S4056(MS-379)

BIOS User Guide

Version 1.0

MSI Enterprise Platform Solutions

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 MS-379 project.

2 BIOS FEATURES OVERVIEW

2.1 BIOS DESCRIPTION

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

2.2 PROCESSOR

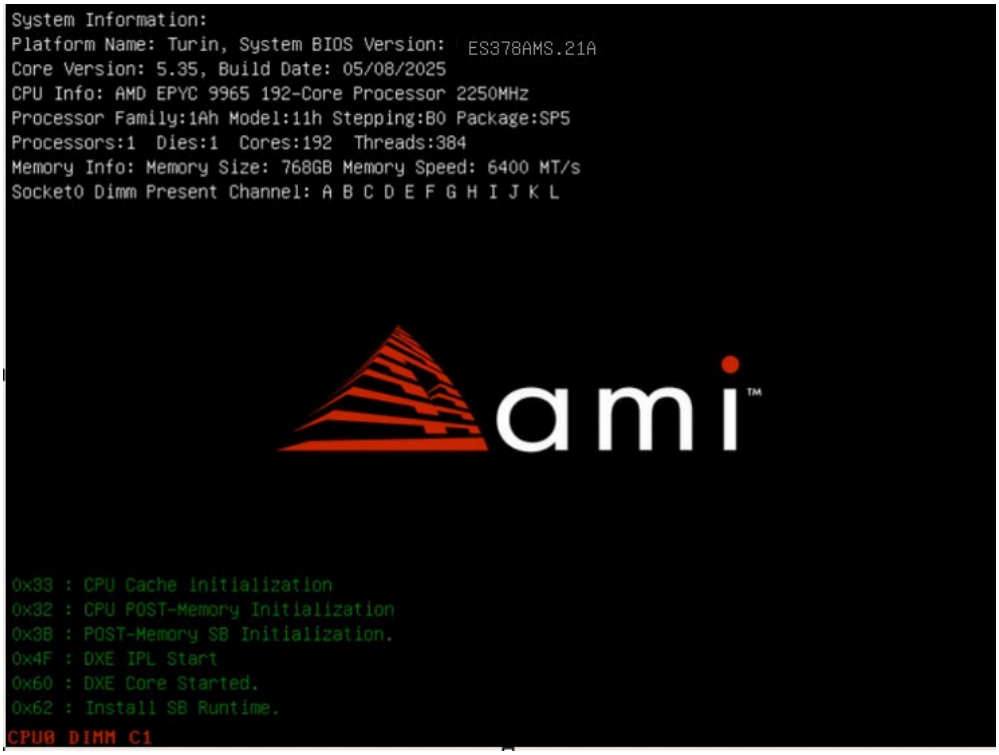
AMD Features	Description
AMD SMT Control	Support
AMD SVM	Support

2.3 MEMORY

Features	Description
Interleaving Mode	Support
Mirroring Mode	Support
ECC (Error-correcting code)	Support
Bad DIMM Location	Support

2.3.1 Bad DIMM Location

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



2.4 STORAGE

Features	Description
USB HDD	Support
USB CD-ROM/DVD-ROM	Support
U.2 NVMe	Support
M.2 NVMe	Support
Hotplug	Support

2.5 NETWORKING

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

2.6 POWER MANAGEMENT

Features	Description
ACPI S0 (Working)	Support
ACPI S5 (Shut down)	Support
Processor C0	Support
Processor C1	Support

Processor C6	Support
Restore on AC Power Loss	Support
Wake On Lan (WOL)	Support
Wake On RTC	Support
Power Capping	Support

2.6.1 Restore on AC Power Loss

The power control policy is managed by the CPU or FCH. When the system's power is restored, the CPU or FCH will control the system's power state as "Always off," "Always on," or "Previous"

- BIOS Setup Item

Item	Settings	Description
Ac Loss Control	[Always off] [Always On] **[Previous]**	Select Ac Loss Control Method

2.7 SECURITY

Features	Description
Secure Boot	Support
TPM 2.0	Support
Password on BIOS Setup Utility	Support
Secure Erase Support (Security Freeze Lock)	Support
Strong BIOS Password	Support

2.7.1 Strong BIOS Password

Strong password policy

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

2.7.2 Trusted Computing (TPM)

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

- BIOS Setup Item:

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

2.8 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
7	Cache Information	Support
8	Port Connector Information	Support
9	System Slots	Support
11	OEM String	Support
12	System Configuration Options	Support
13	BIOS Language Information	Support
16	Physical Memory Array	Support
17	Memory Device	Support
19	Memory Array Mapped Address	Support
20	Memory Device Mapped Address	Support
32	System Boot Information	Support
38	IPMI Device Information	Support
39	System Power Supply	Support
41	Onboard Device Extended Information	Support
42	Management Controller Host Interface	Support
127	End-of-Table	Support

2.9 BMC

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

2.10 MISC

Features	Description
BIOS Recovery Mode	Support
Quiet Boot	Support

SEL (Self Error Log)	Support
Legacy Boot Mode (CSM)	Support
Hot Key	Support
Change Logo	Support
Fixed Boot Order	Support
Early Console	Support
Clear CMOS Mode	Support
Dynamic PCIE Routing Configuration For Different Chassis SKU (1U/2U…)	Support
Endless Boot	Support
Chassis Intrusion	Support

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 Clear CMOS

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

- Error message
  "Error: RTC Power Status Failed, BIOS Defaults are Loaded"
  "Press F1 Skip, F10 Enter Setup"

Note: Passwords will be preserved even after clear CMOS

2.10.4 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.

2.10.5 Chassis Intrusion

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

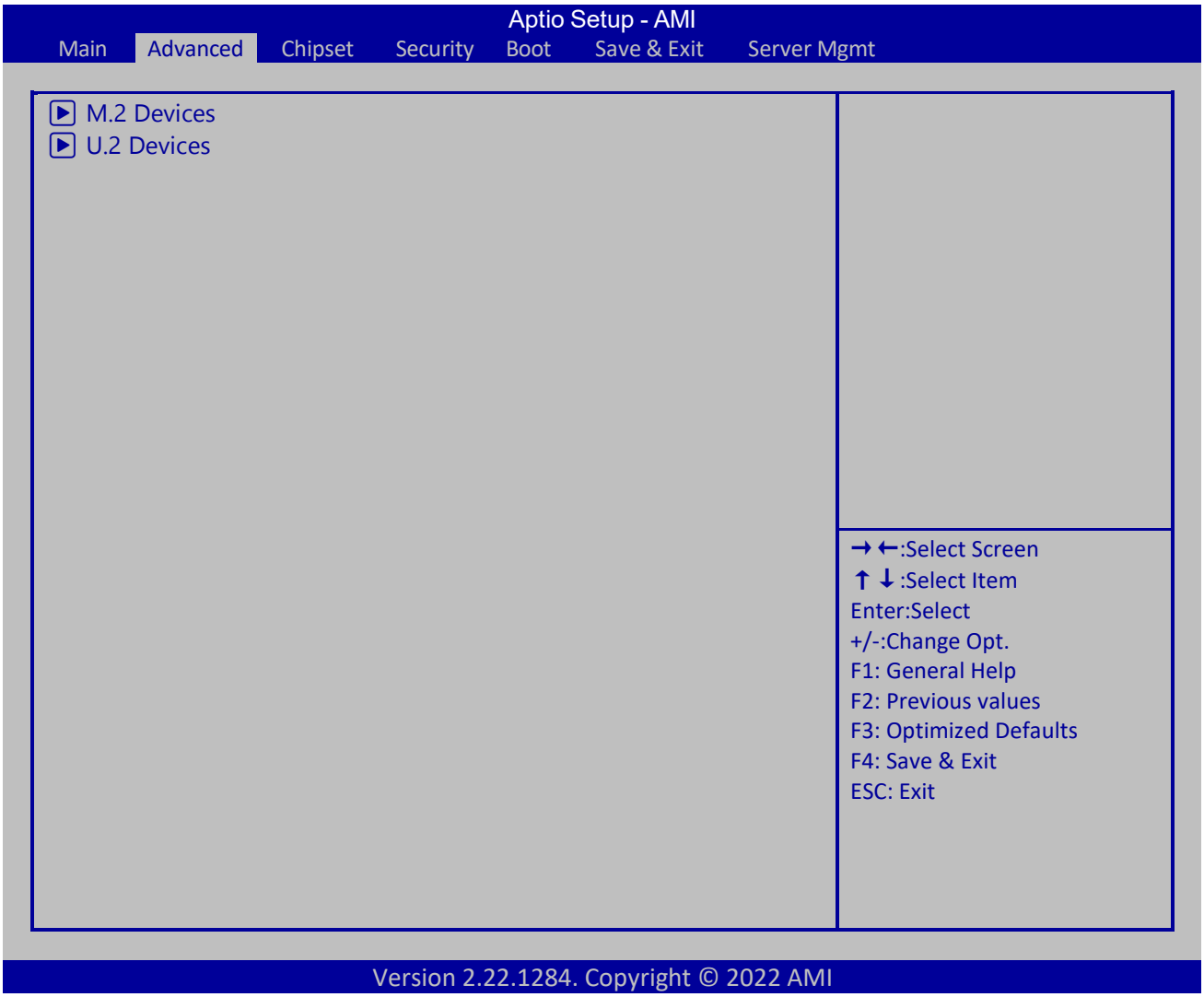
- Error message
  "Error: The Chassis has been opened"
  "Press F1 Skip, F10 Enter Setup and Clear Status"

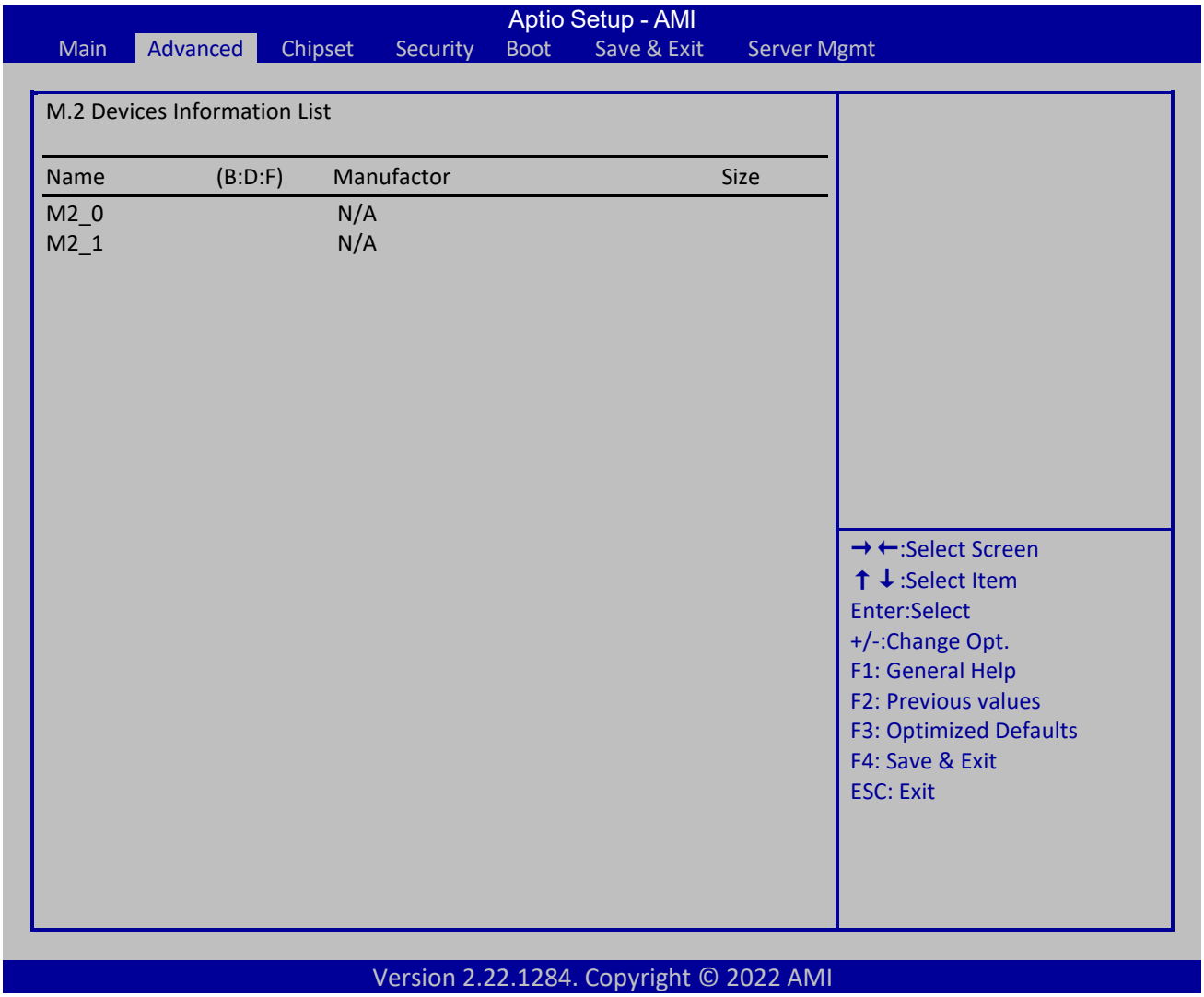
- BIOS Setup Item

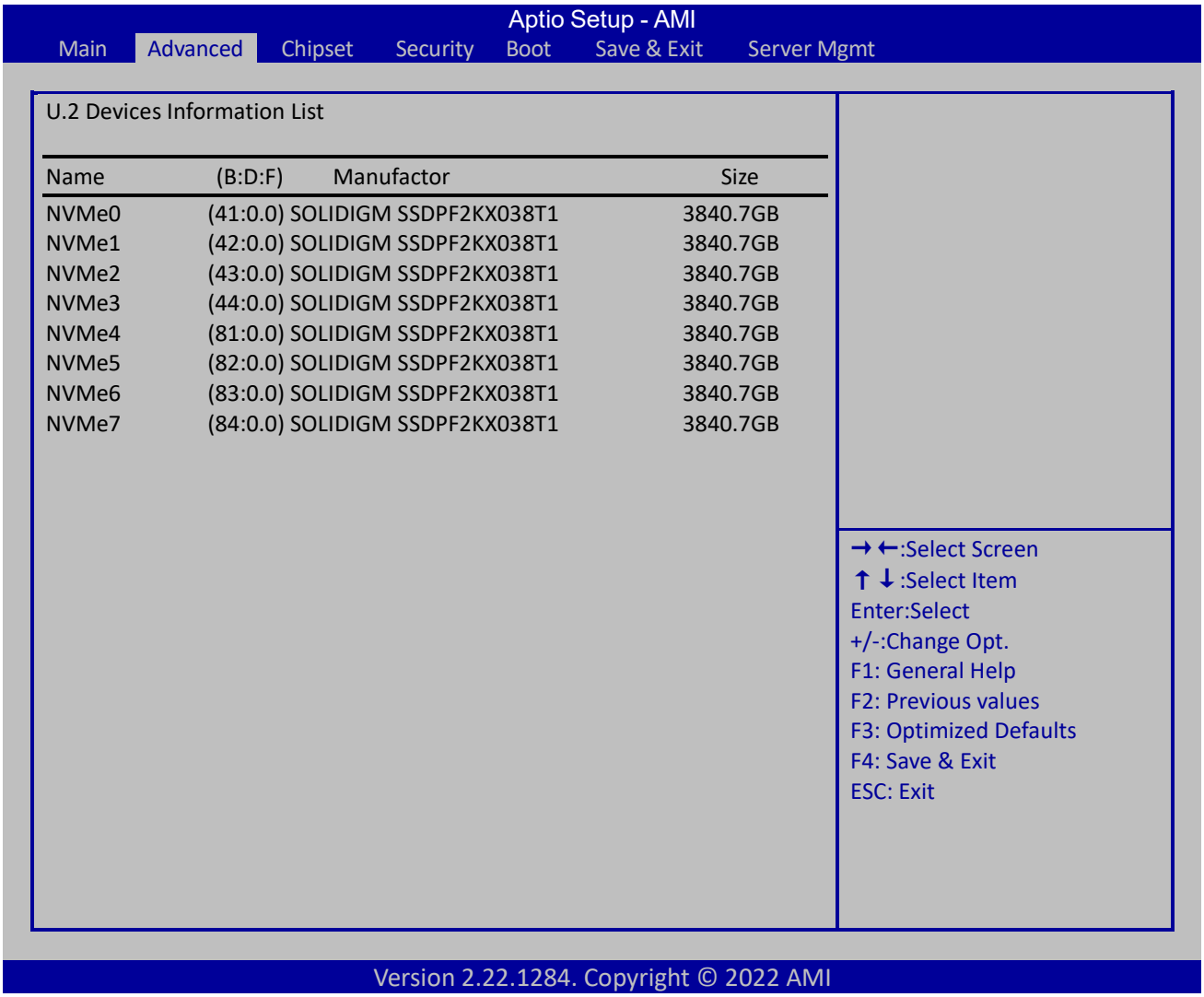
Item	Settings	Description
Chassis Intrusion	**[Enabled]** [Disabled]	Enable or disable chassis intrusion detection.

2.10.6 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 Nvme configuration page t. Nvme slot name must match to slot silkscreen.


Aptio Setup - AMI
Main
Advanced
Chipset
Security
Boot
Save & Exit
Server Mgmt
M.2 Devices
U.2 Devices
→←: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


Aptio Setup - AMI
Main
Advanced
Chipset
Security
Boot
Save & Exit
Server Mgmt
M.2 Devices Information List
Name
(B:D:F)
Manufactor
Size
M2_0
N/A
M2_1
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

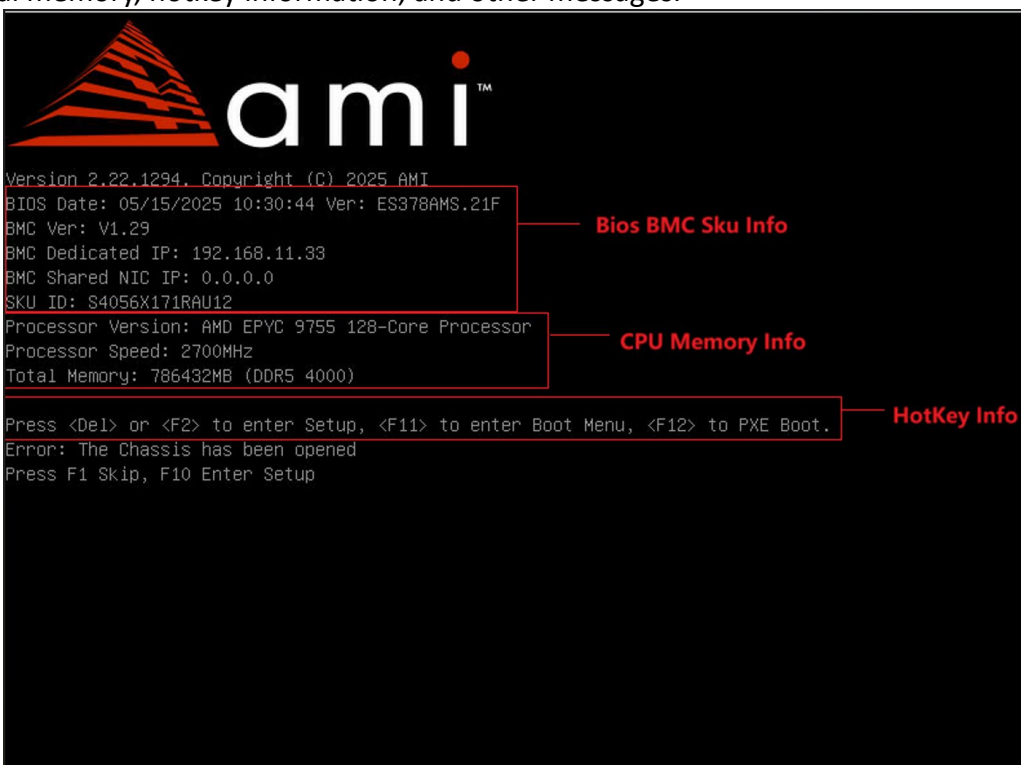
Provide system information, processor information, and memory information. Below information are mandatory. Other information can be displayed according to different platform.

2.11.2 Quiet Boot

Display logo and hotkey information.

2.11.3 POST Information

Provide BIOS version, BIOS build date, BMC version, processor version, processor speed, total memory, hotkey information, and other messages.



3 SYSTEM EVENT LOG

3.1 SEL FOR AMD RAS

3.1.1 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	Event Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error type 0x00 = Correctable ECC 0x01 = Uncorrectable ECC 0x04 = Memory device disabled 0x05 = Correctable error threshold reached
15	Event Data 2	[7:0] - Reserved
16	Event Data 3	[7:5] – Socket ID Number 0x00 = Socket 0 0x01 = Socket 1 0x02 = Socket 2 0x03 = Socket 3 [4:1] – Memory Channel Number 0x00 = Memory channel A 0x01 = Memory channel B 0x02 = Memory channel C 0x03 = Memory channel D 0x04 = Memory channel E 0x05 = Memory channel F 0x06 = Memory channel G 0x07 = Memory channel H 0x08 = Memory channel I 0x09 = Memory channel J 0x0A = Memory channel K 0x0B = Memory channel L 0x0C = Memory channel M 0x0D = Memory channel N 0x0E = Memory channel O 0x0F = Memory channel P [0] – Memory Dimm Number 0x00 = Dimm 0 of channel 0x01 = Dimm 1 of channel

3.1.2 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	0xC0
12	Sensor #	0x00
13	Event Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error Type 0x05 = Configuration Error 0x0B = Machine Check Exception (Uncorrectable) 0x0C = Correctable Machine Check Error
15	Event Data 2	[7:4] – Socket ID 0x00 = Socket 0 0x01 = Socket 1 [3:0] – Die ID
16	Event Data 3	[7:0] – MCA OEM Error Type 0x8A = CPU PSP 0x8B = CPU SMU 0x8E = CPU Gen 0x8F = CPU GMI 0x90 = CPU xGMI 0x93 = WAFL

3.1.3 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	Event Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:0] – Error Type 0x04 = PCIE Bus PERR 0x05 = PCIE Bus SERR 0x07 = PCIE Bus Correctable Error 0x08 = PCIE Bus Uncorrectable Error 0x0A = PCIE Bus Fatal Error 0x0F = Latest Boot PCIE Error
15	Event Data 2	[7:0] – PCI Bus Number

16	Event Data 3	[7:3] – PCI Device Number [2:0] – PCI Function Number

3.1.4 NBIO

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

3.1.5 SMN

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

3.1.6 CXL

Byte	Field	Description
1,2	Record ID	
3	Record Type	0x02
4-7	Timestamp	
8,9	Generator ID	0x0021
10	EvM Rev	0x04

11	Sensor Type	0xC1
12	Sensor #	0x02
13	Event Dir/Event Type	0x6F
14	Event Data 1	[7:6] – 0x02 (OEM code in ED2) [5:4] – 0x02 (OEM code in ED3) [3:2] – CXL Error Log Type 0x0 = CXL IO 0x1 = CXL Memory 0x2 = CXL Component Event [1] – CXL Agent Type [0] – Error Type 0x00 = Correctable Error 0x01 = Uncorrectable Error
15	Event Data 2	[7:0] – Bus Number
16	Event Data 3	[7:3] – Device Number [2:0] – Function Number

3.1.7 PMIC

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

4 SMBIOS

4.1 TYPE 0

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

4.2 TYPE 1

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

5 BMC OEM COMMAND

This section is included in the “BMC OEM Command Spec .docx”.

6 UTILITY

6.1 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

6.2 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

6.3 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)
* System Power Supply (Type 39)

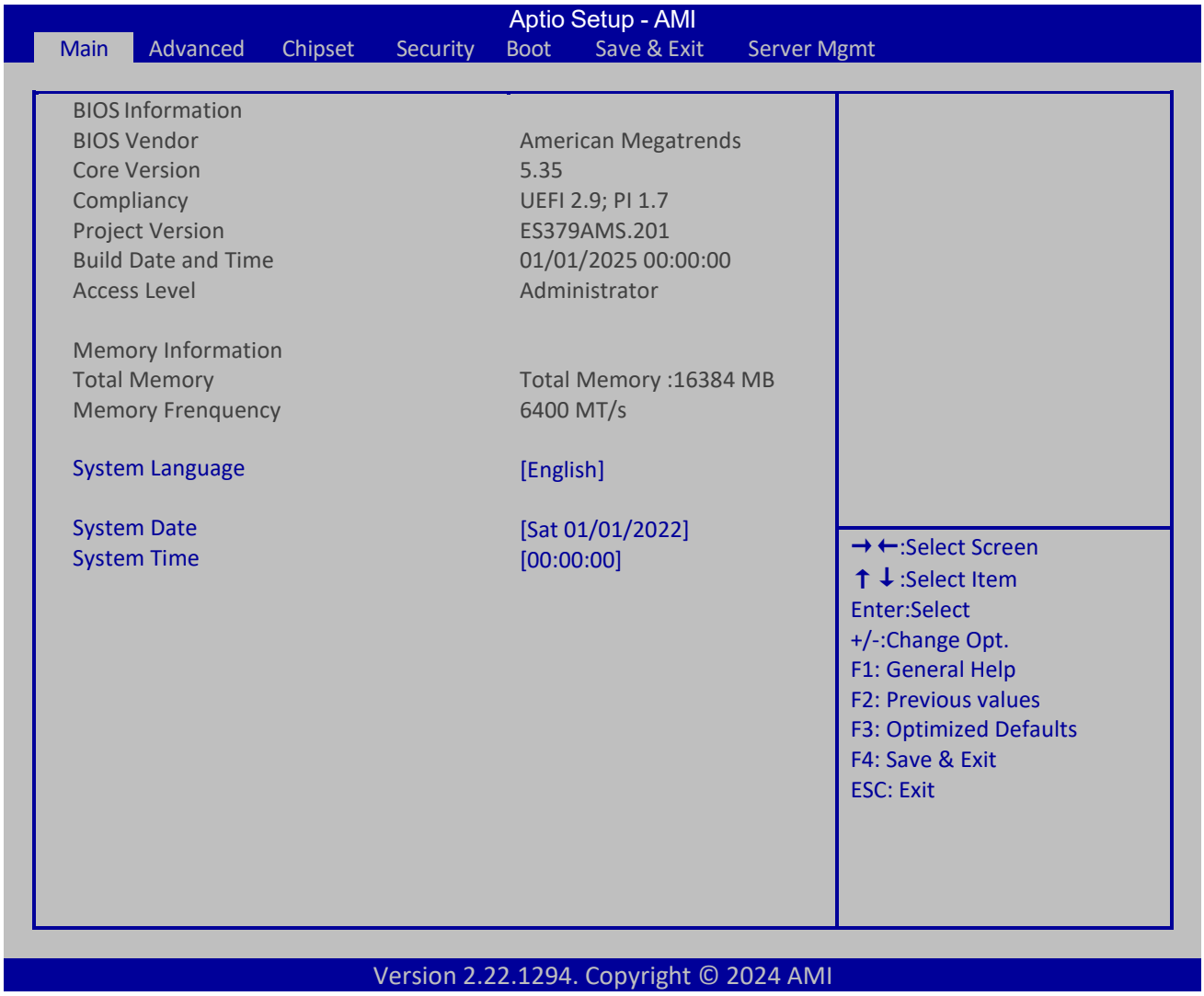
Utilities	Description
DMIEDIT Under EFI Shell	DMIDEEFIx64.EFI

DMIEDIT Under Linux	AMIDELNX_64
DMIEDIT Under Windows	DMIEDITx64.EXE AMIDEWINx64.EXE

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

7 BIOS SETUP

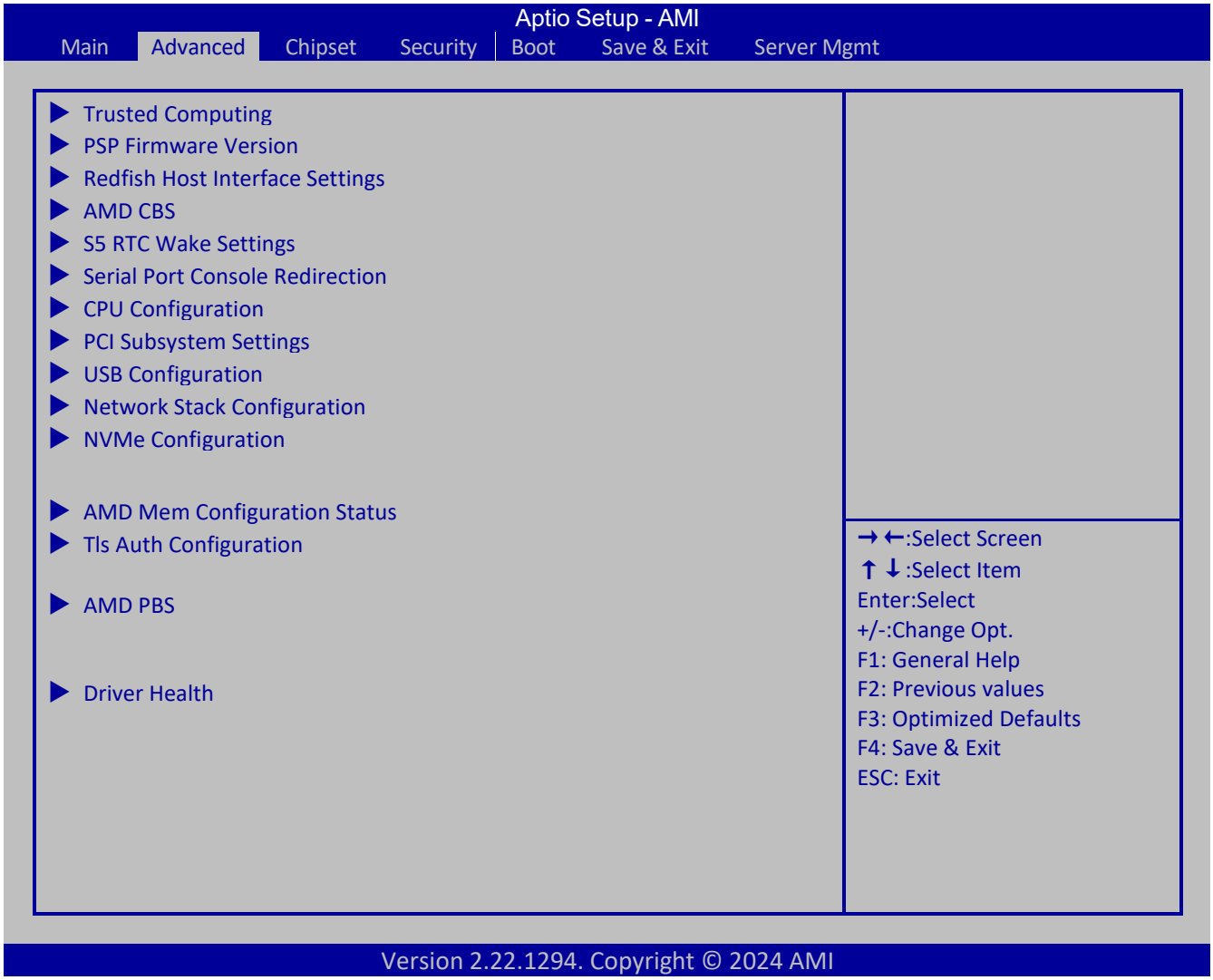
7.1 MAIN MENU



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	x.xx	Displays the BIOS version.
Build Date and Time	xx/xx/xx xx:xx:xx	Displays the BIOS build date and time.
Access Level	Administrator	Displays the control level of setup menu
Memory Information		
Total memory	Y MB	Displays the available memory size
Memory Frenquency	Xxxx MT/s	Display Memory Frequency

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

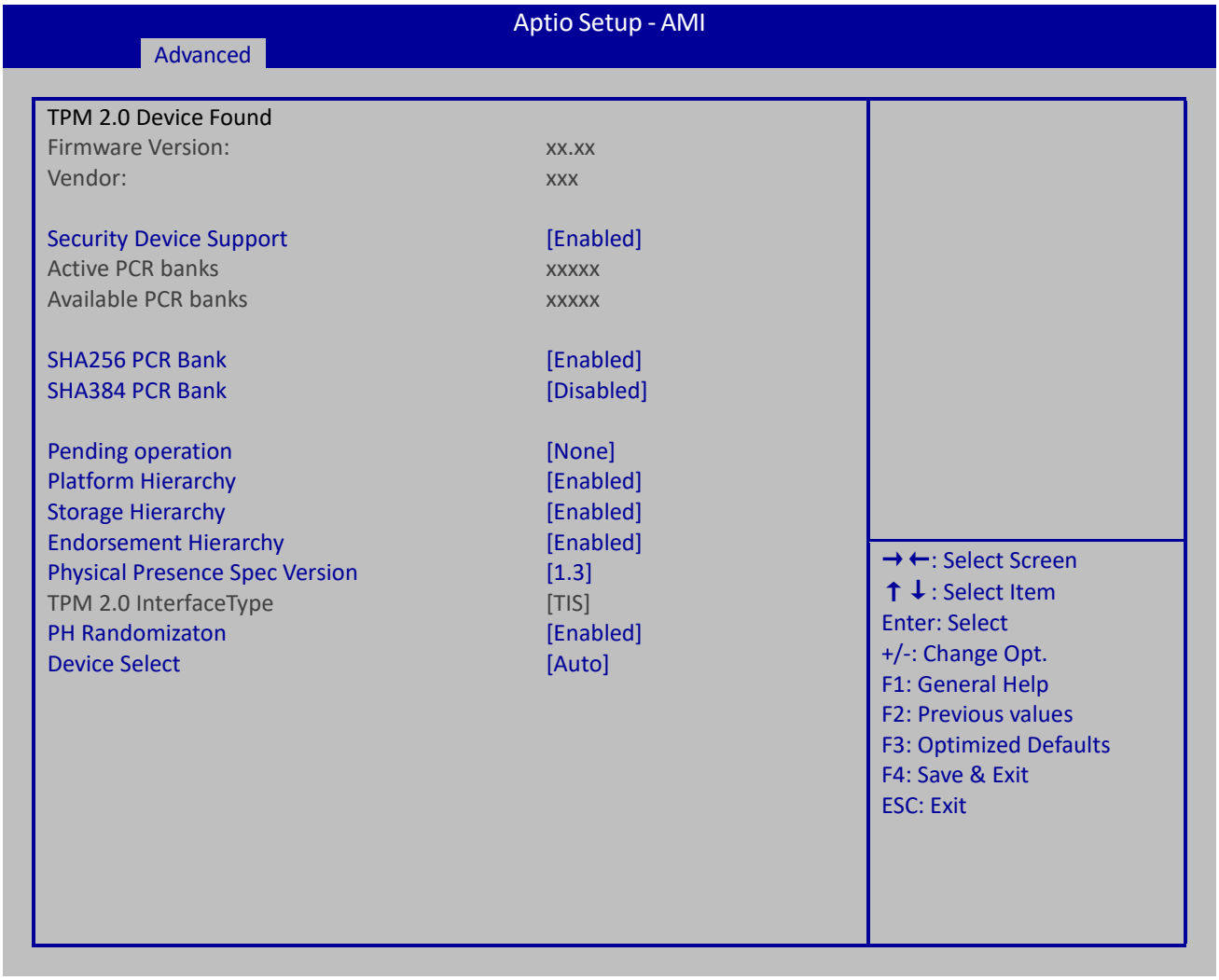
7.2 ADVANCED MENU



Advanced		
Menu Fields	**Settings**	**Comments**
Trusted Computing	Selects sub-menu.	Trusted Computing Settings.
PSP Firmware Versions	Selects sub-menu.	PSP Firmware Versions
Redfish Host Interface Settings	Selects sub-menu.	Redfish Host Interface Parameters.
AMD CBS	Selects sub-menu.	AMD CBS Setup Page
S5 RTC Wake Settings	Selects sub-menu.	Enable System to Wake from S5 using RTC alarm
Serial Port Console Redirection	Selects sub-menu.	Serial Port Console Redirection
CPU Configuration	Selects sub-menu.	CPU Configuration Parameters
PCI Subsystem Settings	Selects sub-menu	PCI Subsystem Settings
USB Configuration	Selects sub-menu	USB Configuration Parameters
Network Stack Configuration	Selects sub-menu.	Network Stack Settings
NVMe Configuration	Selects sub-menu.	NVMe Device Options Settings
AMD Mem Configuration Status	Selects sub-menu.	To display memory configuration (initialized by ABL) status

Advanced		
Menu Fields	**Settings**	**Comments**
Tls Auth Configuration	Selects sub-menu.	Press <Enter> to select Tls Auth Configuration
AMD PBS	Selects sub-menu.	AMD PBS Setup Page

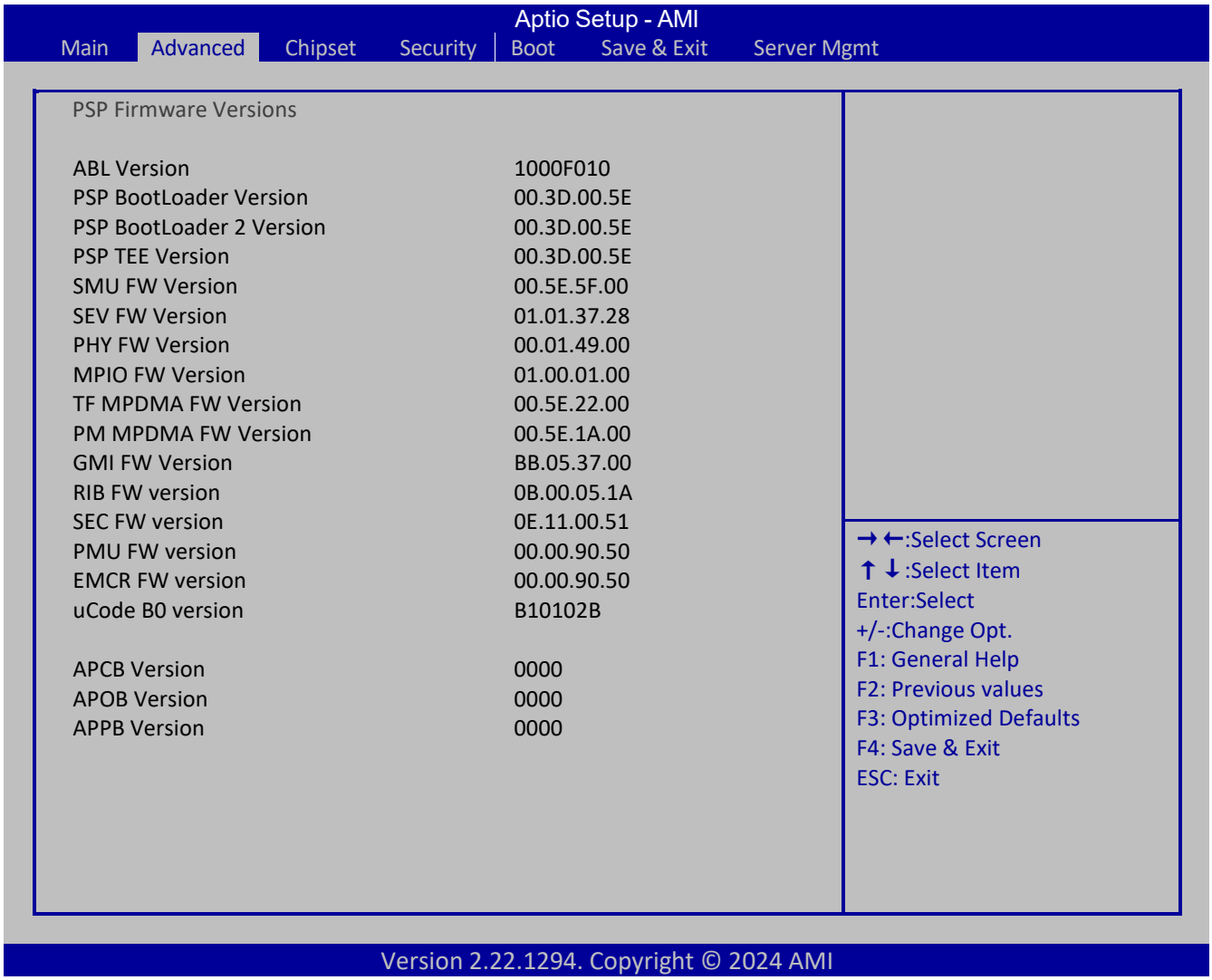
7.2.1 Trusted Computing



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.
Platform Hierarchy	[Disabled] **[Enabled]**	Enable or Disable Platform Hierarchy

Advanced \ Trusted Computing		
Menu Fields	**Settings**	**Comments**
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.
PH Randomizatioon	[Disabled] **[Enabled]**	Enables or Disables Platform Hierarchy randomization. DO NOT ENABLE THIS QUESTION IN PRODUCTION PLATFORMS. THIS IS FOR DEVELOPMENT TESTING. OVERRIDE ChangePlatformAuth ELINK for production platforms supporting TXT.
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

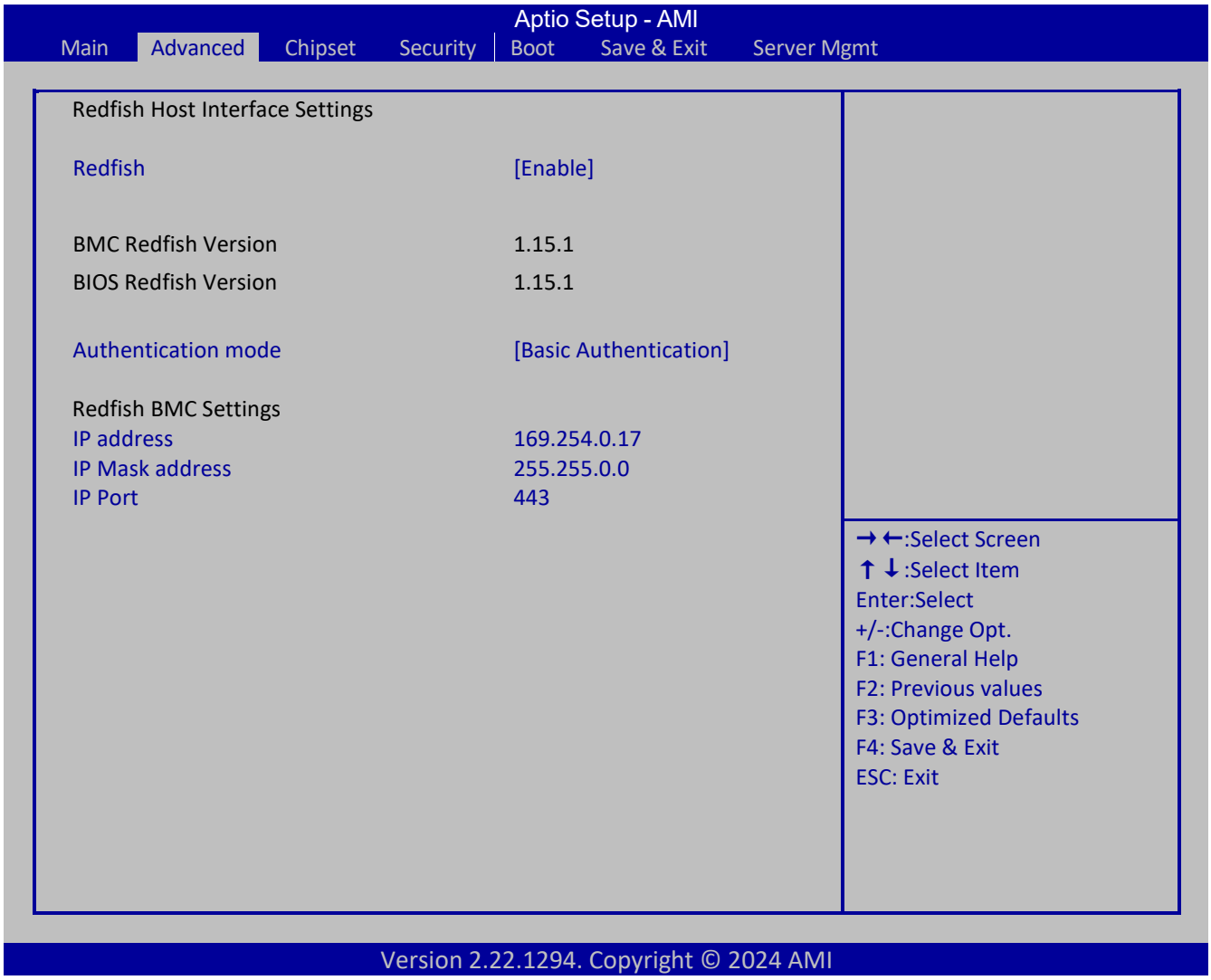
7.2.2 PSP Firmware Versions



Advanced \ PSP Firmware Version		
Menu Fields	**Settings**	**Comments**
ABL Version	xxxxxxxx	Display the ABL version
PSP BootLoader Version	xx.xx.xx.xx	Display the PSP BootLoader Version
PSP BootLoader 2 Version	xx.xx.xx.xx	Display the PSP BootLoader 2 Version
PSP TEE Version	xx.xx.xx.xx	Display the PSP TEE Version
SMU FW Version	xx.xx.xx.xx	Display the SMU FW Version
SEV FW Version	xx.xx.xx.xx	Display the SEV FW Version
PHY FW Version	xx.xx.xx.xx	Display the PHY FW Version
MPIO FW Version	xx.xx.xx.xx	Display the MPIO FW Version
TF MPDMA FW Version	xx.xx.xx.xx	Display the TF MPDMA FW Version
PM MPDMA FW Version	xx.xx.xx.xx	Display the PM MPDMA FW Version
GMI FW Version	xx.xx.xx.xx	Display the GMI FW Version
RIB FW version	xx.xx.xx.xx	Display the RIB FW version
SEC FW version	xx.xx.xx.xx	Display the SEC FW version

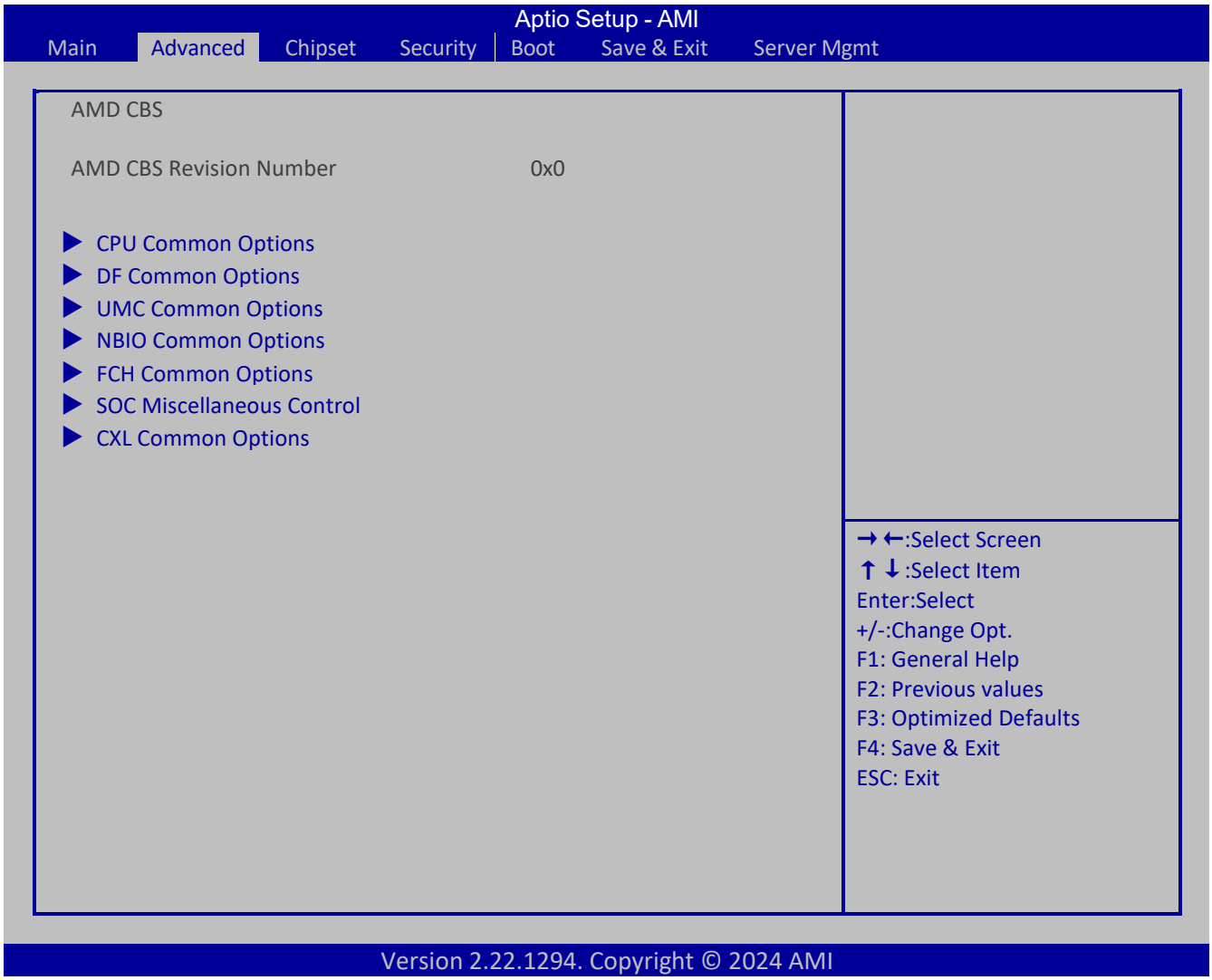
Advanced \ PSP Firmware Version		
Menu Fields	**Settings**	**Comments**
PMU FW version	xx.xx.xx.xx	Display the PMU FW version
EMCR FW version	xx.xx.xx.xx	Display the EMCR FW version
uCode C1 version	xxxxxxxx	Display the uCode C1 version
APCB Version	xxxx	Display the APCB Version
APOB Version	xxxx	Display the APOB Version
APPB Version	xxxx	Display the APPB Version

7.2.3 Redfish Host Interface Settings



Advanced \ Redfish Host Interface Settings		
Menu Fields	**Settings**	**Comments**
Redfish	[Disable] **[Enable]**	Enables or Disables AMI Redfish
BMC Redfish Version	x.xx.x	Redfish version supported by BMC
BIOS Redfish Version	x.xx.x	Redfish version supported by BIOS
Authentications Mode	[Authentication None] [Basic Authentication] [Session Anthernication]	Select authentication mode
IP Aaddress	xxx.xxx.xxx.xxx	Enter IP address
IP Mask address	xxx.xxx.xxx.xxx	Enter IP Mask address
IP Port	xxx	Enter IP Port

7.2.4 AMD CBS



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

7.2.4.1 CPU Common Options

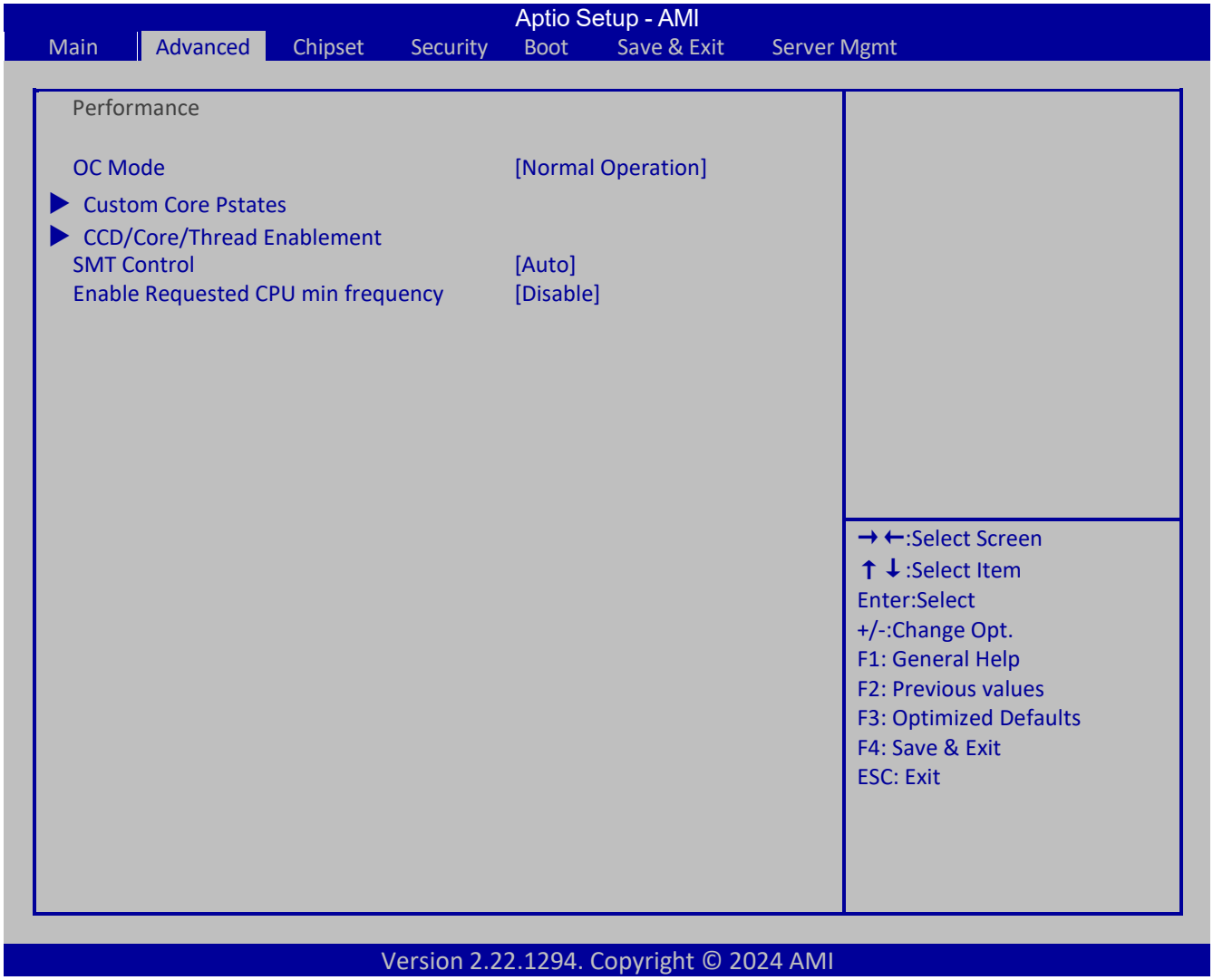
Advanced \ AMD CBS \ CPU Common Options		
Menu Fields	**Settings**	**Comments**
Performance	Select sub-menu	
REP-MOV/STOS Streaming	[Disabled] **[Enabled]**	Allow REP-MOVS/STOS to use non-caching streaming stores for large sizes.
Perfetcher settings	Select sub-menu	
Core Watchdog	Select sub-emnu	

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

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

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

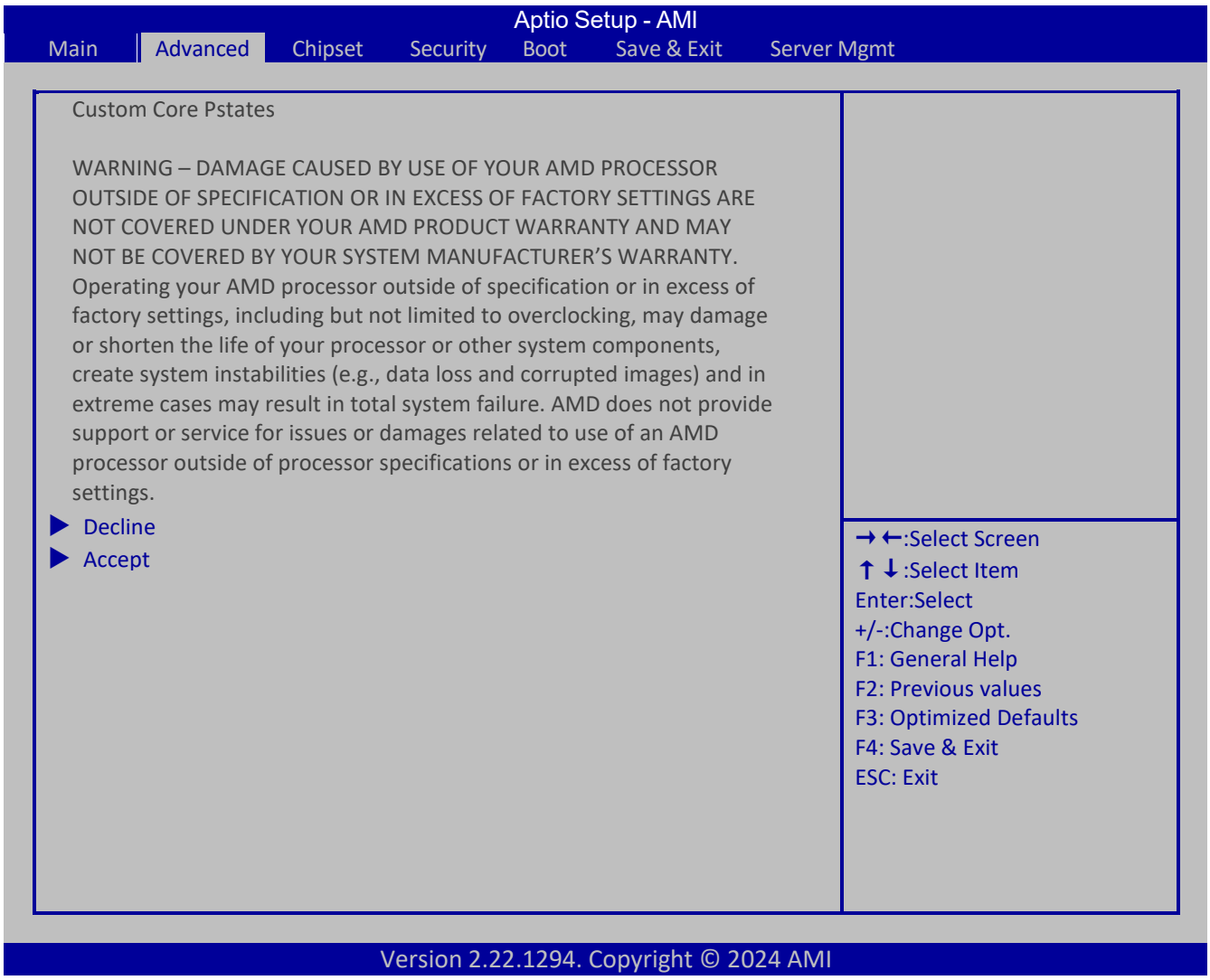
7.2.4.1.1 Performance



Advanced \ AMD CBS \ CPU Common Options \ Performance		
Menu Fields	**Settings**	**Comments**
OC Mode	**[Normal Operation]** [Customized]	Select overlock operation modes
Custom Core Pstats	Select sub-menu	
CCD/Core/Thread Enablement	Select sub-menu	
SMT Control	[Disable] [Enable]	Can be used to disable symmetric multithreading.

