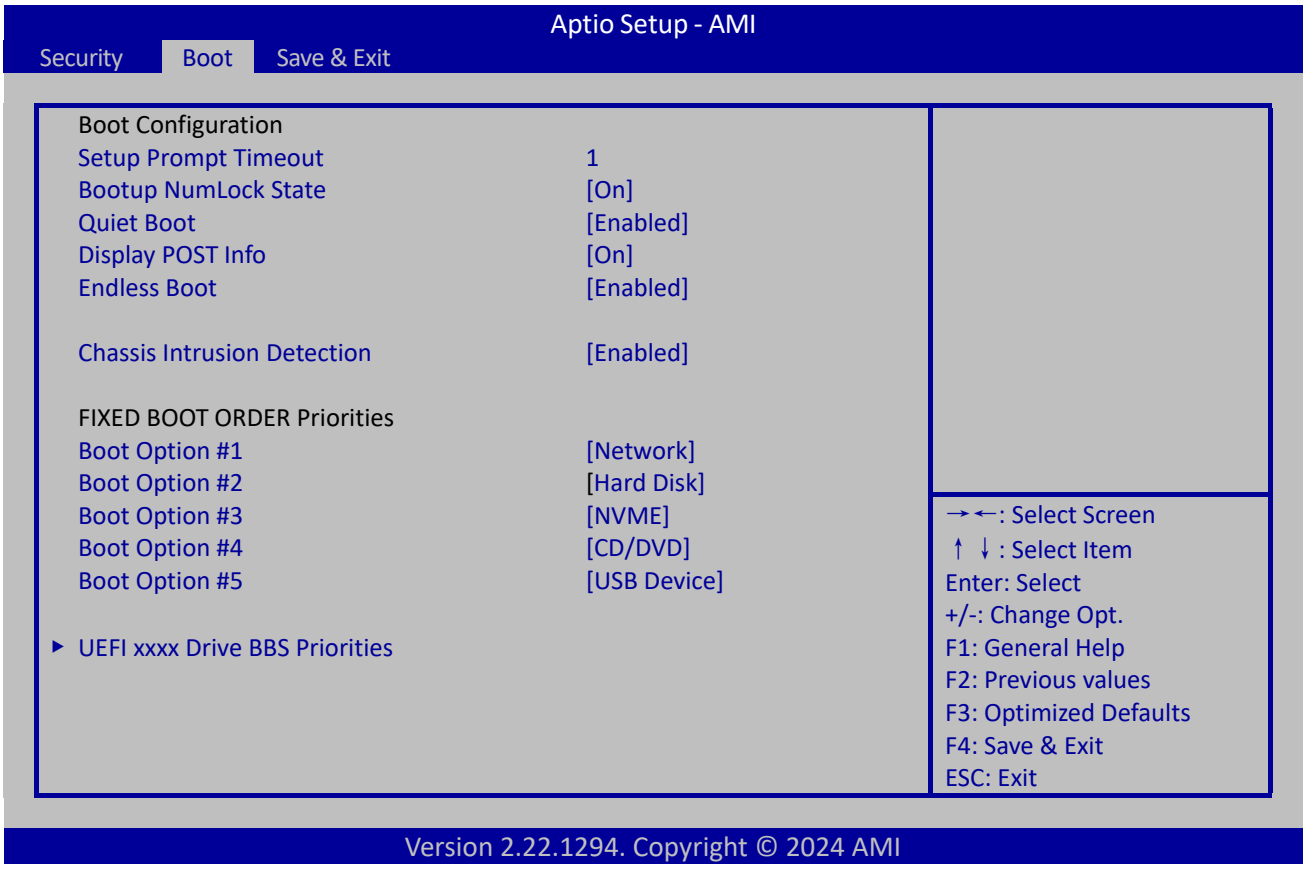
6.6.1.1 Expert Key Management



Security \ Secure Boot \ Expert Key Management		
Menu Fields	**Settings**	**Comments**
Vendor Keys		
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		Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Enroll Efi Image		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		Save NVRAM content of Secure Boot variable to a file
Secure Boot variable Source	| Size | Keys| Key	
Platform Key (PK)	**| 0| 0| No Keys**	

Security \ Secure Boot \ Expert Key Management		
Menu Fields	**Settings**	**Comments**
Key Exchange Key (KEK)	**| 0| 0| No Keys**	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)	**| 0| 0| No Keys**	
Authorized TimeStamps (dbt)	**| 0| 0| No Keys**	
OsRecovery Signatures (dbr)	**| 0| 0| No Keys**	