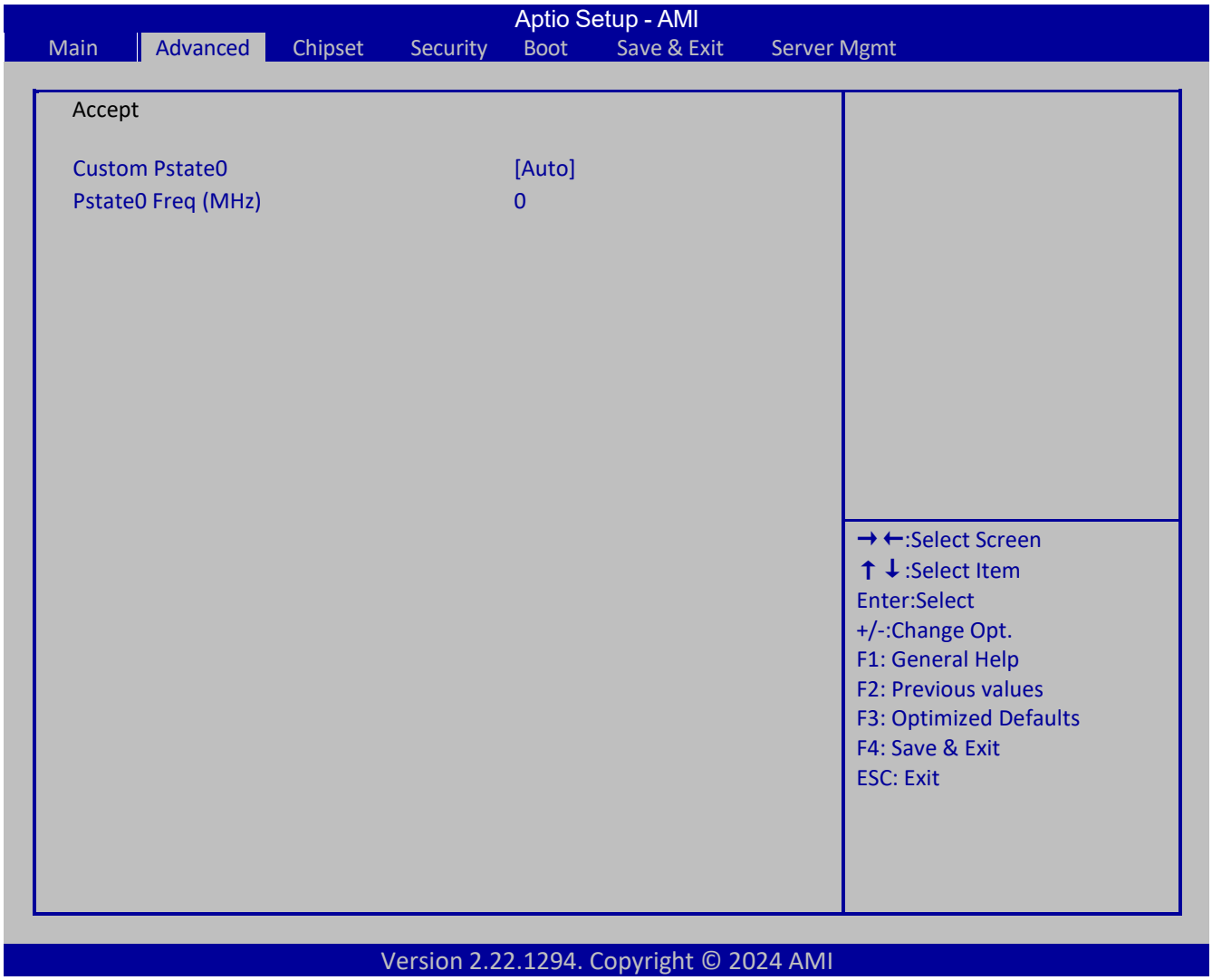
Advanced \ AMD CBS \ CPU Common Options \ Performance		
Menu Fields	**Settings**	**Comments**
	[Auto]	To re-enable SMT, a POWER CYCLE is needed after selecting the 'Enable' option. Select 'Auto' based on BIOS PCD(PcdAmdSmtMode) default setting. WARNING – S3 is NOT SUPPORTED on systems where SMT is disabled.
Enable Requested CPU min frequency	**[Disable]** [Enable]	This allows for minimum requested CPU frequency to be used.

7.2.4.1.1.1 Custom Core Pstates



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

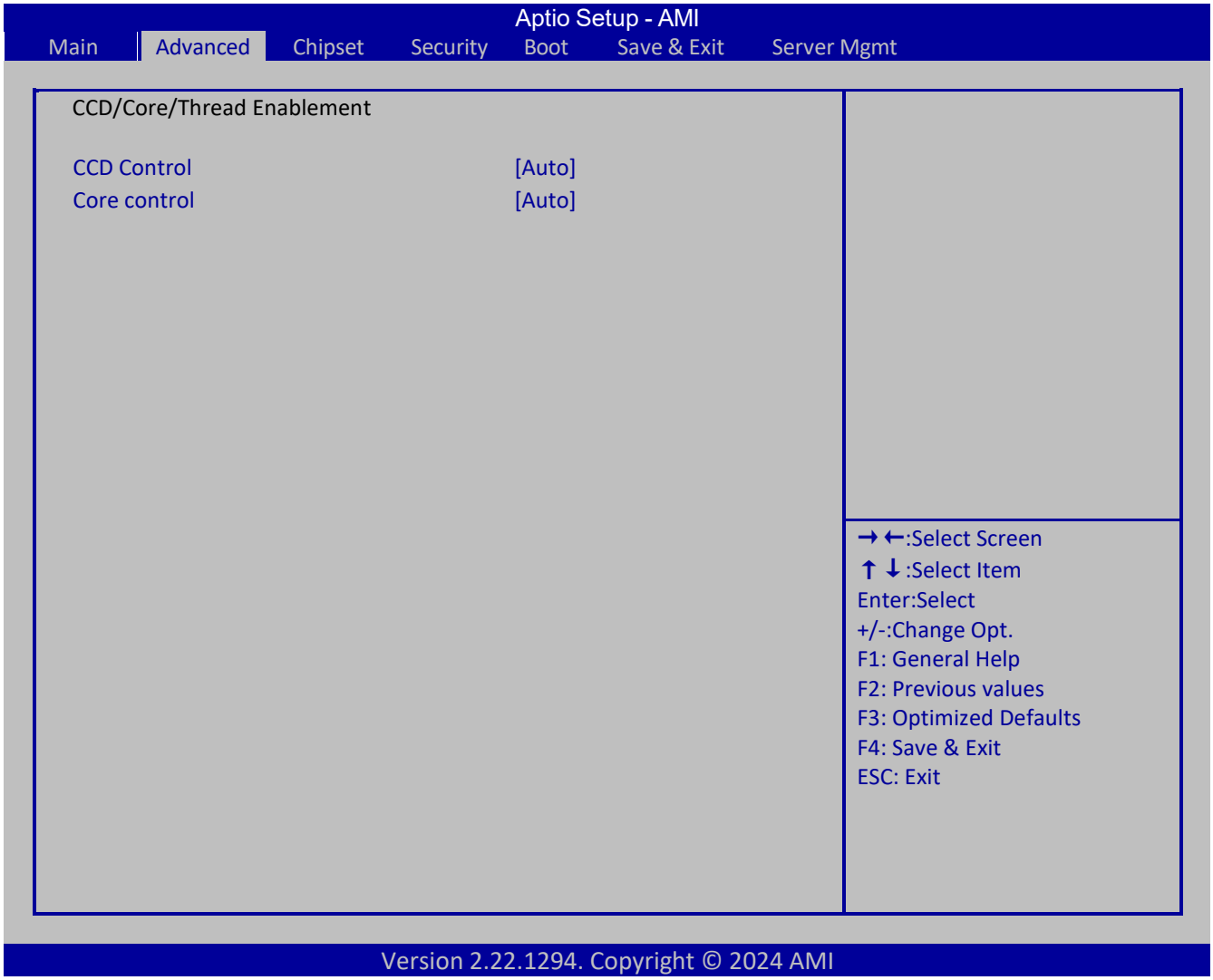
7.2.4.1.1.1.1 Custom Core Pstates - Accept



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

Advanced \ AMD CBS \ CPU Common Options \ Performance \ Custom Core Pstates \Accept		
Menu Fields	**Settings**	**Comments**
		AMD processor outside of processor specifications or in excess of factory settings.
Pstate0 Freq (MHz)	x	Specifies core frequency (MHz)

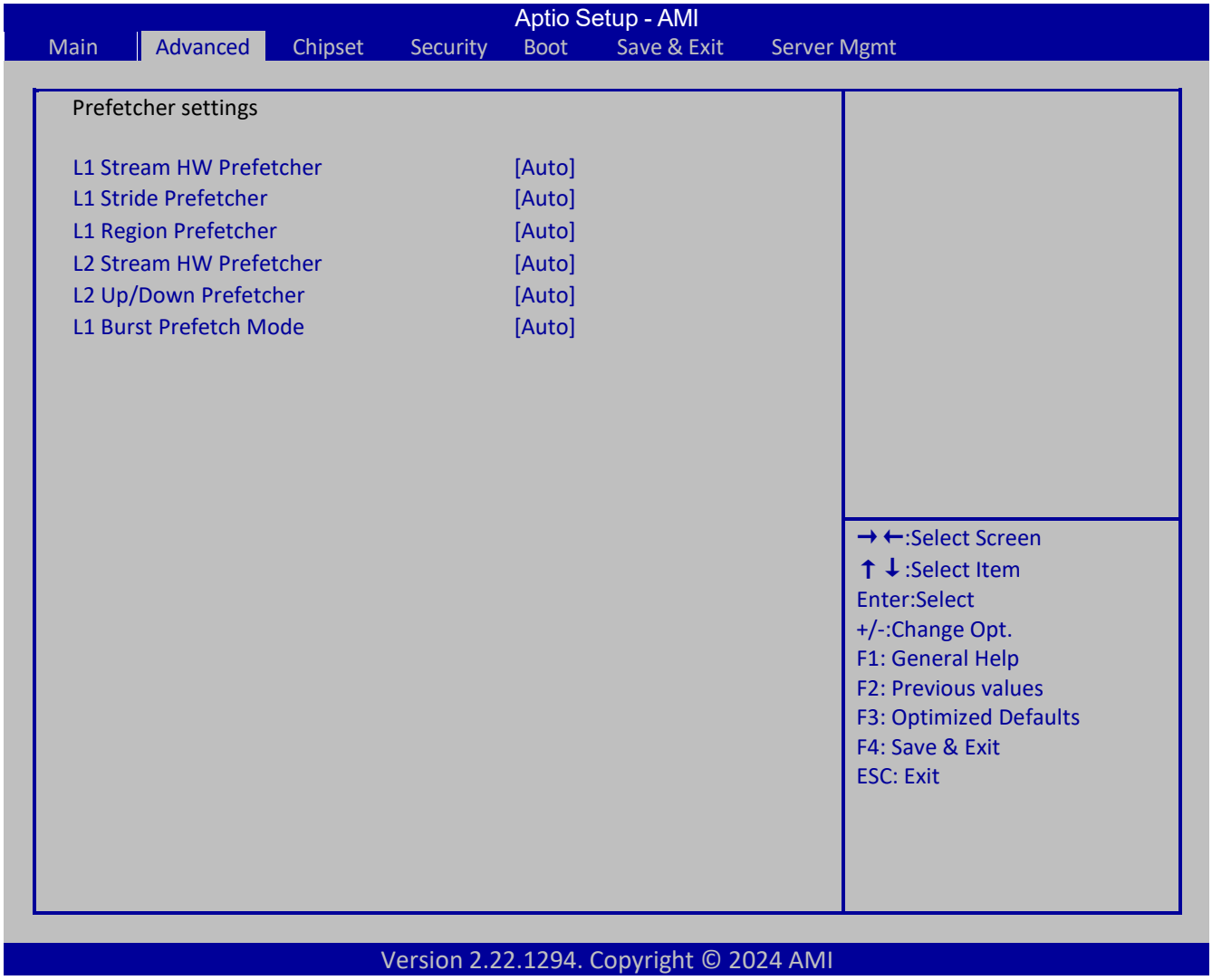
7.2.4.1.1.2 CCD/Core/Thread Enablement



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

Advanced \ AMD CBS \ CPU Common Options \ Performance \ CCD/Core/Thread Enablement		
Menu Fields	**Settings**	**Comments**
	[FOUR (4+0)] [FIVE (5+0)] [SIX (6+0)] [SEVEN (7+0)]	

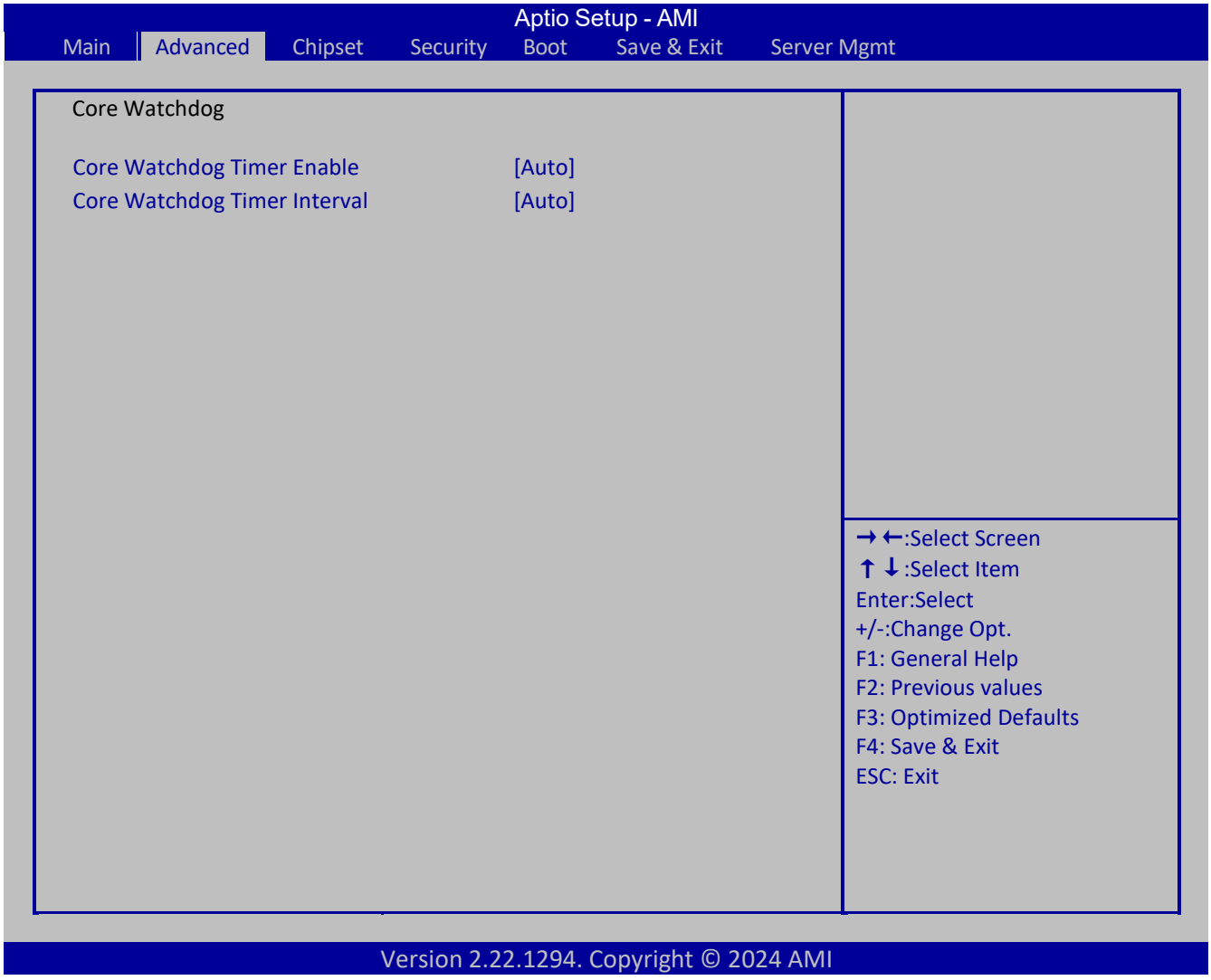
7.2.4.1.2 Prefetched settings



Advanced \ AMD CBS \ CPU Common Options \Prefetcher settings		
Menu Fields	**Settings**	**Comments**
L1 Stream HW Prefetcher	[Disable] [Enable] **[Auto]**	Option to Enable | Disable L1 Stream HW Prefetcher.
L1 Stride Prefetcher	[Disable] [Enable] **[Auto]**	Uses memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous.
L1 Region Prefetcher	[Disable] [Enable] **[Auto]**	Uses memory access history to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses.

Advanced \ AMD CBS \ CPU Common Options \Prefetcher settings		
Menu Fields	**Settings**	**Comments**
L2 Stream HW Prefetcher	[Disable] [Enable] **[Auto]**	Option to Enable | Disable L2 Stream HW prefetcher
L2 Up/Down Prefetcher	[Disable] [Enable] **[Auto]**	Uses memory access history to determine whether to fetch the next or previous line for all memory access
L1 Burst Prefetch Mode	[Disable] [Enable] **[Auto]**	Option to Enable | Disable L1 Burst prefetch Mode

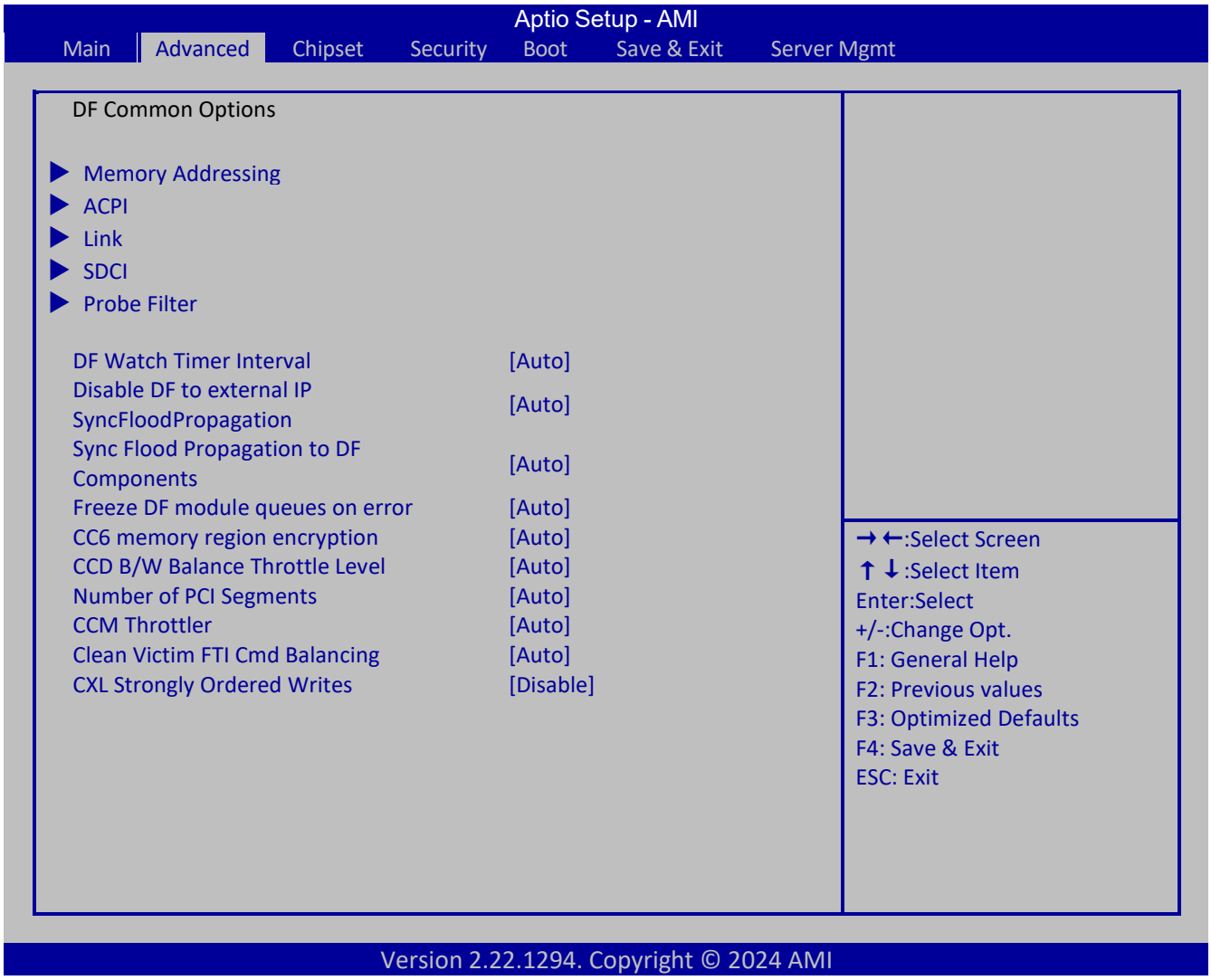
7.2.4.1.3 Core Watchdog



Advanced \ AMD CBS \ CPU Common Options \ Core Watchdog		
Menu Fields	**Settings**	**Comments**
Core Watchdog Timer Enable	[Disabled] [Enabled] **[Auto]**	Enable or disable CPU Watchdog Timer
Core Watchdog Timer Interval	[2.681s] [1.340s]	Select CPU Watchdog Timer interval

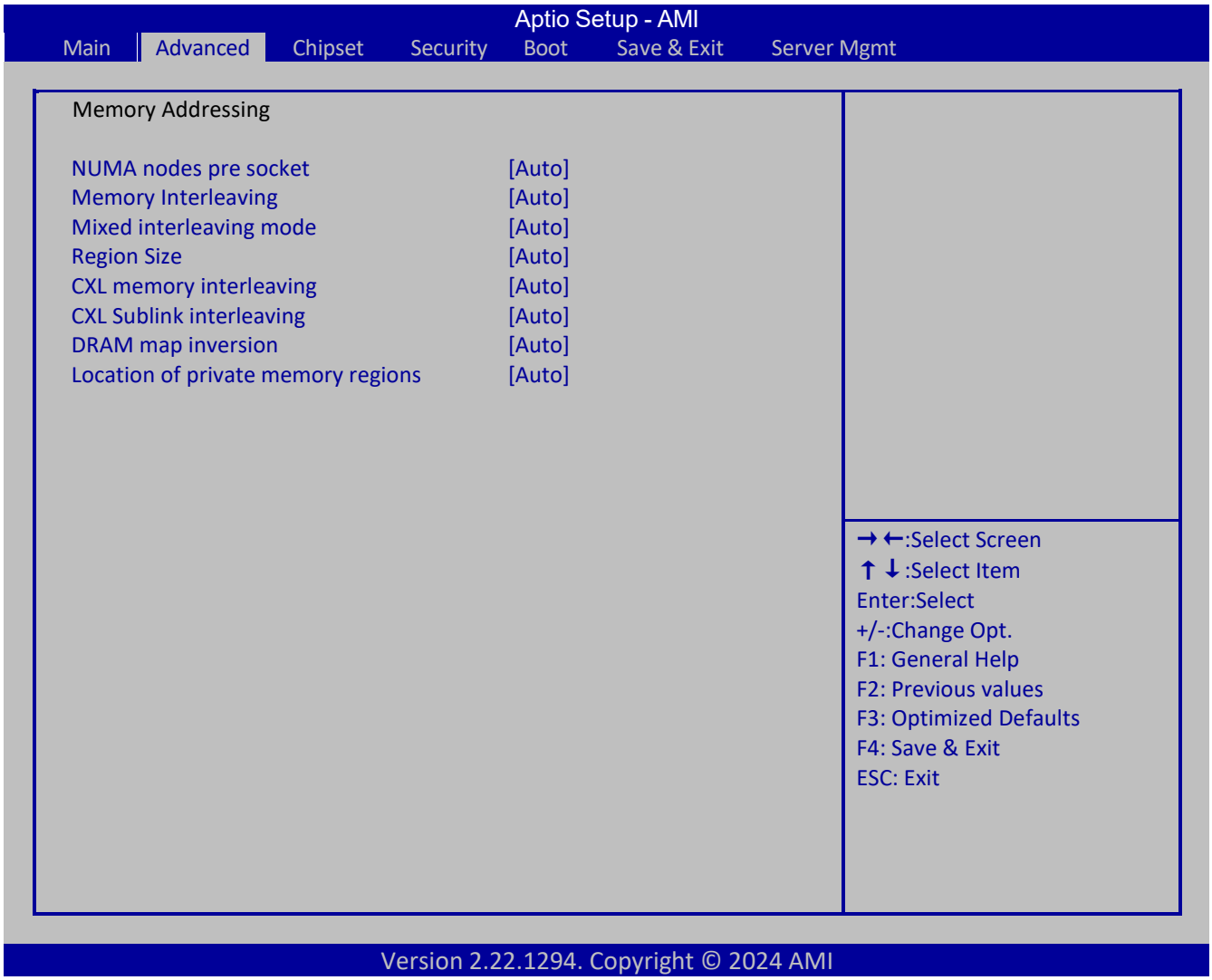
Advanced \ AMD CBS \ CPU Common Options \ Core Watchdog		
Menu Fields	**Settings**	**Comments**
	[669.41ms] [334.05ms] [166.37ms] [82.53ms] [40.61ms] [20.970ms] [10.484ms] [5.241ms] [2.620ms] [1.309ms] [654.08us] [326.4us] [162.56us] [80.64us] [39.68us] **[Auto]**	

7.2.4.2 DF Common Options



Advanced \ AMD CBS \ DF Common Options		
Menu Fields	**Settings**	**Comments**
Memory Addressing	Select sub-menu	Memory Addressing
ACPI	Select sub-menu	ACPI
Link	Select sub-menu	Link
SDCI	Select sub-menu	SDCI
Probe Filter	Select sub-menu	Probe Filter
DF Watch Timer Interval	**[Auto]** [41 ms] [166 ms] [334 ms] [669 ms] [1.34 seconds] [2.68 seconds] [5.36 seconds]	Configure the Data Fabric watchdog timer interval.
Disable DF to external IP SyncFloodPropagation	[Sync flood disabled] [Sync flood enabled] **[Auto]**	Disable SyncFlood to UMC & downstream slaves.
Sync Flood Propagation to DF Components	[Sync flood disabled] [Sync flood enabled] **[Auto]**	Control DF::PIEConfig[DisSyncFloodProp]
Freeze DF module queues on error	[Disabled] [Enabled] **[Auto]**	Controls DF::DfGlobalCtrl [DisImmSyncFloodOnFatalError] Disabling this option sets DF::DfGlobalCtrl [DisImmsyncFloodOnFatalError]
CC6 memory region encryption	[Disabled] [Enabled] **[Auto]**	Control Whether or not the CC6 save/restore memory is encrypted
CCD B/W Balance Throttle Level	**[Auto]** [Level 0] [Level 1] [Level 2] [Level 3] [Level 4]	Enables throttling of memory traffic pre CCD. Increased throttling can reduce imbalance across CCDs (expected to be rare).
Number of PCI Segments	[1 Segment] [2 Segments] [4 Segments] **[Auto]**	No help string
CCM Throttler	**[Auto]** [Enabled] [Disabled]	Limit peak CCM throughput
Clean Victim FTI Cmd Balancing	[Disabled] [Enabled] **[Auto]**	Control Clean Victim FTI Cmd Balancing feature
CXL Strongly Ordered Writes	**[Disabled]** [One at a time]	Determines how the host treats Strongly ordered Writes(ItoMWr and MemWr) from CXL.cache devices. When disabled is chosen Strongly ordered Writes are downgraded to Weakly ordered Writes within the host. When one at a time is chosen the host throttles processing Strongly ordered Writes to a one at a time cadence.

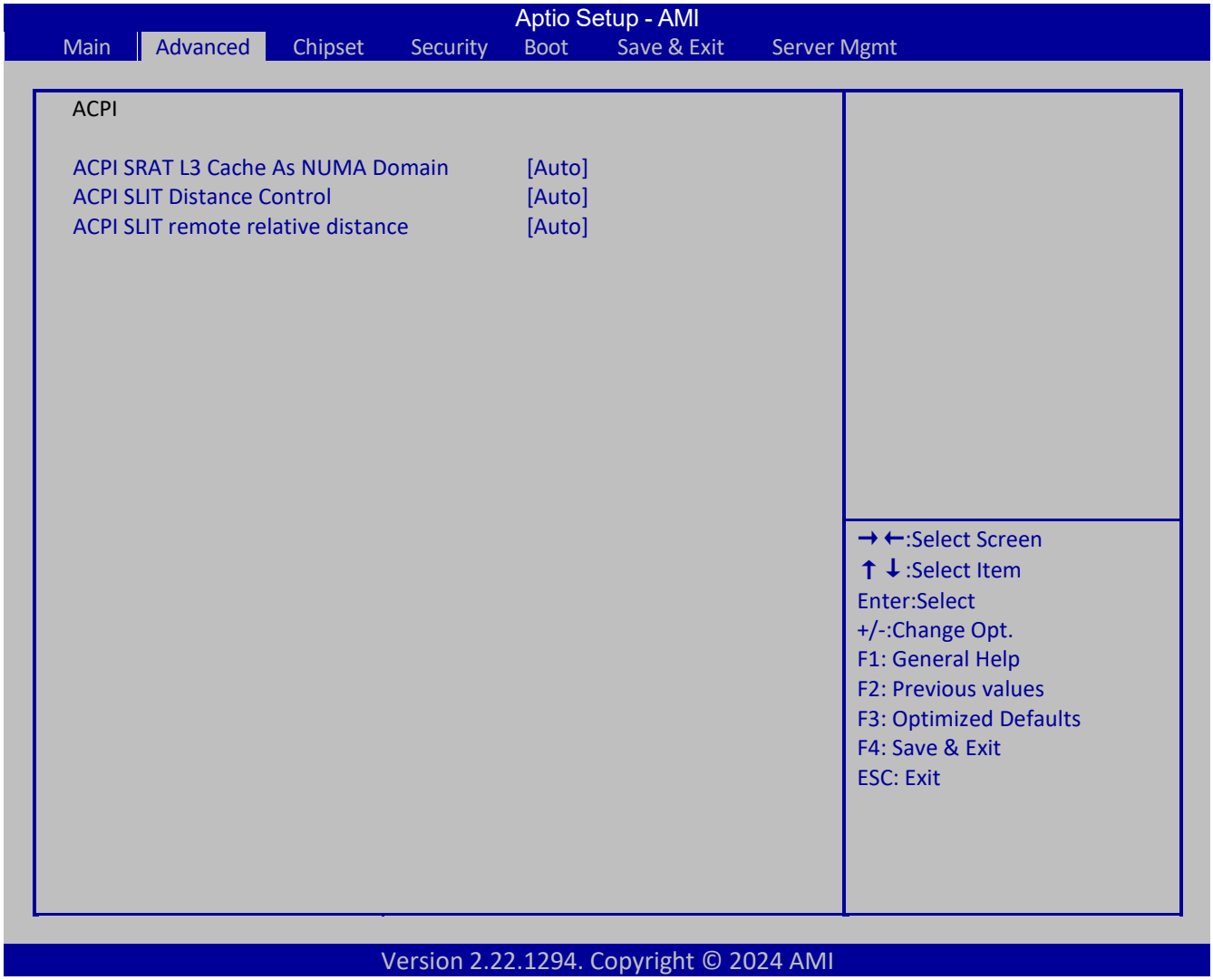
7.2.4.2.1 Memory Addressing



Advanced \ AMD CBS \ DF Common Options \ Memory Addressing		
Menu Fields	**Settings**	**Comments**
NUMA nodes pre socket	[NPS1] [NPS2] [NPS4] **[Auto]**	Specifies the number of desired NUMA nodes pre socket, Zero will attempt to interleave the two sockets together.
Memory Interleaving	[Disabled] [Enabled] **[Auto]**	Allows for disabling memory interleaving. Note that NUMA nodes pre socket will be honored regardless of this setting.
Mixed interleaving mode	[Disabled] [Enabled] **[Auto]**	Allow for interleaving UMC and CXL together.
Region Size	[1K Region Size] [2K Region Size] **[Auto]**	Selects between a 1K or 2K region size.
CXL memory interleaving	[Disabled] [Enabled] **[Auto]**	Allows for enabling/disabling CXL memory devices interleaving. Option inactive when 'CXL Memory Online/offline' is enabled.

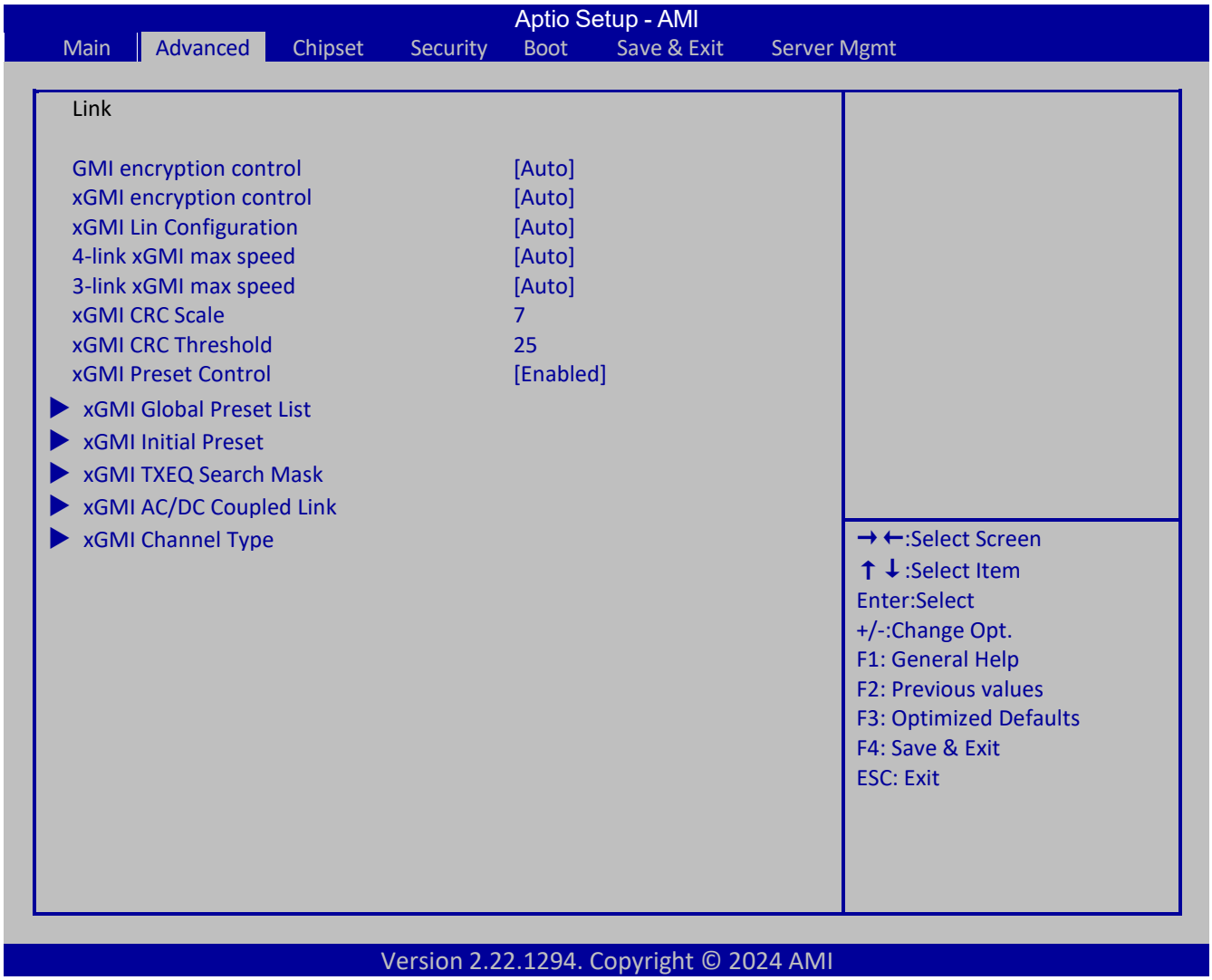
Advanced \ AMD CBS \ DF Common Options \ Memory Addressing		
Menu Fields	**Settings**	**Comments**
CXL Sublink interleaving	[Enable] [Disable] **[Auto]**	Enable or disable CXL sublink interleaving. Option inactive when 'CXL Memory Online/offline' is enabled.
DRAM map inversion	[Disabled] [Enabled] **[Auto]**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

7.2.4.2.2 ACPI



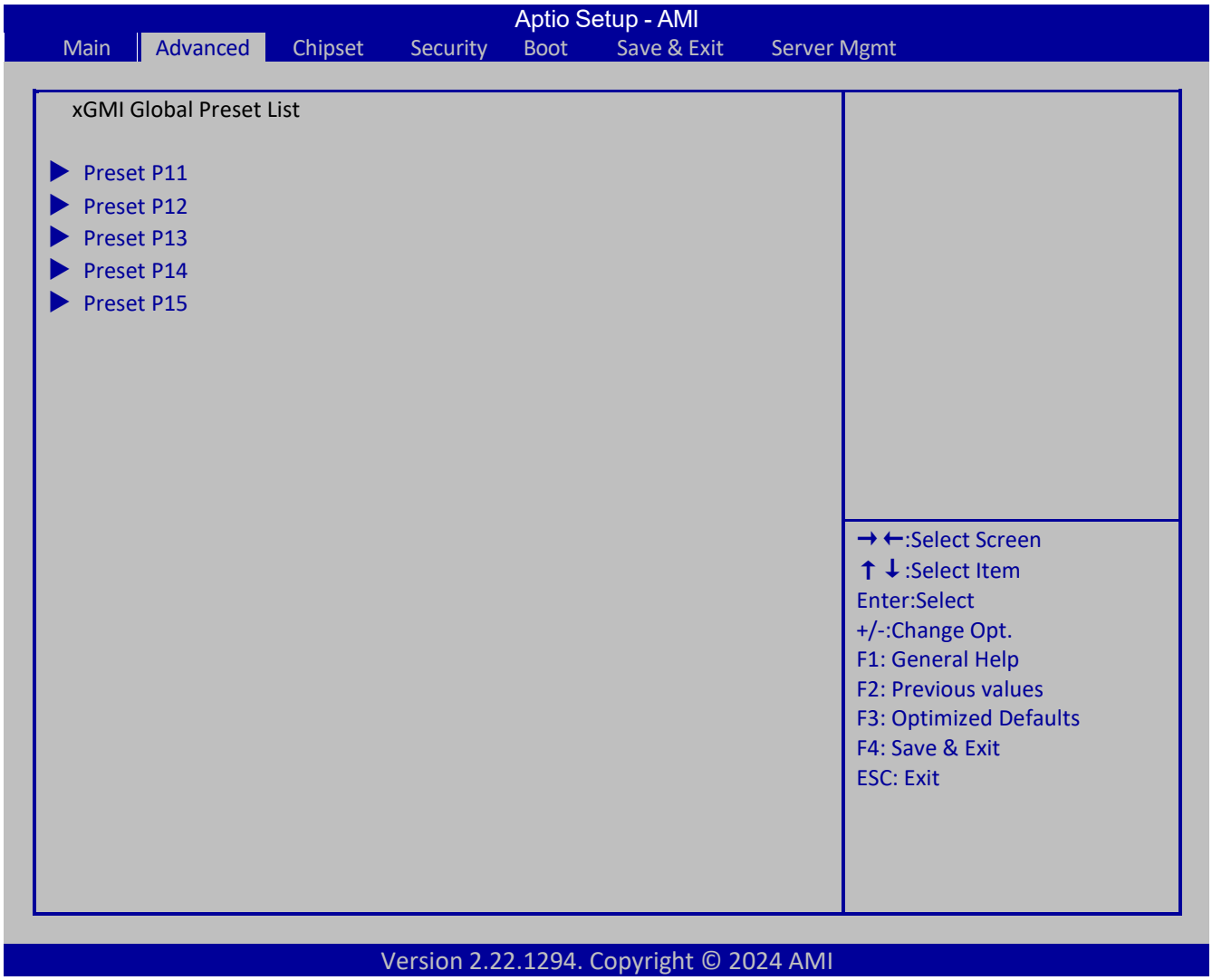
Advanced \ AMD CBS \ DF Common Options \ ACPI		
Menu Fields	**Settings**	**Comments**
ACPI SRAT L3 Cache As NUMA Domain	[Disabled] [Enabled] **[Auto]**	Enabled: Each CCX in the system will be declared as a separate NUMA domain. Disabled: Memory Addressing NUMA nodes per socket will be declared.
ACPI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

7.2.4.2.3 Link



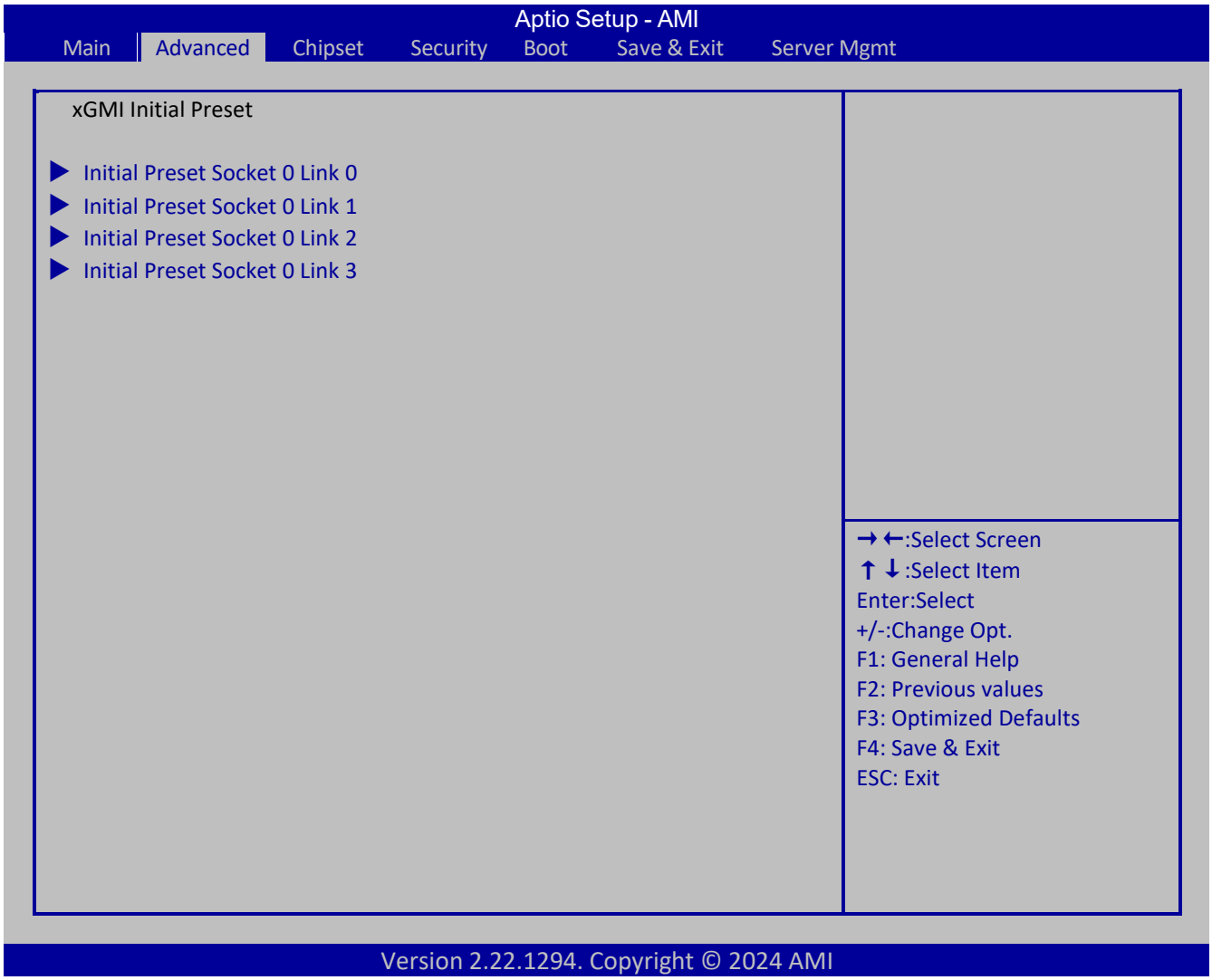
Advanced \ AMD CBS \ DF Common Options \ Link		
Menu Fields	**Settings**	**Comments**
GMI encryption control	[Disabled] [Enabled] **[Auto]**	Control GMI link encryption. Program GMI key to enabling encryption.
xGMI encryption control	[Disabled] [Enabled] **[Auto]**	Control XGMI link encryption. Program XGMI key to enabling encryption.
xGMI Lin Configuration	**[Auto]** [3 xGMI Links] [4 xGMI Links] [2 xGMI Links + 2PCI Links]	Configures the number of XGMI2 link used on a multi-socket system.
4-link xGMI max speed	[20Gbps] [25Gbps] [32Gbps] **[Auto]**	Specifies the max frequency used for XGMI PState in a 4-link topology.
3-link xGMI max speed	[20Gbps] [25Gbps] [32Gbps] **[Auto]**	Specifies the max frequency used for XGMI PState in a 3-link topology.
xGMI CRC Scale	x	Configure leaky bucket scale for XGMI and WAFL CRC errors. Every scale milliseconds an error will leak from the CRC counter.
xGMI CRC Threshold	x	Configure leaky bucket threshold for XGMI and WAFL CRC error. If link CRC counter exceeds this threshold, an error will be logged.
xGMI Preset Control	[Disabled] **[Enabled]** [Auto]	Enable/Disable XGMI Preset Control options
xGMI Global Preset List	Selects sub-menu	xGMI Global Preset List
xGMI Initial Preset	Selects sub-menu	xGMI Initial Preset
xGMI TXEQ Search Mask	Selects sub-menu	xGMI TXEQ Search Mask
xGMI AC/DC Coupled Link	Selects sub-menu	xGMI AC/DC Coupled Link
xGMI Channel Type	Selects sub-menu	xGMI Channel Type

7.2.4.2.3.1 xGMI Global Preset List



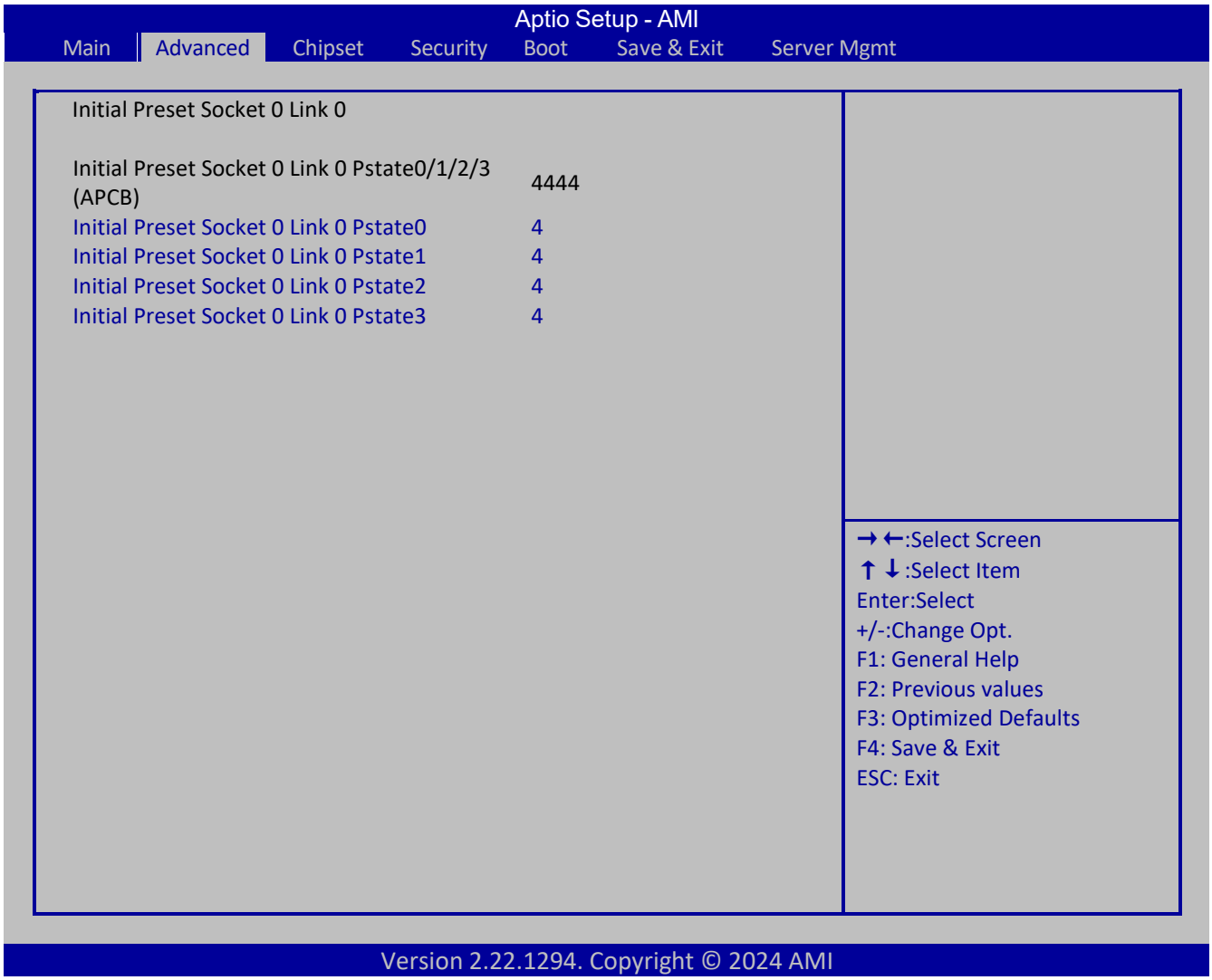
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Global Preset List		
Menu Fields	**Settings**	**Comments**
Preset P11	Selects sub-menu	Preset P11
Preset P12	Selects sub-menu	Preset P12
Preset P13	Selects sub-menu	Preset P13
Preset P14	Selects sub-menu	Preset P14
Preset P15	Selects sub-menu	Preset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

7.2.4.2.3.2 xGMI Initial Preset



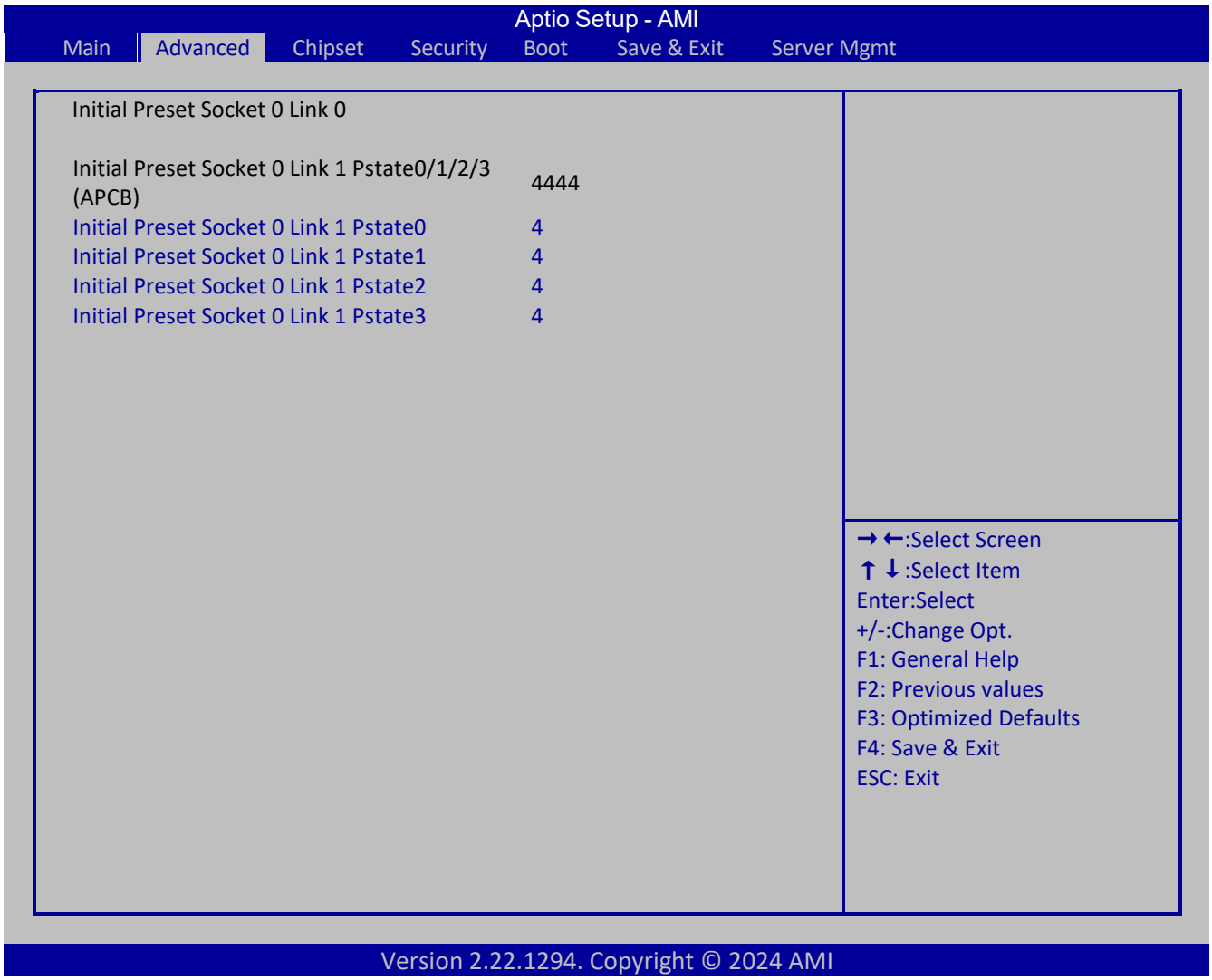
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset		
Menu Fields	**Settings**	**Comments**
Initial Preset Socket 0 Link 0	Selects sub-menu	Initial Preset Socket 0 Link 0
Initial Preset Socket 0 Link 1	Selects sub-menu	Initial Preset Socket 0 Link 1
Initial Preset Socket 0 Link 2	Selects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

7.2.4.2.3.2.1 Initial Preset Socket 0 Link 0



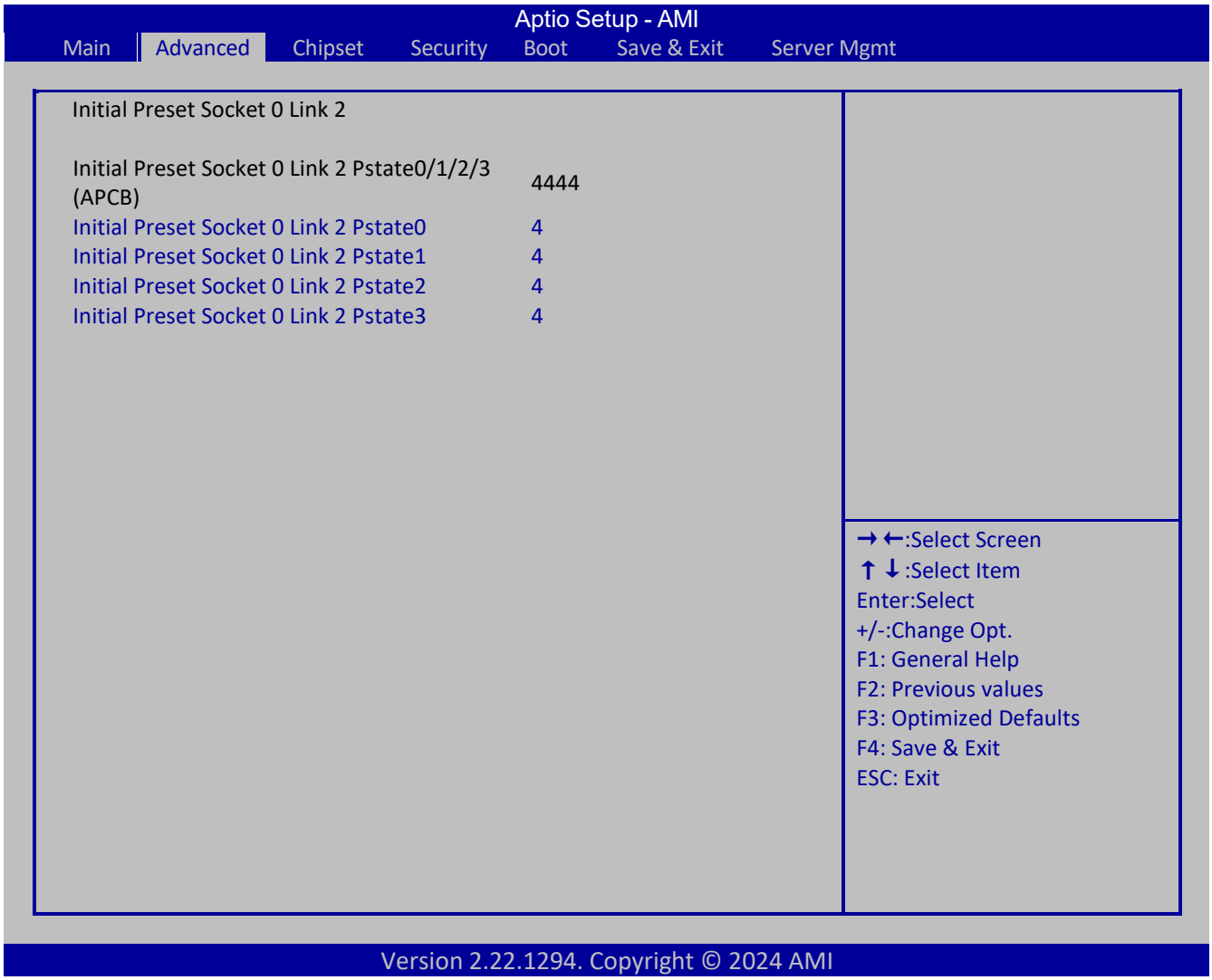
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 0		
Menu Fields	**Settings**	**Comments**
Initial Preset Socket 0 Link 0 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 0 Pstate0
Initial Preset Socket 0 Link 0 Pstate1	X	Enable/Disable Initial Preset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

7.2.4.2.3.2.2 Initial Preset Socket 0 Link 1



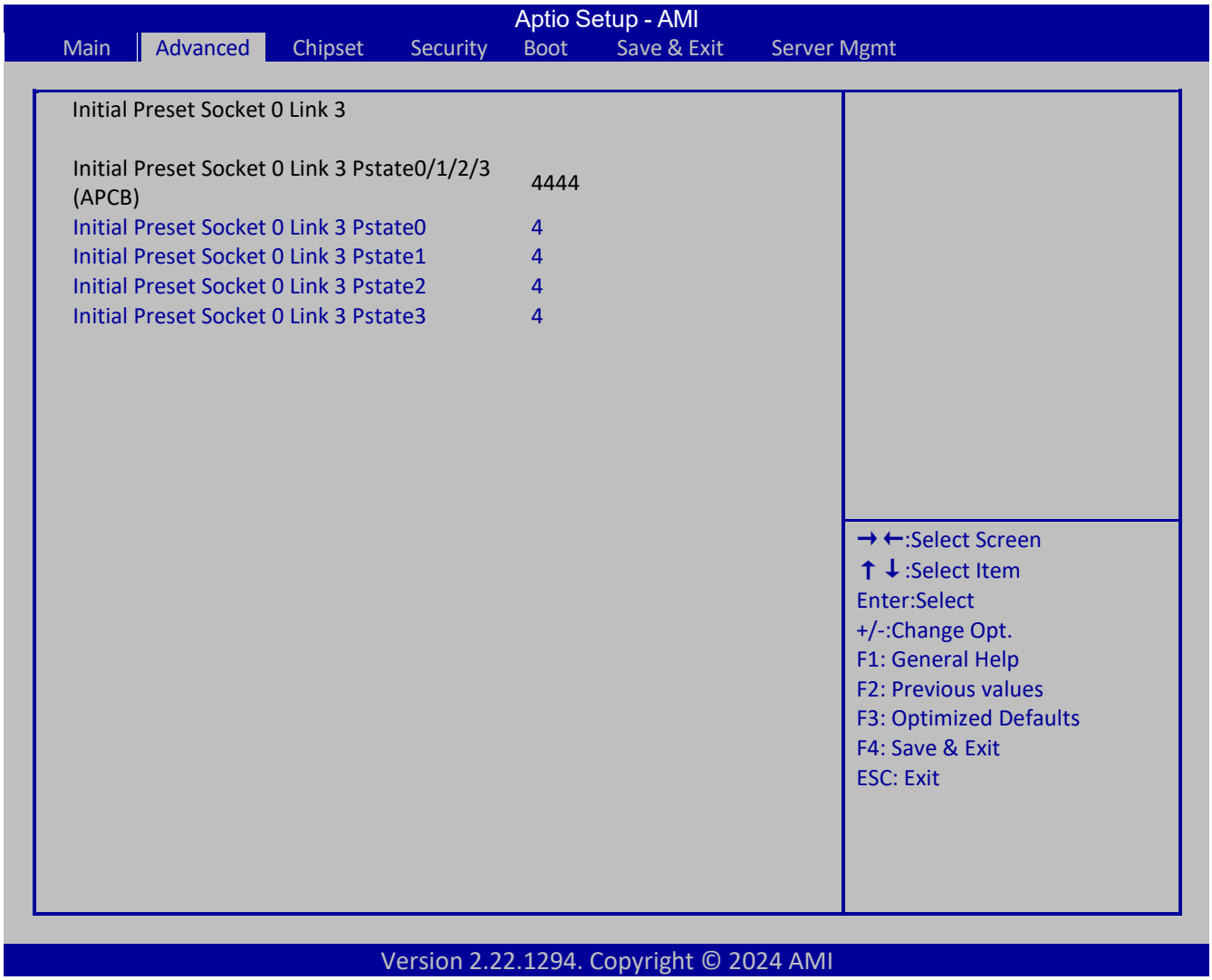
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 1		
Menu Fields	**Settings**	**Comments**
Initial Preset Socket 0 Link 1 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 1 Pstate0
Initial Preset Socket 0 Link 1 Pstate1	X	Enable/Disable Initial Preset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

7.2.4.2.3.2.3 Initial Preset Socket 0 Link 2



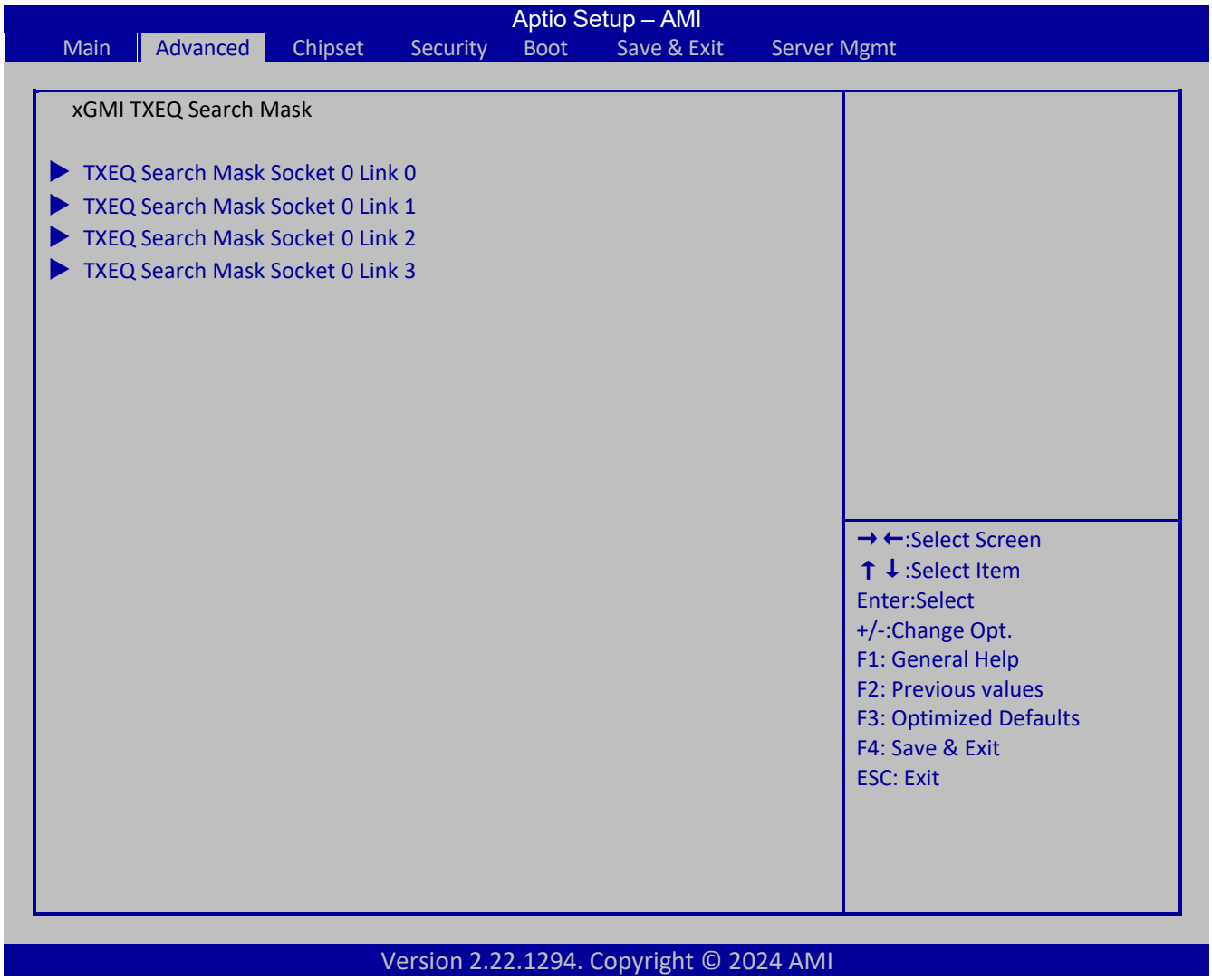
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 2		
Menu Fields	**Settings**	**Comments**
Initial Preset Socket 0 Link 2 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 2 Pstate0
Initial Preset Socket 0 Link 2 Pstate1	X	Enable/Disable Initial Preset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

7.2.4.2.3.2.4 Initial Preset Socket 0 Link 3



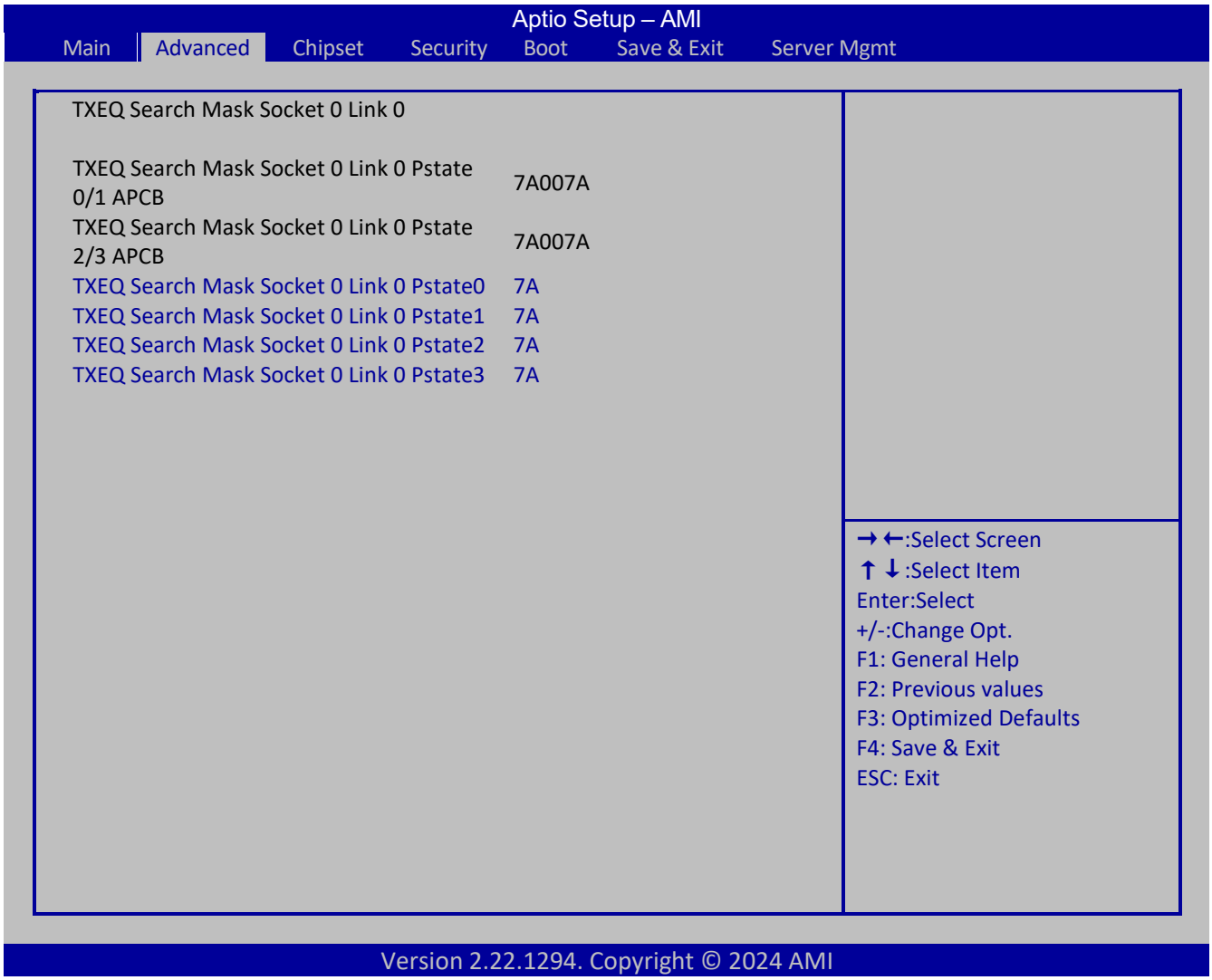
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Initial Preset \ Initial Preset Socket 0 Link 3		
Menu Fields	**Settings**	**Comments**
Initial Preset Socket 0 Link 3 Pstate0	X	Enable/Disable Initial Preset Socket 0 Link 3 Pstate0
Initial Preset Socket 0 Link 3 Pstate1	X	Enable/Disable Initial Preset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

7.2.4.2.3.3 xGMI TXEQ Search Mask



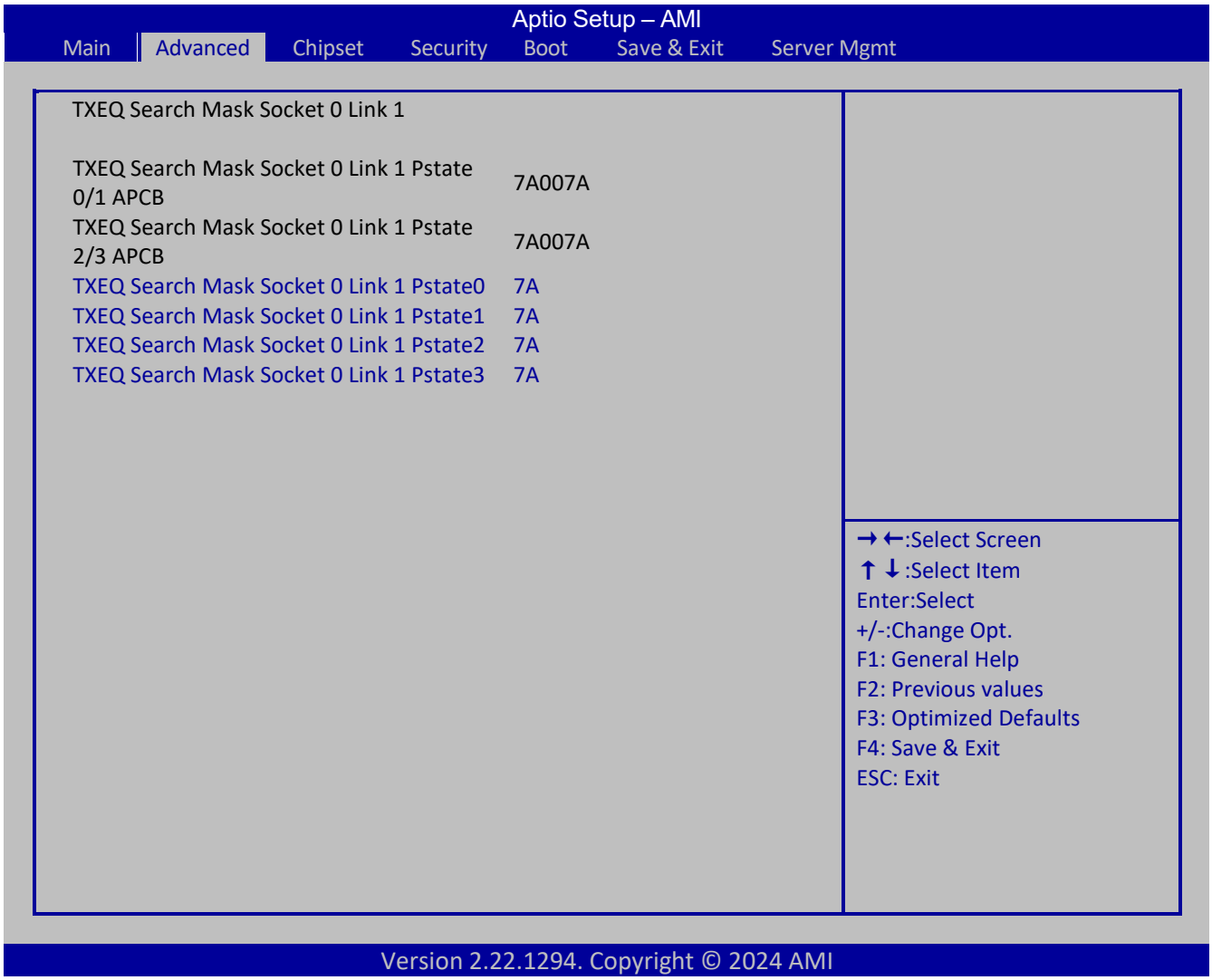
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask		
Menu Fields	**Settings**	**Comments**
TXEQ Search Mask Socket 0 Link 0	Selects sub-menu	TXEQ Search Mask Socket 0 Link 0
TXEQ Search Mask Socket 0 Link 1	Selects sub-menu	TXEQ Search Mask Socket 0 Link 1
TXEQ Search Mask Socket 0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

7.2.4.2.3.3.1 TXEQ Search Mask Socket 0 Link 0



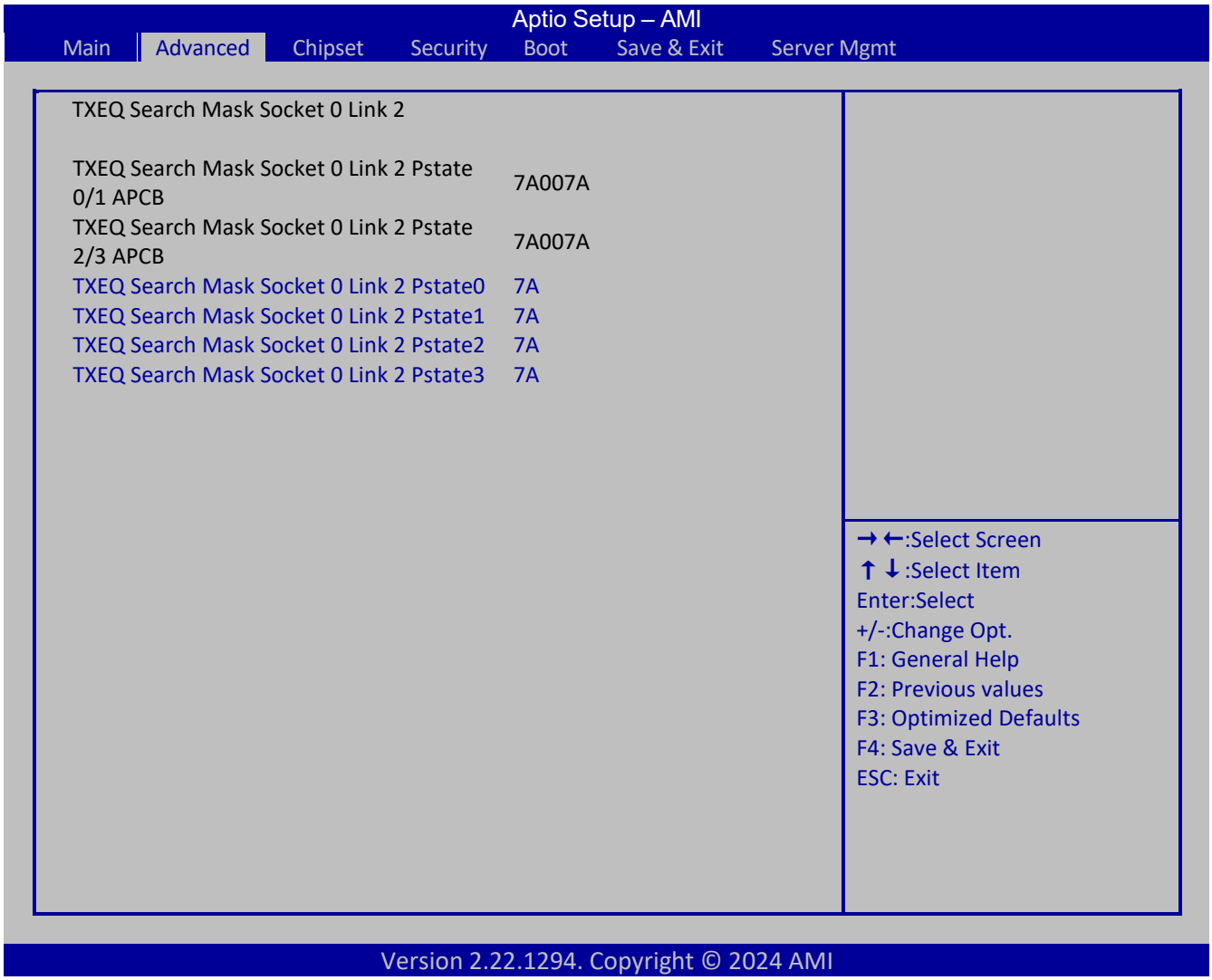
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 0		
Menu Fields	**Settings**	**Comments**
TXEQ Search Mask Socket 0 Link 0 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 0 Pstate0
TXEQ Search Mask Socket 0 Link 0 Pstate1	X	Enable/Disable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

7.2.4.2.3.3.2 TXEQ Search Mask Socket 0 Link 1



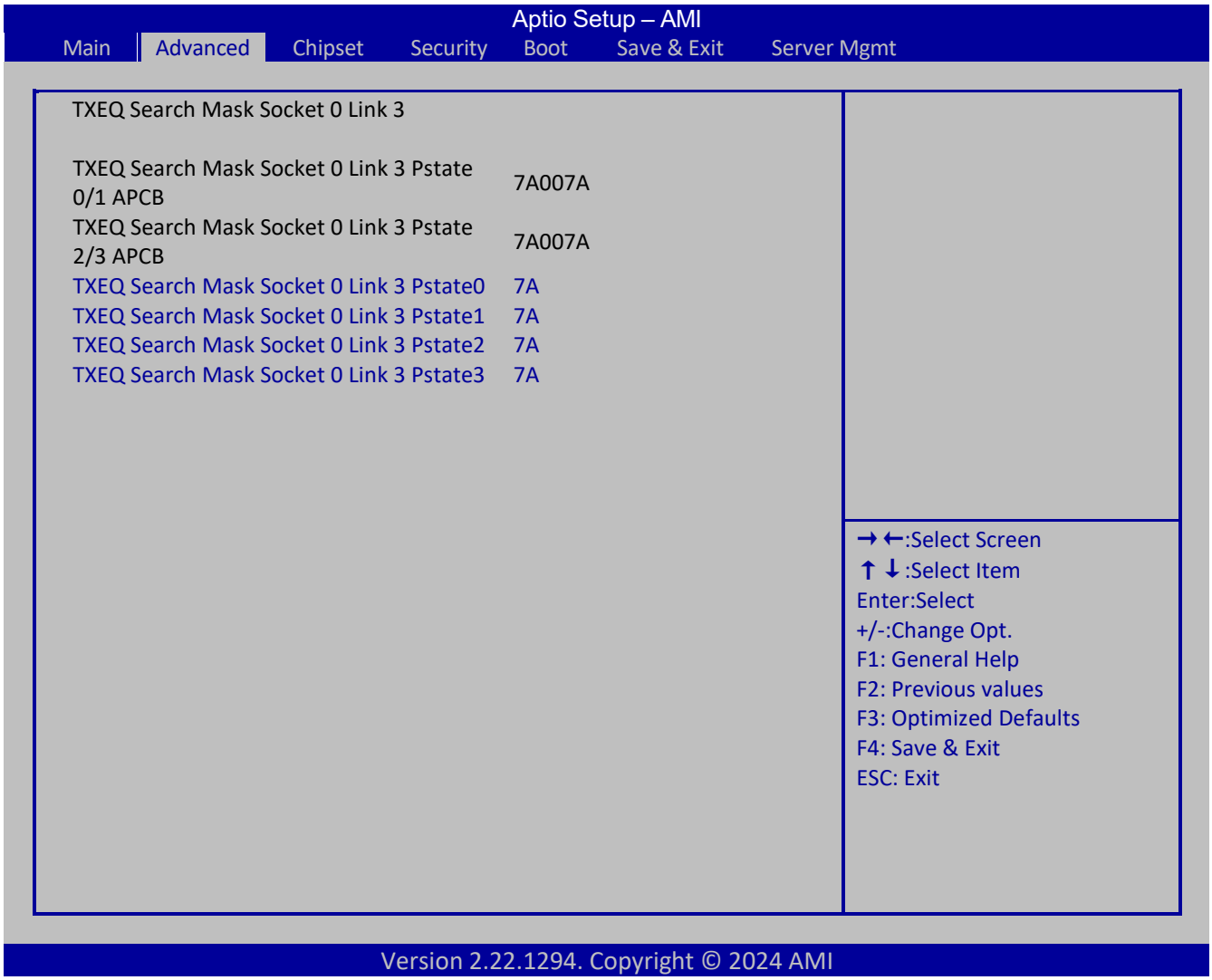
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask		
Menu Fields	**Settings**	**Comments**
TXEQ Search Mask Socket 0 Link 1 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate0
TXEQ Search Mask Socket 0 Link 1 Pstate1	X	Enable/Disable TXEQ Search Make Socket 0 Link 1 Pstate1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

7.2.4.2.3.3.3 TXEQ Search Mask Socket 0 Link 2



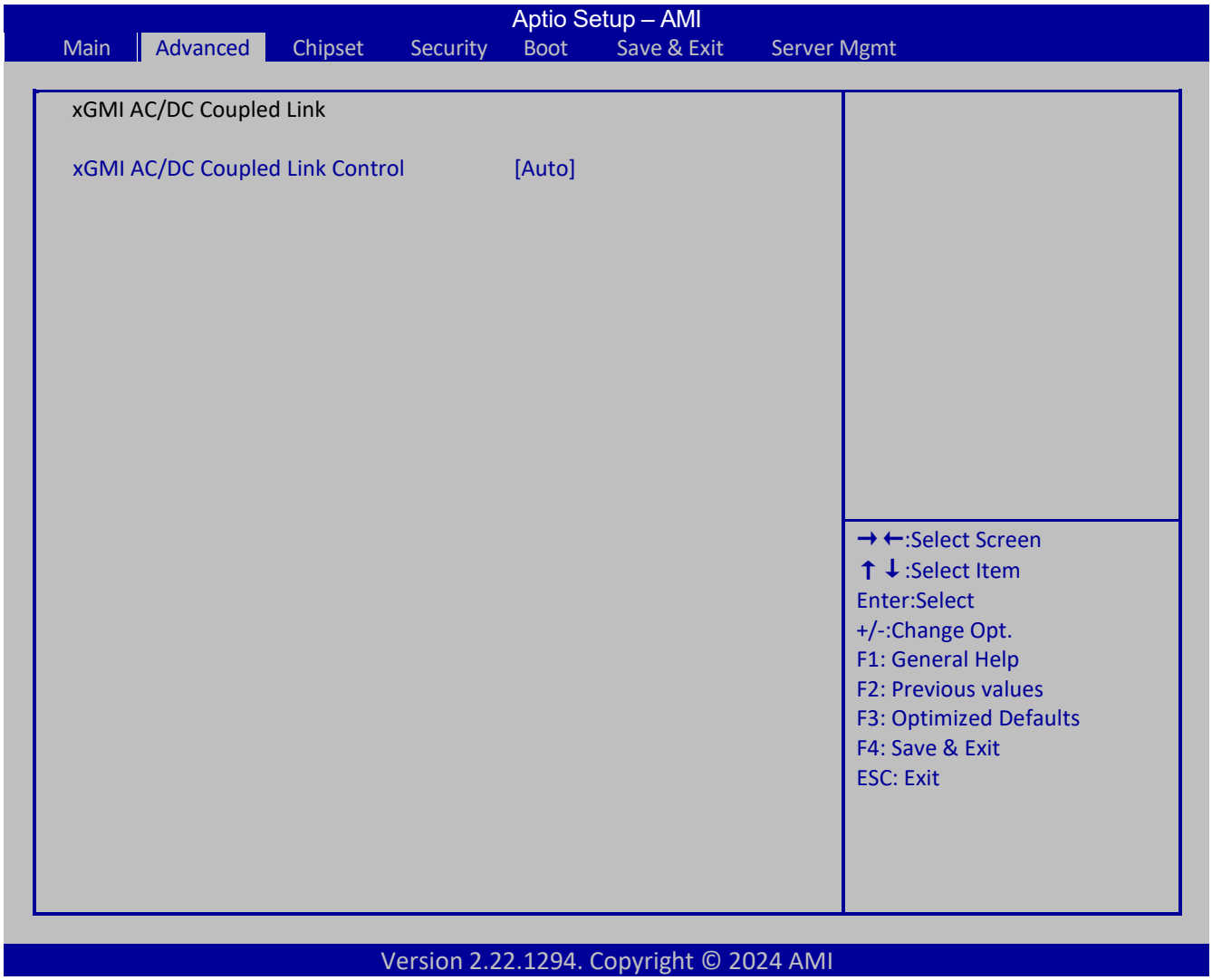
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 2		
Menu Fields	**Settings**	**Comments**
TXEQ Search Mask Socket 0 Link 2 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 2 Pstate0
TXEQ Search Mask Socket 0 Link 2 Pstate1	X	Enable/Disable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

7.2.4.2.3.3.4 TXEQ Search Mask Socket 0 Link 3



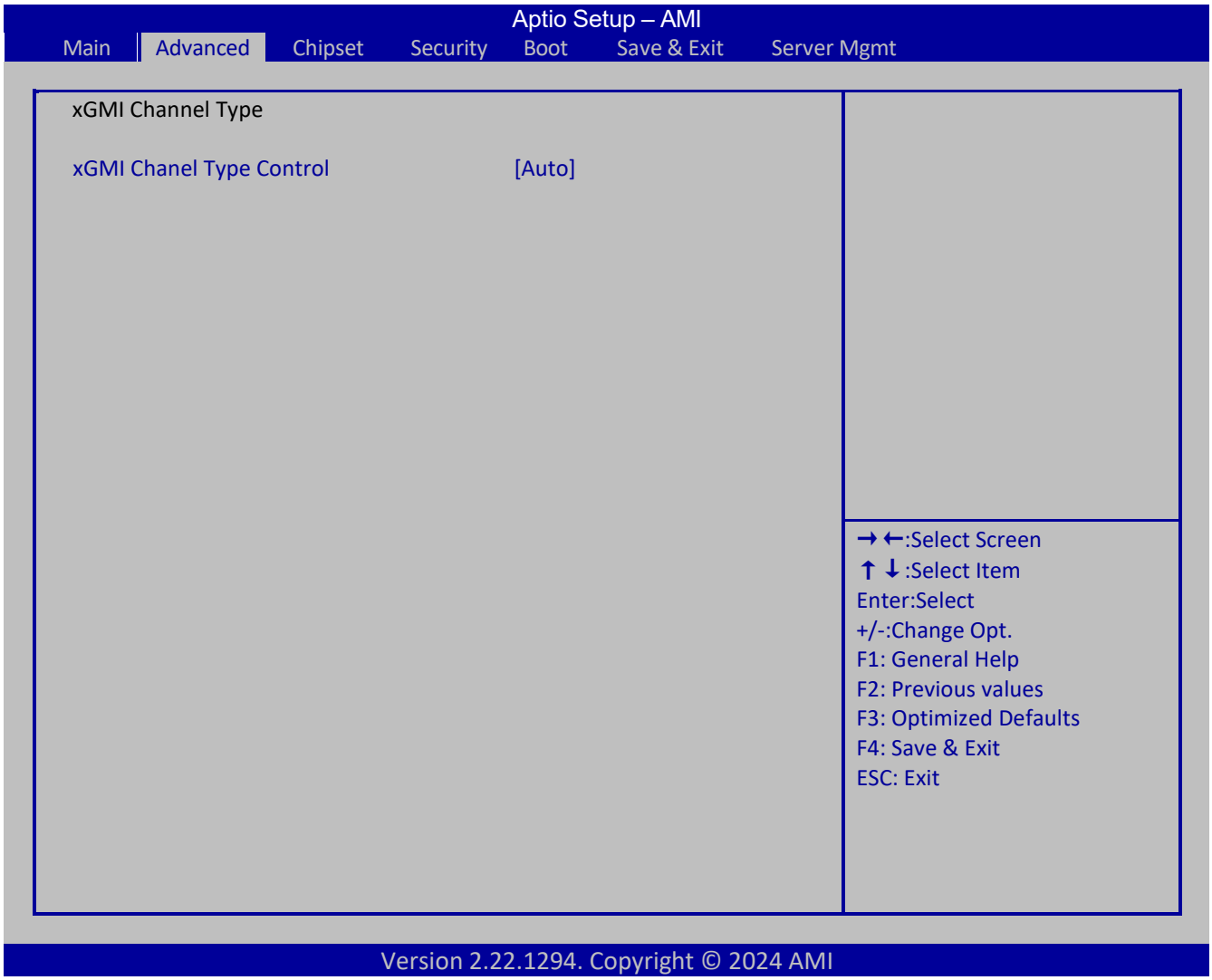
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI TXEQ Search Mask \ TXEQ Search Make Socket 0 Link 3		
Menu Fields	**Settings**	**Comments**
TXEQ Search Mask Socket 0 Link 3 Pstate0	X	Enable/Disable TXEQ Search Make Socket 0 Link 3 Pstate0
TXEQ Search Mask Socket 0 Link 3 Pstate1	X	Enable/Disable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

7.2.4.2.3.4 xGMI AC/DC Coupled Link



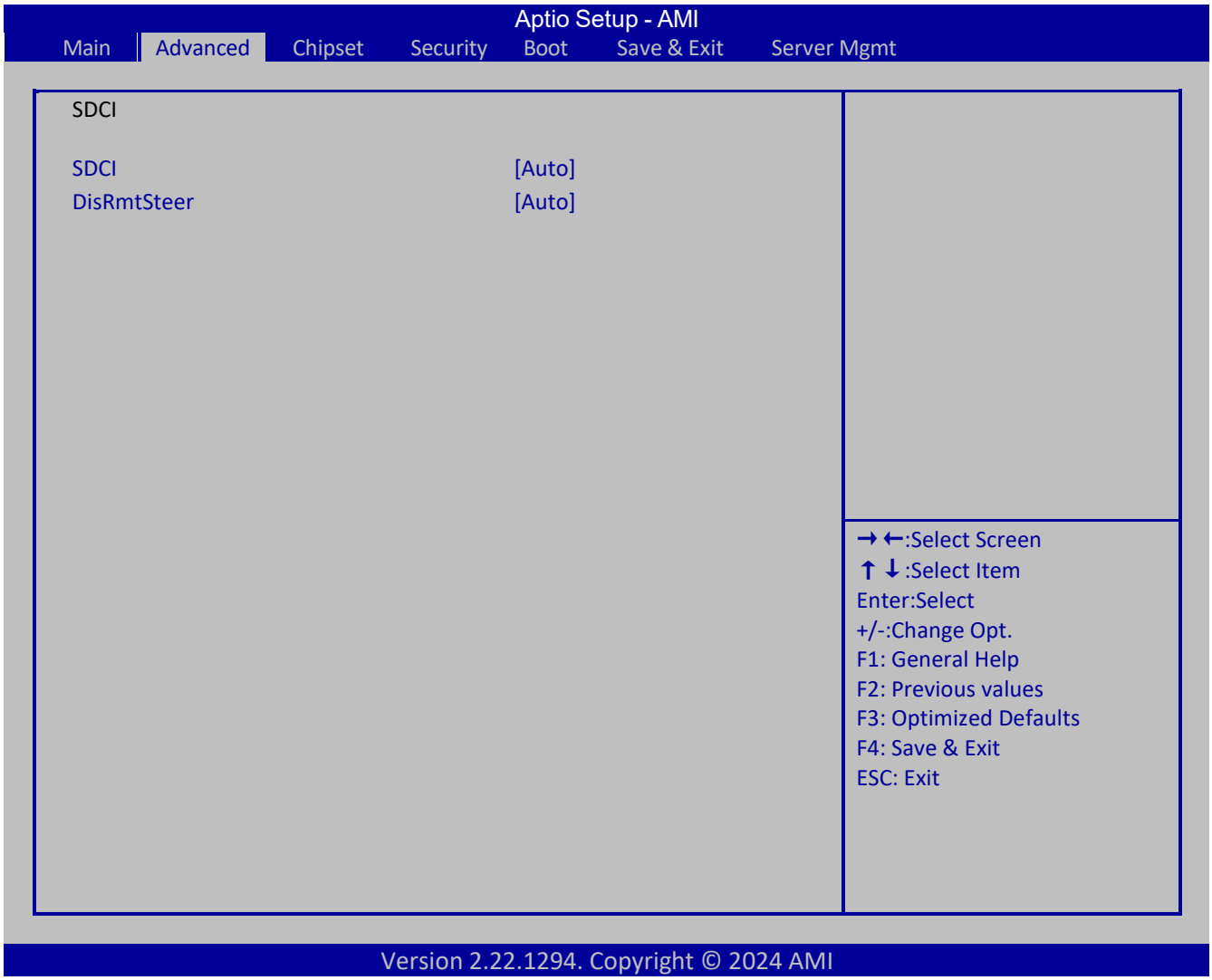
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI AC/DC Coupled Link		
Menu Fields	**Settings**	**Comments**
xGMI AC/DC Coupled Link Control	[Manual] **[Auto]**	Control XGMI AC/DC Coupled Link. Valid value: 0: AC Coupled 1: DC Coupled

7.2.4.2.3.5 xGMI Channel Type



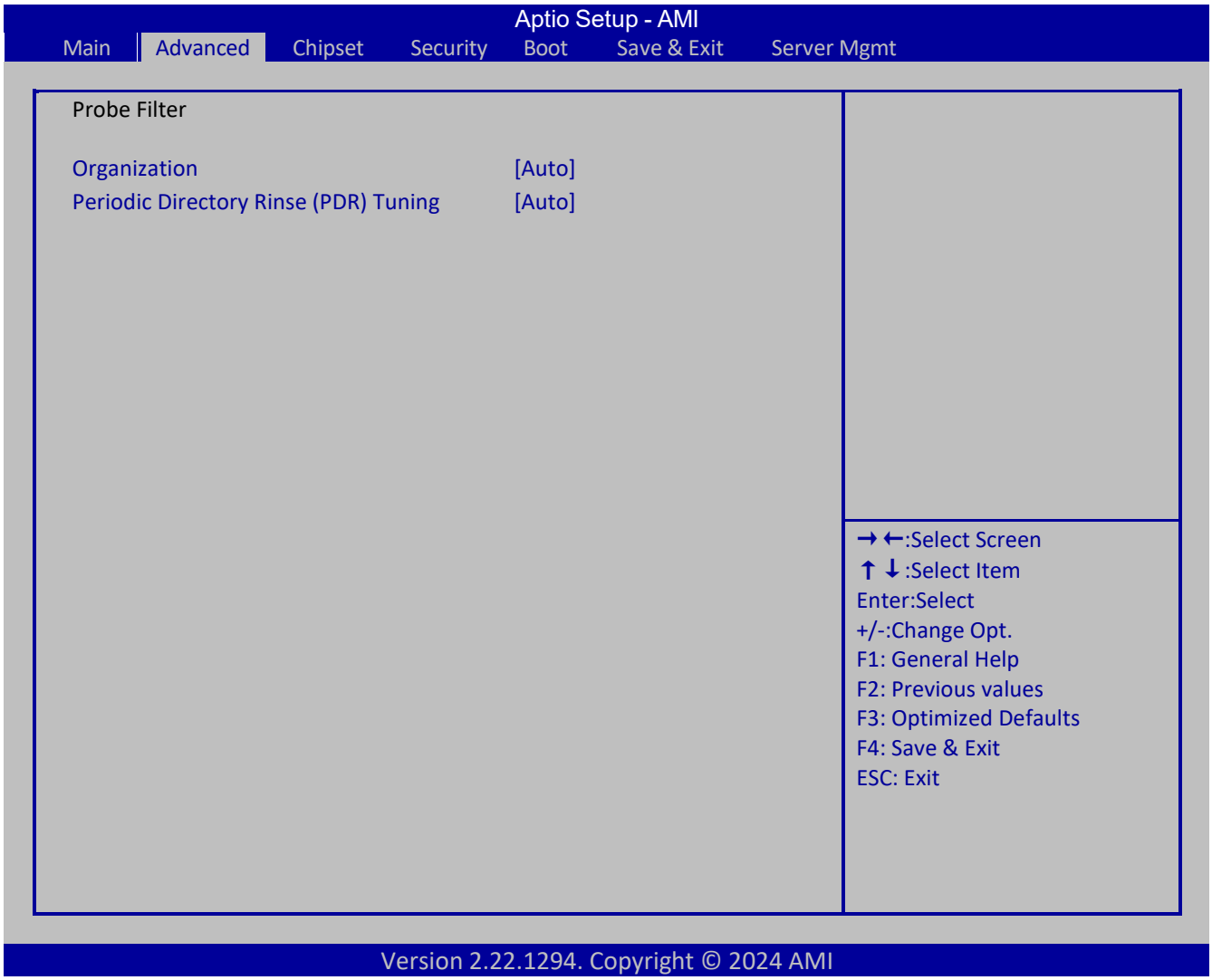
Advanced \ AMD CBS \ DF Common Options \ Link \ xGMI Channel Type		
Menu Fields	**Settings**	**Comments**
xGMI Channel Type Control	[Manual] **[Auto]**	Control XGMI Channel Type. Valid Channel Type: 0: Disable 1: Long Reach

7.2.4.2.4 SDCI



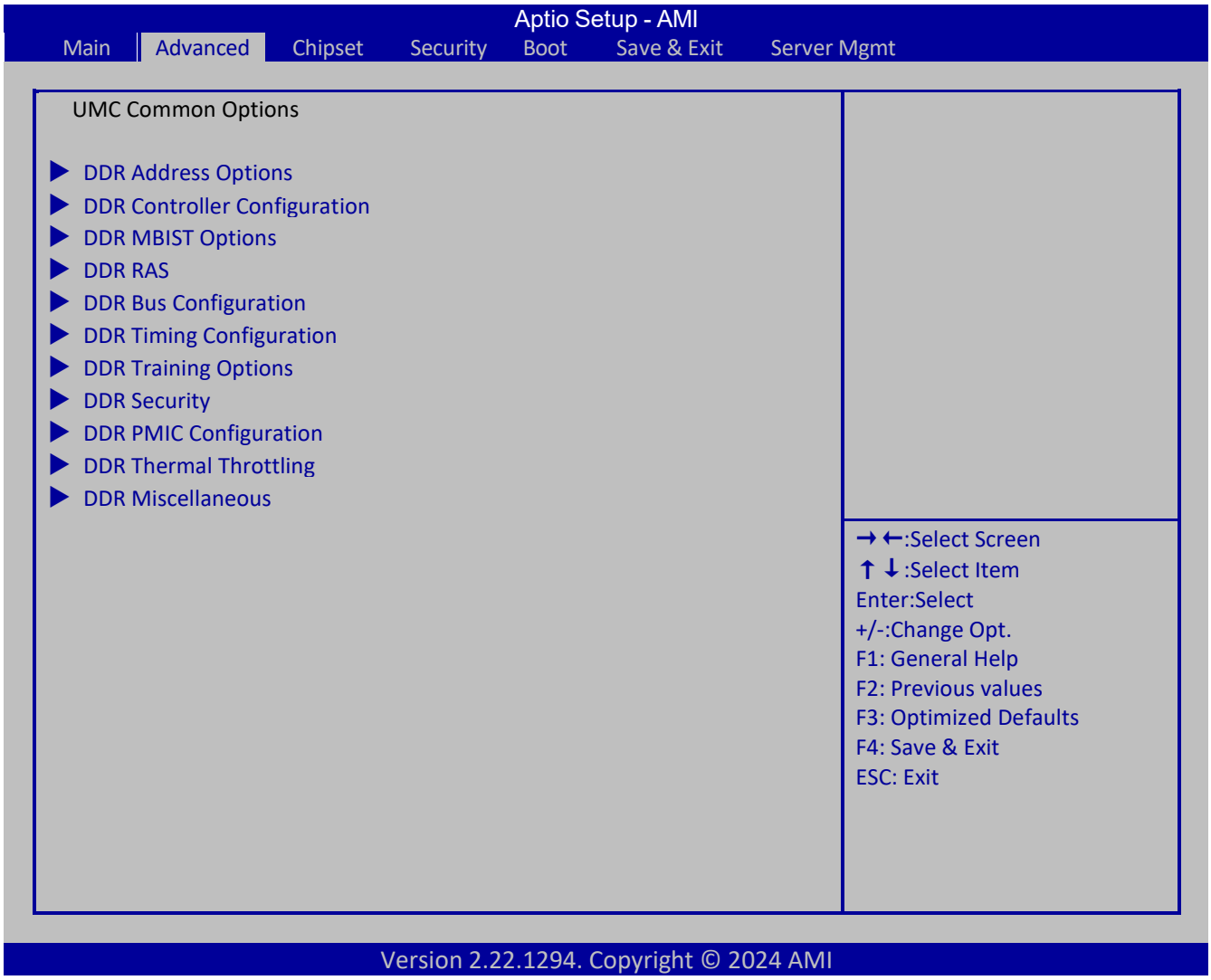
Advanced \ AMD CBS \ DF Common Options \ SDCI		
Menu Fields	**Settings**	**Comments**
SDCI	[Disabled] [Enabled] **[Auto]**	Enable or Disable smart Data Cache Injection feature.
DisRmtSteer	[Disabled] [Enabled] **[Auto]**	When set, this bit disables the sending of steering probes to remote socket.