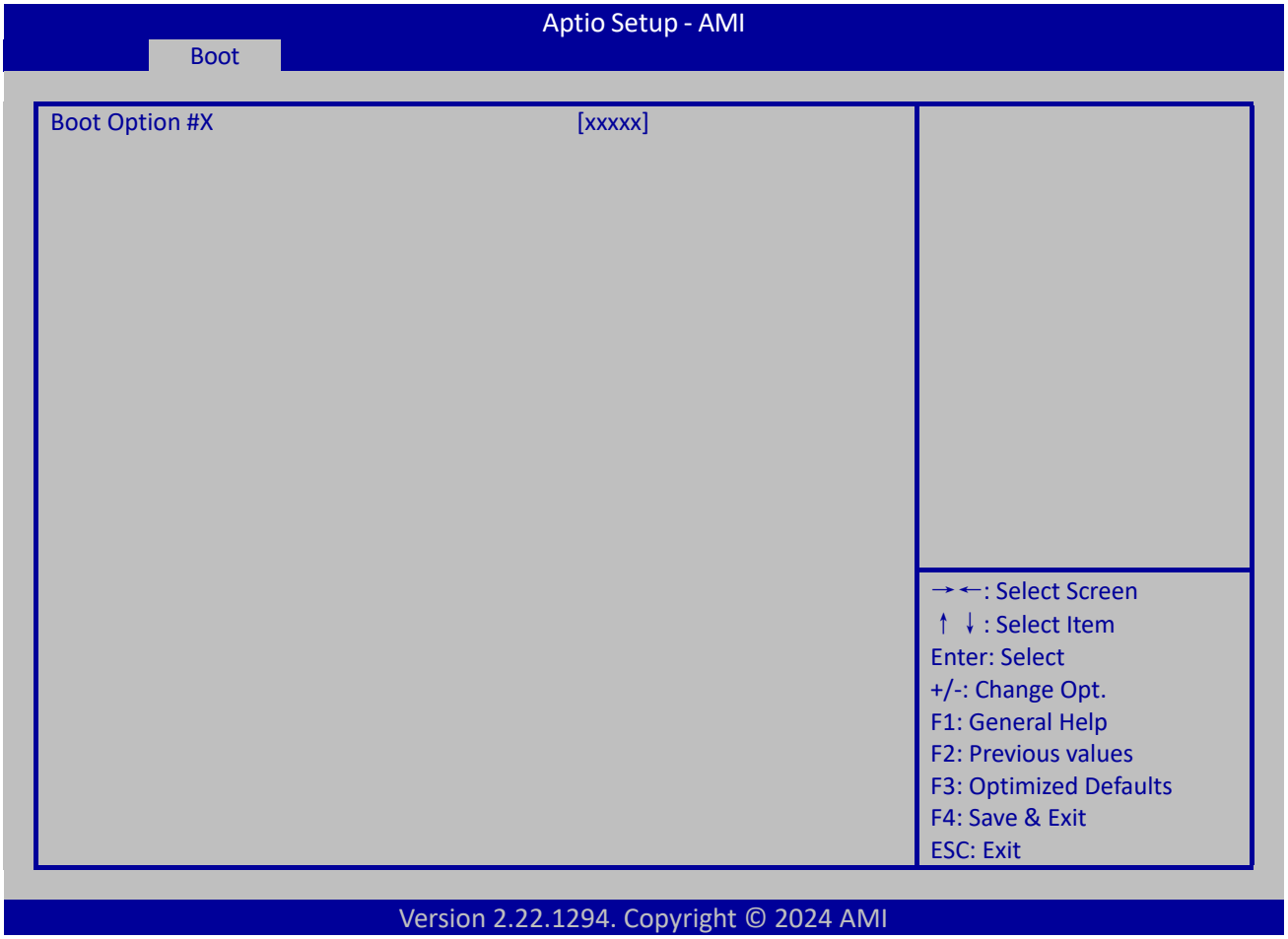
6.7 BOOT



Boot		
Menu Fields	**Settings**	**Comments**
Setup Prompt Timeout	**1**	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
Display POST Info	[Off] **[On]**	Display POST Info after LOGO
Endless Boot	[Disabled] **[Enabled]**	Enabled: BIOS try bootable devices constantly in loop until finding a bootable device (Excluding Built-in EFI Shell)
Chassis Intrusion Detection	[Disabled] **[Enabled]**	Chassis Intrusion Detection
FIXED BOOT ORDER Priorities		
Boot Option #1	**[Network]** [Hard Disk] [NVME] [CD/DVD] [USB Device] [Disabled]	Sets the system boot order
Boot Option #2	[Network] **[Hard Disk]**	Sets the system boot order