7.2.4.2.5 Probe Filter



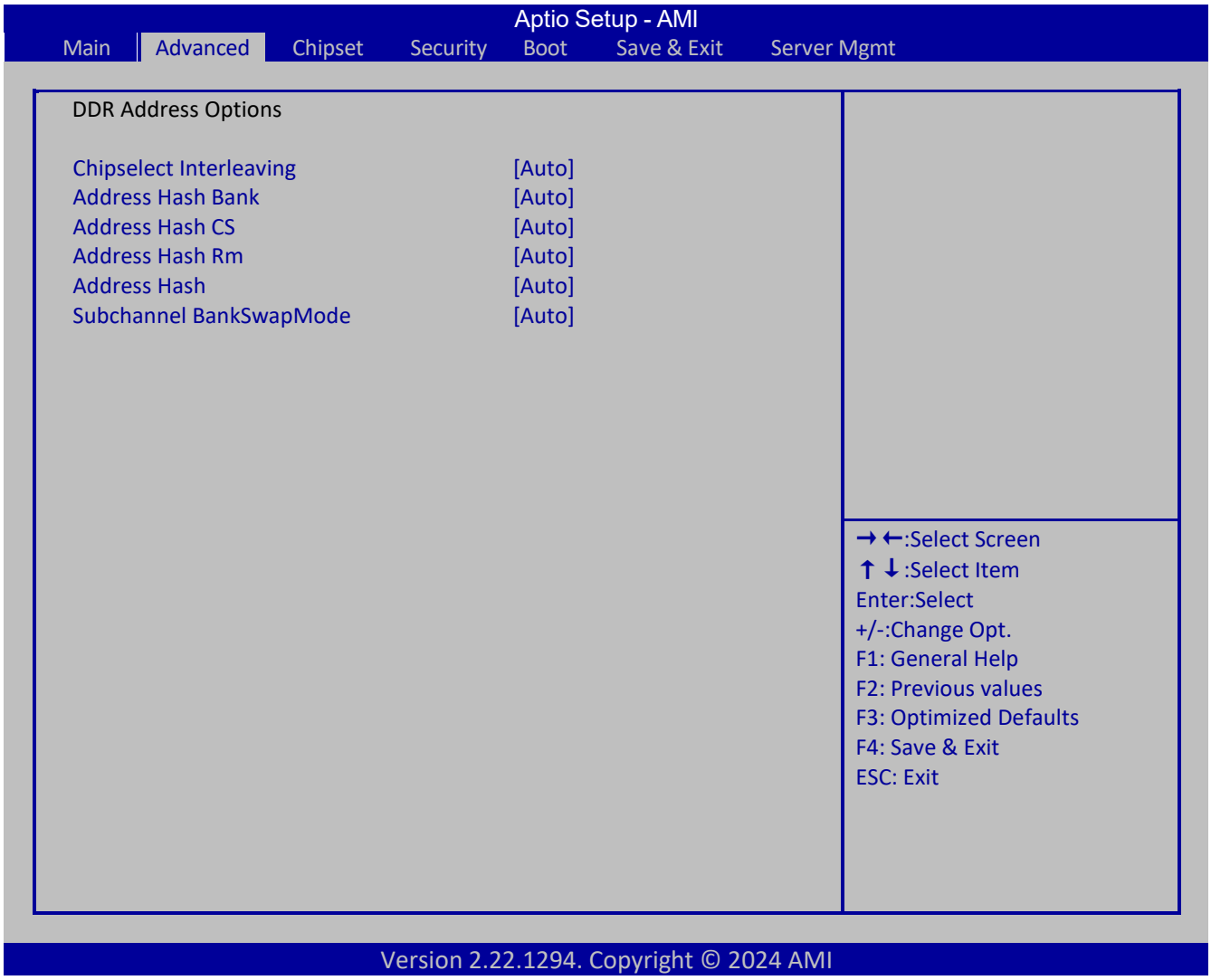
Advanced \ AMD CBS \ DF Common Options \ Probe Filter		
Menu Fields	**Settings**	**Comments**
Organization	**[Auto]** [Dedicated] [Shared]	Specifies whether multiple memory/CXL Channels will share probe filter storage. For memory sizes of 16TB or larger , this feature is ignored as it is auto-selected to 'shared'
Periodic Directory Rinse (PDR) Tuning	[Periodic] [Blended] **[Auto]**	Control PDR Settings that may impact performance by workload and/or processor. Periodic (RefClock Based Floss Only): Rate based Directory Rinse. Blended (Cache Load Based Floss with Background RefClock Based Floss): Demand based Directory Rinse.

7.2.4.3 UMC Common Options



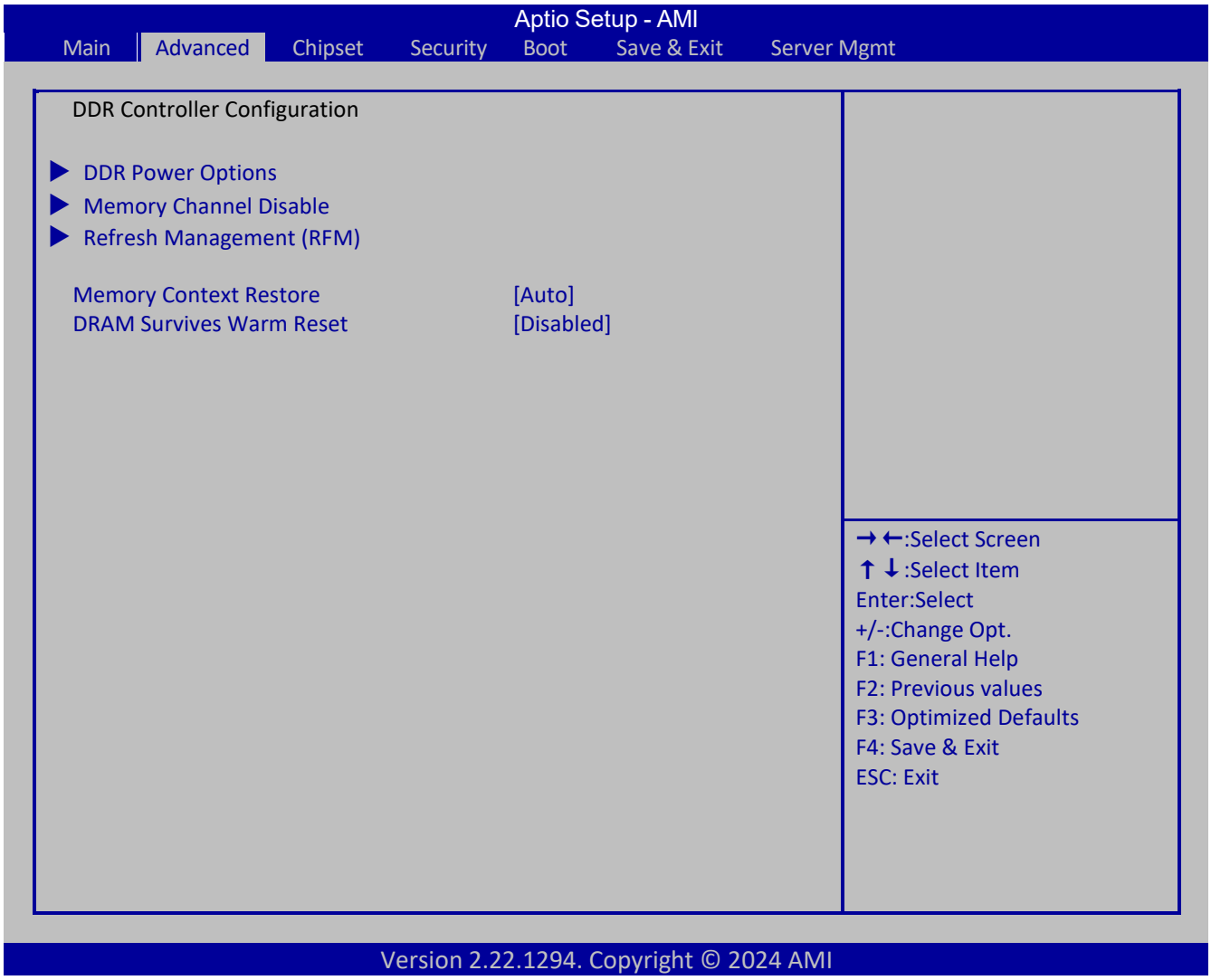
Advanced \ AMD CBS \ UMC Common Options		
Menu Fields	**Settings**	**Comments**
DDR Address Options	Selects sub-menu.	
DDR Controller Configuration	Selects sub-menu.	
DDR MBIST Options	Selects sub-menu.	
DDR RAS	Selects sub-menu.	
DDR Bus Configuration	Selects sub-menu.	
DDR Timing Configuration	Selects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

7.2.4.3.1 DDR Address Options



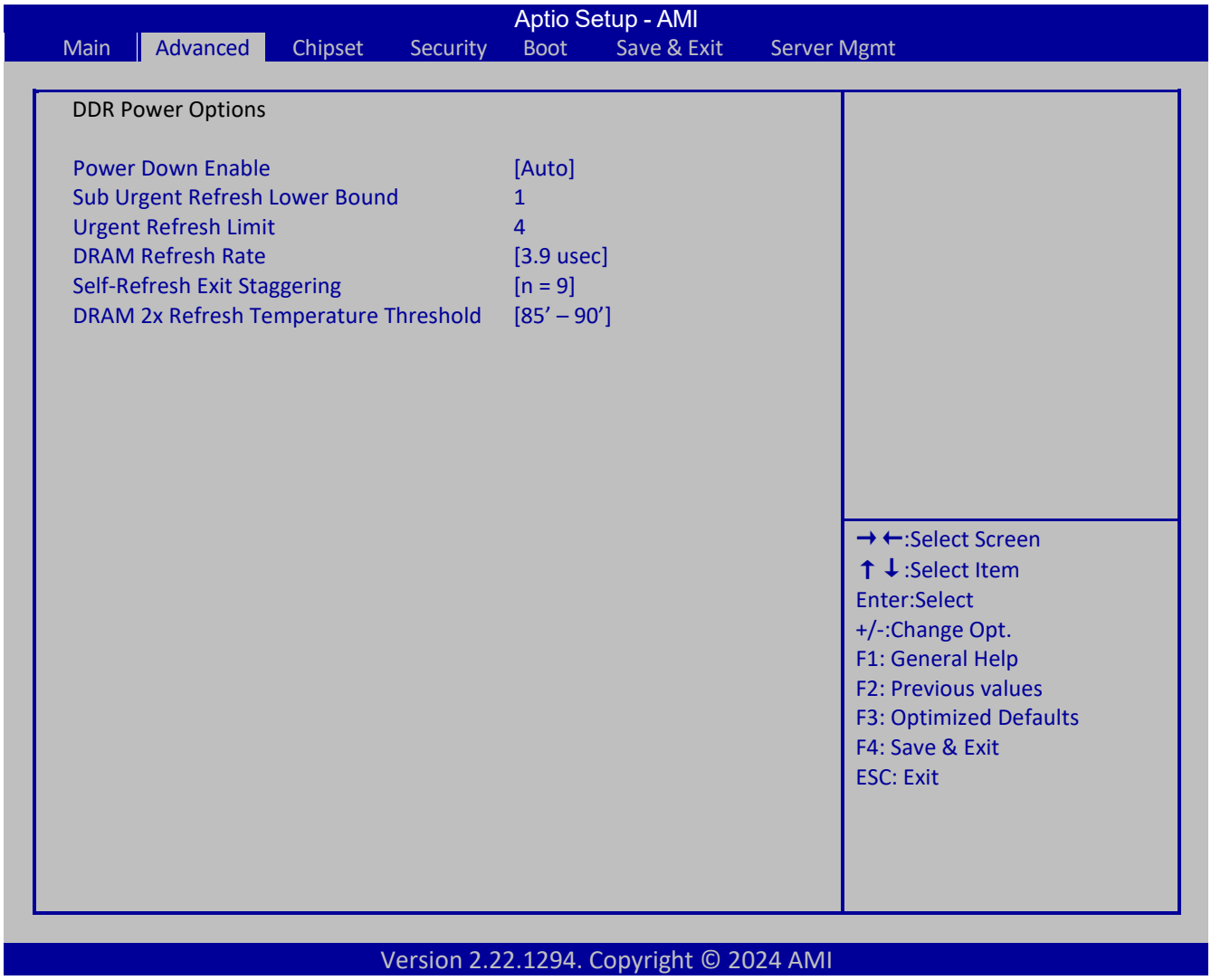
Advanced \ AMD CBS \ UMC Common Options \ DDR Addressing Options		
Menu Fields	**Settings**	**Comments**
Chipselect Interleaving	[Disabled] **[Auto]**	Interleave memory blocks across the DRAM chip selects for node 0.
Address Hash Bank	[Disabled] [Enabled] **[Auto]**	Enable or disable bank address hashing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

7.2.4.3.2 DDR Controller Configuration



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

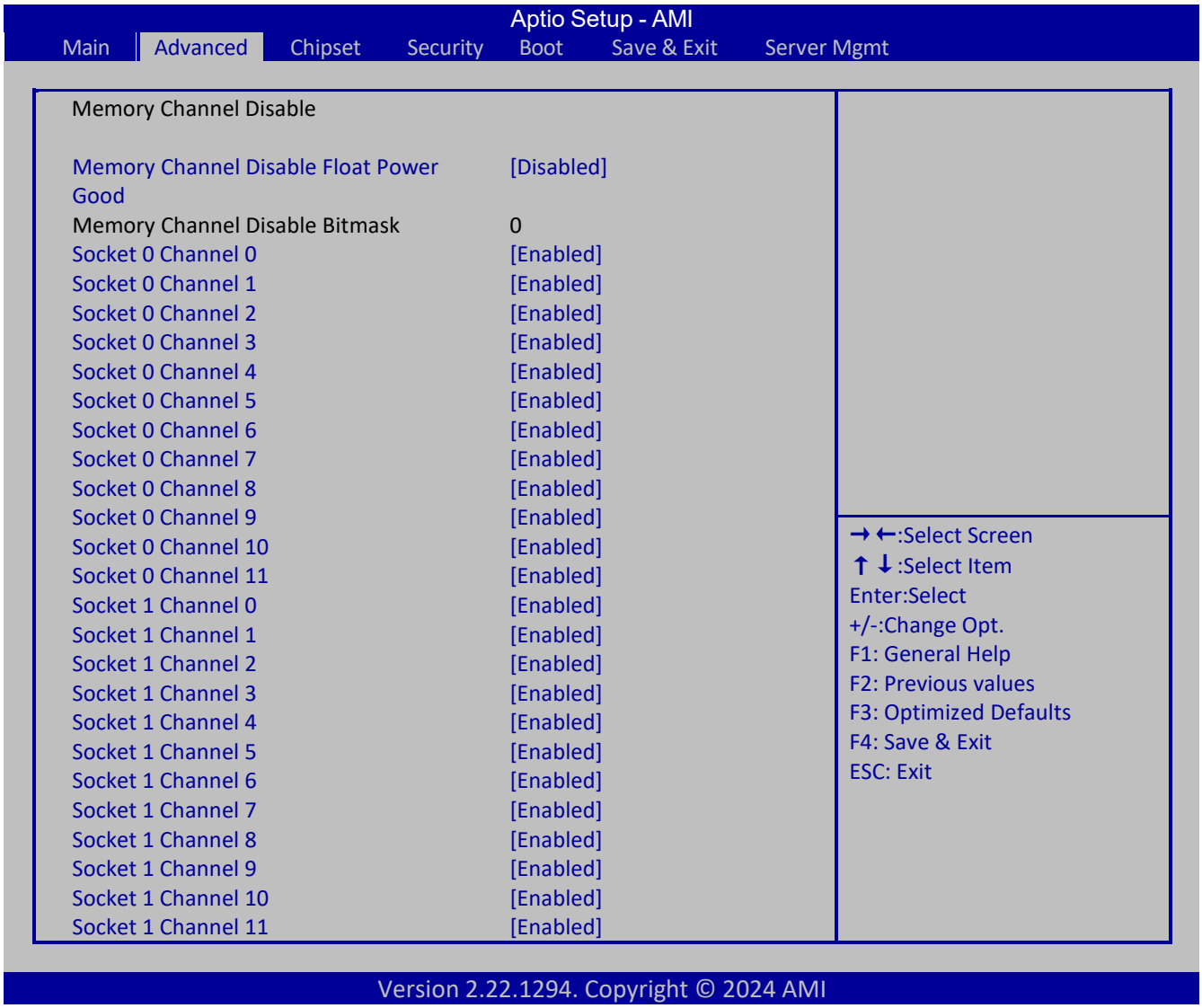
7.2.4.3.2.1 DDR Power Options



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

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

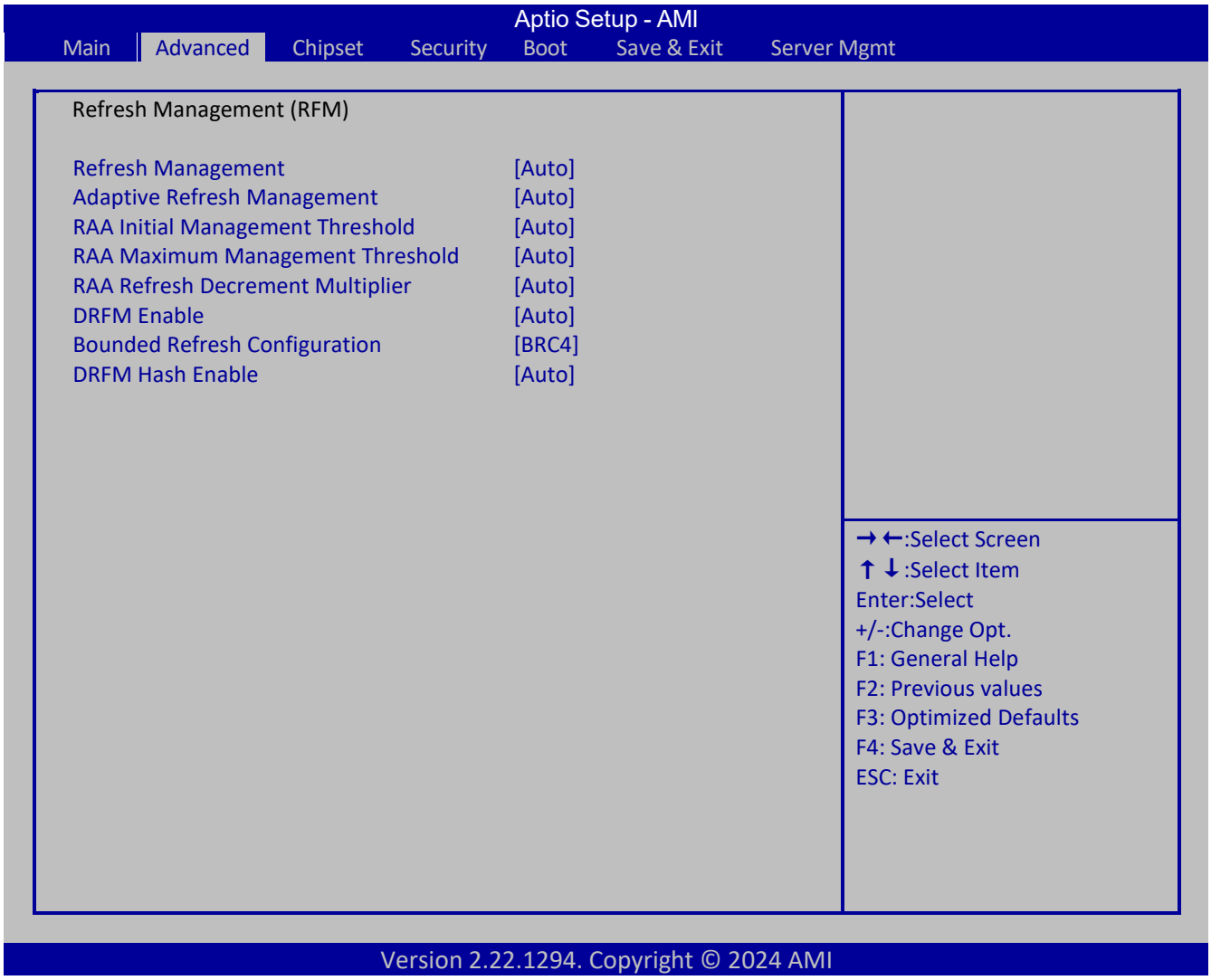
7.2.4.3.2.2 Memory Channel Disable



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

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

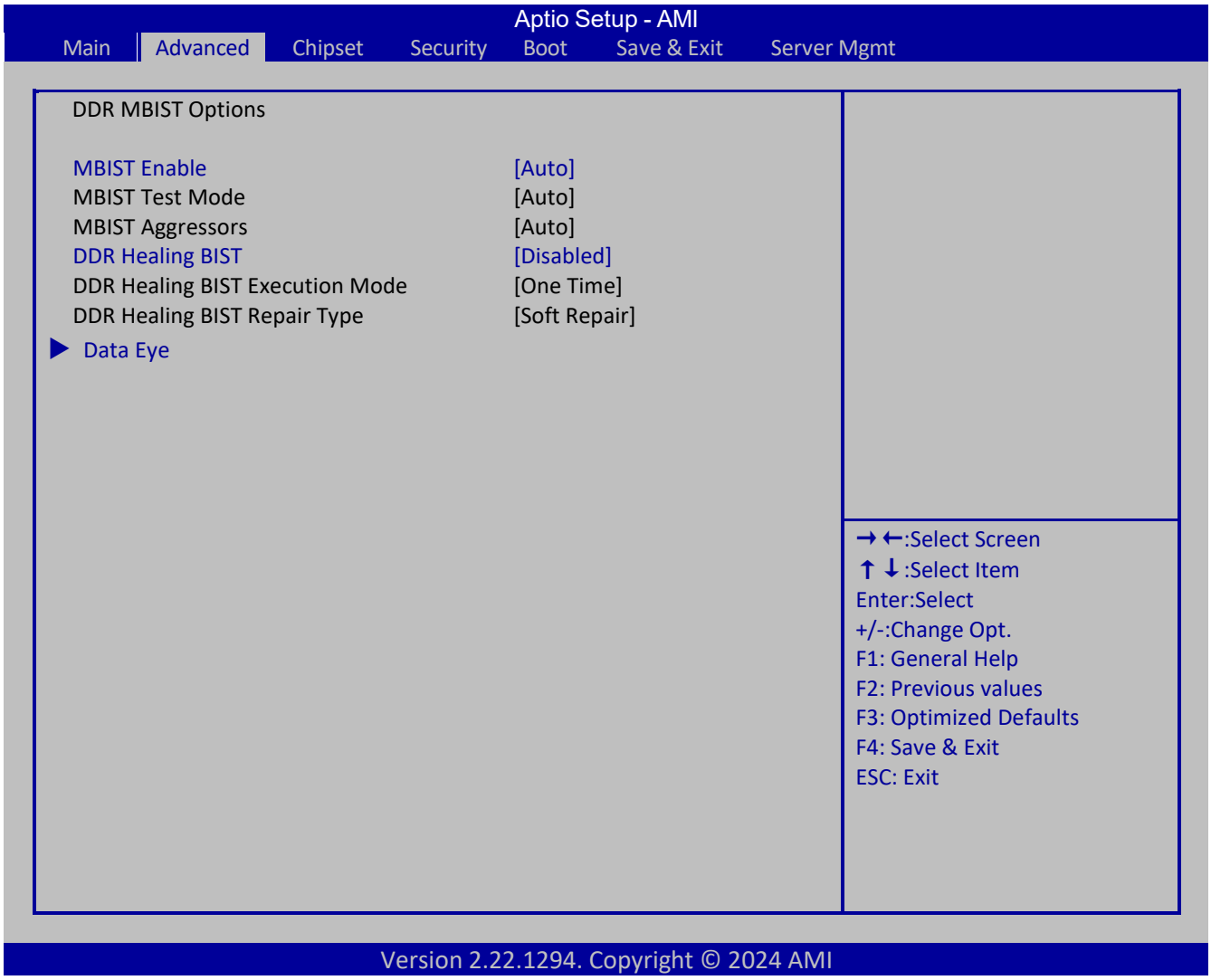
7.2.4.3.2.3 Refresh Management (RFM)



Advanced \ AMD CBS \ UMC Common Options \ DDR Controller Configuration \ Refresh Management (RFM)		
Menu Fields	**Settings**	**Comments**
Refresh Management	**[Auto]** [Disable] [Enable] [Force Enable]	Auto Disable: Disable RFM for all Ranks. Enable: Enable RFM for Ranks which support RFM. Force Enable: Enable RFM for all Ranks regardless of support. Selecting 'Force Enable' will cause REFpb/REFsb to be disabled if all ranks do not support RFM<
Adaptive Refresh Management	**[Auto]** [Disable] [ARFM Level A] [ARFM Level B] [ARFM Level C]	Apply the Settings for RAAIMT, RAAMMT, and RefDecrement which are associated with the selected level.
RAA Initial Management Threshold	**[Auto]** [32] [40] [48] [56] [64]	Override Rolling Accumulated ACT Initial Management Threshold Auto: BIOS will choose the lowest supported value from SPD. Choices from list are for Normal Refresh Mode. In Fine Granularity Mode, the value will be divided by 2

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

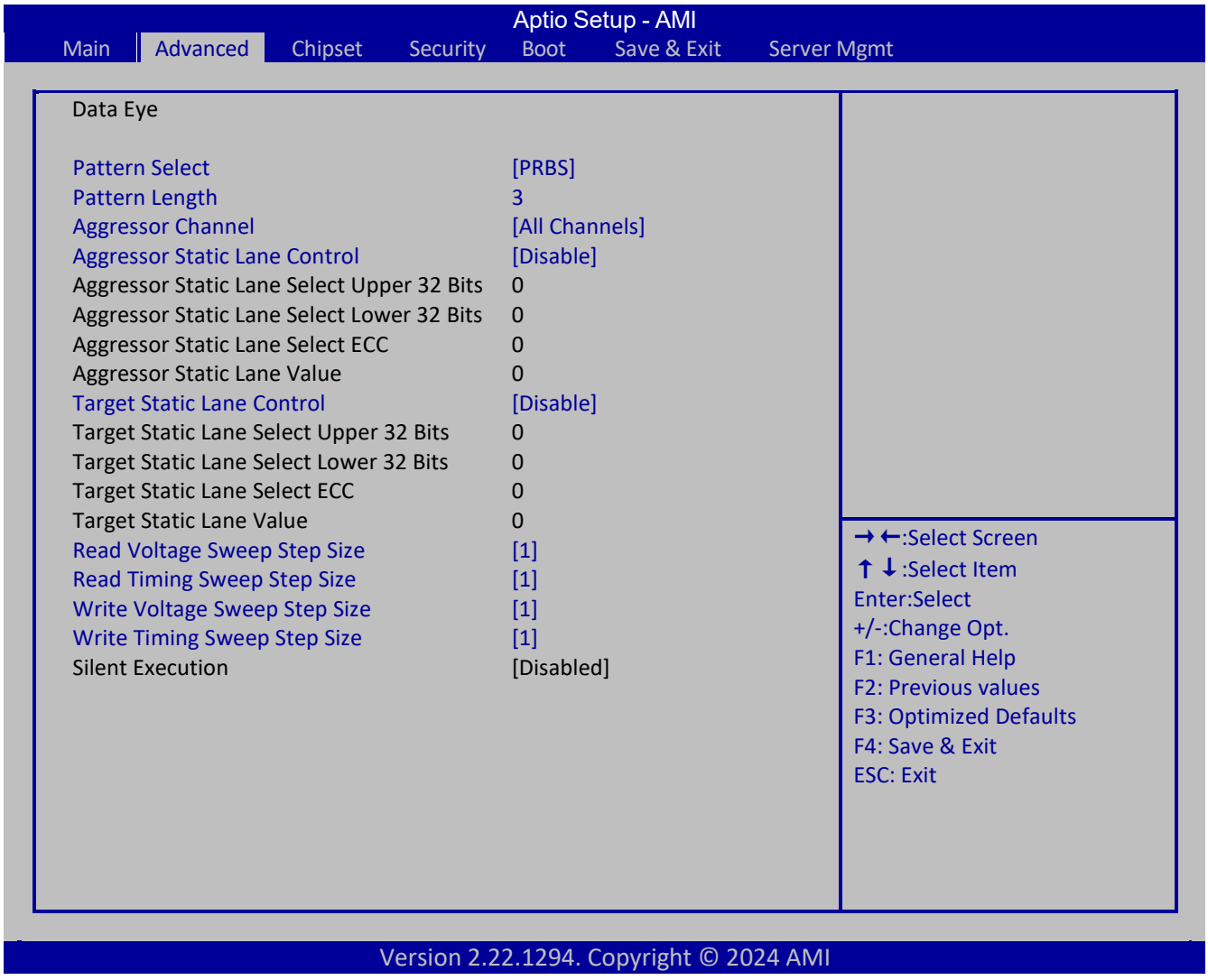
7.2.4.3.3 DDR MBIST Options



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

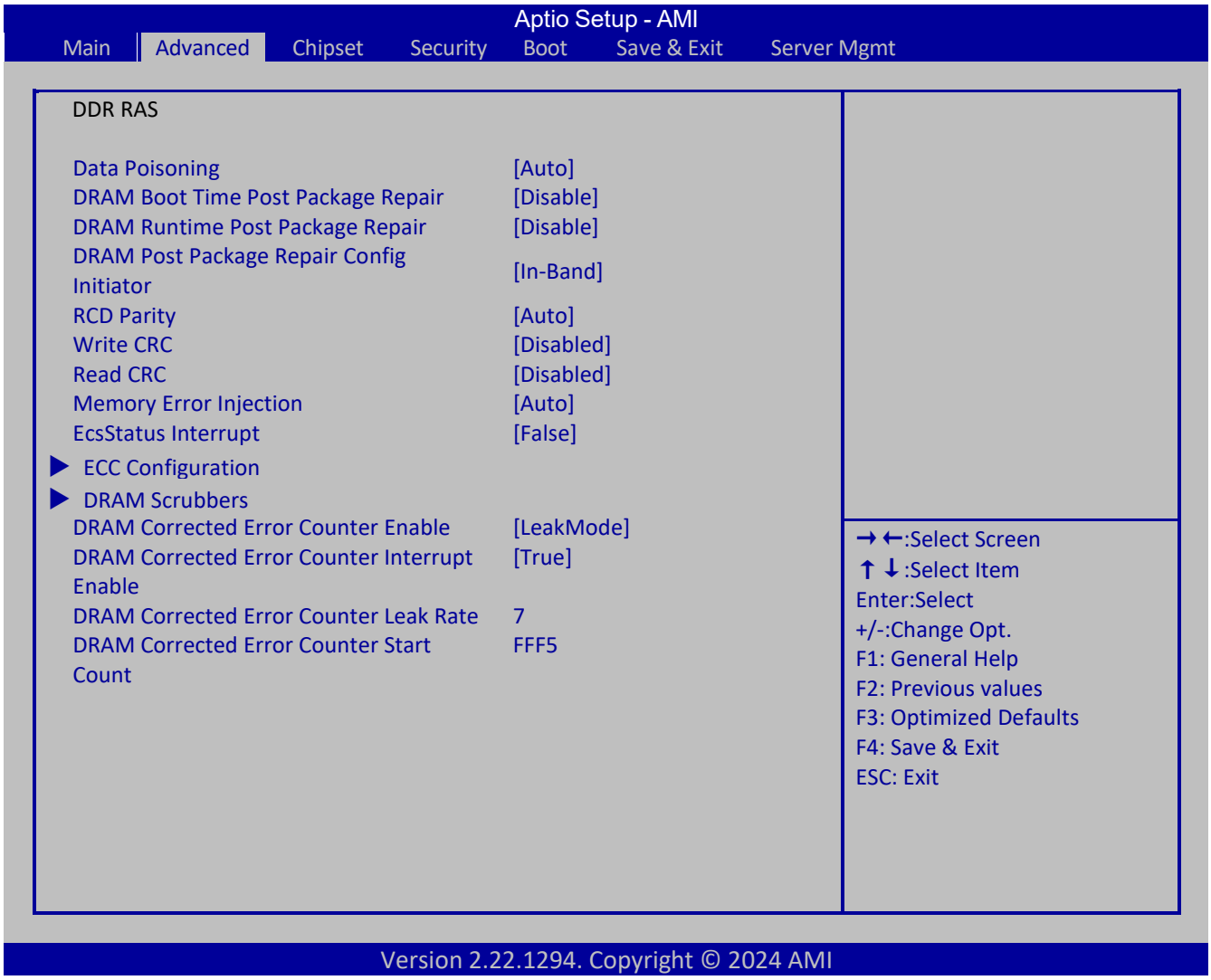
Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options		
Menu Fields	**Settings**	**Comments**
		Self-Healing Mem BIST: this runs the JEDEC DRAM self healing, if the device and DIMM support the feature. The DRAM will do a hard repair for failing memory. PMU and Self-Healing Mem BIST: this option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

7.2.4.3.3.1 Data Eye



Advanced \ AMD CBS \ UMC Common Options \ DDR MBIST Options \ Data Eye		
Menu Fields	**Settings**	**Comments**
Pattern Select	**[PRBS]** [SSO] [Both]	MBIST Data Eye Pattern Type. 0 - PRBS (default), 1 - SSO, 2 - Both
Pattern Length	X	This token determine the pattern length, available options: 3...C (input hex number, not decimal)
Aggressor Channel	[One Sub-Channel] [Half Channels] **[All Channels]**	One Sub-Channel enables the non-target subchannel on the target channel to be an aggressor. Half Channels enables all non-target channels on one half of the processor to be aggressors. All Channels enables all non-target channels to be aggressors.
Aggressor Static Lane Control	**[Disabled]** [Enabled]	This option, if enabled, will control the Aggressor Static Lane Controls.
Aggressor Static Lane Select Upper 32 Bits	X	Static Lane Select for Upper 32 bits. The bit mask represents the bits to be read
Aggressor Static Lane Select Lower 32 Bits	X	Static Lane Select for Lower 32 bits. The bit mask represents the bits to be read
Aggressor Static Lane Select ECC	X	Static Lane Select for ECC Lanes. The bit mask represents the bits to be read
Aggressor Static Lane Value	X	TBD
Target Static Lane Control	**[Disabled]** [Enabled]	Enable Mbist Target Static Lane Control
Target Static Lane Select Upper 32 Bits	X	Static Lane Select for Upper 32 bit. The bit mask represents the bits to be read
Target Static Lane Select Lower 32 Bits	X	Static Lane Select for Lower 32 bit. The bit mask represents the bits to be read
Target Static Lane Select ECC	X	TBD
Target Static Lane Value	X	Value for Mbsit target static lane. Enable 'Target Static Lane Control' option to enter the value
Read Voltage Sweep Step Size	**[1]** [2] [4]	This option determines the step size for Read Data Eye voltage sweep, Supported options are 1,2 and 4
Read Timing Sweep Step Size	**[1]** [2] [4]	This option supports step size for Read Data Eye. Supported options are 1, 2 and 4
Write Voltage Sweep Step Size	**[1]** [2] [4]	This option determines the step size for write Data Eye voltage sweep, Supported options are 1,2 and 4
Write Timing Sweep Step Size	**[1]** [2] [4]	This option supports step size for write Data Eye. Supported options are 1, 2 and 4
Silent Execution	**[Disabled]** [Enabled]	Execute MBIST Data Eye silently without ABL log output Disabled - MBIST Enable will not be overridden Enabled - Execute MBIST Data Eye silently without ABL log output

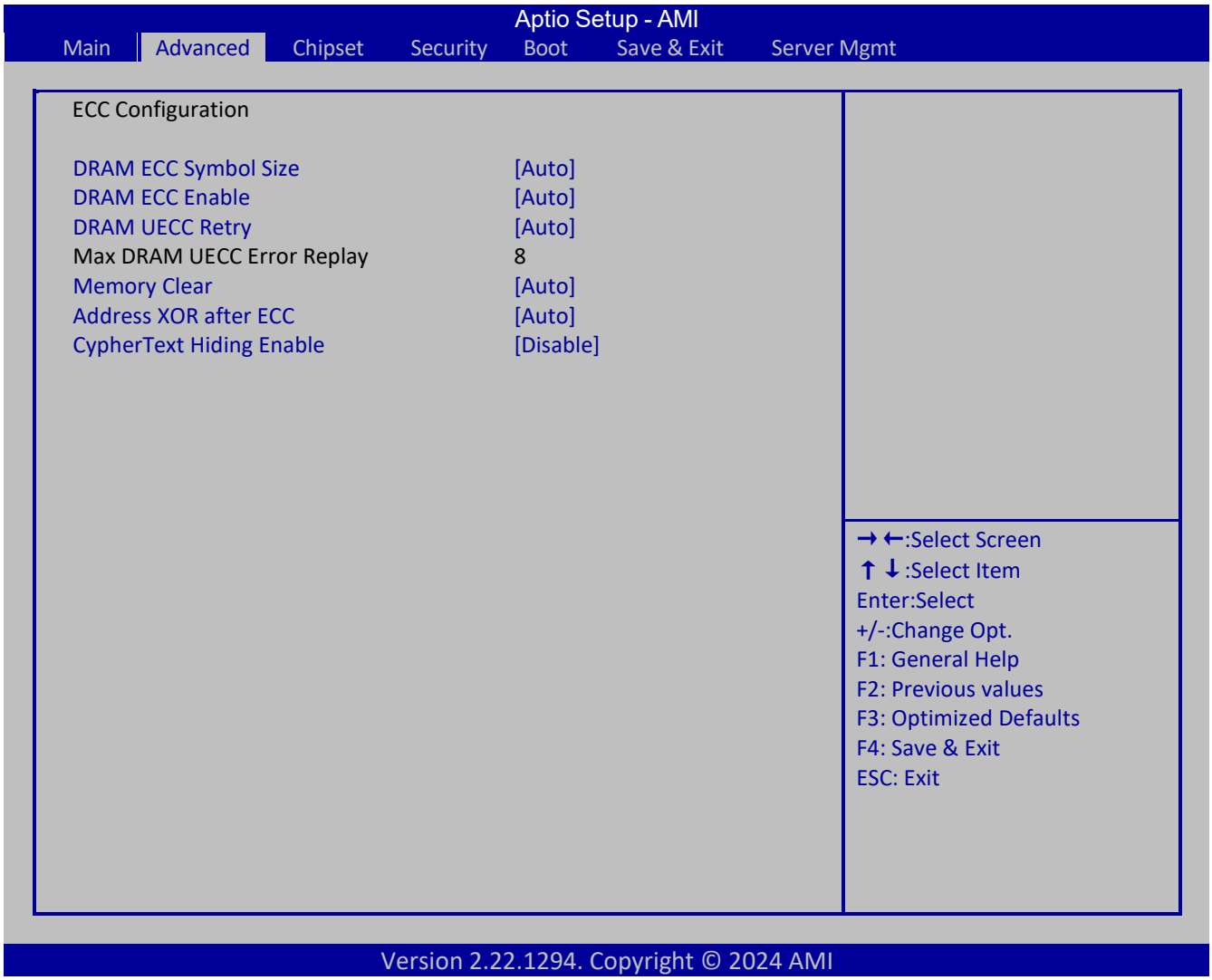
7.2.4.3.4 DDR RAS



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

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

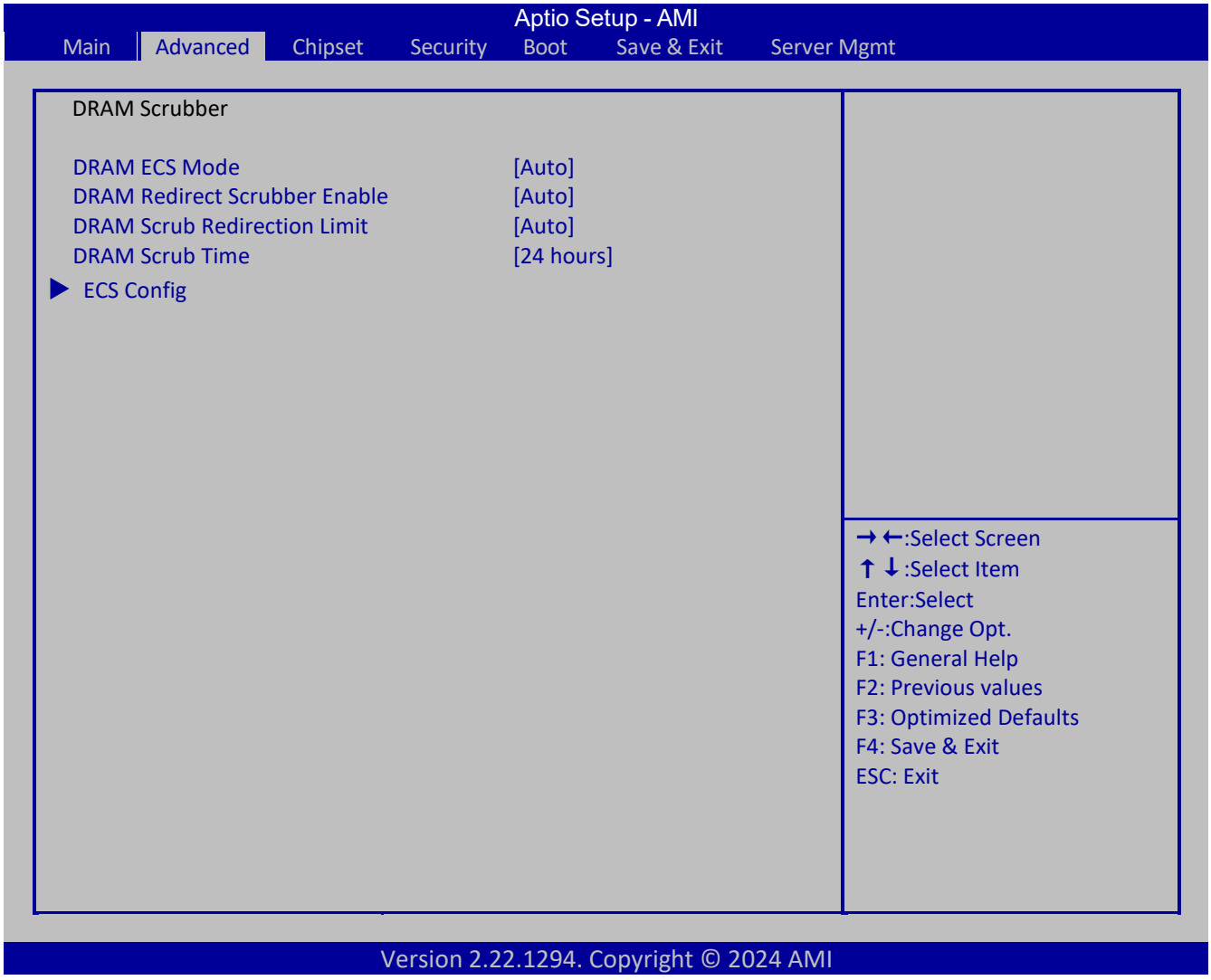
7.2.4.3.4.1 ECC Configuration



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

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

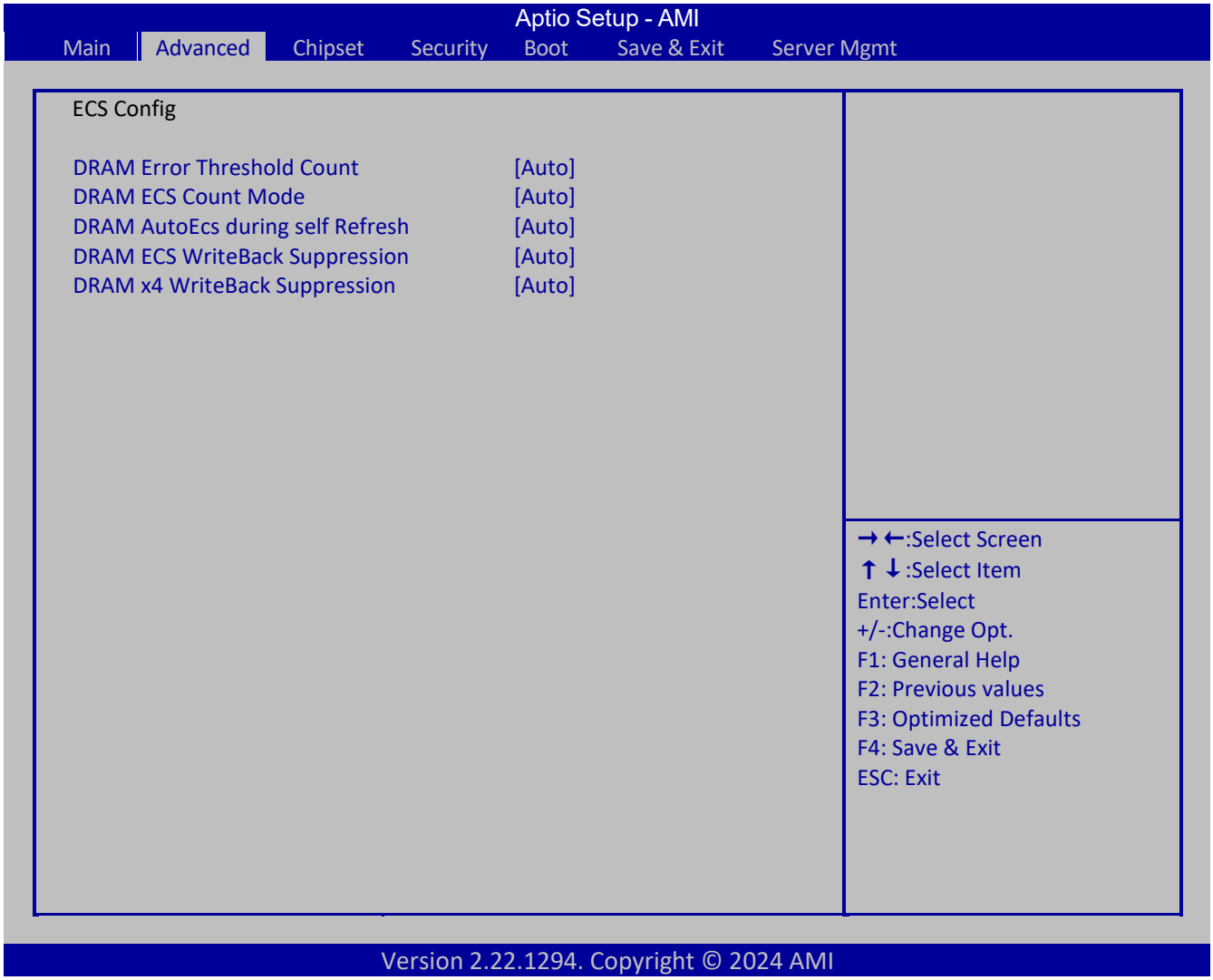
7.2.4.3.4.2 DRAM Scrubbers



Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers		
Menu Fields	**Settings**	**Comments**
DRAM ECS Mode	[AutoECS] [ManualECS] **[Auto]** [DisableECS]	0 = AutoECS Mode, 1 = ManualECS mode Disable ECS mode disables only the controller and does not disable it on the DRAM

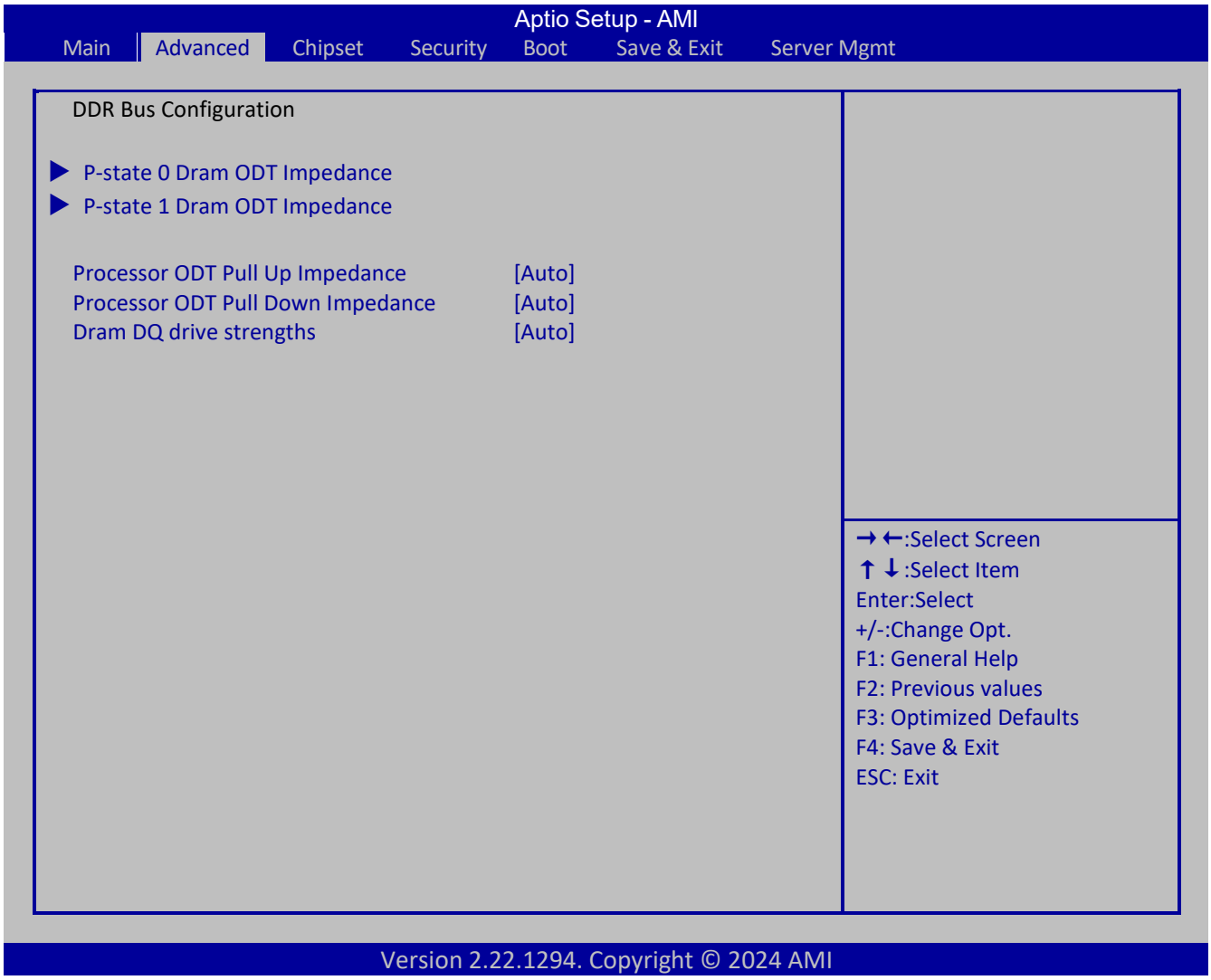
Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers		
Menu Fields	**Settings**	**Comments**
DRAM Redirect Scrubber Enable	[Disabled] [Enabled] **[Auto]**	Enable/Disable Dram Redirect Scrubber and poison scrubber
DRAM Scrub Redirection Limit	[8 Scrubs] [4 Scrubs] [2 Scrubs] [1 Scrub] **[Auto]**	Dram ECC Scrub Redirection Limit: 0=8 scrubs, 1=4 scrubs, 2=2 scrubs, 3=1 scrub
DRAM Scrub Time	[Disabled] [1 hour] [4 hours] [6 hours] [8 hours] [12 hours] [16 hours] **[24 hours]** [48 hours]	Provide a value that is the number of hours to scrub memory.
ECS Config	Selects Sub-Menu	

7.2.4.3.4.2.1 ECS Config



Advanced \ AMD CBS \ UMC Common Options \ DDR RAS \ DRAM Scrubbers \ ECS Config		
Menu Fields	**Settings**	**Comments**
DRAM Error Threshold Count	[ETC_4] [ETC_16] [ETC_64] [ETC_256] [ETC_1024] [ETC_4096] **[Auto]**	List of Values: 0 = ETC_4, 1 = ETC_16, 2 = ETC_64, 3 = ETC_256 (default - Auto), 4 = ETC_1024, 5 = ETC_4096
DRAM ECS Count Mode	[Row Count Mode] [Code Word Count Mode] **[Auto]**	0: RowCount Mode 1: CodeWord Mode 0xFF: Auto - ABL decides default as CodeWord Mode
DRAM AutoEcs during self Refresh	[AutoEcs Disabled] [AutoEcs Enabled] **[Auto]**	0: AutoEcs Disabled 1: AutoEcs Enabled 0xFF: Auto - ABL choose AutoEcs Disabled
DRAM ECS WriteBack Suppression	[Disable] [Enable] **[Auto]**	To enable/Disable ECS Error Correction Writeback suppression 0: ECS Writeback Suppression Disabled 1: ECS Writeback Suppression Enabled 0xFF: Auto - ABL chooses Writeback Suppression to be Enabled by default
DRAM x4 WriteBack Suppression	[Disable] [Enable] **[Auto]**	To enable/Disable X4 device Error Correction Writeback suppression 0: X4 Writeback Suppression Disabled 1: X4 Writeback Suppression Enabled 0xFF: Auto

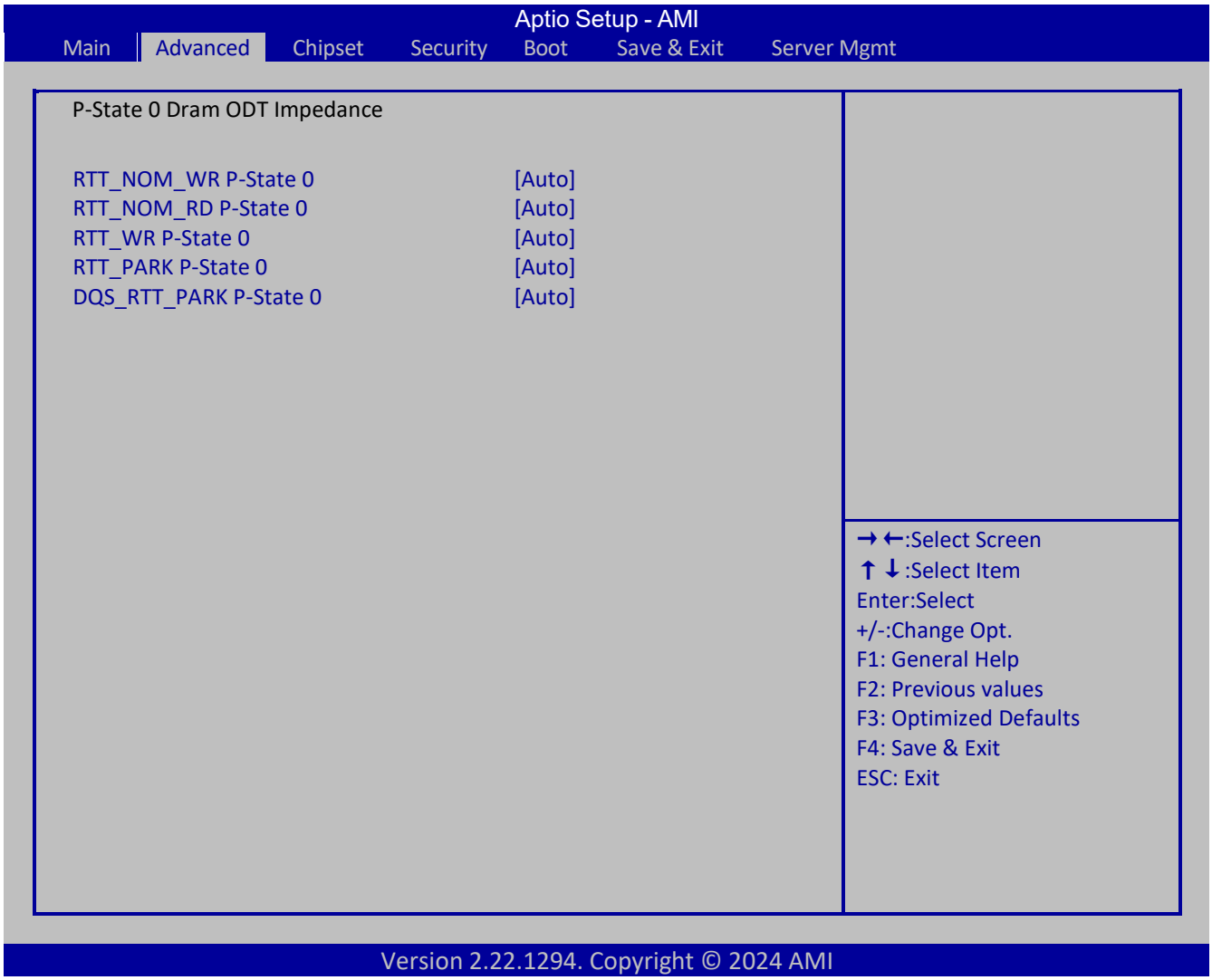
7.2.4.3.5 DDR Bus Configuration



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

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

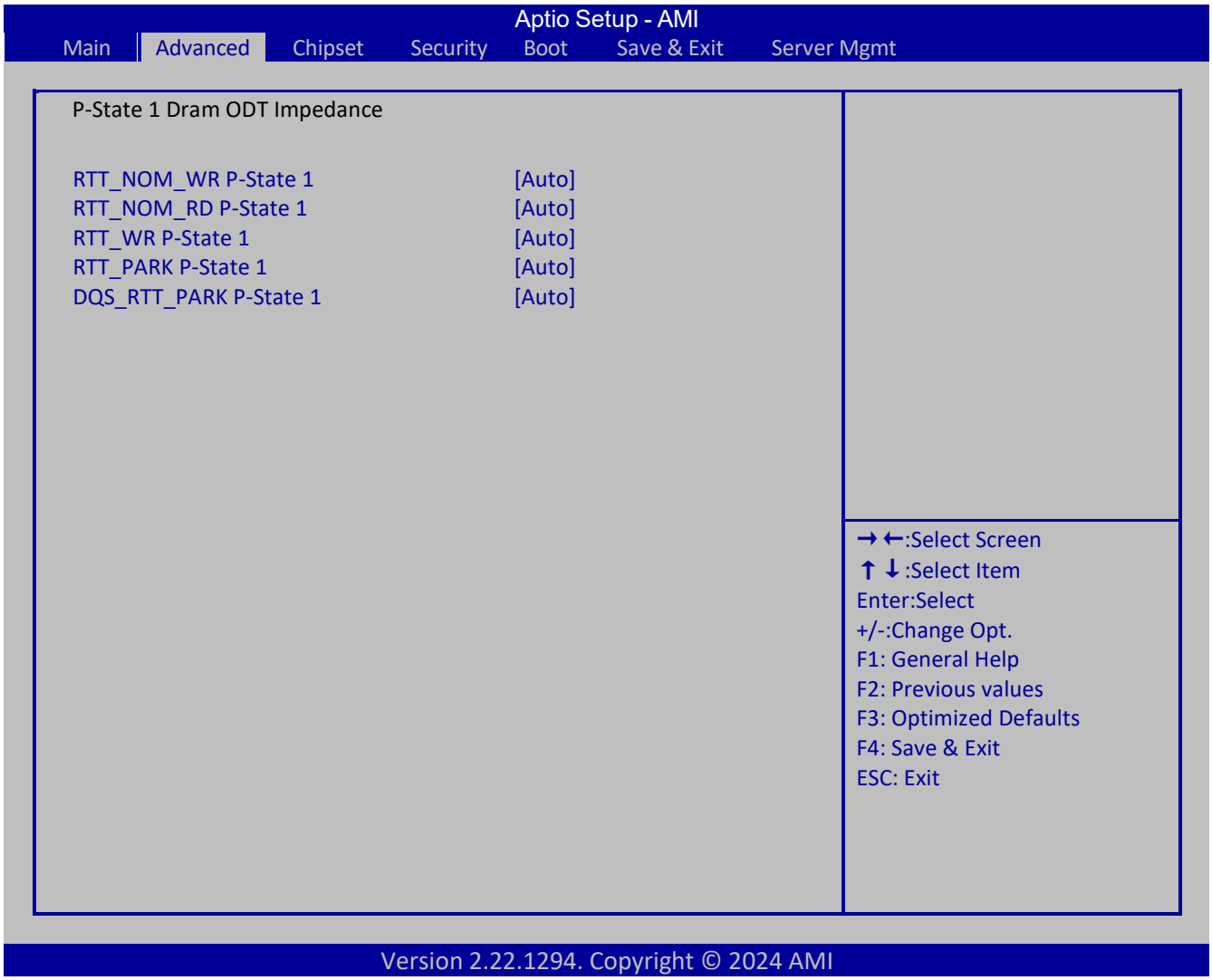
7.2.4.3.5.1 P-state 0 Dram ODT Impedance



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

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

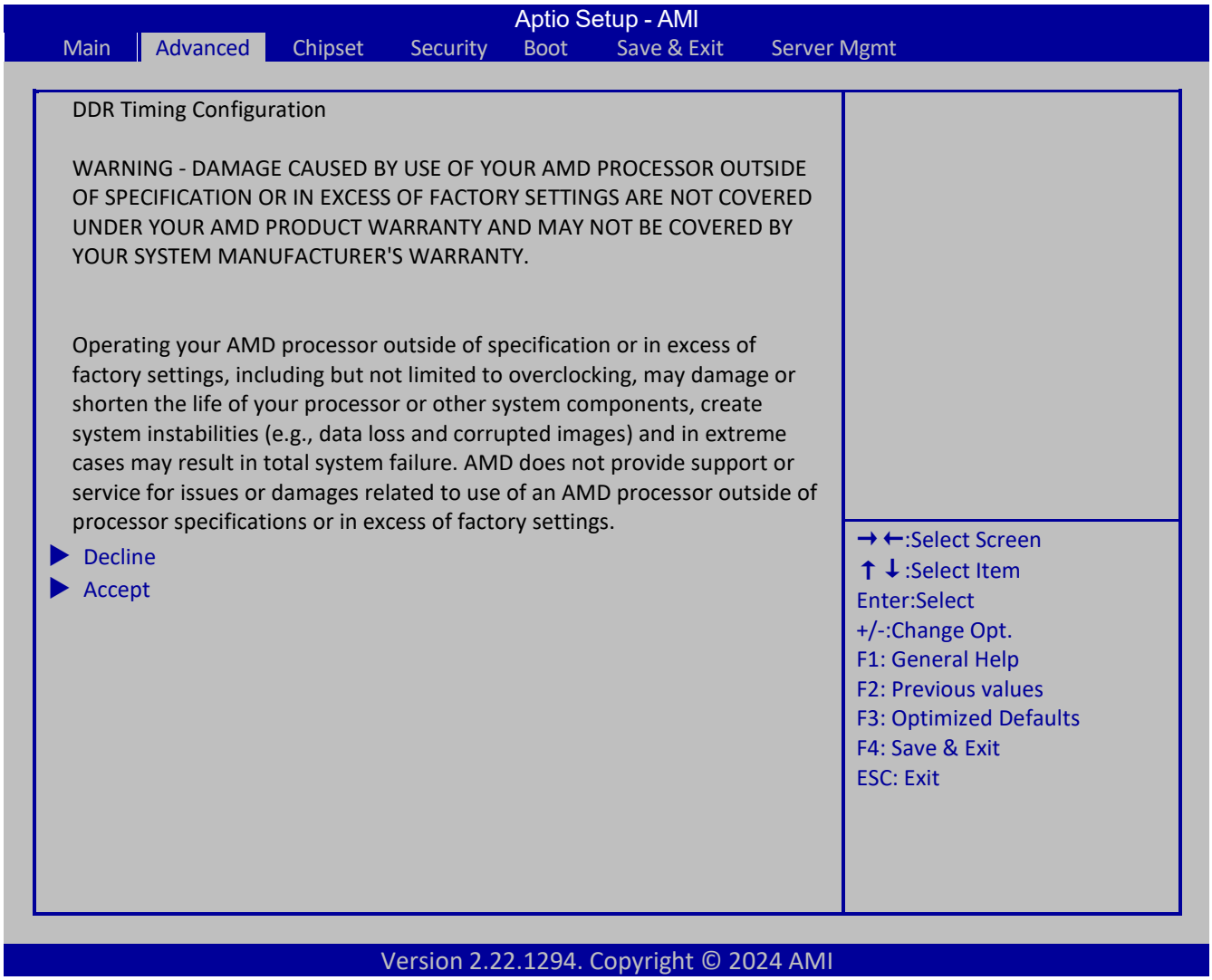
7.2.4.3.5.2 P-state 1 Dram ODT Impedance



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

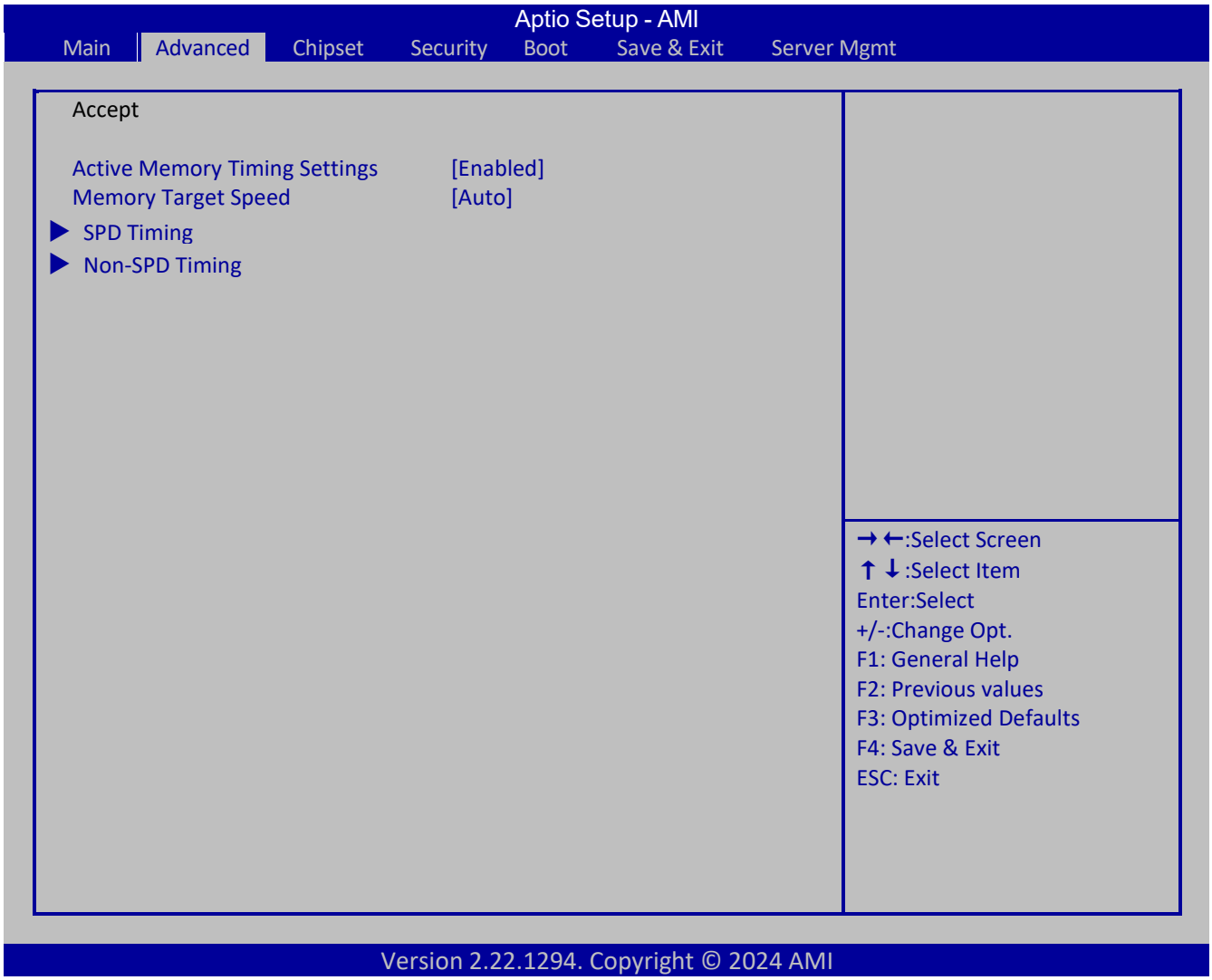
Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration \ P-state 1 Dram ODT Impedance		
Menu Fields	**Settings**	**Comments**
RTT_WR P-State 1	**[Auto]** [RTT_OFF] [RZQ (240)] [RZQ/2 (120)] [RZQ/3 (80)] [RZQ/4 (60)] [RZQ/5 (48)] [RZQ/6 (40)] [RZQ/7 (34)]	Select the DRAMs On-die Termination impedance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

7.2.4.3.6 DDR Timing Configuration



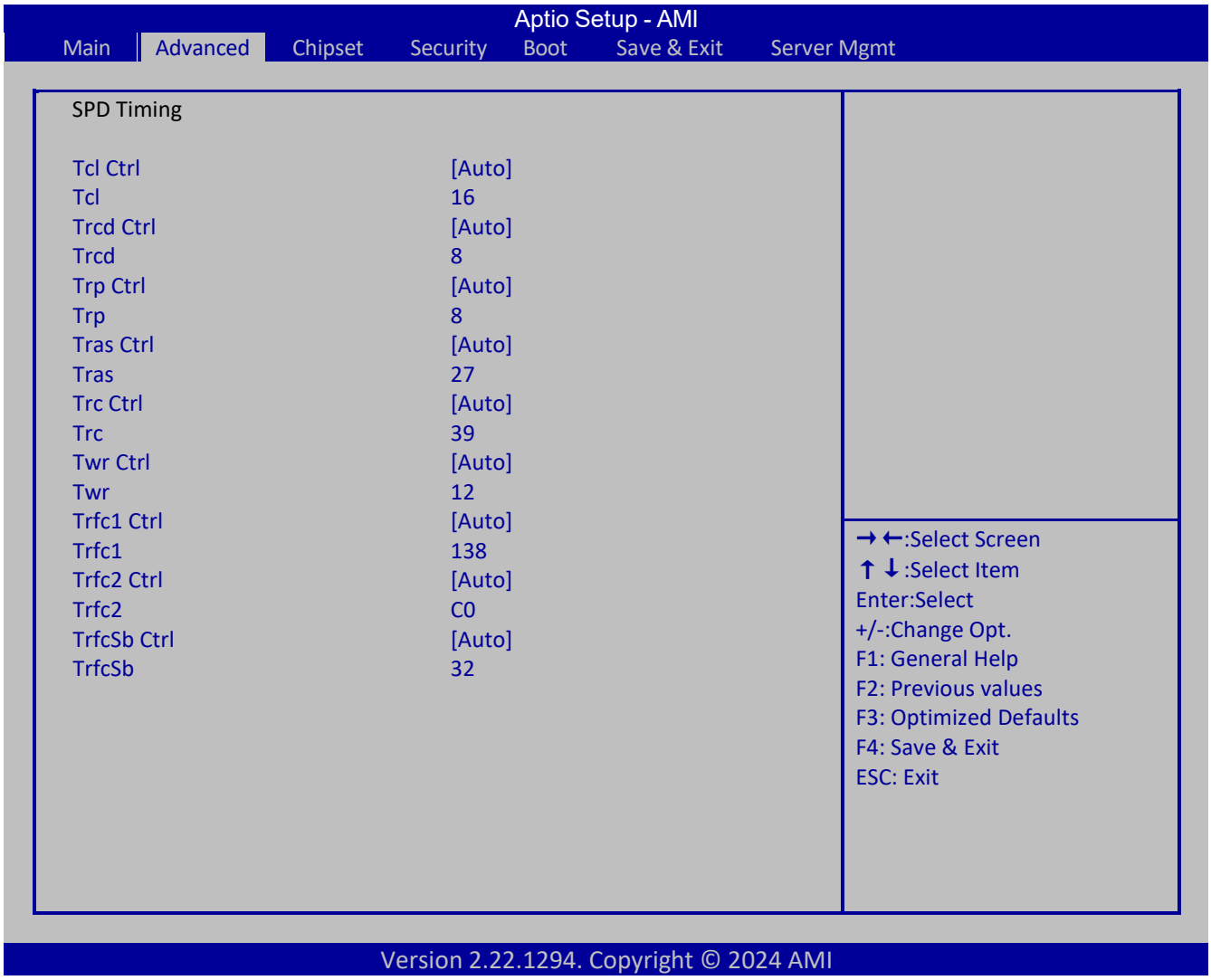
Advanced \ AMD CBS \ UMC Common Options \ DDR Bus Configuration		
Menu Fields	**Settings**	**Comments**
Decline	Selects Previous menu	
Accept	Selects sub-menu	

7.2.4.3.6.1 DDR Timing Configuration-Accept



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

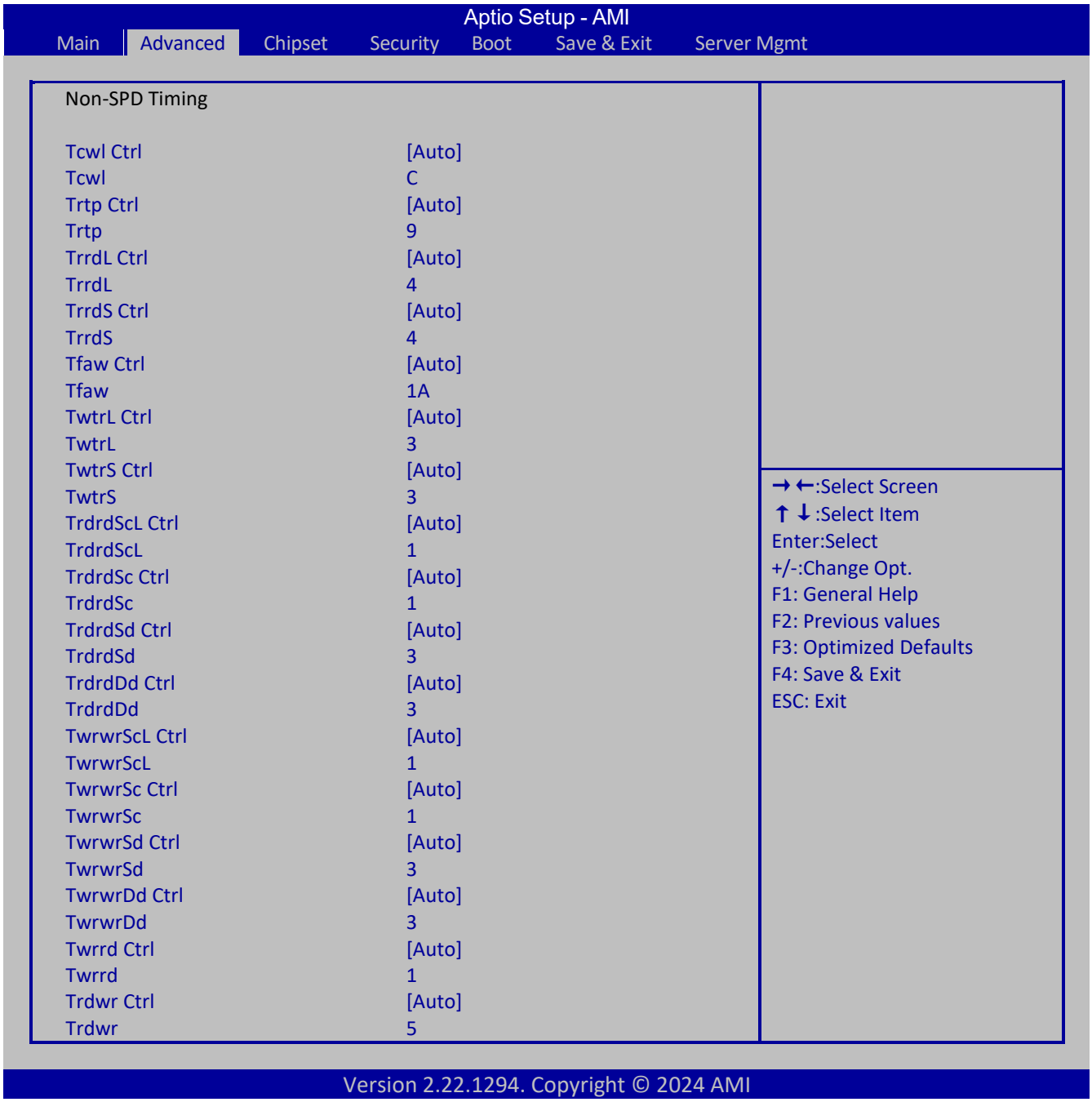
7.2.4.3.6.1.1 SPD Timing



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

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

7.2.4.3.6.1.2 Non-SPD Timing

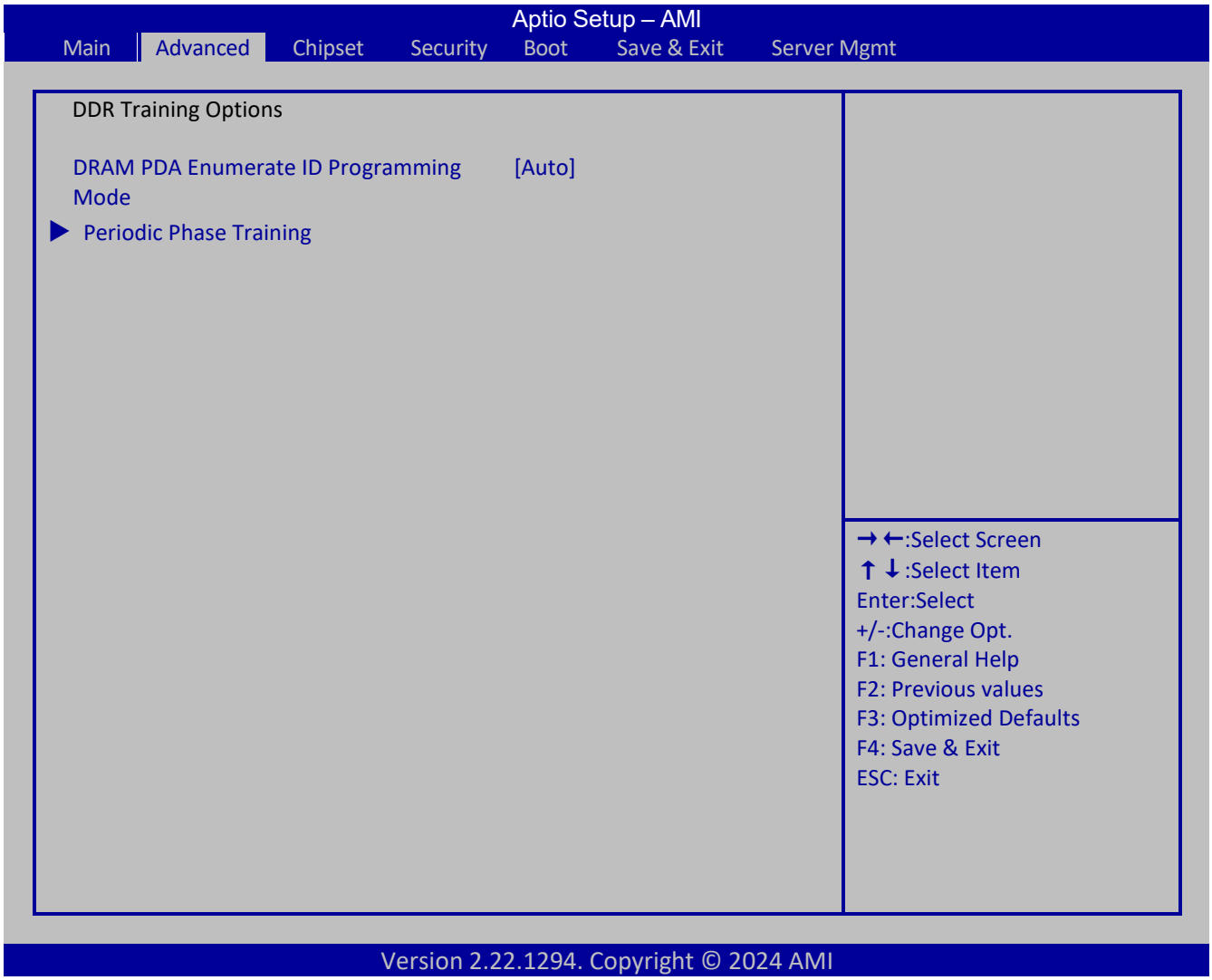


Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ Non-SPD Timing		
Menu Fields	**Settings**	**Comments**
Tcwl Ctrl	**[Auto]** [Manual]	Auto: Follow default setting, Manual: Manually specify
Tcwl	X	Specifies the CAS Write Latency. Valid Values: 0x9 ~ 0x16
Trtp Ctrl	**[Auto]**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

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

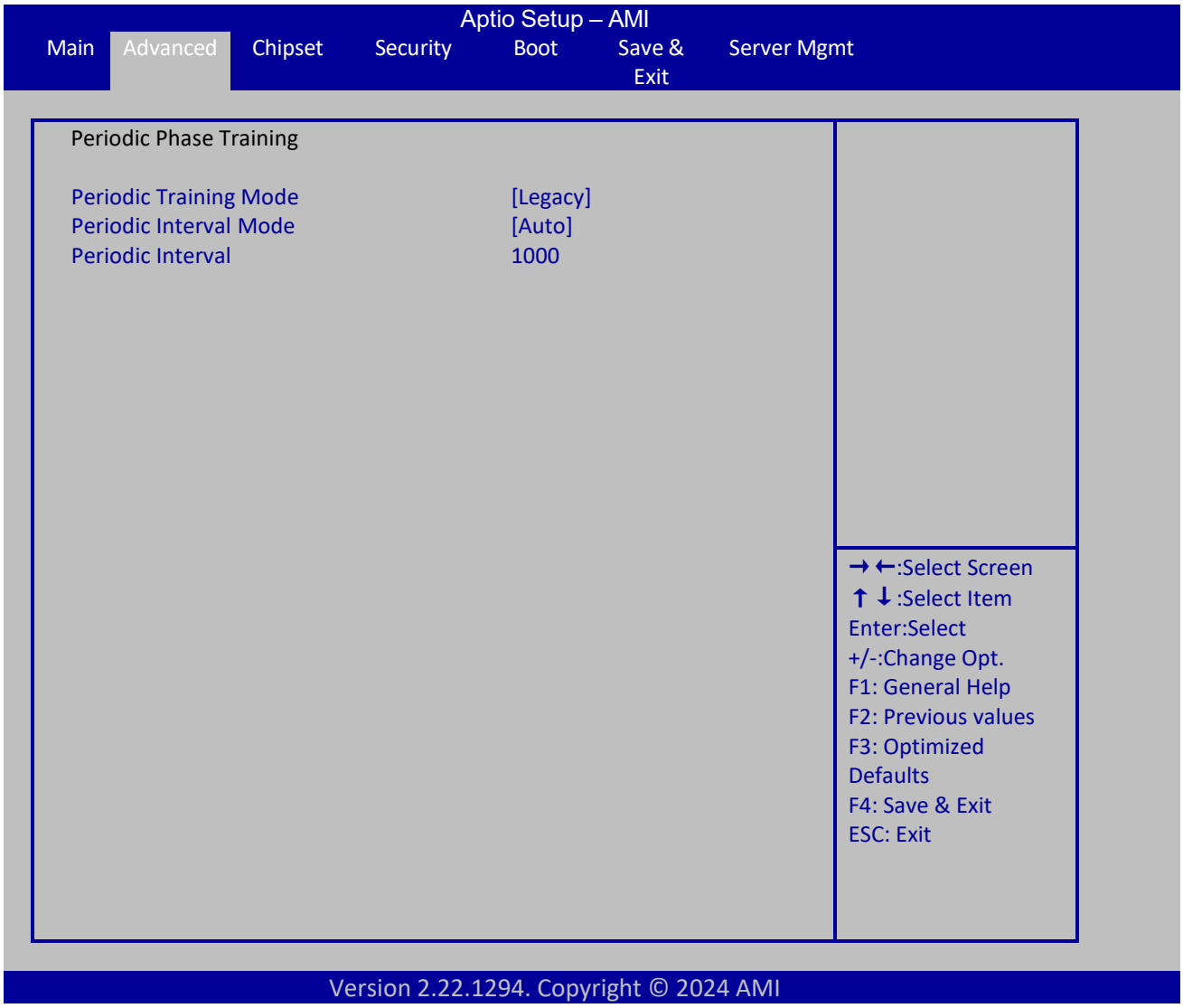
Advanced \ AMD CBS \ UMC Common Options \ DDR Timing Configuration \ Accept \ Non-SPD Timing		
Menu Fields	**Settings**	**Comments**
TwrwrDd Ctrl	**[Auto]** [Manual]	Auto: Follow default setting, Manual: Manually specify
TwrwrDd	X	Specifies the Write to Write turnaround timing in a different DIMM. Valid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

7.2.4.3.7 DDR Training Options



Advanced \ AMD CBS \ UMC Common Options \ DDR Training Options		
Menu Fields	**Settings**	**Comments**
DRAM PDA Enumerate ID Programming Mode	**[Auto]** [Toggling PDA enumeration mode] [Legacy PDA enumeration mode]	Specify PDA enumeration mode Auto : default 0 : Continuous DQS toggling PDA enumeration mode (default) 1 : Legacy PDA enumeration mode
Periodic Phase Training	Selects Sub-menu	

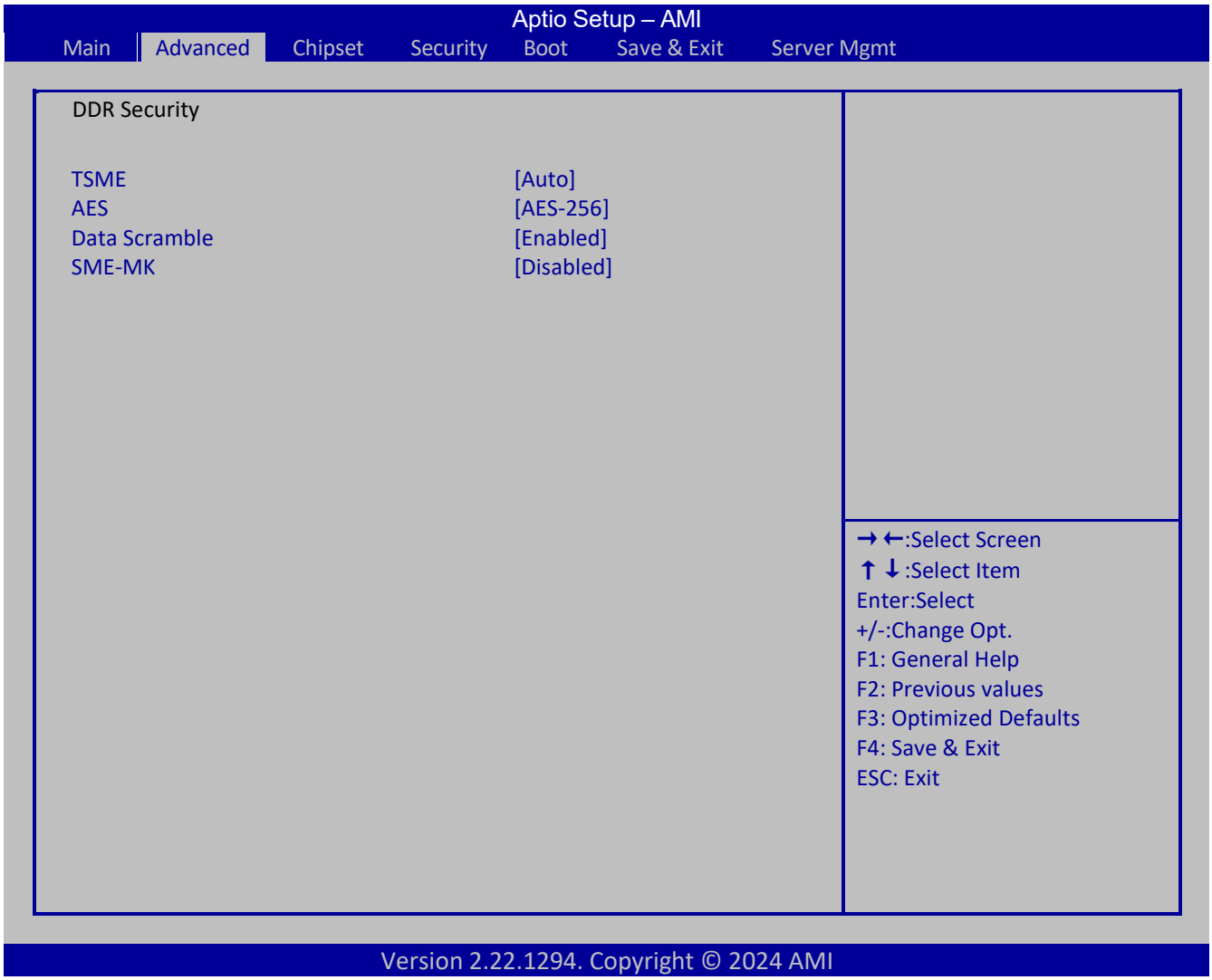
7.2.4.3.7.1 Periodic Phase Training



Advanced \ AMD CBS \ UMC Common Options \ DDR Training Options \ Periodic Phase Training		
Menu Fields	**Settings**	**Comments**
Periodic Training Mode	[Disabled] **[Legacy]**	Specify the PPT Control
Periodic Interval Mode	**[Auto]** [Manual]	0: Auto. The Periodic Interval value is decided by BIOS automatically. 1: Manual. It is specified by the CBS option Periodic Interval.

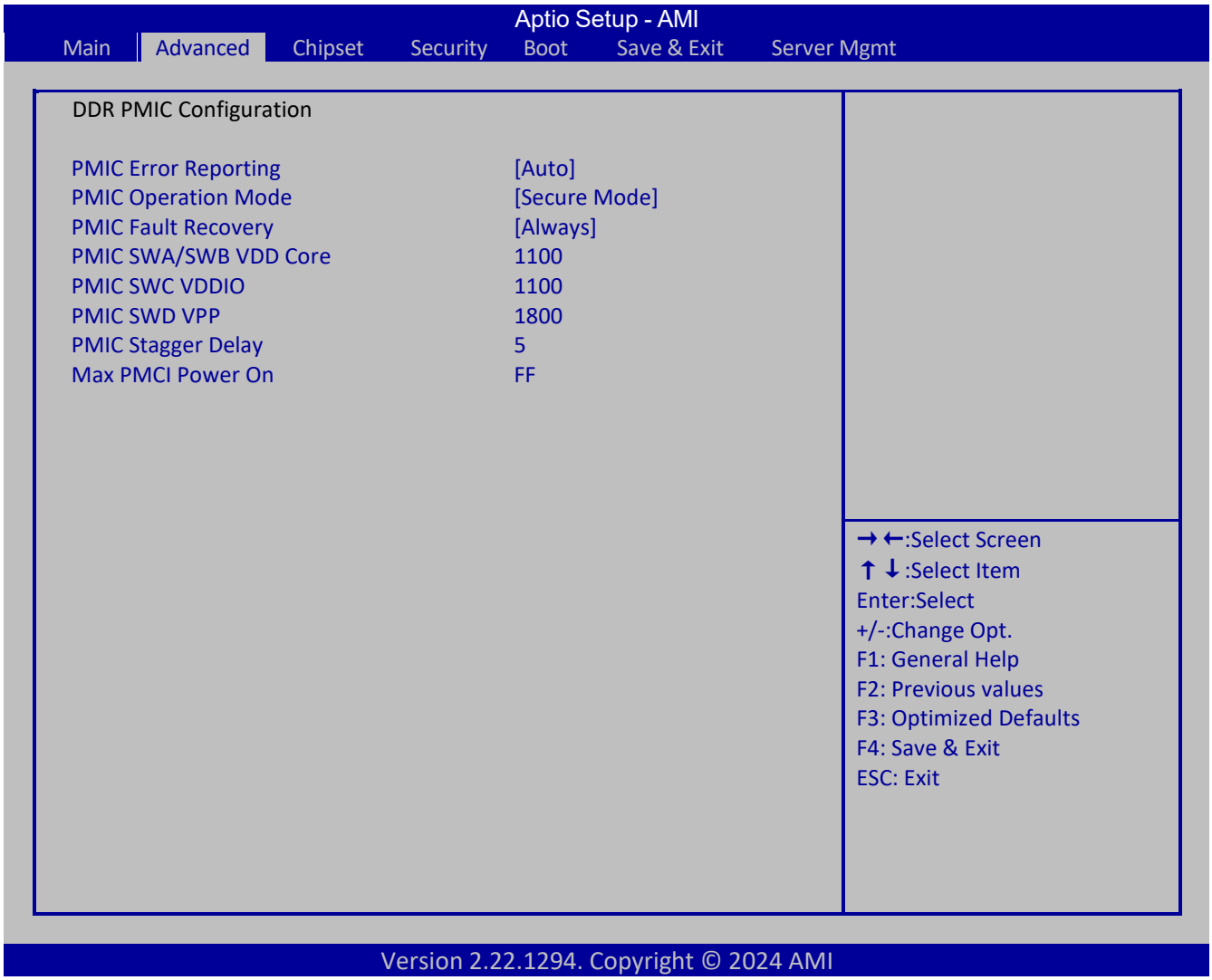
Advanced \ AMD CBS \ UMC Common Options \ DDR Training Options \ Periodic Phase Training		
Menu Fields	**Settings**	**Comments**
Periodic Interval	X	Periodic Interval value in milli-second, in decimal. Range 100 ~ 4095 ms.

7.2.4.3.8 DDR Security



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

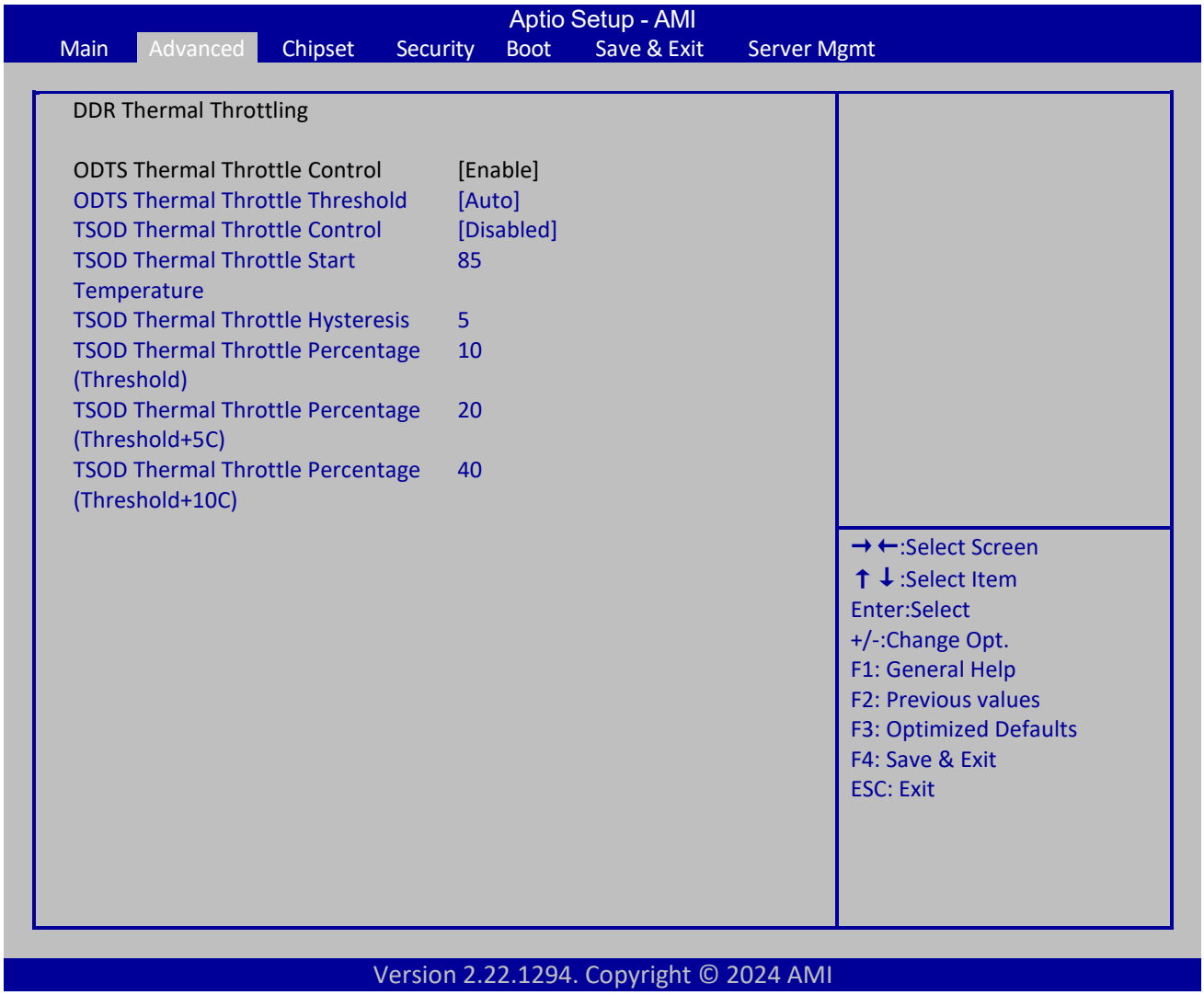
7.2.4.3.9 DDR PMIC Configuration



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

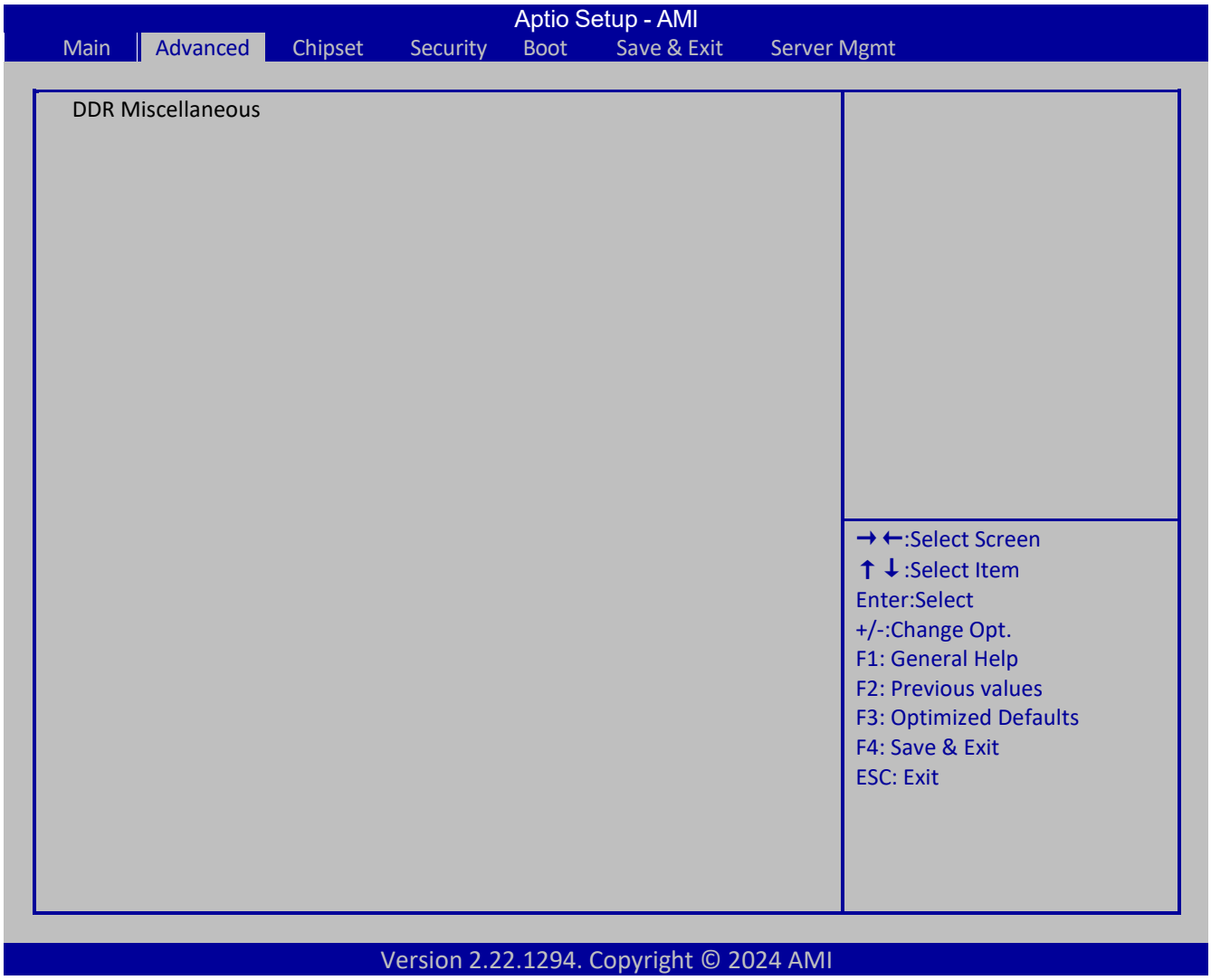
Advanced \ AMD CBS \ UMC Common Options \ DDR PMIC Configuration		
Menu Fields	**Settings**	**Comments**
		Apply to PMIC register 0x21, 0x23.
PMIC SWC VDDIO	X	Range is from 1000mV to 1200mV; default of 1100mV. Apply to PMIC register 0x25.
PMIC SWD VPP	X	Range is from 1500mV to 2135mV; default of 1800mV.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

7.2.4.3.10 DDR Thermal Throttling

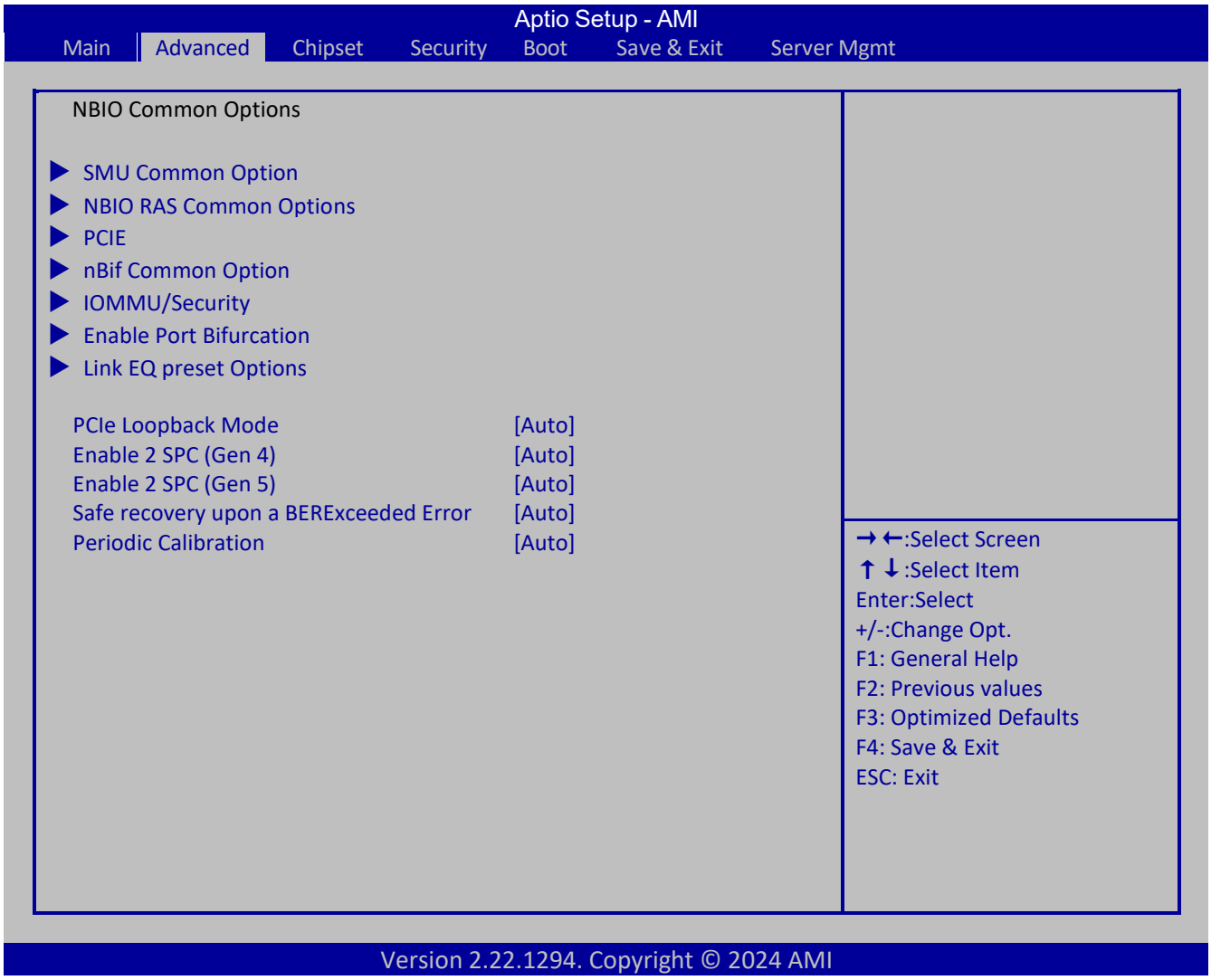


Advanced \ AMD CBS \ UMC Common Options \ DDR Miscellaneous		
Menu Fields	**Settings**	**Comments**
ODTS Thermal Throttle Control	[Auto] **[Enabled]** [Disabled]	ODTS Thermal Throttle control is a HW function that is always enabled
ODTS CMD Throttle Threshold	**[Auto]** [> 85’ C] [> 90’ C] [> 95’ C]	Dram MR4 Temperature status value to start ODTS Command Thermal Throttling.
TSOD Thermal Throttle Control	[Enabled] **[Disabled]**	TSOD = Thermal Sensor On DIMM Enables SoC (PM firmware) based thermal management of DDR5 memory, based on thermal sensor located on DIMM
TSOD Thermal Throttle Start Temperature	X	Sets an integer temperature threshold at which TSOD (Thermal Sensor on DIMM) based memory throttling begins. Applies to all installed and enabled DIMMs
TSOD Thermal Throttle Hysteresis	X	Sets an integer number of degrees the reported TSOD(Thermal Sensor On DIMM) temperature must drop below the "TSOD Thermal Throttle Start Temperature" before memory throttling is removed. Applies to all installed and enabled DIMMs
TSOD Thermal Throttle Percentage (Threshold)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded.
TSOD Thermal Throttle Percentage (Threshold+5C)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded by more than 5C.
TSOD Thermal Throttle Percentage (Threshold+10C)	X	Sets an integer value for the DDR throttling applied when the "TSOD Thermal Throttle Start Temperature" is exceeded by more than 10C.