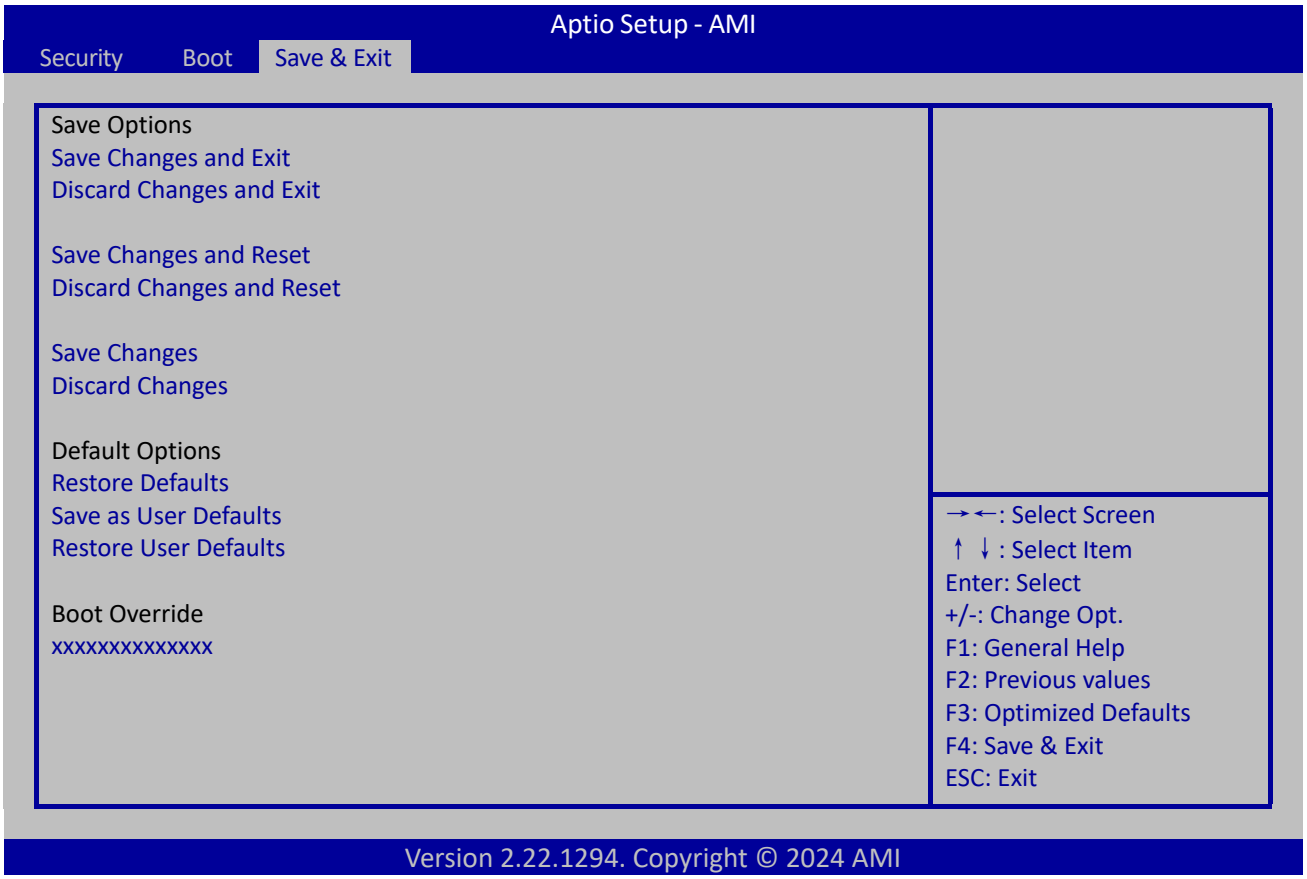
Boot		
Menu Fields	**Settings**	**Comments**
	[NVME] [CD/DVD] [USB Device] [Disabled]	
Boot Option #3	[Network] [Hard Disk] **[NVME]** [CD/DVD] [USB Device] [Disabled]	Sets the system boot order
Boot Option #4	[Network] [Hard Disk] [NVME] **[CD/DVD]** [USB Device] [Disabled]	Sets the system boot order
Boot Option #5	[Network] [Hard Disk] [NVME] [CD/DVD] **[USB Device]** [Disabled]	Sets the system boot order
UEFI xxxx BBS Priorities	Selects sub-menu.	

6.7.1 UEFI xxxx BBS Priorities



Boot \ UEFI xxxx BBS Priorities		
Menu Fields	**Settings**	**Comments**
Boot Option #X	**[xxxxx]** [xxxxx] .... [Disable]	Sets the system boot order

6.8 SAVE & EXIT



Save & Exit		
Menu Fields	**Settings**	**Comments**
Save Options		
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
Save Changes		Save Changes done so far to any of the setup options.
Discard Changes		Discard Changes done so far to any of the setup options.
Default Options		
Restore Defaults		Restore/Load Default values for all the setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override		
xxxxxxxxxxxxxx		Displays the bootable options.

7 STATUS CODES LIST

7.1 AMI STANDARD STATUS CODE

The UEFI defines SEC, PEI, DXE, BDS phases during POST. AMI define several status code 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)

Status Code	Description
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)
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

Status Code	Description
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 AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is stared (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 AMI 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
0xEC-0xEF	Reserved for future AMI 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 AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found

Status Code	Description
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI 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 DXEIPL 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)

Status Code	Description
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
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

Status Code	Description
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
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.

MSI.COM

EPS.MSI.COM