7.2.4.3.11 DDR Miscellaneous



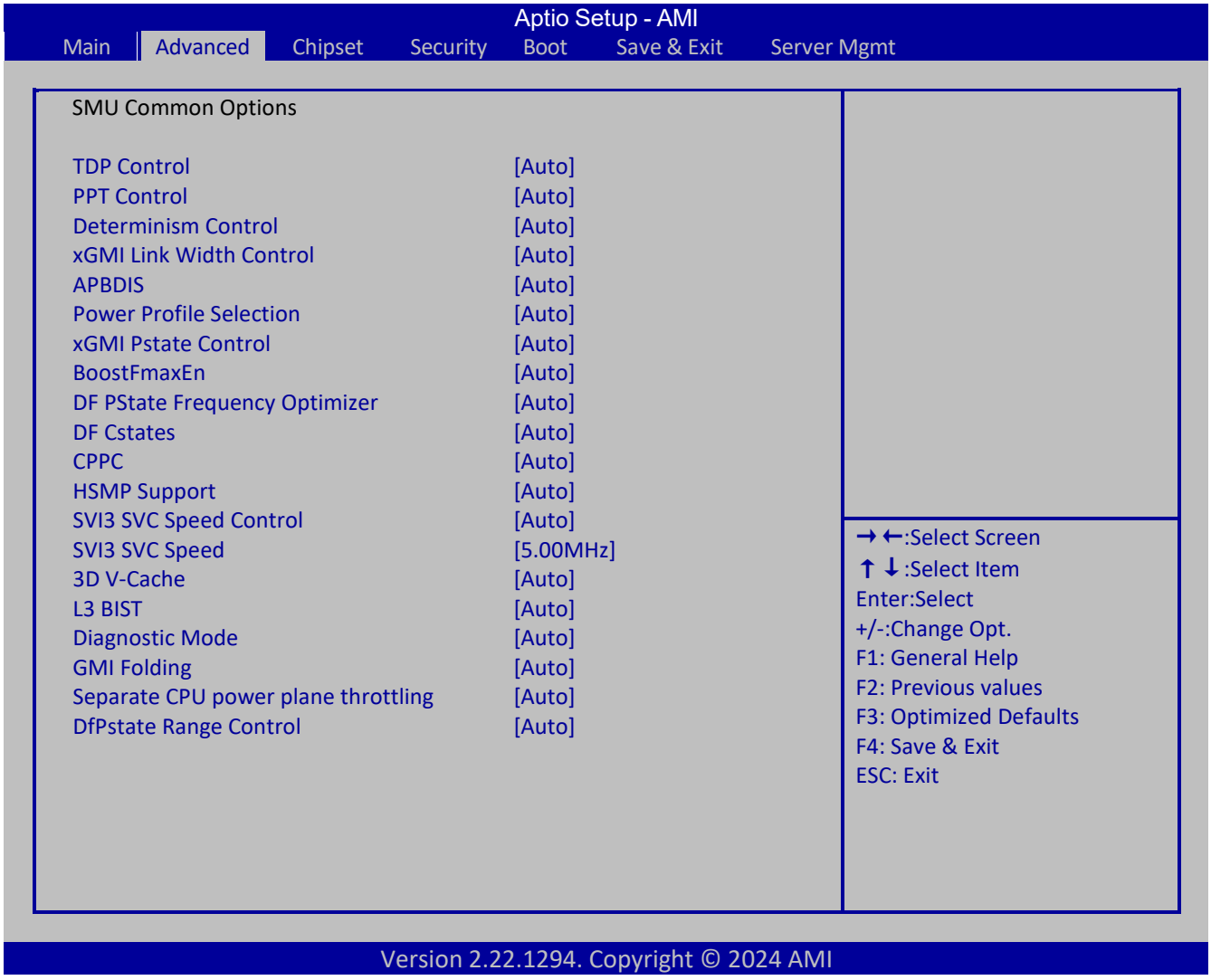
7.2.4.4 NBIO Common Options



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

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

7.2.4.4.1 SMU Common Options

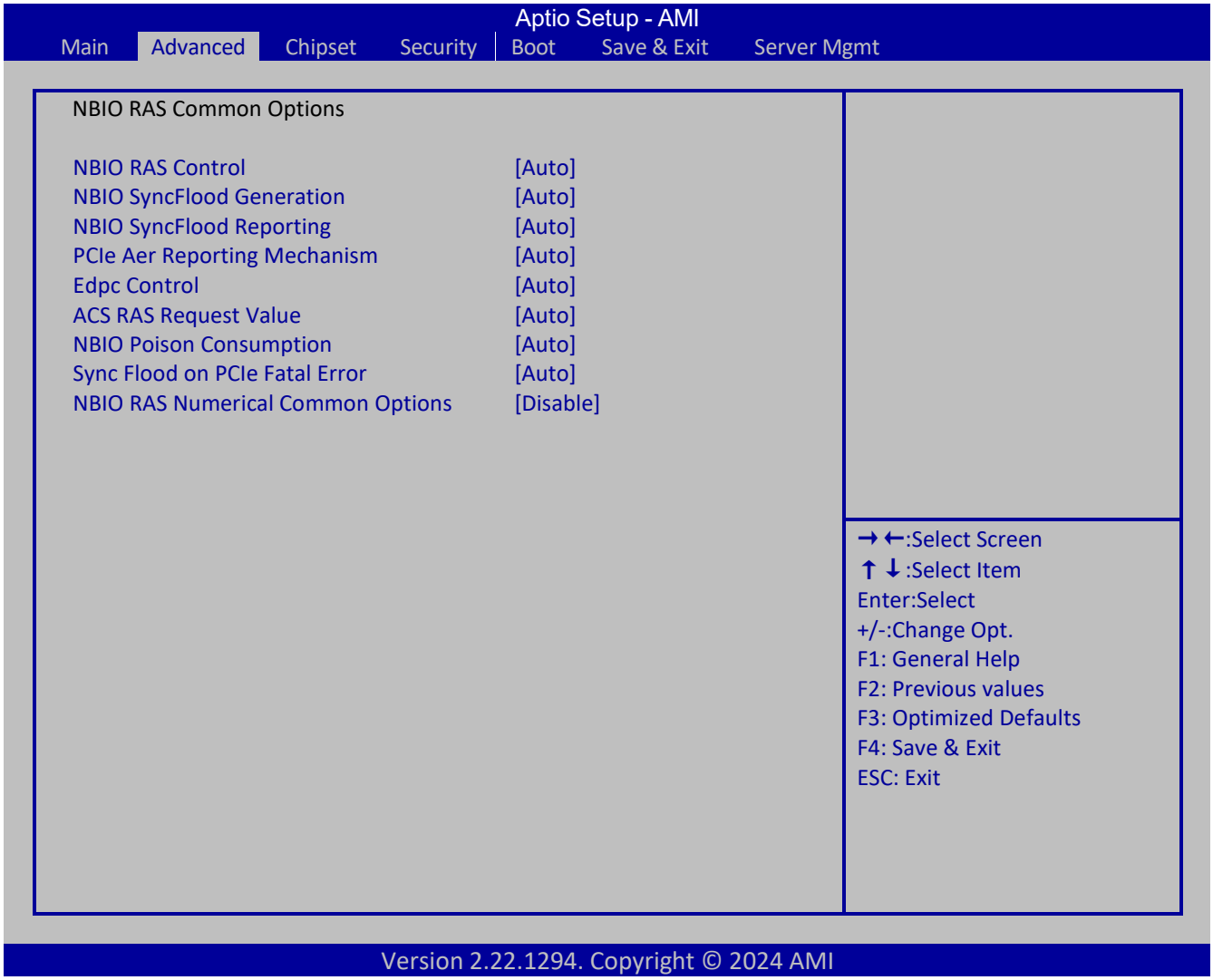


Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	**Settings**	**Comments**
TDP Control	[Manual] **[Auto]**	Auto = Use the fused TDP Manual = User can set customized TDP
PPT Control	[Manual] **[Auto]**	Auto = Use the fused PPT Manual = User can set customized PPT
Determinism Control	[Manual] **[Auto]**	Auto = Use default performance determinism settings

Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	**Settings**	**Comments**
		Manual = User can set custom performance determinism settings
xGMI Link Width Control	[Manual] **[Auto]**	Auto = Use default xGMI link width controller settings. Manual = User can set custom xGMI link width controller settings.
APBDIS	[0] [1] **[Auto]**	0 = not APBDIS (mission mode) 1 = APBDIS
Power Profile Selection	[High Preformance Mode] [Efficiency Mode] [Maxumim OP Performance Mode] [Balanced Memory Performance Mode] [Balanced Core Performance Mode] Balanced Core Memory Performance Mode] **[Auto]**	[0 = High Performance Mode; 1 = Efficiency Mode; 2 = Maximum IO Performance Mode; 3 = Balanced Memory Performance Mode; 4 = Balanced Core Performance Mode; 5 = Balanced Core Memory Performance Mode; 0xFF = Auto]
xGMI Pstate Control	**[Auto]** [Manual]	If manual, set XgmiPstateRangeSupportEn=1, else 0
BoostFmaxEn	[Manual] **[Auto]**	Auto = Use the default Fmax Manual = User can set the boost Fmax
DF PState Frequency Optimizer	**[Auto]** [Enabled] [Disabled]	Disabled - means disable the DFPstate CCLK effective frequency optimizer Enabled - means enable the DFPstate CCLK effective frequency optimizer
DF Cstates	[Disabled] [Enabled] **[Auto]**	Enable = Enable the feature : Disable = Disable the feature
CPPC	[Disabled] [Enabled] **[Auto]**	Enable = Enable the feature : Disable = Disable the feature
HSMP Support	[Disabled] [Enabled] **[Auto]**	Select HSMP support enable or disable
SVI3 SVC Speed Control	**[Auto]** [Manual]	Enables for programming of the SVI3 SVC speed. Auto = Use default SVI3 speed control Manual = User can set custom SVI3 speed control settings
SVI3 SVC Speed	[20.00MHz] [13.33MHz] **[5.00MHz]**	0=50.00MHz 1=40.00MHz 2=26.67MHz 3=20.00MHz 4=16.00MHz 5=13.33MHz 6=10.00MHz 7=8.00MHz 8=5.00MHz
3D V-Cache	[Auto] [Disable] [1 stack]	Override of X3D technology
L3 BIST	[Disable] [Enable] **[Auto]**	Enable or Disable L3 BIST
Diagnostic Mode	[Disabled]	Select Diag mode enable or disable

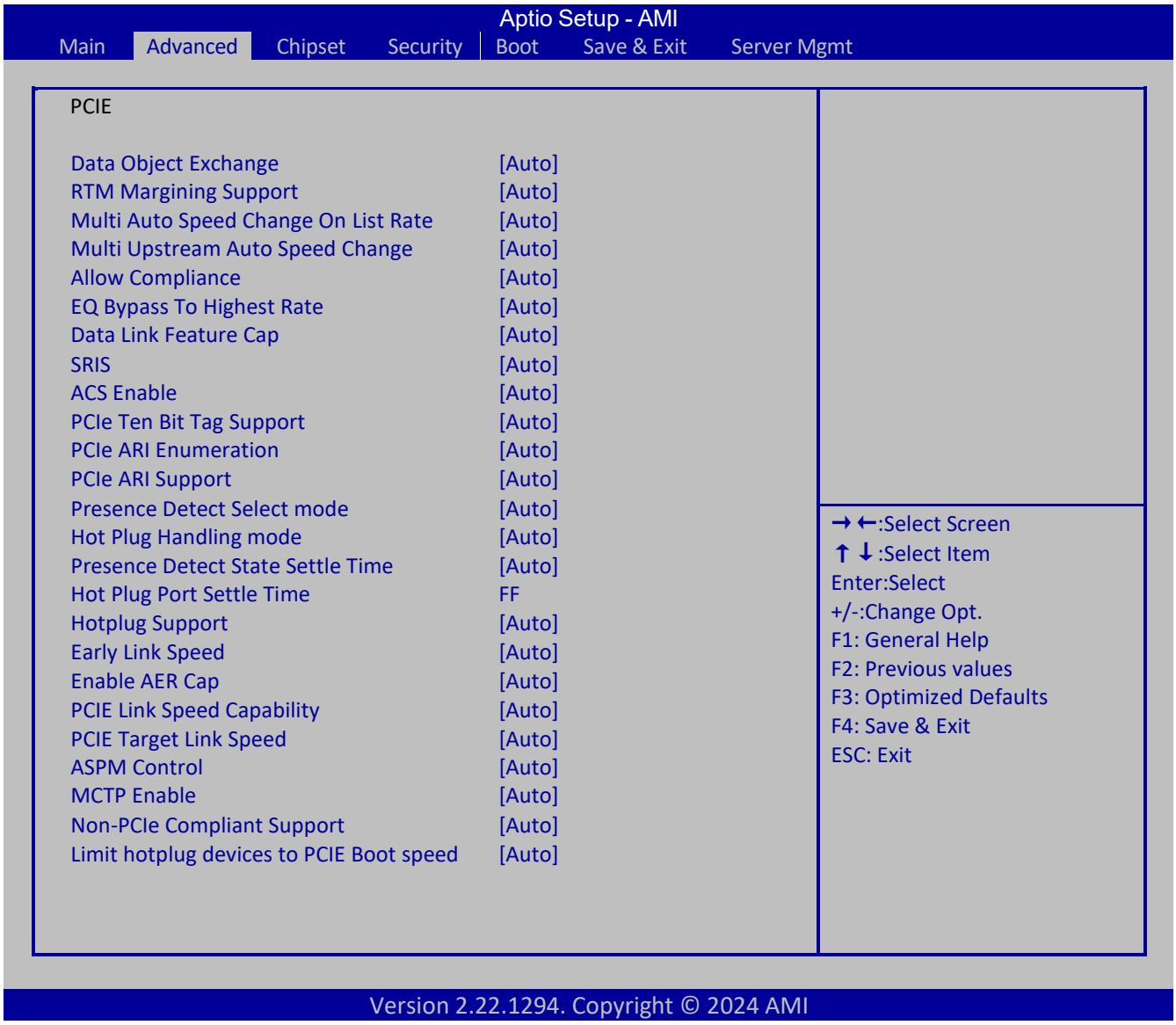
Advanced \ AMD CBS \ NBIO Common Options \ SMU Common Options		
Menu Fields	**Settings**	**Comments**
	[Enabled] **[Auto]**	
GMI Folding	[Disabled] [Enabled] **[Auto]**	Enable = Enable the feature : Disable = Disable the feature
Separate CPU power plane throttling	[Enable] [Disable] **[Auto]**	Disable=link throttling for CPU planes; Enable=unlink throttling for CPU planes
DfPstate Range Control	[Disable] [Enable] **[Auto]**	Disable - Disable DF Pstate Range Control Enable - Enable DF Pstate Range Control DF Pstate selection is overridden by the APBDIS BIOS option if it is selected. If this feature is enabled, the range value setting should follow the rule that the DF Pstate Max Index must be less than or equal to the DF Pstate Min Index. Otherwise, DF Pstate Range selections will not work.

7.2.4.4.2 NBIO RAS Common Options



Advanced \ AMD CBS \ NBIO Common Options \ NBIO RAS Common Options		
Menu Fields	**Settings**	**Comments**
NBIO RAS Control	[Disable] [MAC] **[Auto]**	(0) Disabled, (1) MCA
NBIO SyncFlood Generation	[Enabled] [Disabled] **[Auto]**	This value may be used to mask SyncFlood caused by NBIO RAS options. When set to TRUE SyncFlood from NBIO is masked. When set to FALSE NBIO is capable of generating SyncFlood.
NBIO SyncFlood Reporting	[Enabled] [Disabled] **[Auto]**	This value may be used to enable SyncFlood reporting to APML. When set to TRUE SyncFlood will be reported to APML. When set to FALSE that reporting well be disabled
PCIe Aer Reporting Mechanism	[Firmware First] [Firmware First but allow OS First] [OS First] **[Auto]**	This value selects the method of reporting AER errors from PCI Express. A value of 1 allows OS First handling of the errors through generation of a system control interrupt (SCI). A value of 2 provides for Firmware First handling of errors through generation of a system management interrupt (SMI).
Edpc Control	[Disabled] [Enabled] **[Auto]**	(0) Disabled; (1) Enabled; (3) Auto
ACS RAS Request Value	[Direct Request Access Enabled] [Request Blocking Enabled] [Request Redirect Enabled] **[Auto]**	No help String
NBIO Poison Consumption	**[Auto]** **[**Disabled] [Enabled]	NBIO Poison Consumption
Sync Flood on PCIe Fatal Error	**[Auto]** [True] [False]	When "Sync Flood on PCIe Fatal Error" is True, PcdAmdPcieSyncFloodOnFatal should be set to True. When "Sync Flood on PCIe Fatal Error" is False, PcdAmdPcieSyncFloodOnFatal should be set to False. When "Sync Flood on PCIe Fatal Error" is Auto, PcdAmdPcieSyncFloodOnFatal should retain its AGESA default.
NBIO RAS Numerical Common Options	**[Disable]** [Manual]	All the numerical RAS CBS options override the PCD values automatically. Disable: Keep original PCD values Manual: Display custom numerical RAS CBS options

7.2.4.4.3 PCIE

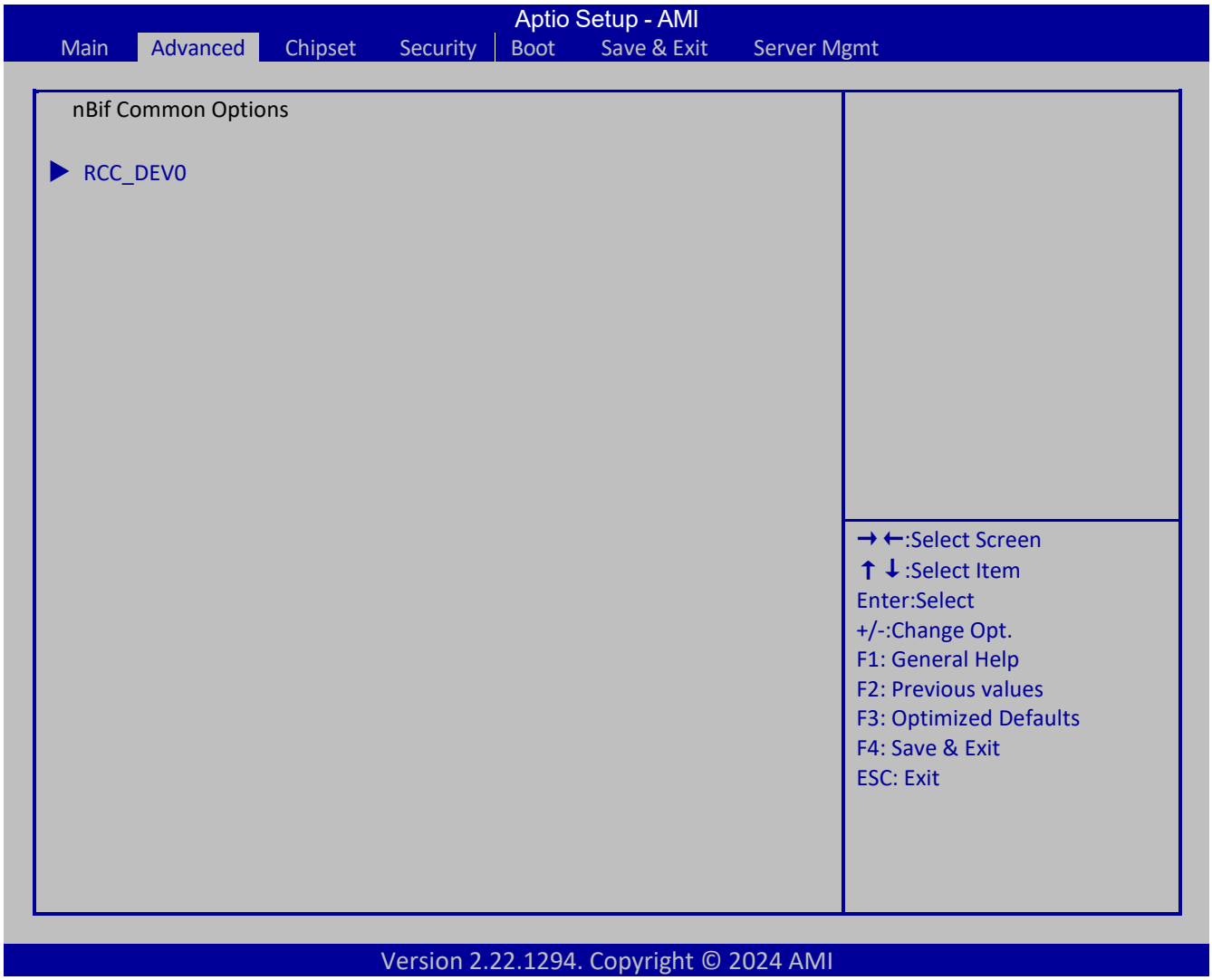


Advanced \ AMD CBS \ NBIO Common Options \ PCIE		
Menu Fields	**Settings**	**Comments**
Data Object Exchange	[Disabled] [Enabled] **[Auto]**	Data Object Exchange (DOE)
RTM Margining Support	[Disable] [Enable] **[Auto]**	RTM Margining Support
Multi Auto Speed Change On List Rate	[Disable] [Enable] **[Auto]**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

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

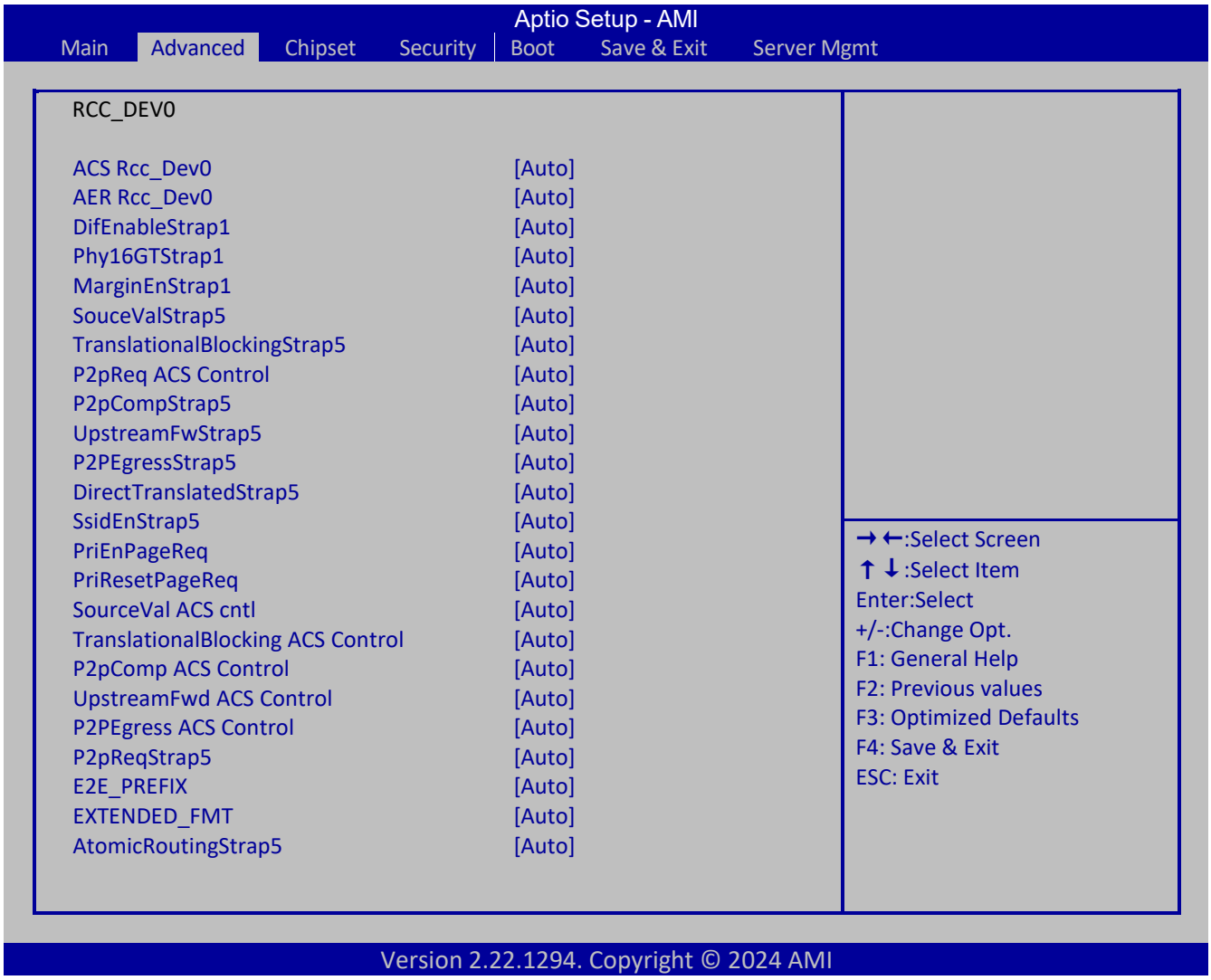
Advanced \ AMD CBS \ NBIO Common Options \ PCIE		
Menu Fields	**Settings**	**Comments**
	[GEN2] [GEN3] [GEN4] [GEN5] **[Auto]**	
PCIE Target Link Speed	[Maximum speed] [GEN1] [GEN2] [GEN3] [GEN4] [GEN5] **[Auto]**	Set PCIe speed on all ports
ASPM Control	[Disable] [L0s] [L1] **[Auto]**	No help String
MCTP Enable	[Disable] [Enable] **[Auto]**	Enable/Disable MCTP
Non-PCIe Compliant Support	[Disable] [Enable] **[Auto]**	Enable this setting to send command to disable Extended EIEOS, DLF, and Gen 5 Support on training failure for non-pcie compliant devices.
Limit hotplug devices to PCIE Boot Speed	**[Auto]** [Enable] [Disable]	Enabled: Limit hotplug slots to Gen4 if system booted with only Gen4 devices, which optimizes idle power Disabled: Do not limit hotplug slots to Gen4 if system booted with only Gen4 devices, increases idle power

7.2.4.4.4 nBif Common Options



Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options		
Menu Fields	**Settings**	**Comments**
RCC_DEV0	Selects sub-menu	

7.2.4.4.4.1 RCD_DEV0

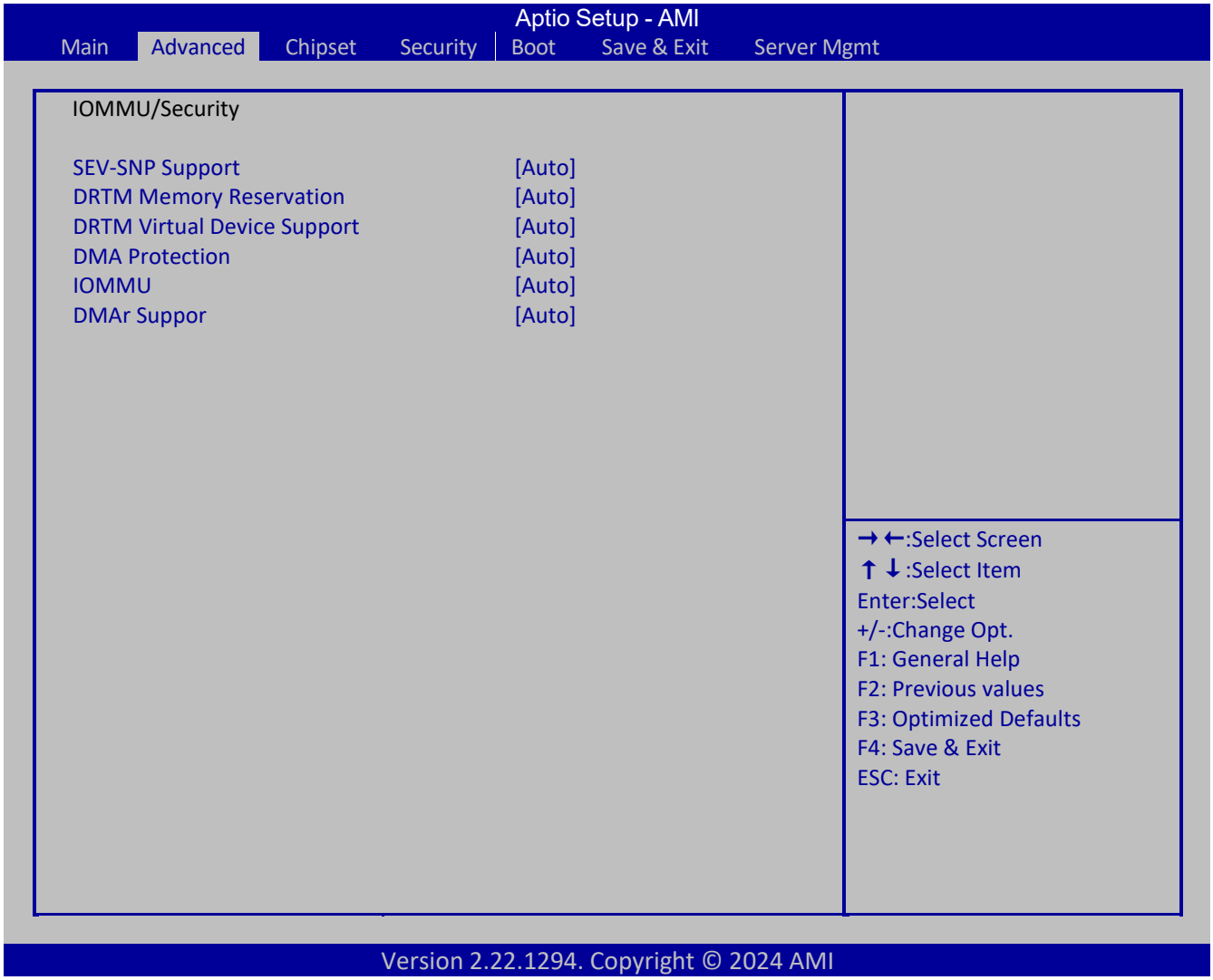


Advanced \ AMD CBS \ NBIO Common Options \ nBif Common Options \ RCC_DEV0		
Menu Fields	**Settings**	**Comments**
ACS Rcc_Dev0	**[Auto]** [Disable] [Enable]	Enable ACS enable for RCC_DEV0 ,STRAP_ACS_EN_DN_DEV0
AER Rcc_Dev0	**[Auto]** [Disable] [Enable]	Enable AER enable for RCC_DEV0 ,STRAP_AER_EN_DN_DEV0
DifEnableStrap1	**[Auto]** [Disable] [Enable]	RCC_BIF_STRAP1,STRAP_DLF_EN=1
Phy16GTStrap1	**[Auto]** [Disable] [Enable]	RCC_BIF_STRAP1 ,STRAP_PHY_16GT_EN=1
MarginEnStrap1	**[Auto]** [Disable] [Enable]	RCC_BIF_STRAP1 ,STRAP_MARGIN_EN=1
SouceValStrap5	**[Auto]** [Disable]	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,Source Validation bit [23]

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

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

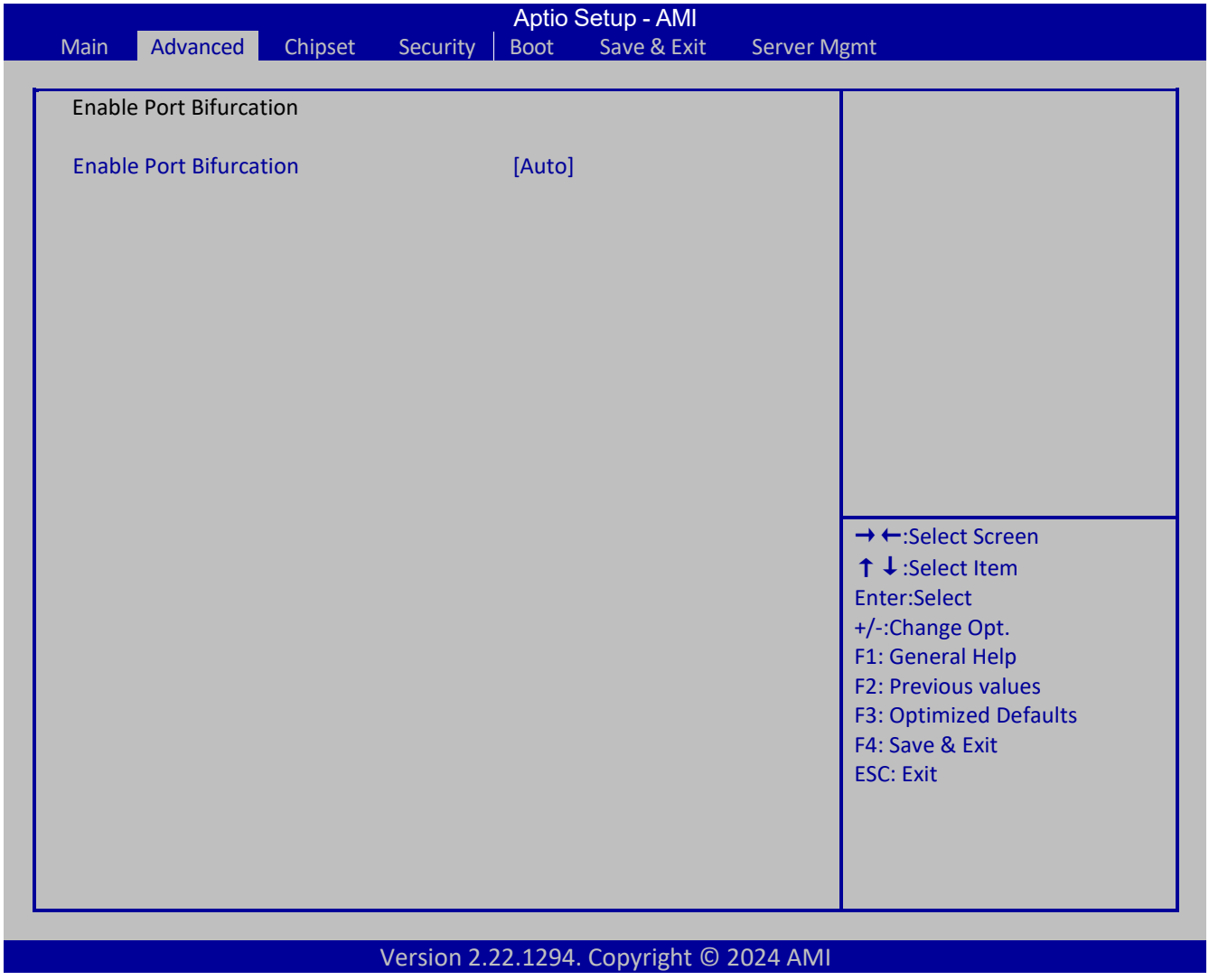
7.2.4.4.5 IOMMU/Security



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

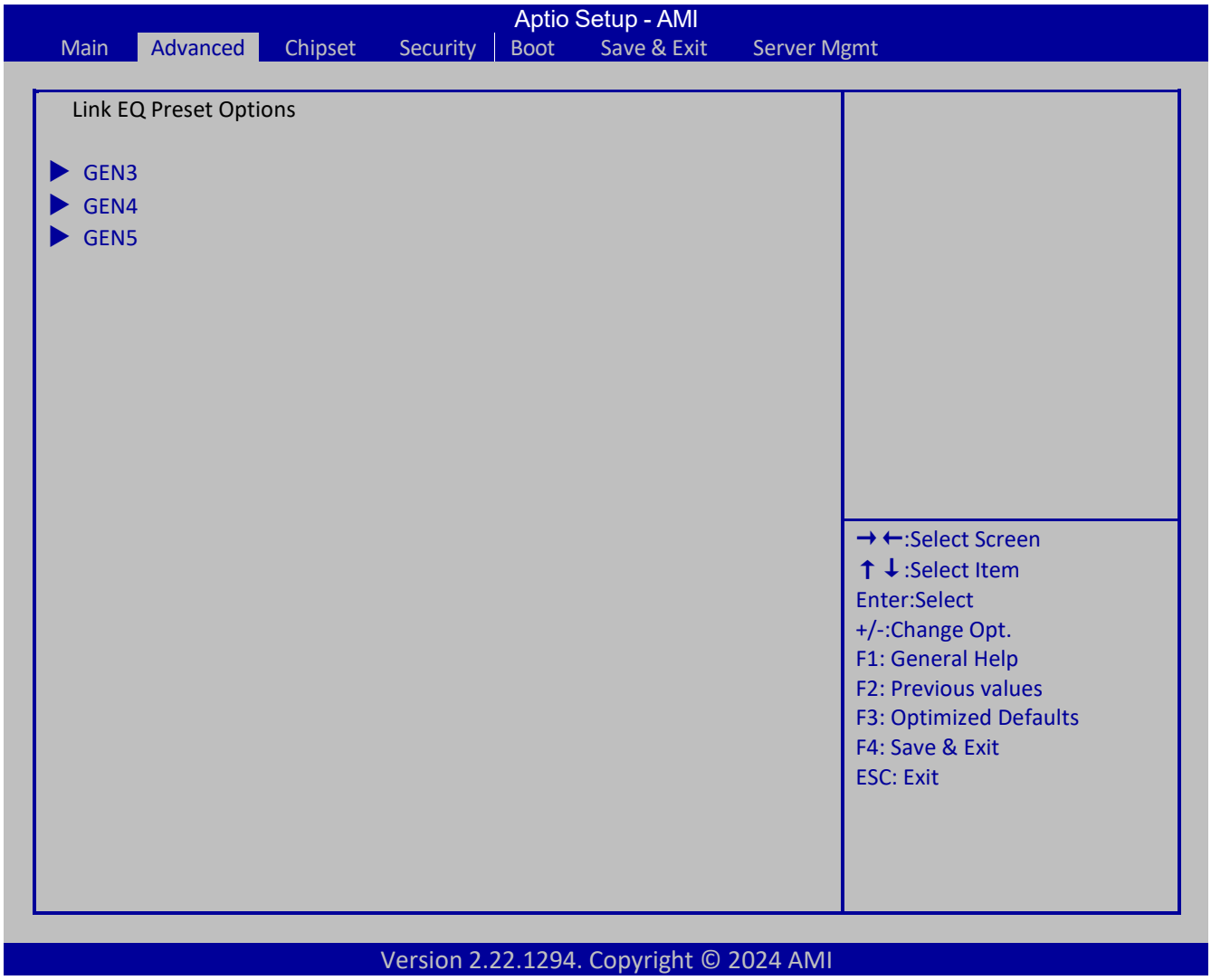
Advanced \ AMD CBS \ NBIO Common Options \ IOMMU/Security		
Menu Fields	**Settings**	**Comments**
	[Disabled]	
IOMMU	[Disabled] [Enabled] **[Auto]**	Enable/Disable IOMMU
DMAr Suppor	[Disabled] [Enabled] **[Auto]**	Enable DMAr system protection during POST.

7.2.4.4.6 Enable Port Bifurcation



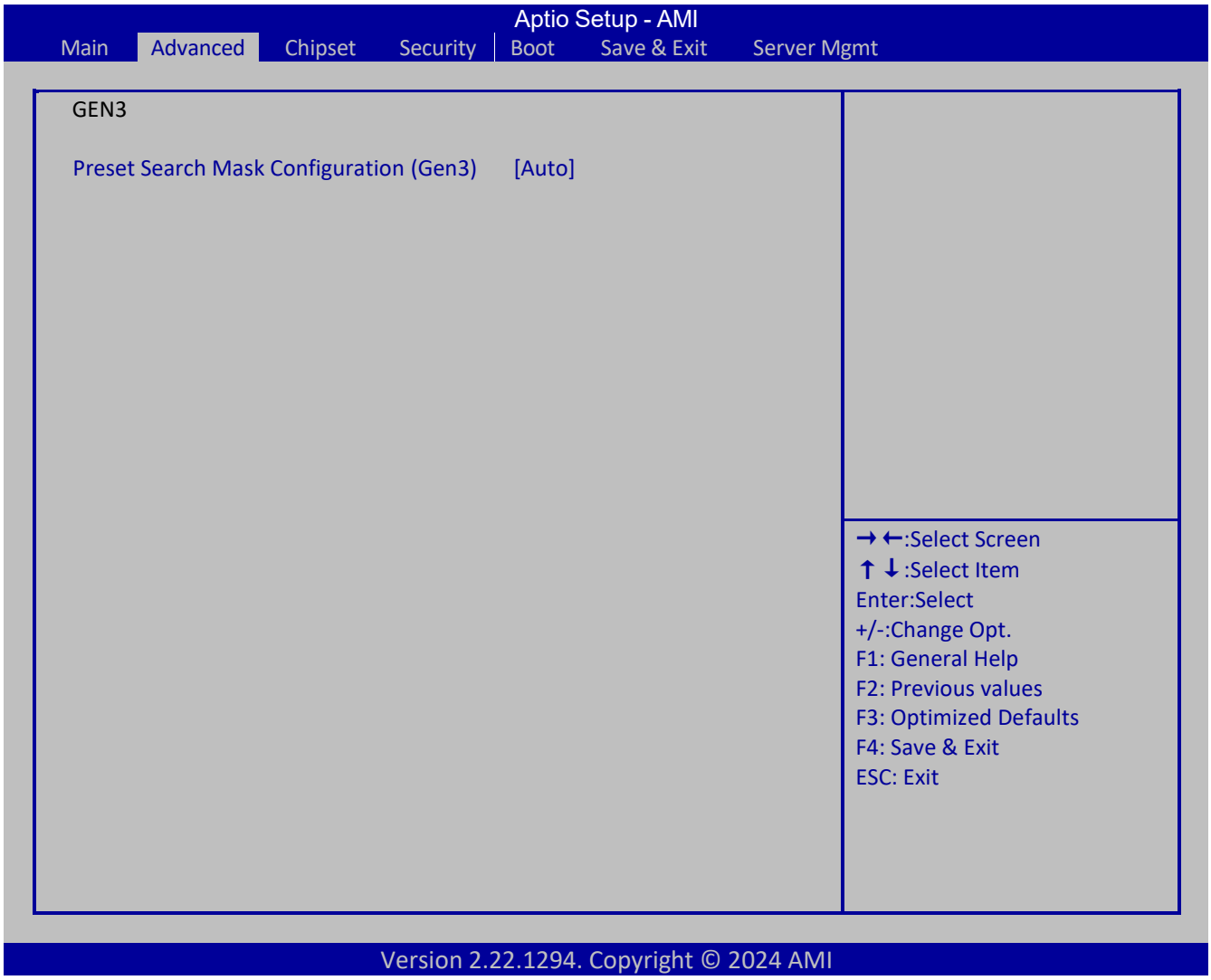
Advanced \ AMD CBS \ NBIO Common Options \ Enable Port Bifurcation		
Menu Fields	**Settings**	**Comments**
Enable Port Bifurcation	**[Auto]** [Enable] [Disable]	Change the configuration of each PCIe link individually. By default, each link is configured 1 port of 16 lanes. (x16)

7.2.4.4.7 Link EQ Preset Options



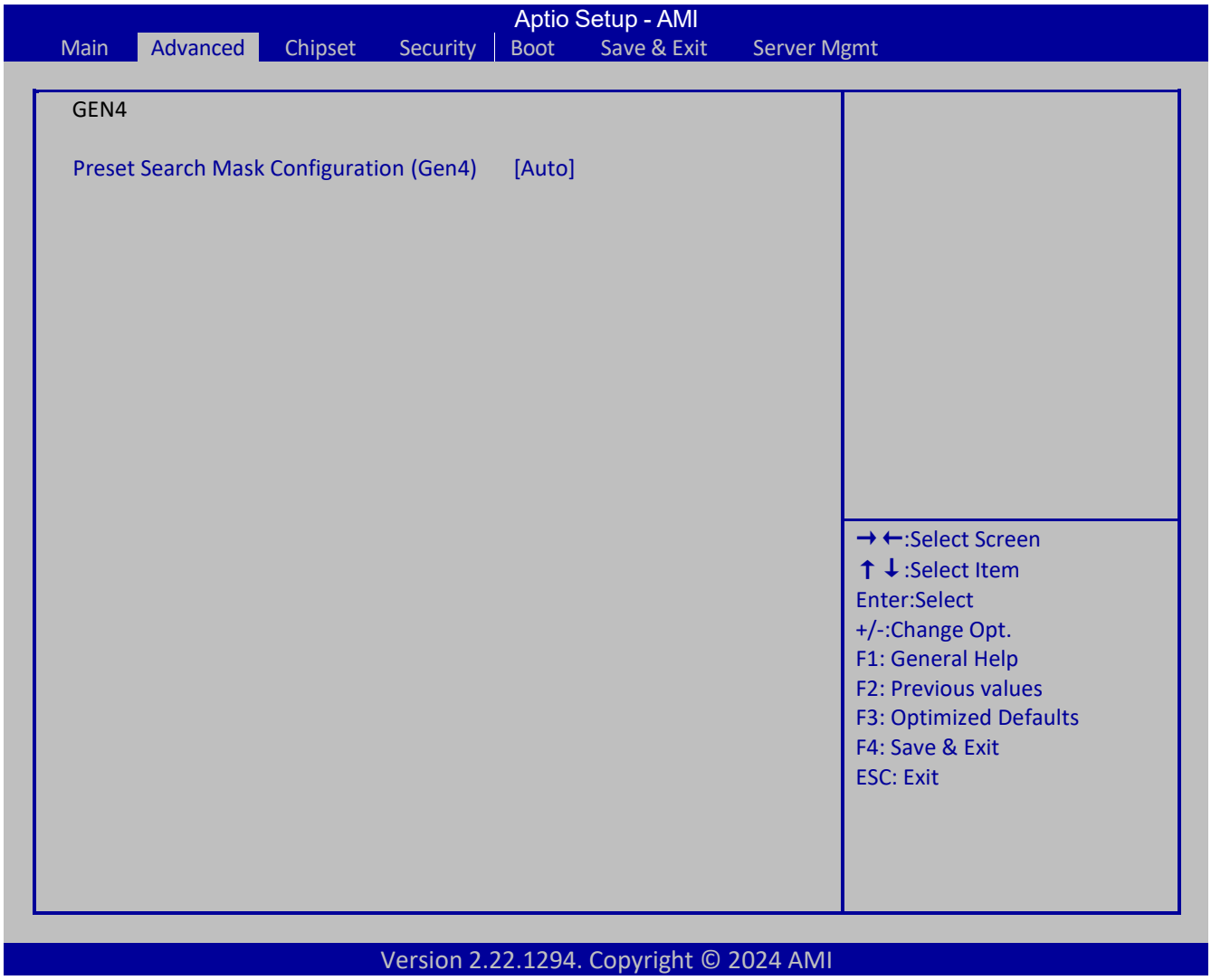
Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options		
Menu Fields	**Settings**	**Comments**
GEN3	Selects Sub-menu.	
GEN4	Selects Sub-menu.	
GEN5	Selects Sub-menu.	

7.2.4.4.7.1 GEN3



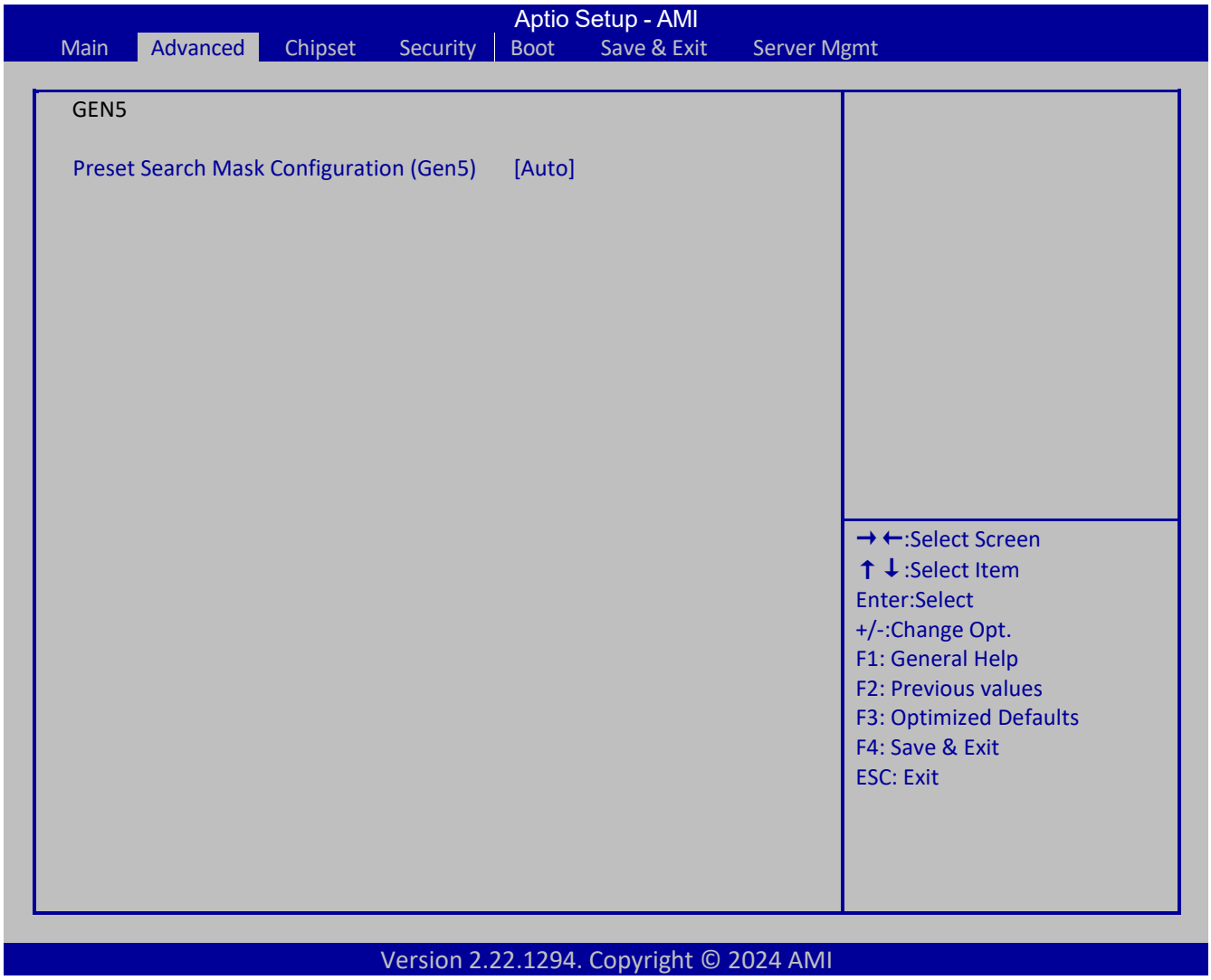
Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN3		
Menu Fields	**Settings**	**Comments**
Preset Search Mask Configuration (Gen3)	[Custom] **[Auto]**	Configuration for Gen3 Preset Mask. Select Custom to modify Gen3 Preset Search Mask. Auto will default to platform configurations.

7.2.4.4.7.2 GEN4



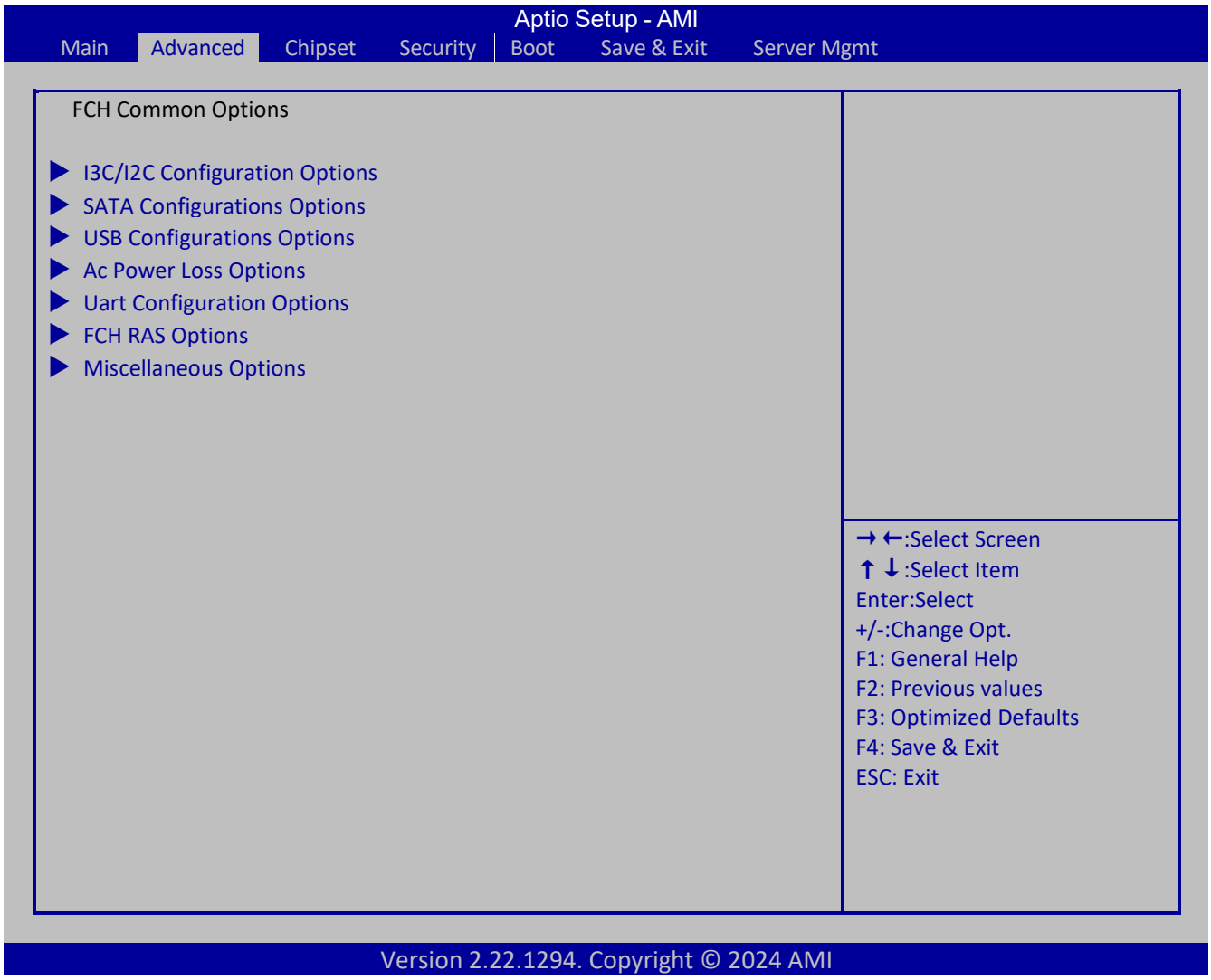
Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN4		
Menu Fields	**Settings**	**Comments**
Preset Search Mask Configuration (Gen4)	[Custom] **[Auto]**	Configuration for Gen4 Preset Mask. Select Custom to modify Gen4 Preset Search Mask. Auto will default to platform configurations.

7.2.4.4.7.3 GEN5



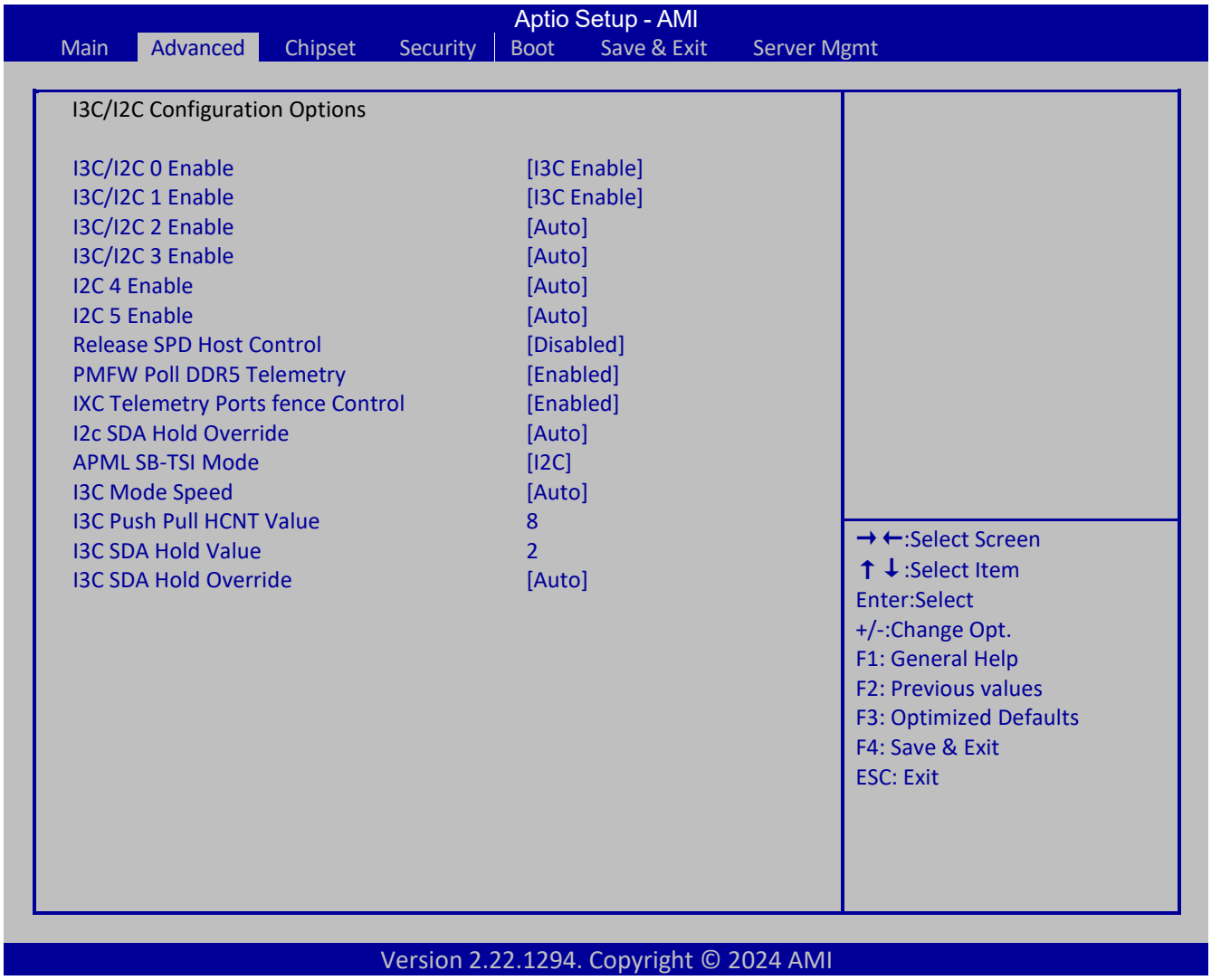
Advanced \ AMD CBS \ NBIO Common Options \ Link EQ Preset Options \ GEN5		
Menu Fields	**Settings**	**Comments**
Preset Search Mask Configuration (Gen5)	[Custom] **[Auto]**	Configuration for Gen5 Preset Mask. Select Custom to modify Gen5 Preset Search Mask. Auto will default to platform configurations.

7.2.4.5 FCH Common Options



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

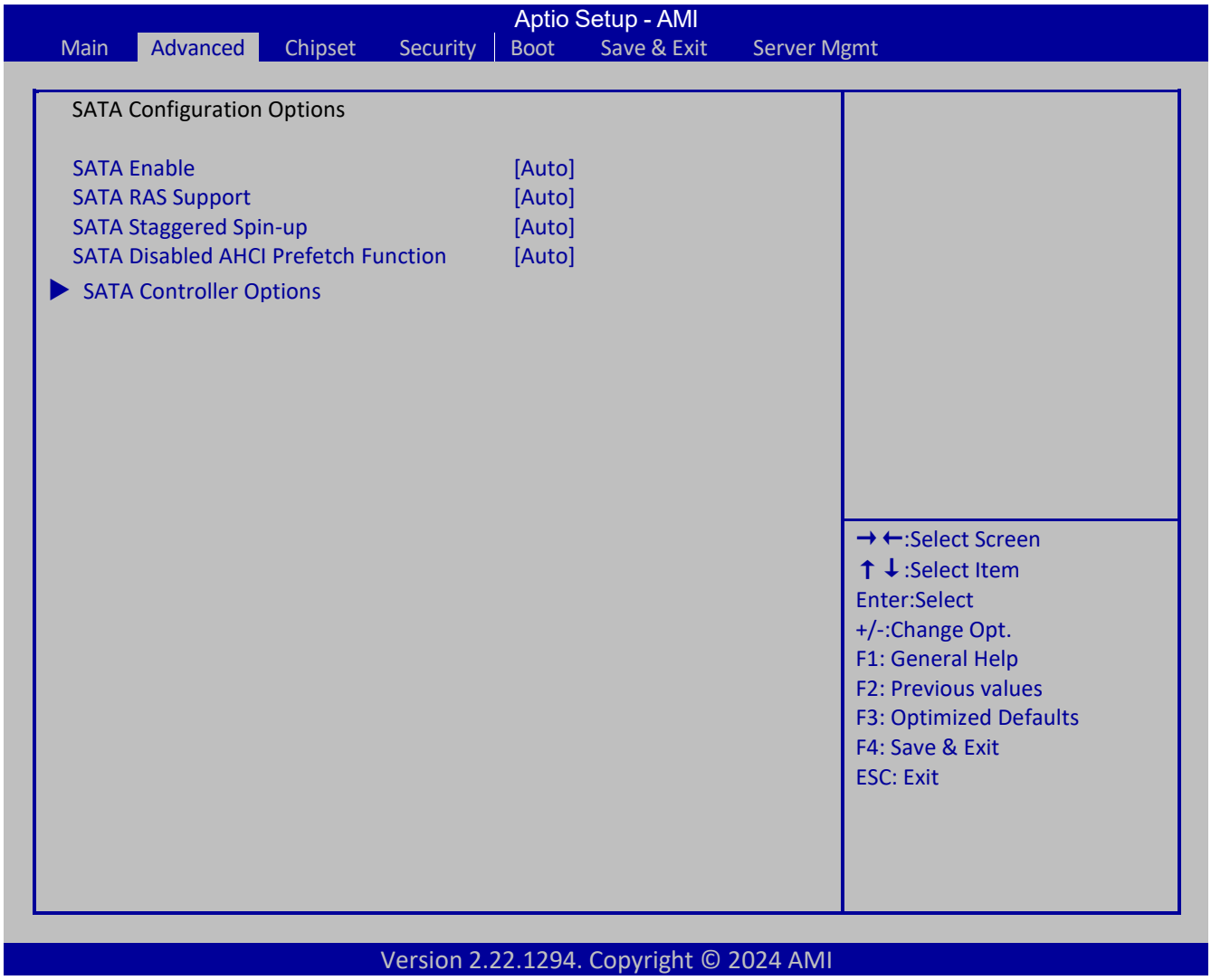
7.2.4.5.1 I3c/I2c Configuration Options



Advanced \ AMD CBS \ FCH Common Options \ I3C/I2C Configuration Options		
Menu Fields	**Settings**	**Comments**
I3C/I2C 0 Enable	[Both Disabled] **[I3C Enable]** [I2C Enable] [Auto]	Enable or disable Inter-Integrated Circuit Control 0
I3C 0 Mode	**[I3C]** [I2C] [Auto]	Choose I3C basic mode or I2C mode
I3C/I2C 1 Enable	[Both Disabled] **[I3C Enable]** [I2C Enable] [Auto]	Enable or disable Inter-Integrated Circuit Control 1
I3C 1 Mode	**[I3C]** [I2C] [Auto]	Choose I3C basic mode or I2C mode
I3C/I2C 2 Enable	[Both Disabled] **[I3C Enable]** [I2C Enable]	Enable or disable Inter-Integrated Circuit Control 2

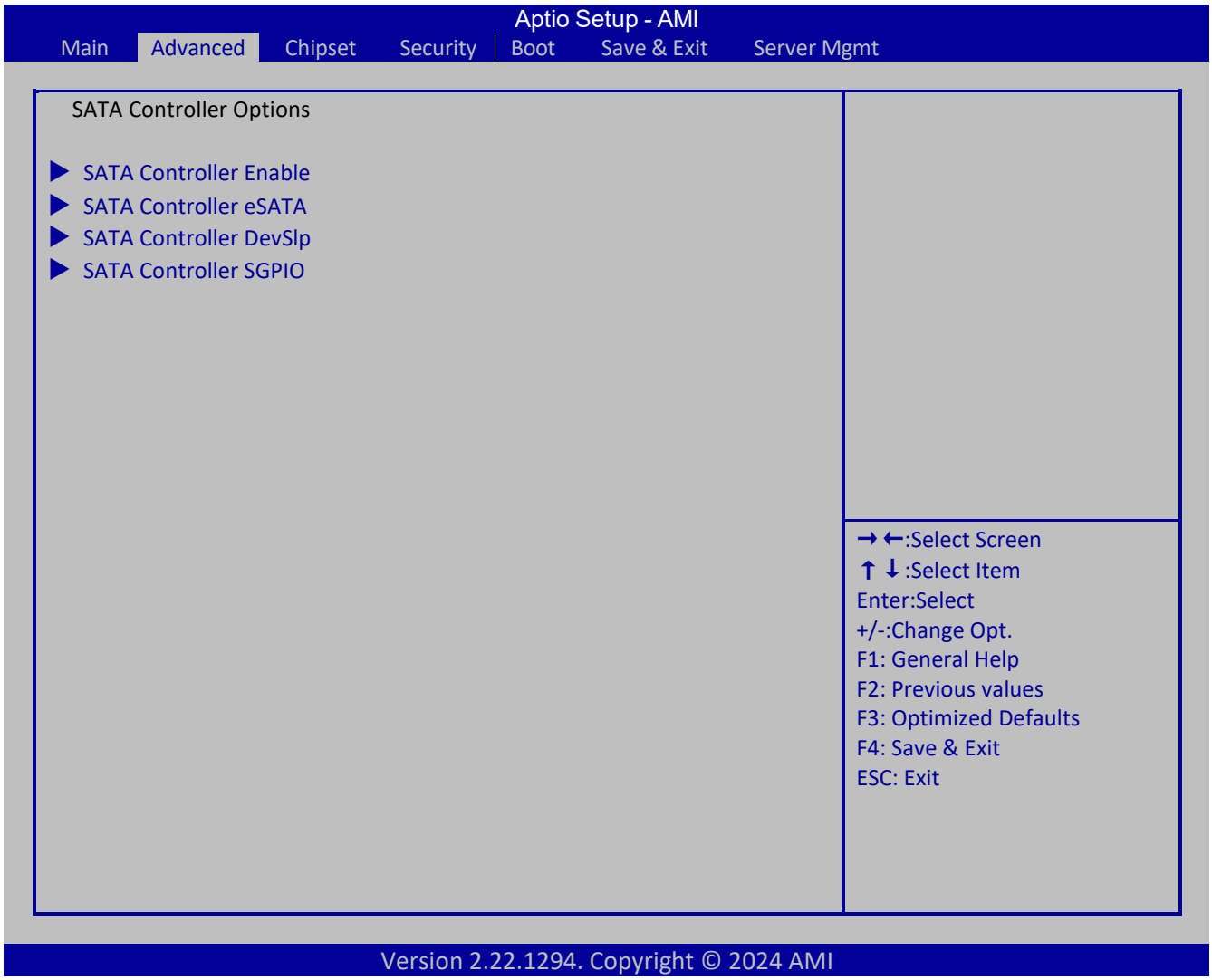
Advanced \ AMD CBS \ FCH Common Options \ I3C/I2C Configuration Options		
Menu Fields	**Settings**	**Comments**
	[Auto]	
I3C 2 Mode	**[I3C]** [I2C] [Auto]	Choose I3C basic mode or I2C mode
I3C/I2C 3 Enable	[Both Disabled] **[I3C Enable]** [I2C Enable] [Auto]	Enable or disable Inter-Integrated Circuit Control 3
I3C 3 Mode	**[I3C]** [I2C] [Auto]	Choose I3C basic mode or I2C mode
I2C 4 Enable	[Disabled] [Enabled] **[Auto]**	Enable or disable Inter-Integrated Circuit Control 4
I2C 5 Enable	[Disabled] [Enabled] **[Auto]**	Enable or disable Inter-Integrated Circuit Control 5
Release SPD Host Control	[Disabled] **[Enabled]**	Release SPD Host Control, so that BMC can take over the ownership of I2C/I3C bus
PMFW Poll DDR5 Telemetry	[Disabled] **[Enabled]**	Send message to PMFW for polling DDR5 telemetry at the end of POST
IXC Telemetry Ports fence Control	[Disabled] **[Enabled]**	Controls the Fencing off for I2C/I3C ports which are involved in DDR Telemetry. If this option is enabled, then the associated Ixc ports registers will be put in the secure region. Note: If this option is disabled, there is a risk of collision happening between x86 accessing IxC and PMFW running DDR Telemetry which can cause undefined behavior.
I2C SDA Hold Override	[Disabled] [Enabled] **[Auto]**	Override I2C SDA_TX_HOLD and SDA_RT_HOLD
APML SB-TSI Mode	[I3C] **[I2C]**	Select APML SB-TSI over I3C or I2C. In I3C mode, the slave controller can support both I3C and I2C(Adaptive mode).
I3C Mode Speed	[SDR2 (6 MHz)] [SDR0 (12.5 MHz)] **[Auto]**	I3C Transfer Speed
I3C Push Pull HCNT Value	X	SCL push-pull High count for I3C transfers targeted to I3C devices
I3C SDA Hold Value	X	I3C SDA Hold Value
I3C SDA Hold Override	[Disabled] [Enabled] **[Auto]**	I2C3 IC SDA TX HOLD value

7.2.4.5.2 SATA Configuration Options



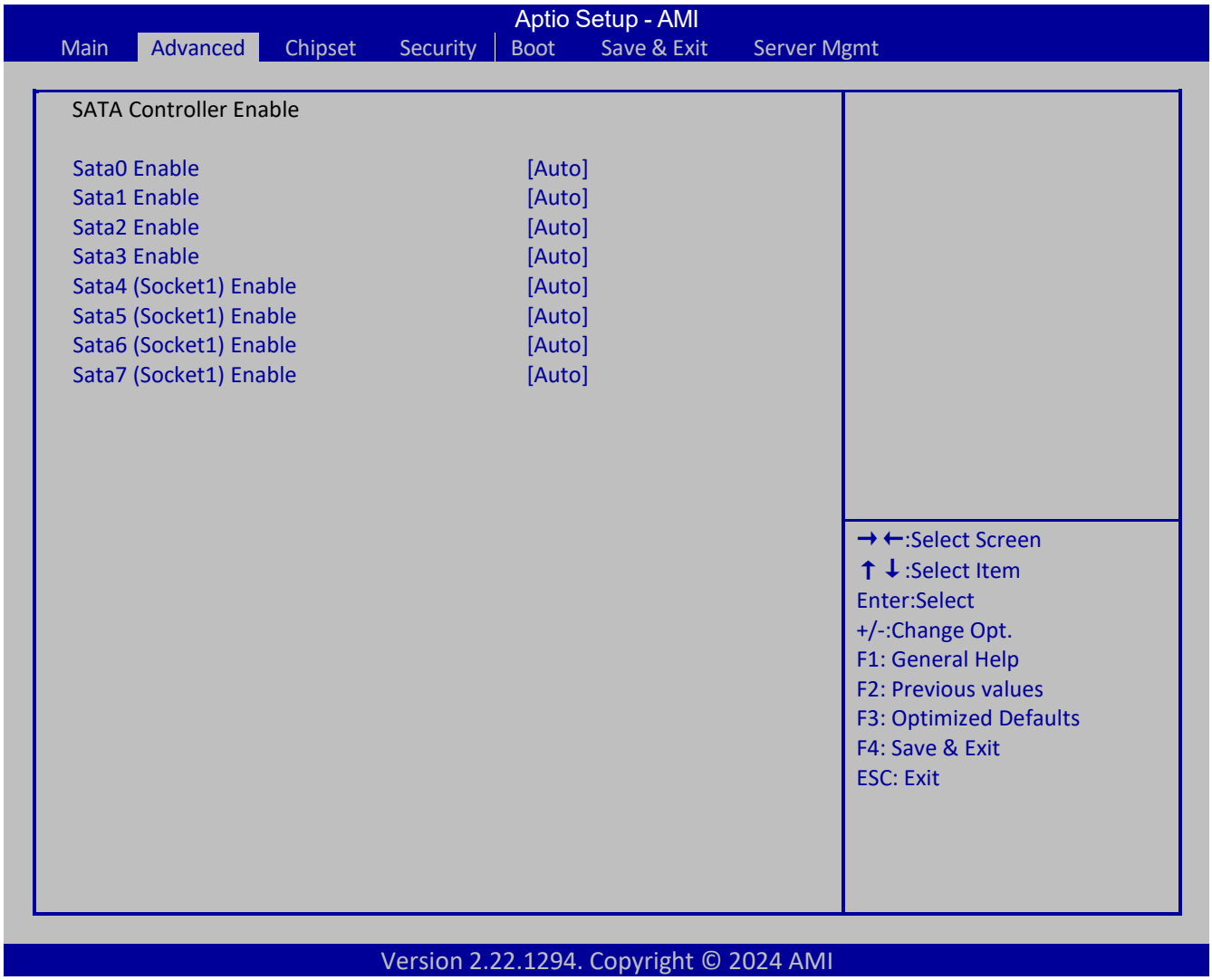
Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options		
Menu Fields	**Settings**	**Comments**
SATA Enable	[Disabled] [Enabled] **[Auto]**	Disable or enable OnChip SATA controller
SATA RAS Support	[Disabled] [Enabled] **[Auto]**	Disable or enable Sata RAS Support
SATA Staggered Spin-up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

7.2.4.5.2.1 SATA Controller Options



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

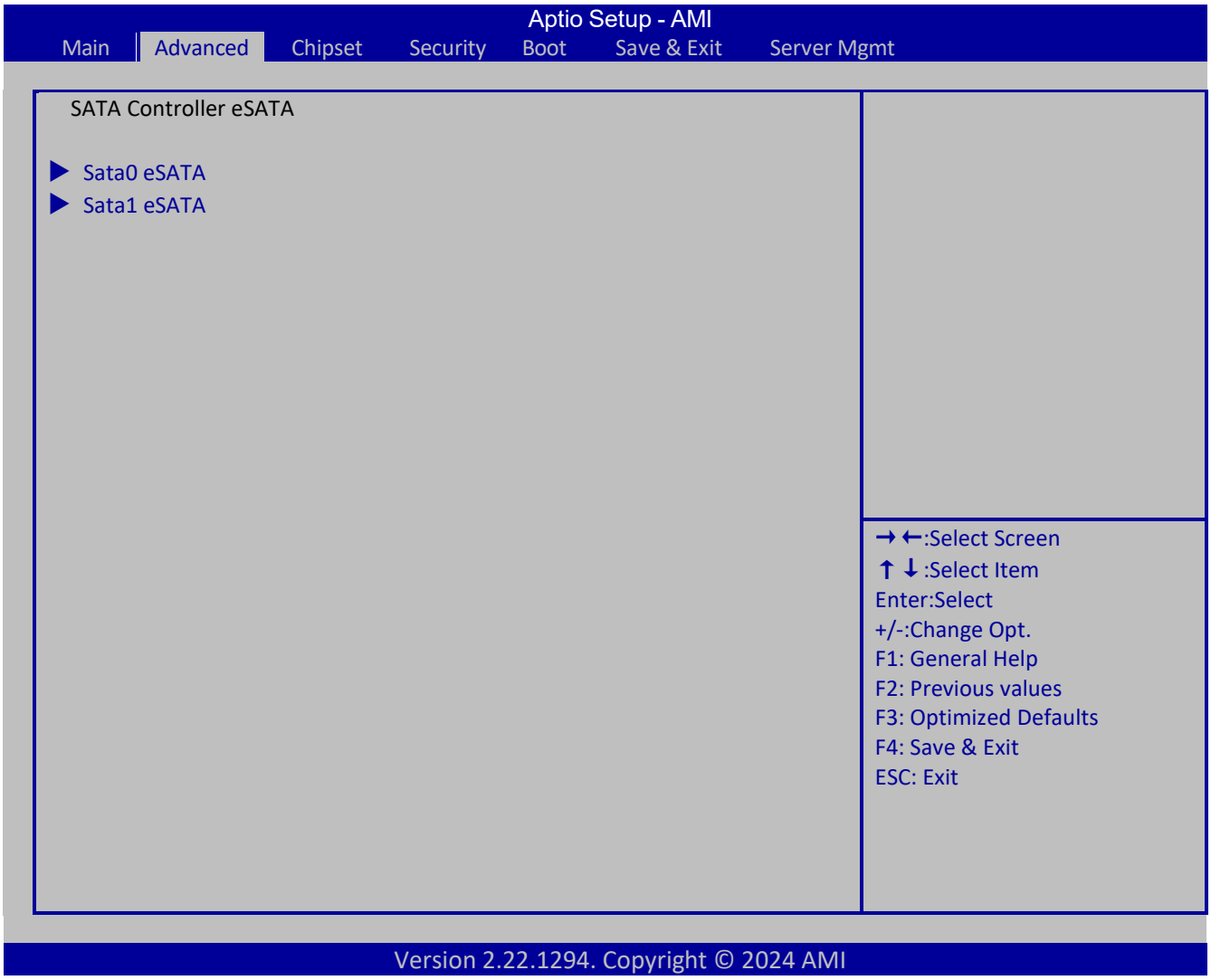
7.2.4.5.2.1.1 SATA Controller Enable



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

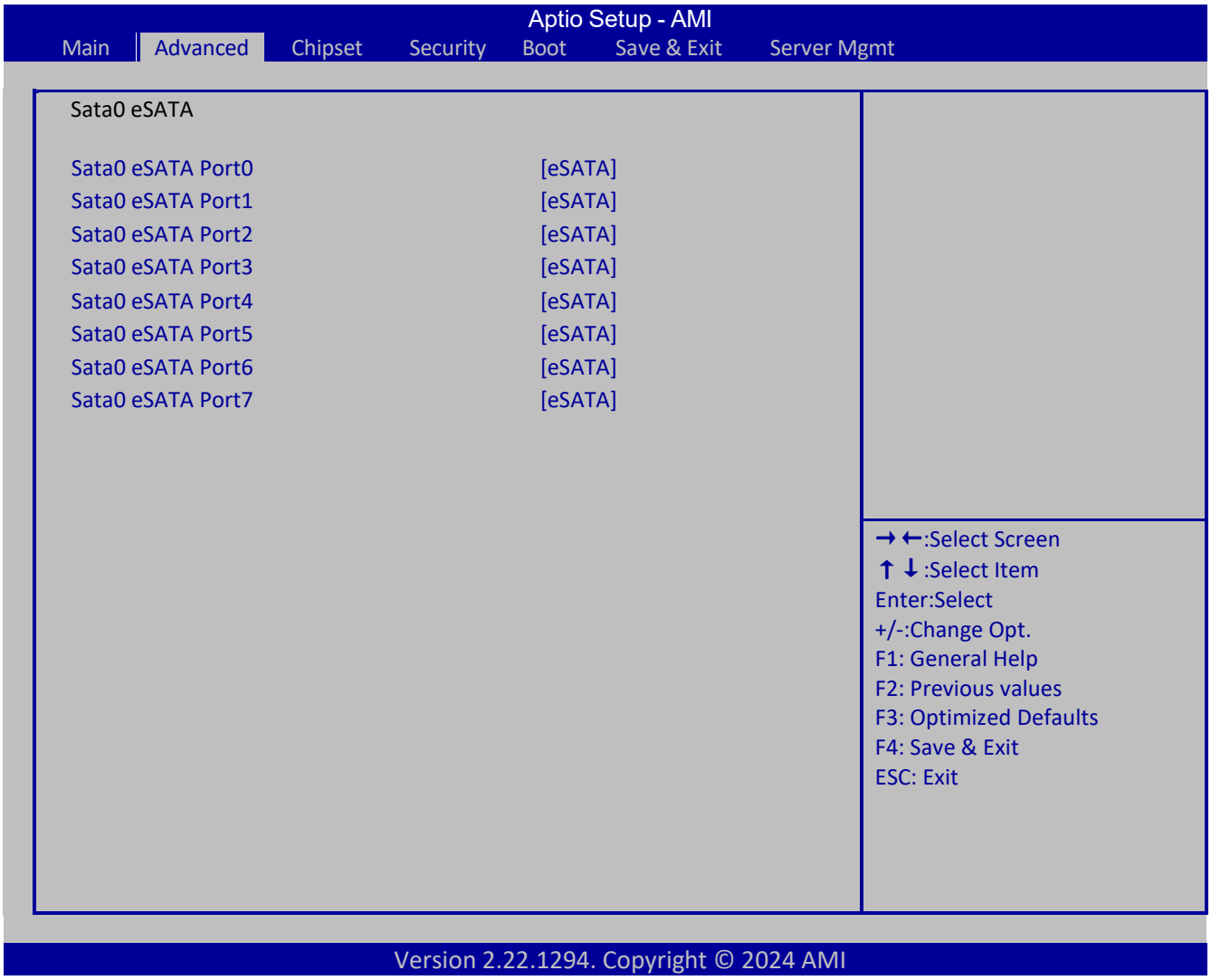
Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller Enable		
Menu Fields	**Settings**	**Comments**
	[Auto]	
Sata6 (Socket1) Enable	[Disabled] [Enabled] **[Auto]**	Enable or Disable Sata6 on Socket 1 (IOD1).. Each IOD has 4 Sata Controllers.
Sata7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

7.2.4.5.2.1.2 SATA Controller eSATA



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

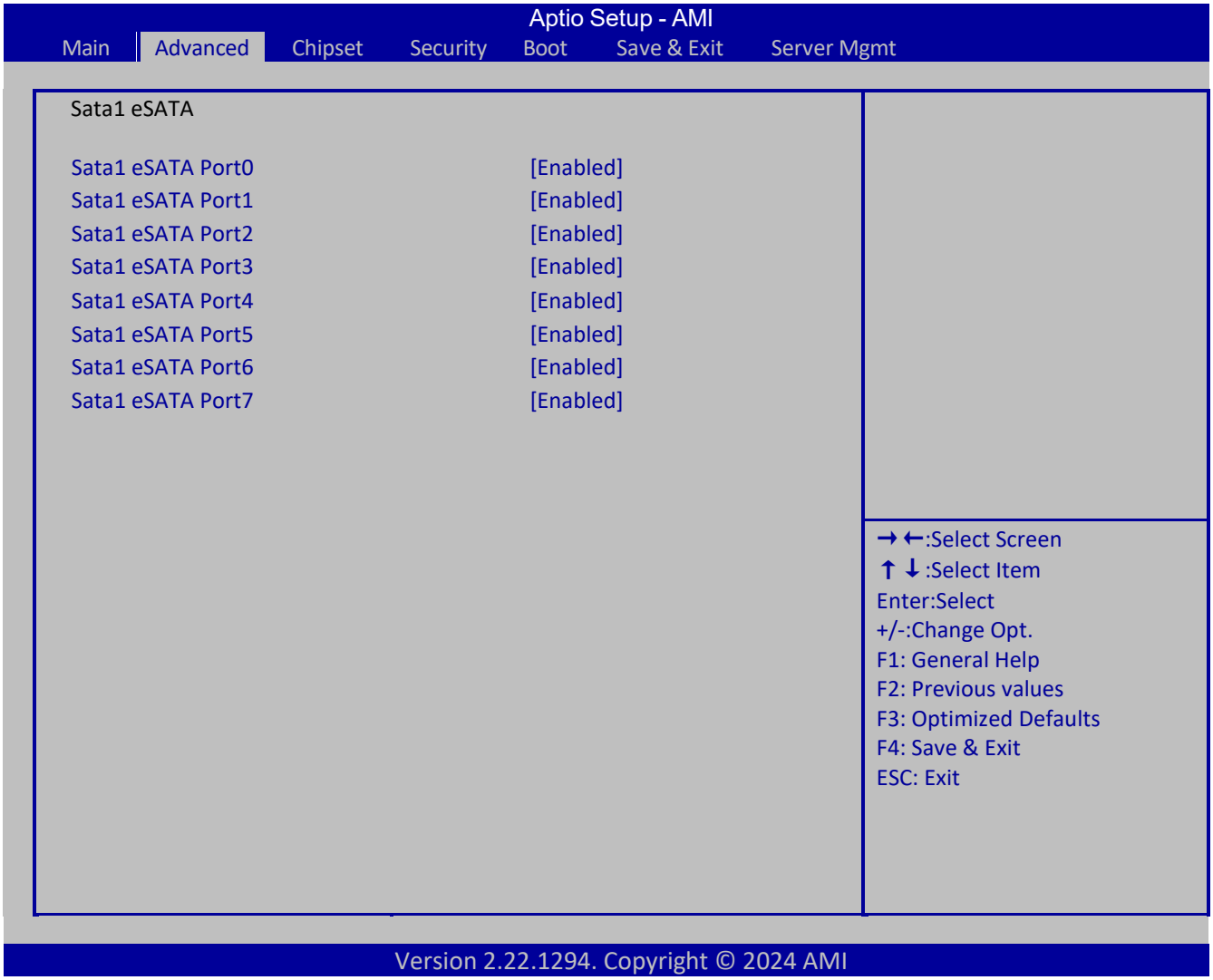
7.2.4.5.2.1.2.1 Sata0 eSATA



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

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

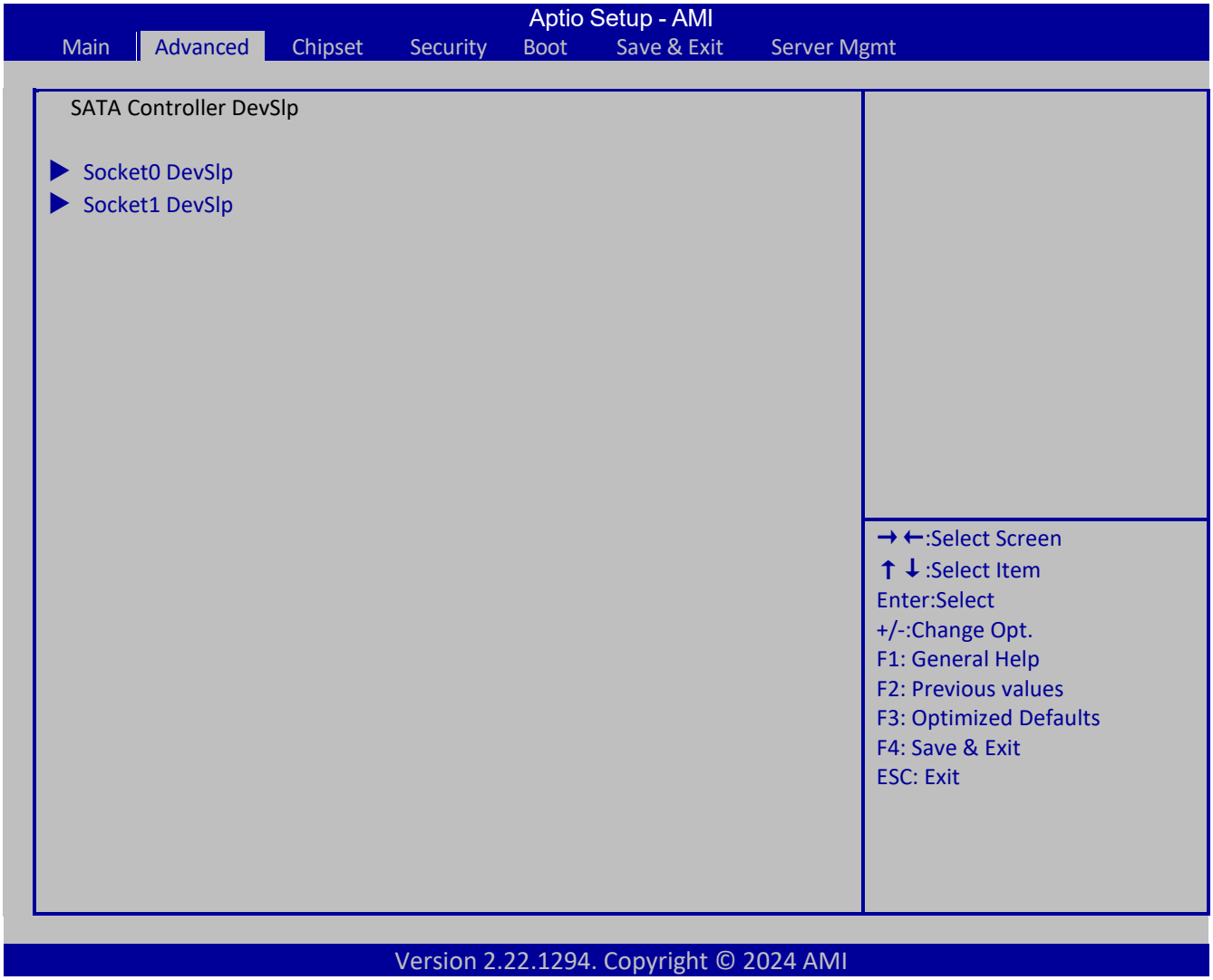
7.2.4.5.2.1.2.2 Sata1 eSATA



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

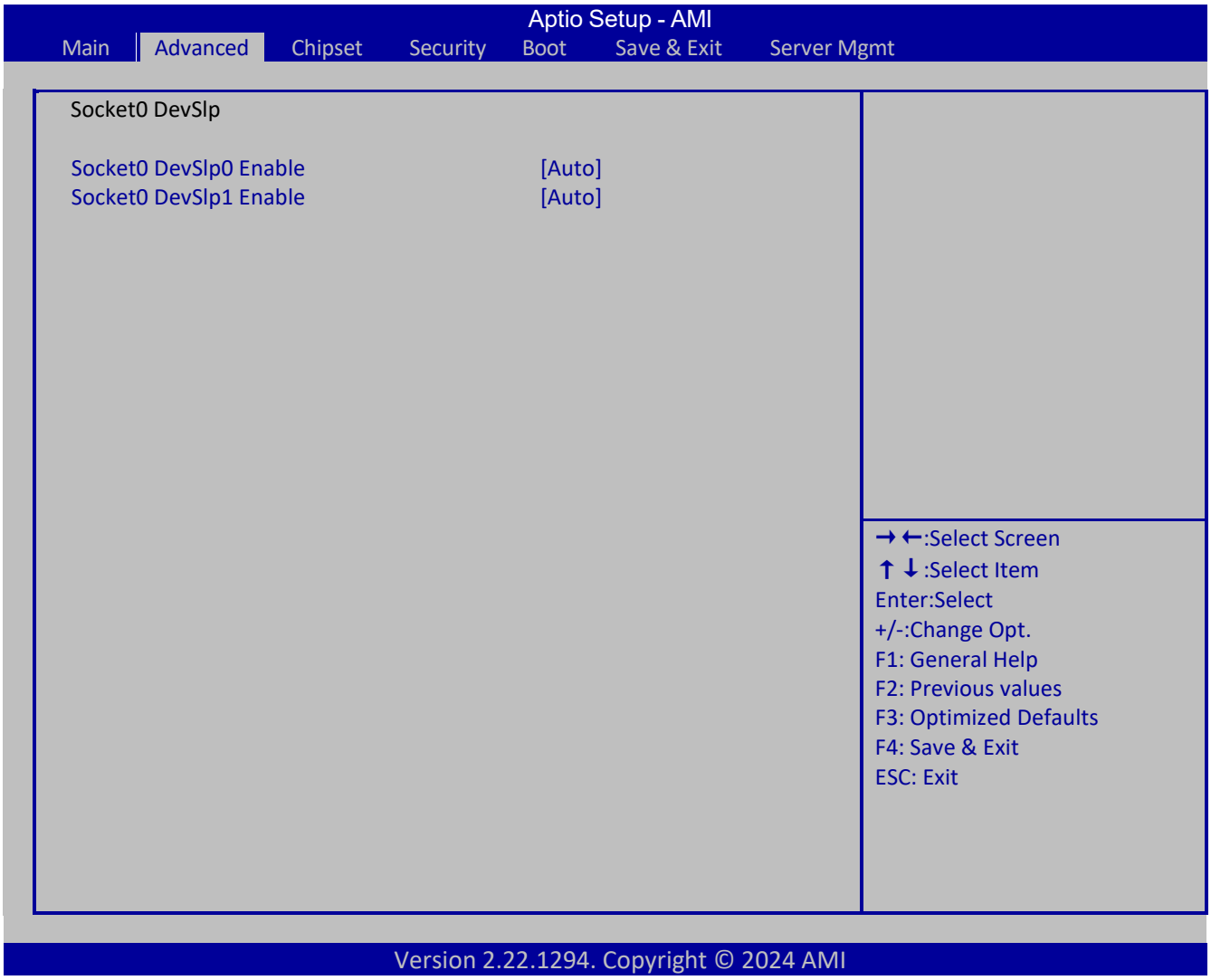
Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller eSATA \ Sata1 eSATA		
Menu Fields	**Settings**	**Comments**
Sata1 eSATA Port2	[Disabled] [Enabled] **[Auto]**	External SATA Port support
Sata1 eSATA Port3	[Disabled] [Enabled] **[Auto]**	External SATA Port support
Sata1 eSATA Port4	[Disabled] [Enabled] **[Auto]**	External SATA Port support
Sata1 eSATA Port5	[Disabled] [Enabled] **[Auto]**	External SATA Port support
Sata1 eSATA Port6	[Disabled] [Enabled] **[Auto]**	External SATA Port support
Sata1 eSATA Port7	[Disabled] [Enabled] **[Auto]**	External SATA Port support

7.2.4.5.2.1.3 SATA Controller DevSlp



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

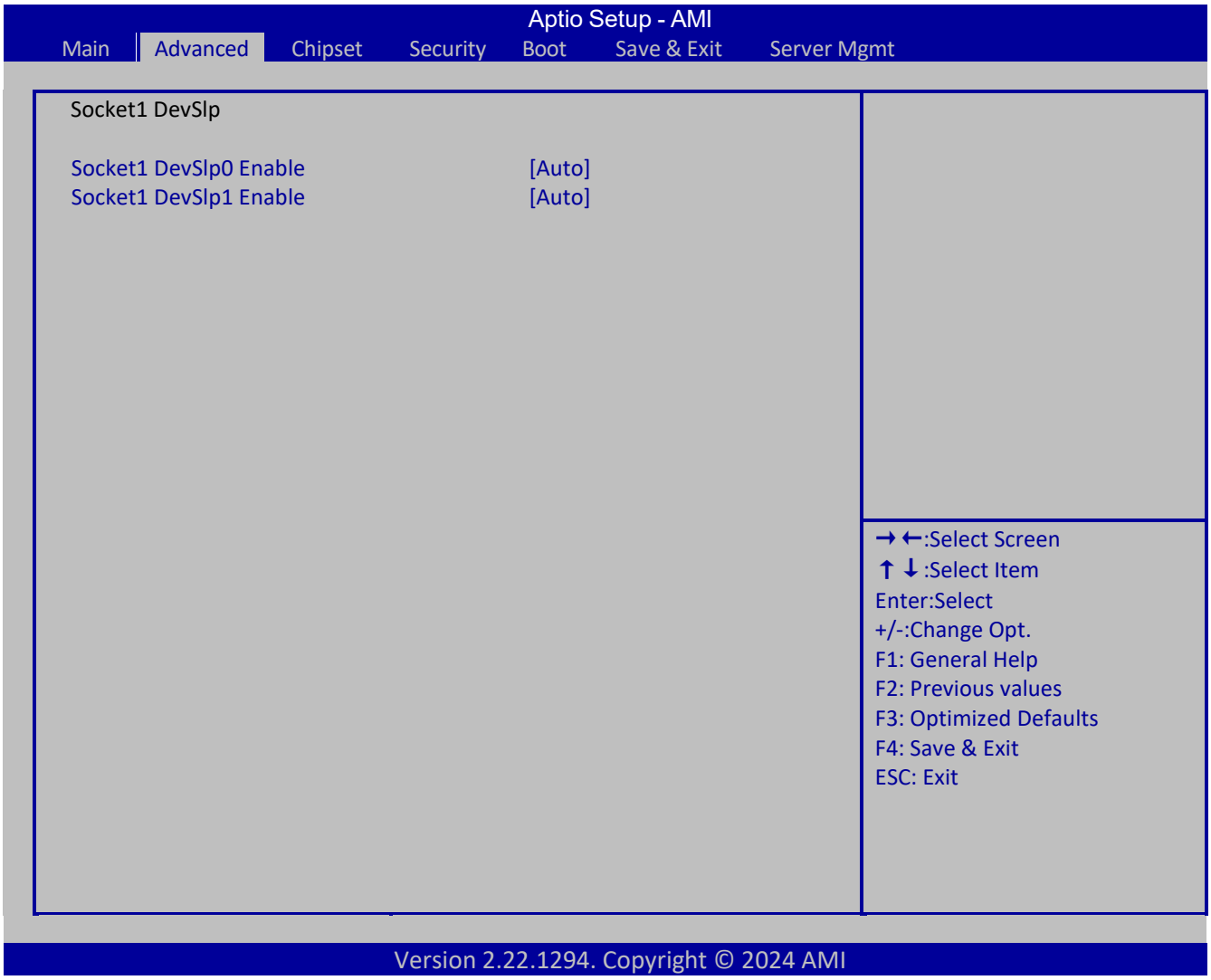
7.2.4.5.2.1.3.1 Soctet0 DevSlp



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

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller DevSlp \ Socket0 Devslp		
Menu Fields	**Settings**	**Comments**
		Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.

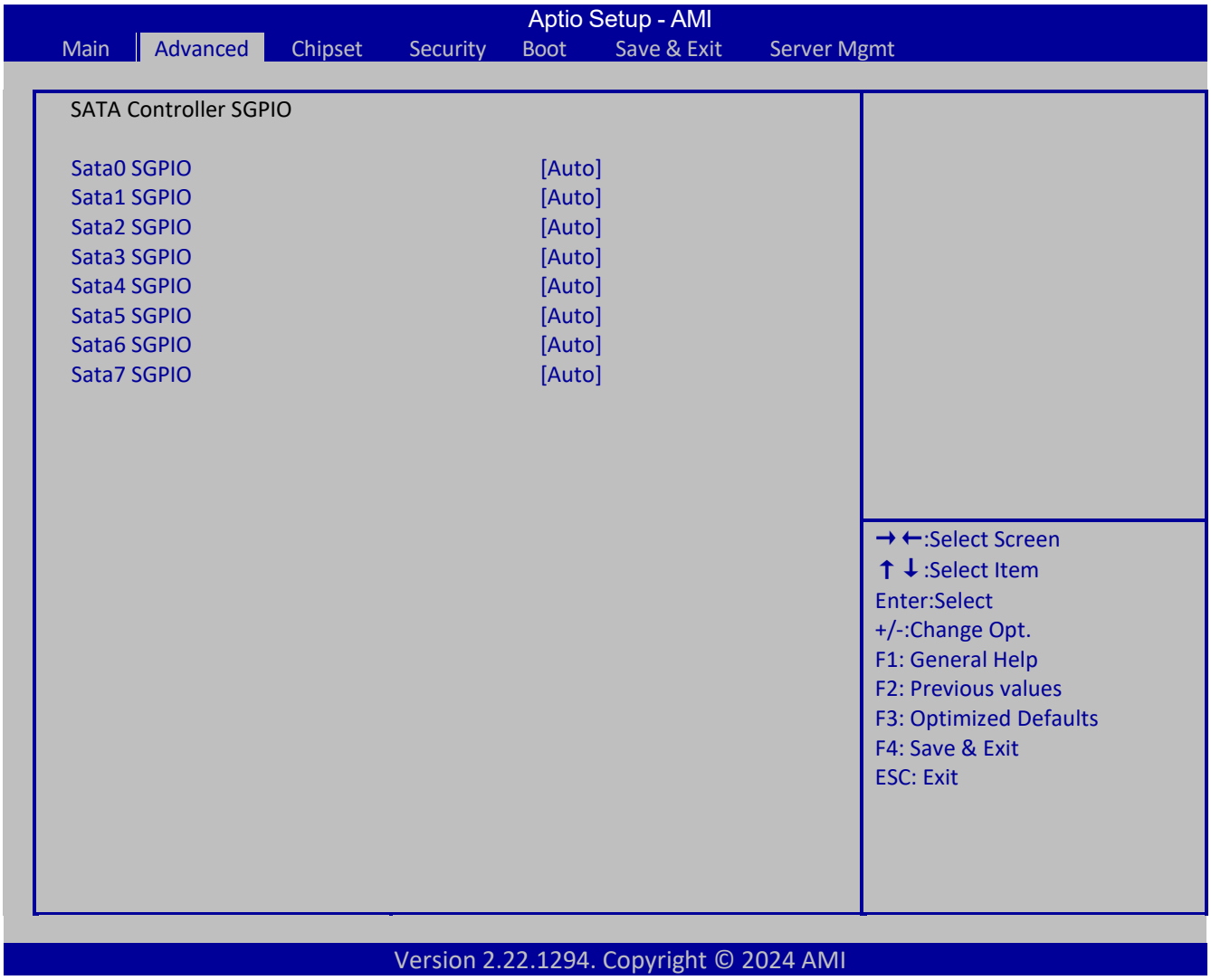
7.2.4.5.2.1.3.2 Soctet1 DevSlp



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

Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller DevSlp \ Socket1 Devslp		
Menu Fields	**Settings**	**Comments**
		Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.

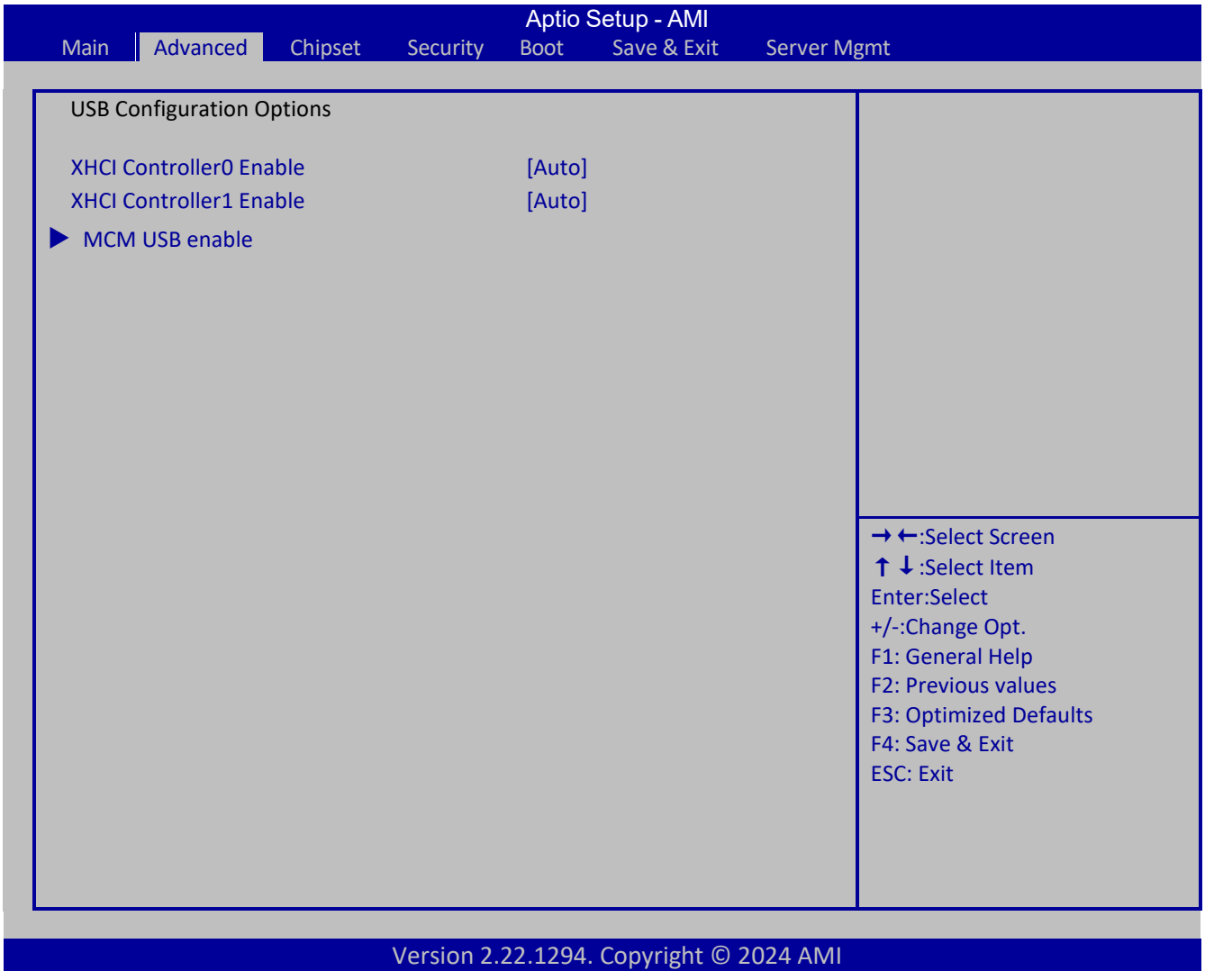
7.2.4.5.2.1.4 SATA Controller SGPIO



Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller SGPIO		
Menu Fields	**Settings**	**Comments**
Sata0 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata0
Sata1 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata1
Sata2 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata2

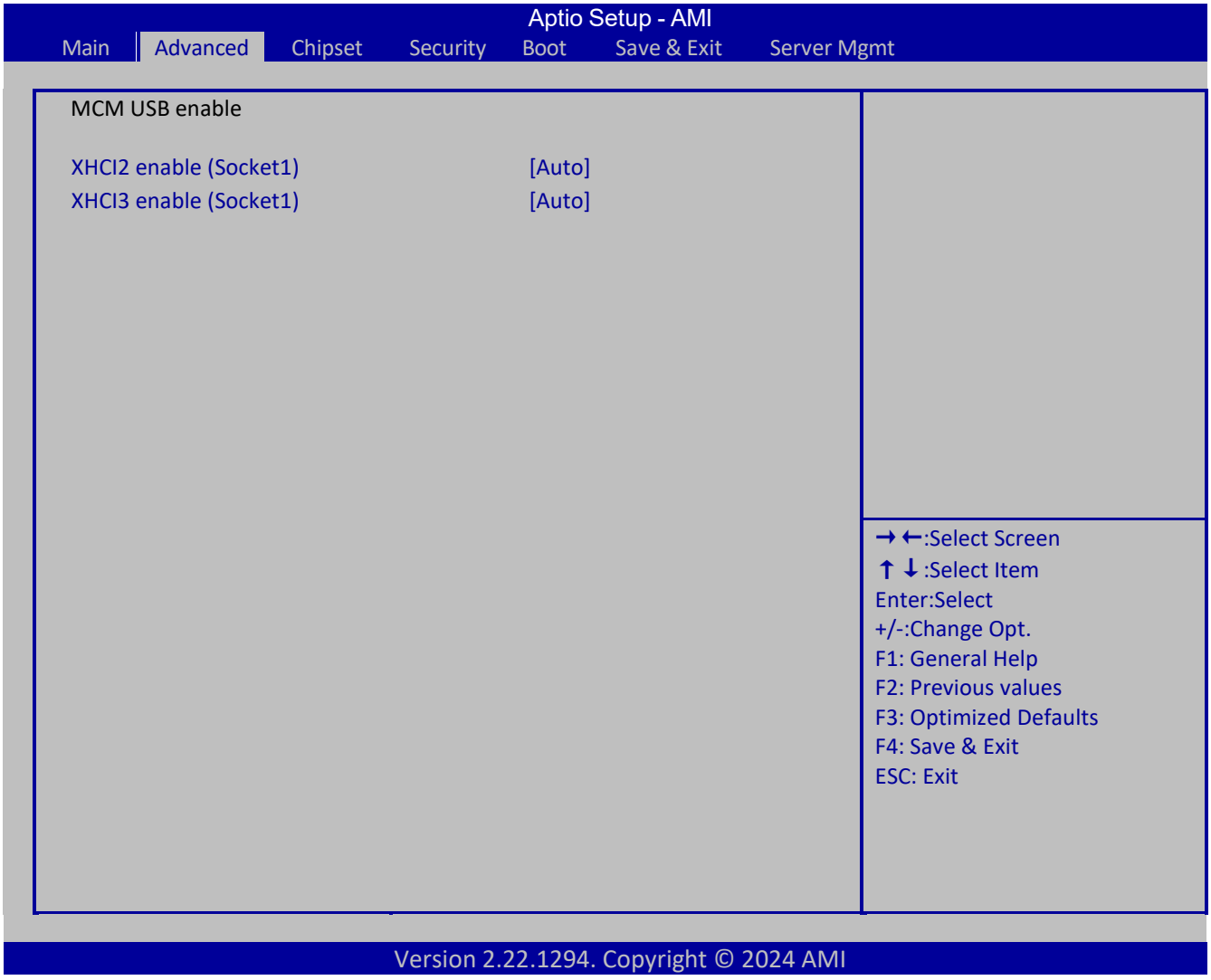
Advanced \ AMD CBS \ FCH Common Options \ SATA Configuration Options\ SATA Controller Options \SATA Controller SGPIO		
Menu Fields	**Settings**	**Comments**
Sata3 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata3
Sata4 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata4 (Socket1)
Sata5 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata5 (Socket1)
Sata6 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata6 (Socket1)
Sata7 SGPIO	[Disabled] [Enabled] **[Auto]**	Enable or Disable SataSgpio on Sata7 (Socket1)

7.2.4.5.3 USB Configuration Options



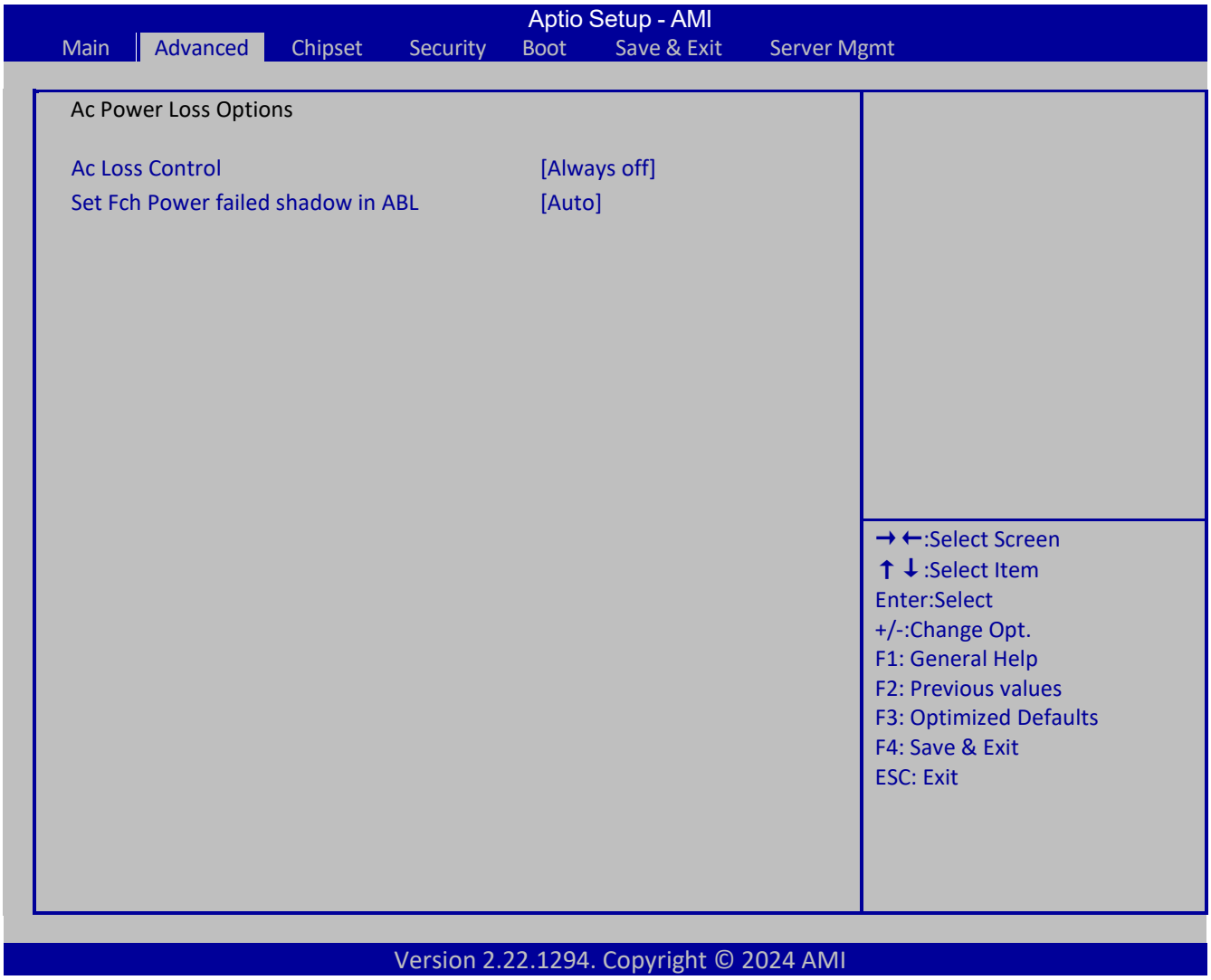
**Advanced \ AMD CBS \ FCH Common Options ** USB Configuration Options		
Menu Fields	**Settings**	**Comments**
XHCI Controller0 Enable	[Enabled] [Disabled] **[Auto]**	Enable or disable USB3 controller
XHCI Controller1 Enable	[Enabled] [Disabled] **[Auto]**	Enable or disable USB3 controller
MCM USB enable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

7.2.4.5.3.1 MCM USB enable



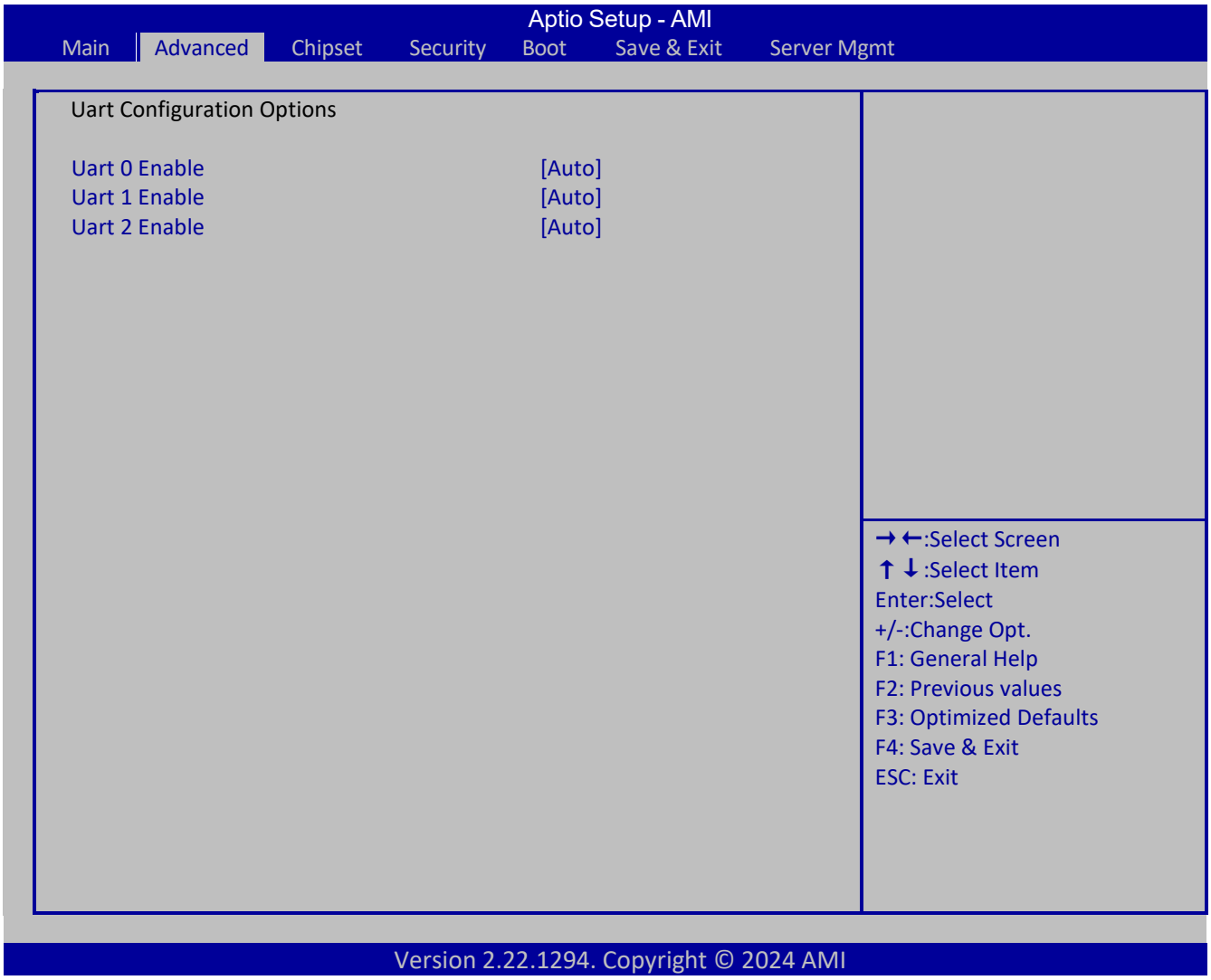
**Advanced \ AMD CBS \ FCH Common Options ** USB Configuration Options \ MCM USB enable		
Menu Fields	**Settings**	**Comments**
XHCI2 enable (Socket1)	[Enabled] [Disabled] **[Auto]**	Enable or disable USB3 controller
XHCI3 enable (Socket1)	[Enabled] [Disabled] **[Auto]**	Enable or disable USB3 controller

7.2.4.5.4 AC Power Loss Options



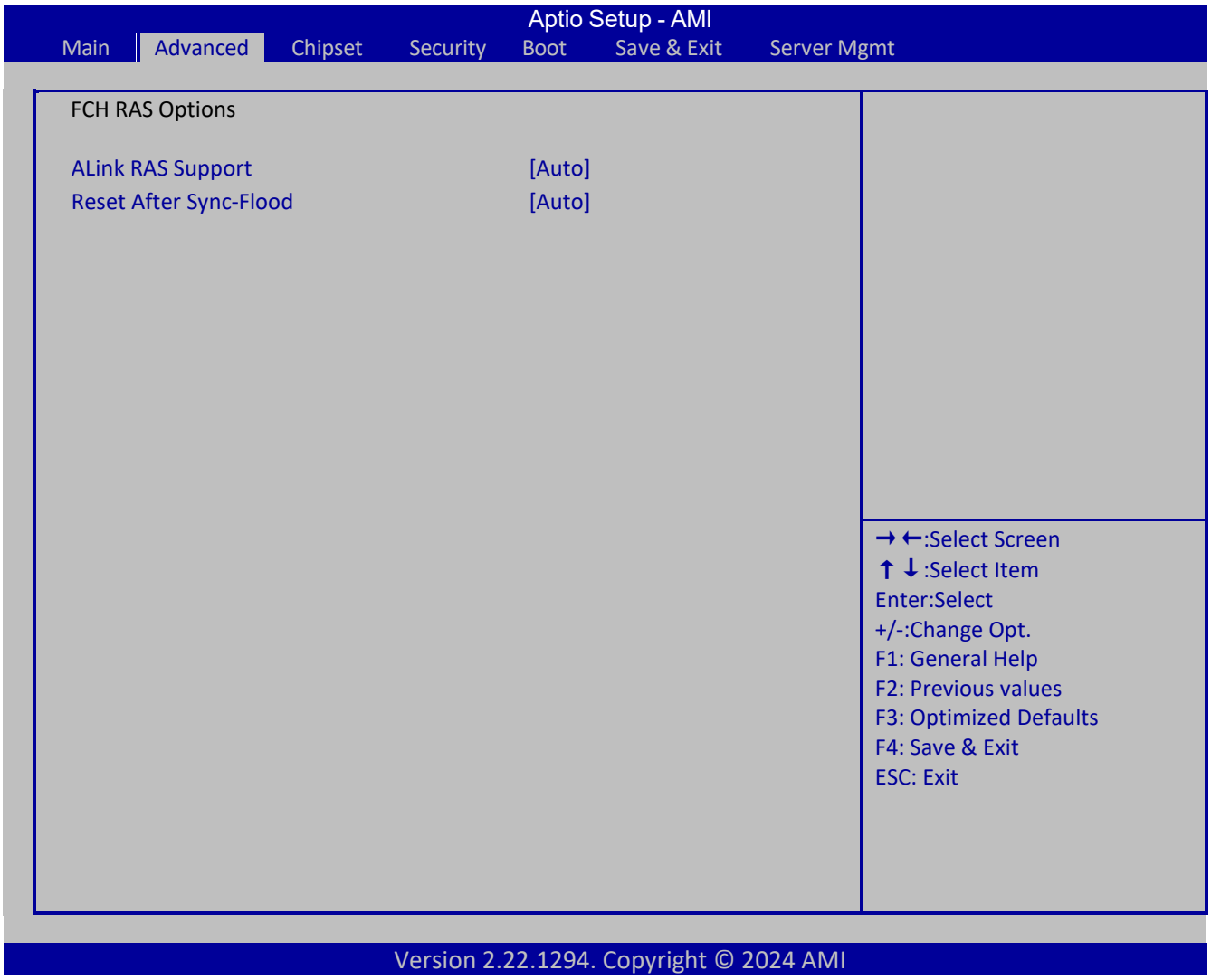
Advanced \ AMD CBS \ FCH Common Options \ USB Configuration Options \ Ac Power Loss Options		
Menu Fields	**Settings**	**Comments**
Ac Loss Control	**[Always off]** [Always on] [Reserved] [Previous] [Auto]	Select Ac Loss Control Method
Set Fch Power failed shadow in ABL	[Enabled] [Disabled] **[Auto]**	

7.2.4.5.5 Uart Configuration Options



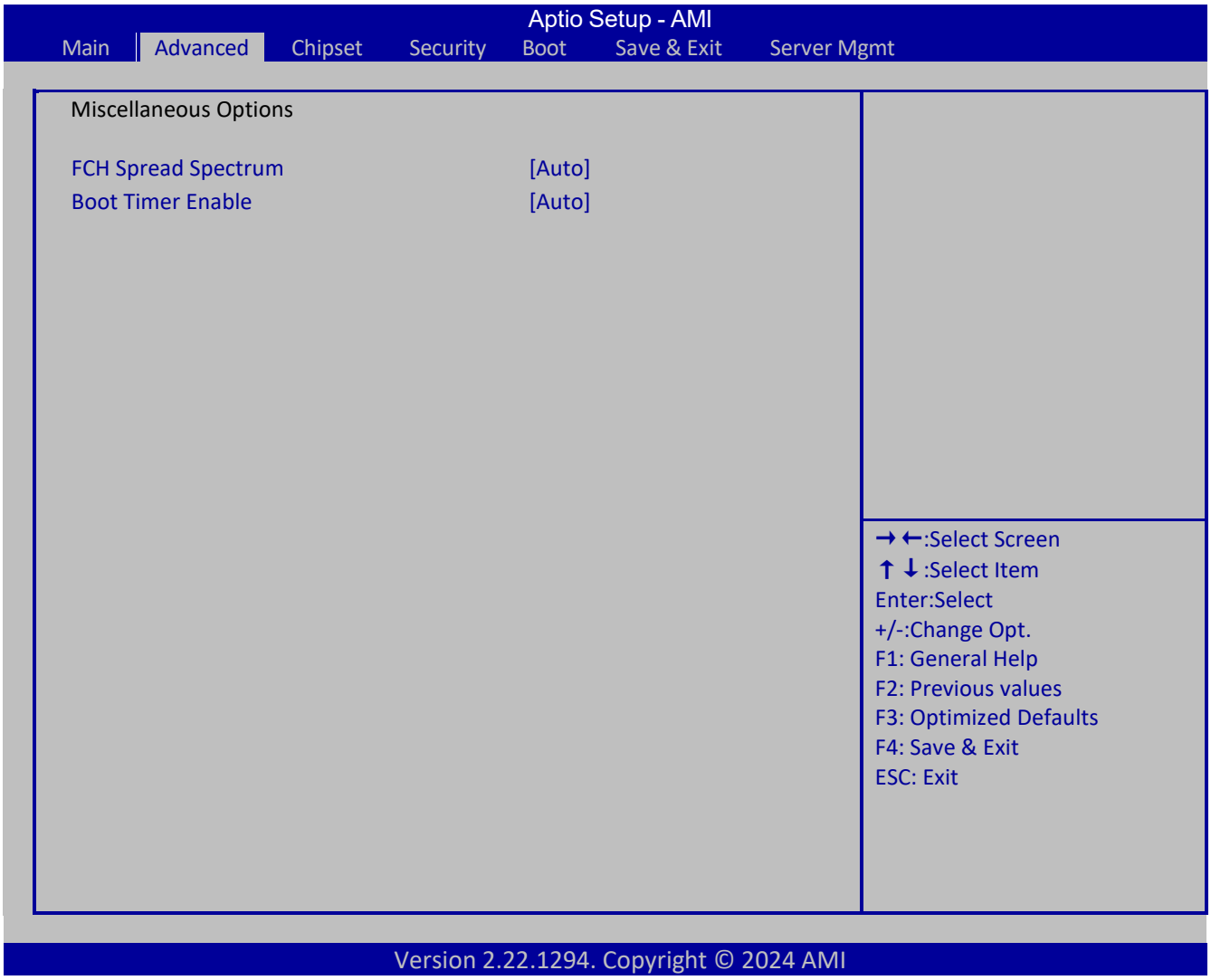
Advanced \ AMD CBS \ FCH Common Options \ Uart Configuration Options		
Menu Fields	**Settings**	**Comments**
Uart 0 Enable	[Disabled] [Enabled] **[Auto]**	Enable or disable Uart0. Uart 0 has no HW flow control if Uart 2 is enabled
Uart 1 Enable	[Disabled] [Enabled] **[Auto]**	Enable or disable Uart1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

7.2.4.5.6 FCH RAS Options



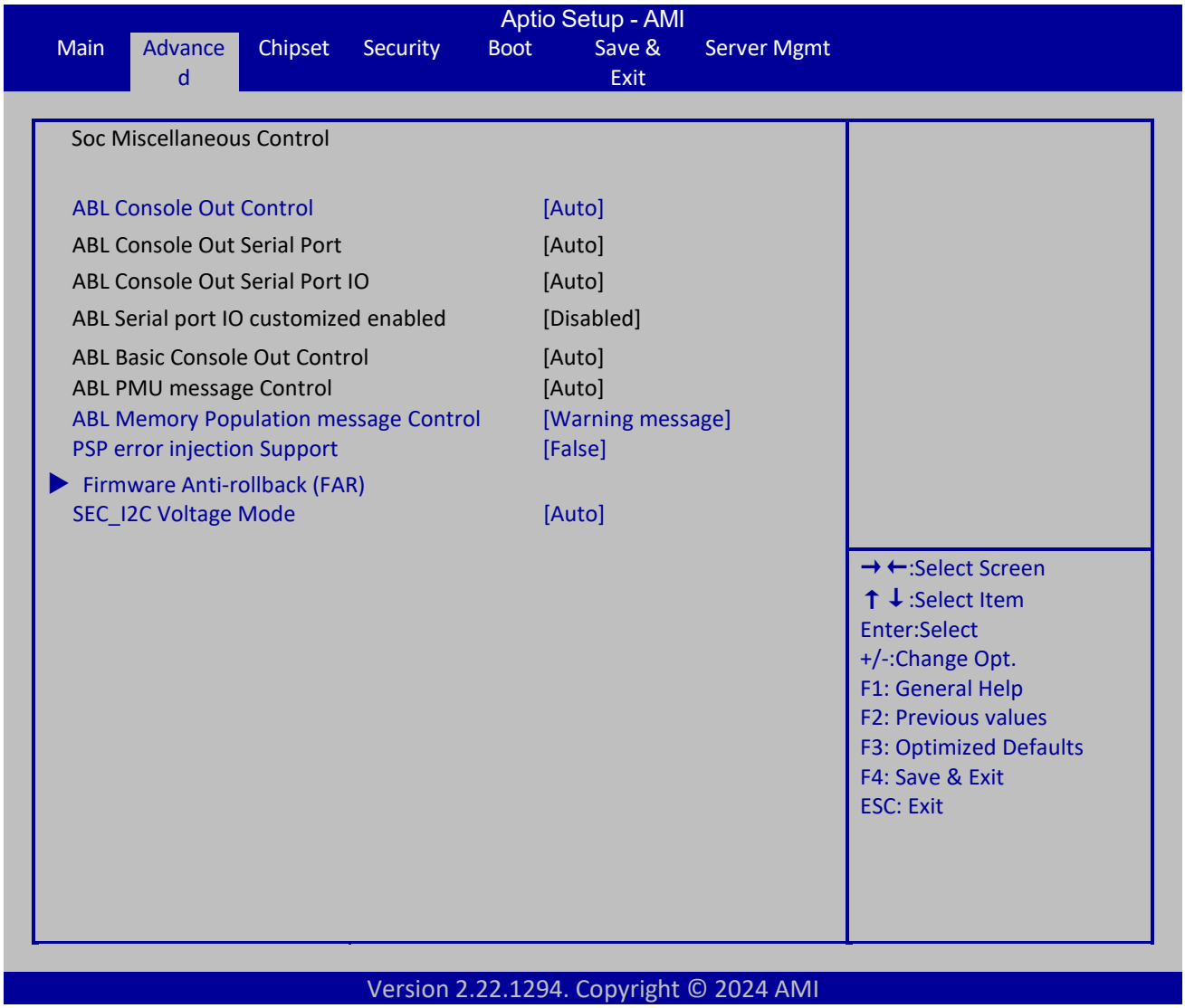
Advanced \ AMD CBS \ FCH Common Options \ FCH RAS Options		
Menu Fields	**Settings**	**Comments**
ALink RAS Support	[Disabled] [Enabled] **[Auto]**	Enable FCH A-Link parity error
Reset After Sync-Flood	[Disabled] [Enabled] **[Auto]**	Enable AB to forward downstream sync-flood message to system controller.

7.2.4.5.7 Miscellaneous Options



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

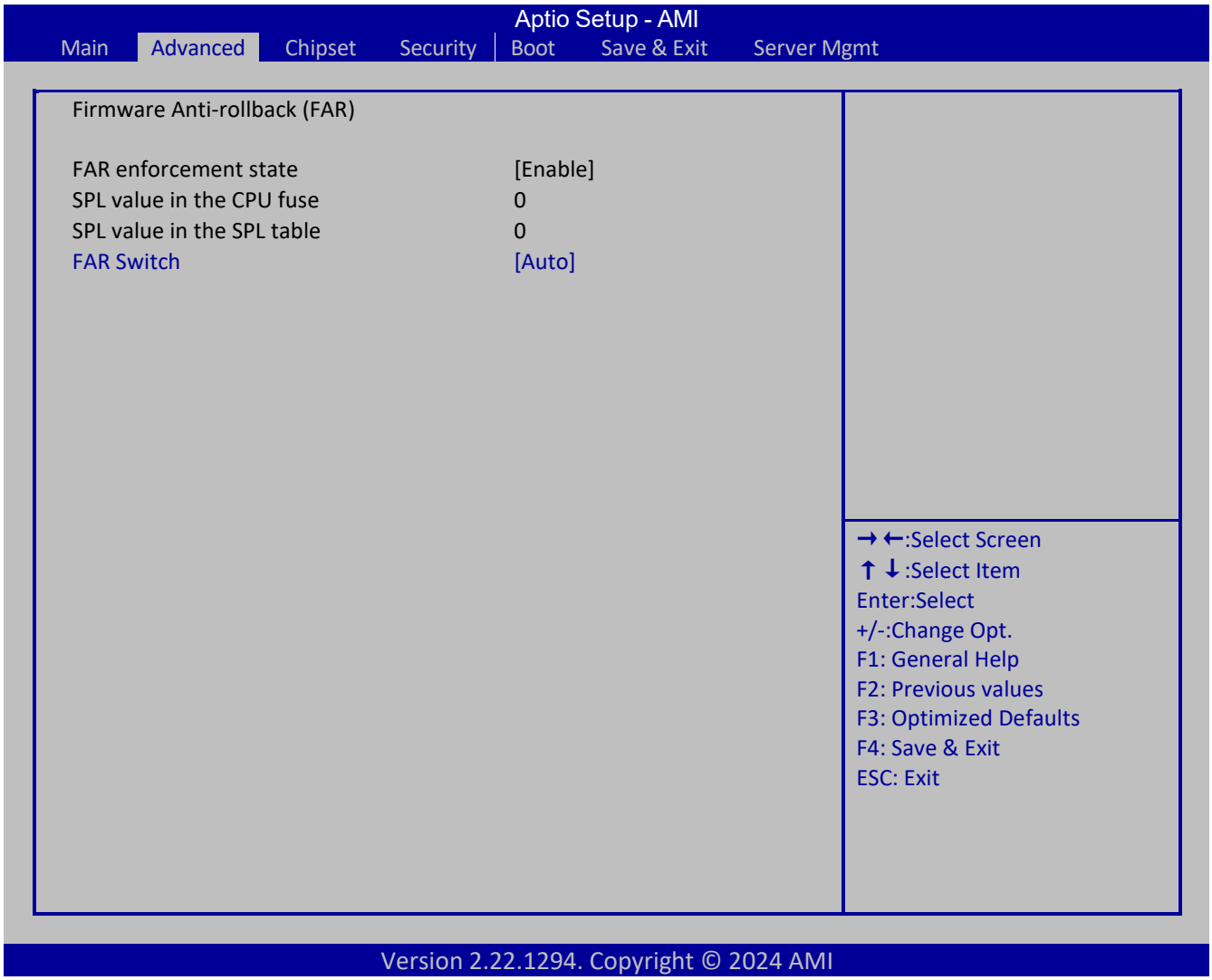
7.2.4.6 Soc Miscellaneous Control



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

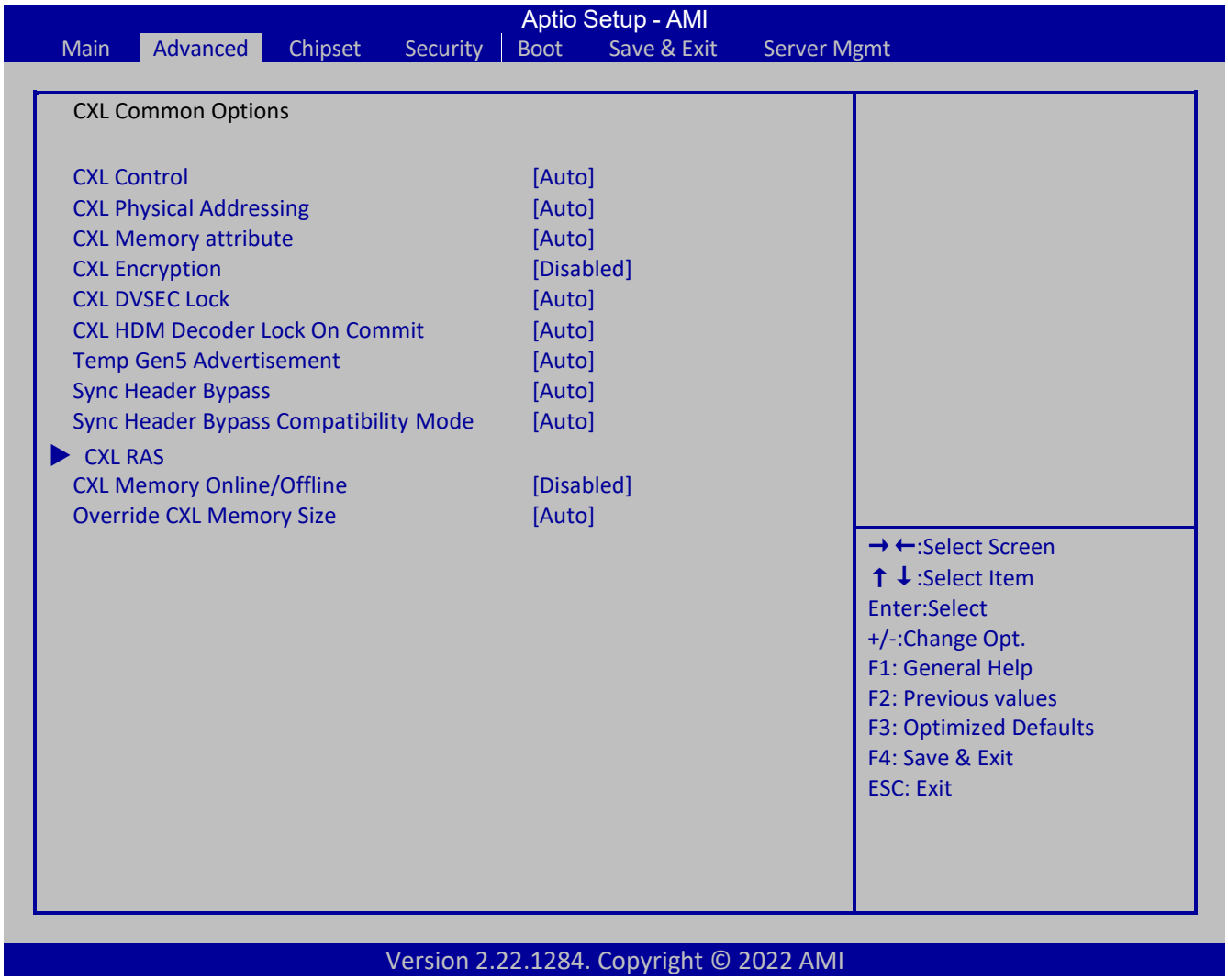
Advanced \ AMD CBS \ Soc Miscellaneous Control		
Menu Fields	**Settings**	**Comments**
		CRB only fills 0x3F8,0x2F8 in it by default.
ABL Serial port IO customized enabled	**[Disabled]** [Enabled]	Enabled: Can input IO based for ABL console out Serial Port IO by ABL. Console out Serial port IO Customized.
ABL Console out Serial Port IO Customized	**0**	0: disabled. no supported (default value). Please input your eSPI UART io based in non zero value. Also please make sure the selected eSPI IO base and length has been filled in APCB_FCH_TYPE_ESPI_INIT or APCB_FCH_TYPE_ESPI1_INIT EspiInitConfiguration table.
ABL Basic Console Out Control	[Disable] [Enable] **[Auto]**	Enable: Enable Basic ConsoleOut Function for ABL. Disable: Disable Basic ConsoleOut Function for ABL. Auto: Keep default behavior.
ABL PMU message Control	[Detailed debug message] [Coarse debug message] [Stage completion] **[Auto]**	To control the total number of PMU debug messages. Several major controls are listed below: 1. Detailed debug messages (e.g. Eye delays) 2. Coarse debug messages (e.g. rank information) 3. Stage completion
ABL Memory Population message Control	**[Warning message]** [Fatal error]	Non-Recommended configurations may be functional but may not be validated by AMD. Select 'warning message': To show warning messages if Memory channel configuration does Not follow SP5 Memory Population Guidelines. 'Fatal error': To show the messages and halt the system.
PSP error injection Support	**[False]** [True]	Enable EINJ support
Firmware Anti-rollback (FAR)	Selects sub-menu.	
SEC_I2C Voltage Mode	**[Auto]** [1.8 V] [1.1 V]	This option allows to select SEC I2C voltage. Valid options: - Auto (Leave it to silicon initial value) - 1.8V 1.1V

7.2.4.6.1 Firmware Anti-rollback (FAR)



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

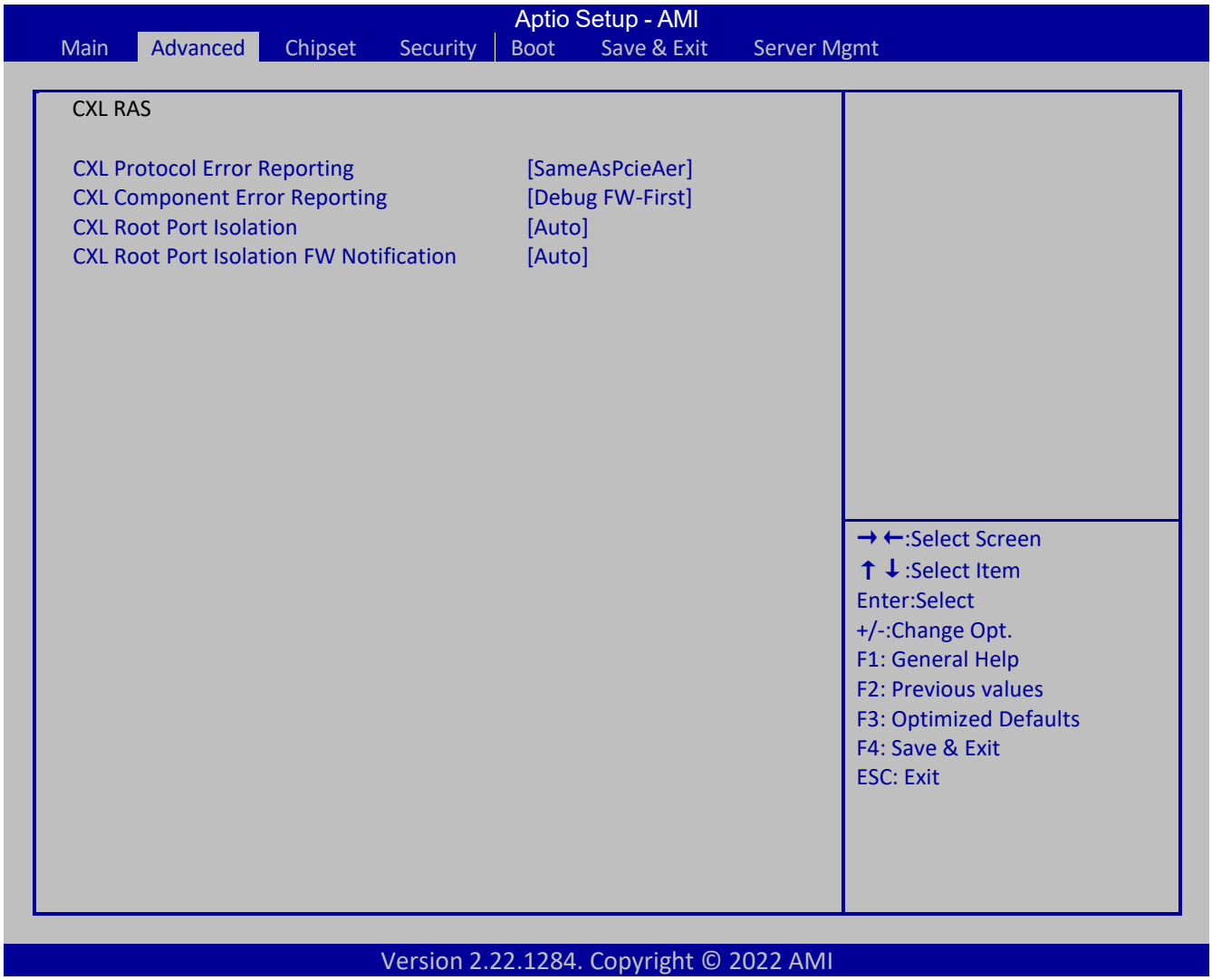
7.2.4.7 CXL Common Options



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

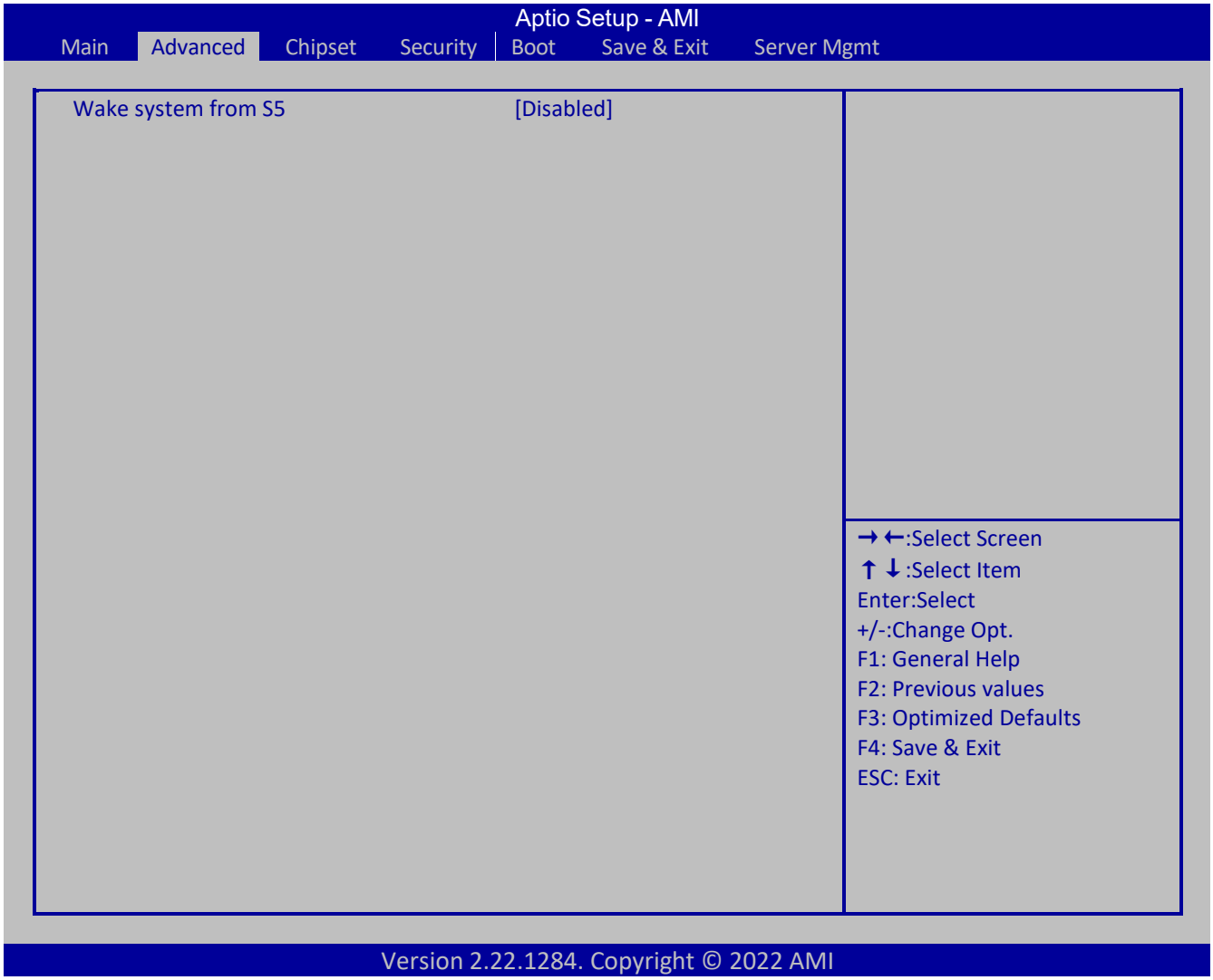
Advanced \ AMD CBS \ CXL Common Options		
Menu Fields	**Settings**	**Comments**
Temp Gen5 Advertisement	[Disable] [Enable] **[Auto]**	Temp Gen5 Advertisement for Alternate Protocol
Sync Header Bypass	**[Auto]** [Enabled] [Disabled]	Enable/Disable Sync Header Bypass
Sync Header Bypass Compatibility Mode	**[Auto]** [Enabled] [Disabled]	Enable/Disable Sync Header Bypass Compatibility Mode
CXL RAS	Selects sub-menu.	
CXL Memory Online/Offline	**[Disabled]** [Enabled]	All 4 Plink slots support memory online/offline Only slot4 of Amber supports hot plug CXL memory interleaving automatically disabled globally when this CBS is enabled
Override CXL Memory Size	[32GB] [64GB] [128GB] **[Auto]**	No help String

7.2.4.7.1 CXL RAS



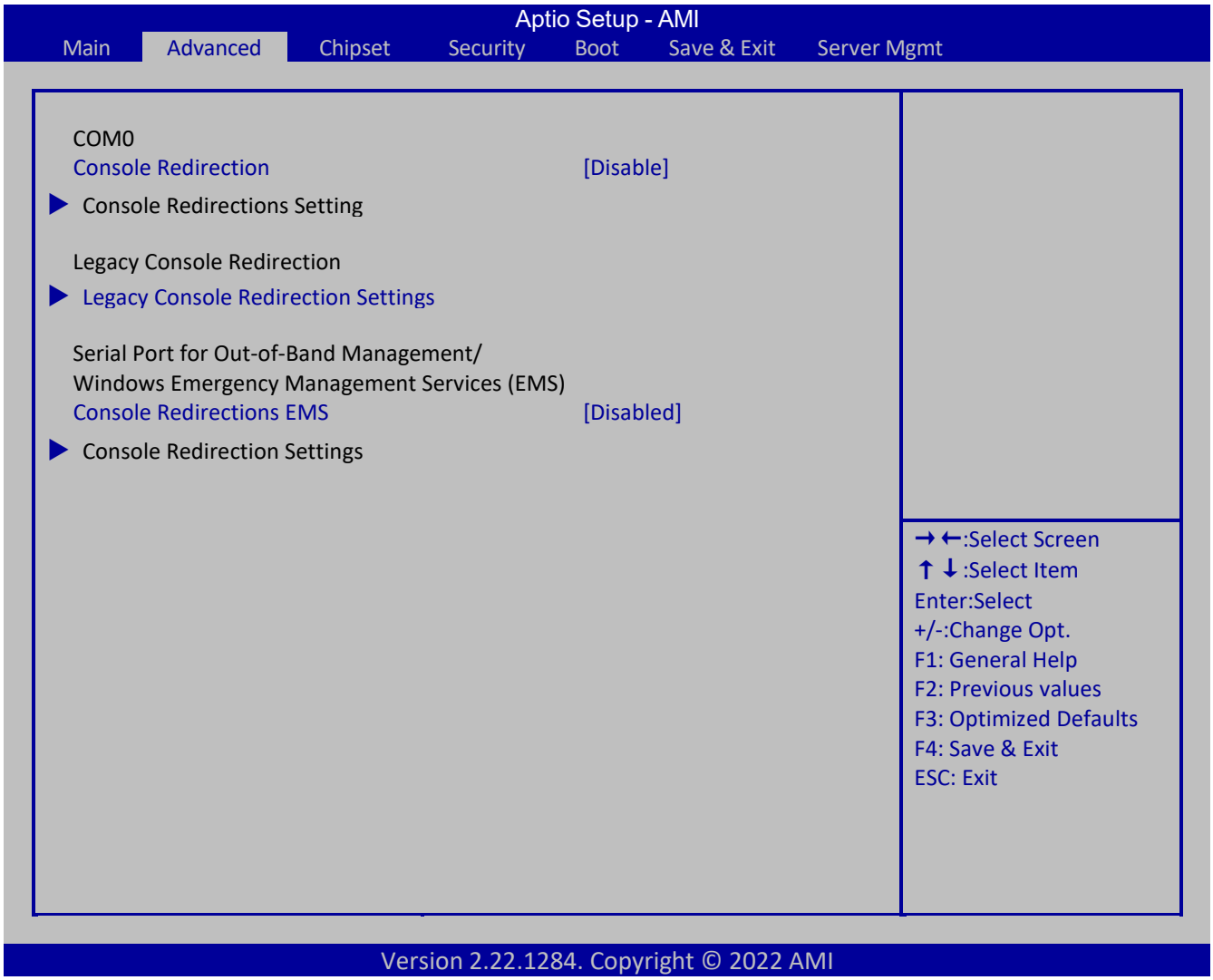
Advanced \ AMD CBS \ CXL Common Options \CXL RAS		
Menu Fields	**Settings**	**Comments**
CXL Protocol Error Reporting	[Disabled] **[SameAsPcieAer]** [ForceAerFWFirstIfCxlPresent]	Configure CXL Protocol Error reporting mechanism
CXL Component Error Reporting	[Allow OS-First] [Force FW-First] **[Debug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

7.2.5 S5 RTC Wake Settings



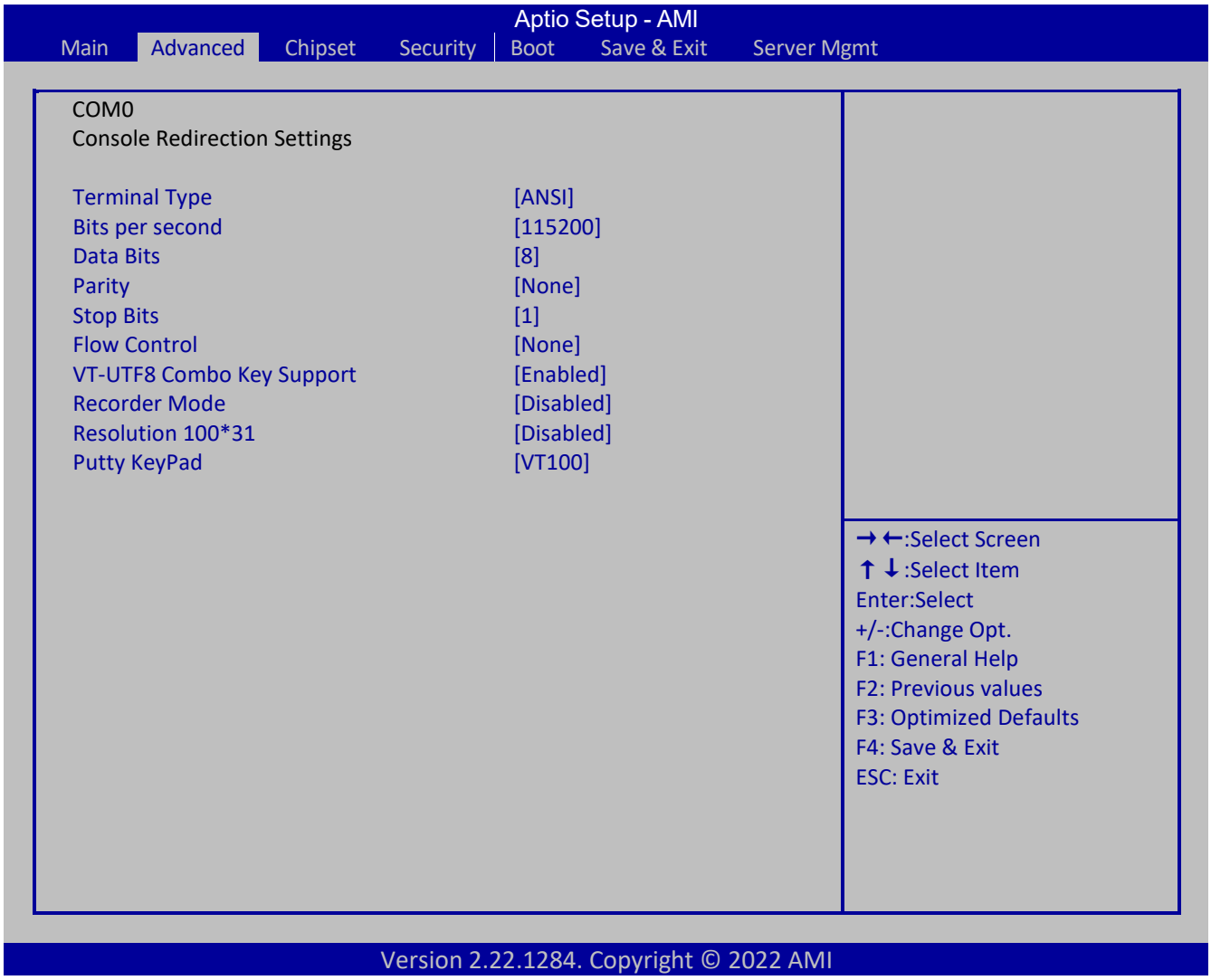
Advanced \ S5 RTC Wake Settings		
Menu Fields	**Settings**	**Comments**
Wake system from S5	**[Disabled]** [Fixed Time] [Dynamic Time]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time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

7.2.6 Serial Port Console Redirection



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

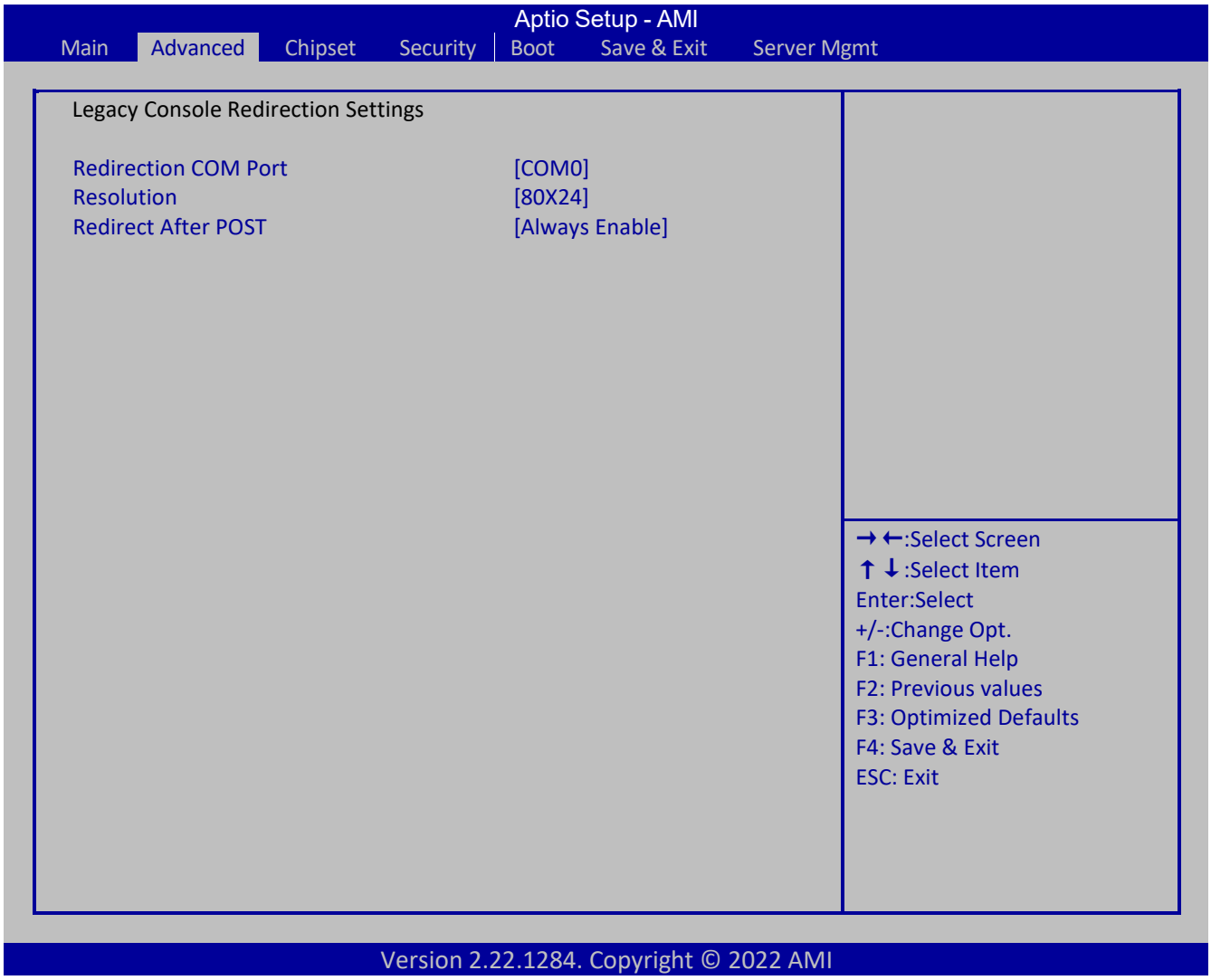
7.2.6.1 COM0 Console Redirection Setting



Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	**Settings**	**Comments**
Terminal Type	[VT100] [VT100Plus] [VT-UTF8] **[ANSI]**	Terminal Type for Redirection Via AMI Debugger. Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	[9600] [19200] [38400] [57600] **[115200]** [230400] [460800] [921600]	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	[7] **[8]**	Data Bits

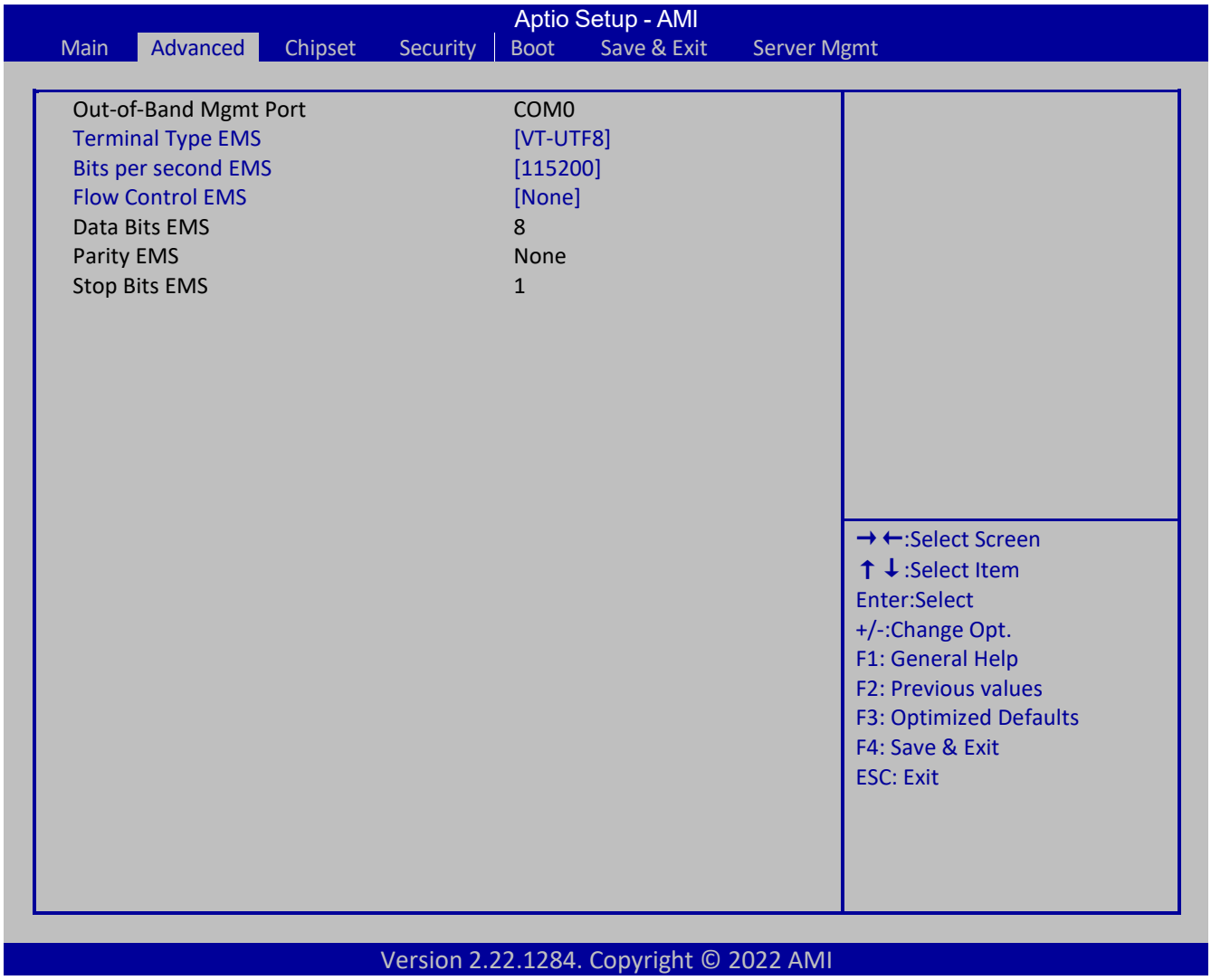
Advanced \ Serial Port Console Redirection \ Console Redirection Settings		
Menu Fields	**Settings**	**Comments**
Parity	**[None]** [Even] [Odd] [Mark] [Space]	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. 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	**[1]** [2]	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**[None]** [Hardware RTS/CTS]	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTFB Combo Key Support	[Disabled] **[Enabled]**	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	**[Disabled]** [Enabled]	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100*31	**[Disabled]** [Enabled]	Enables or disables extended terminal resolution
Putty KeyPad	**[VT100]** [LINUX] [XTERMR6] [SC0] [ESCN] [VT400]	Select FunctionKey and KeyPad on Putty.

7.2.6.2 Legacy Console Redirection Settings



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

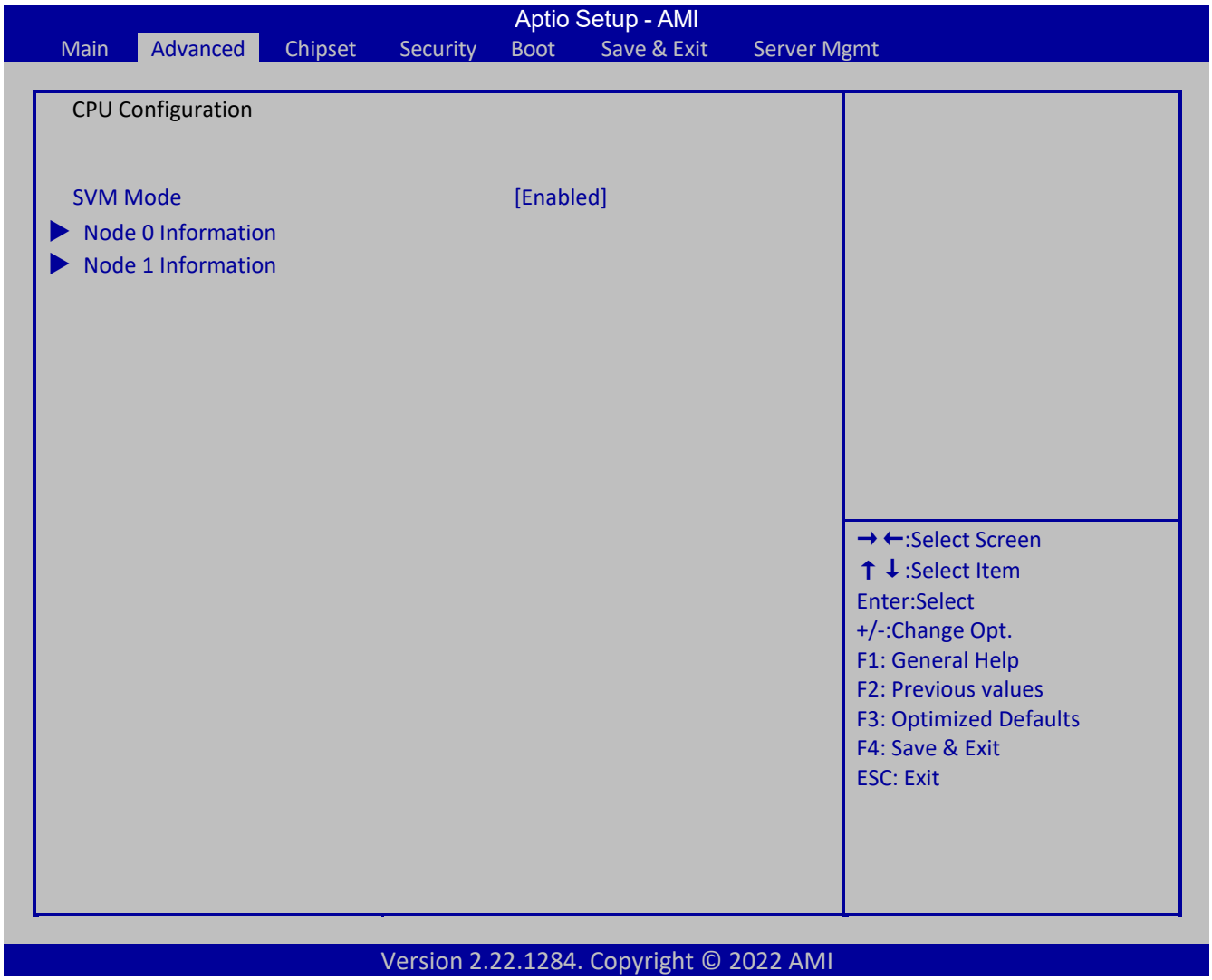
7.2.6.3 Console Redirection Setting



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

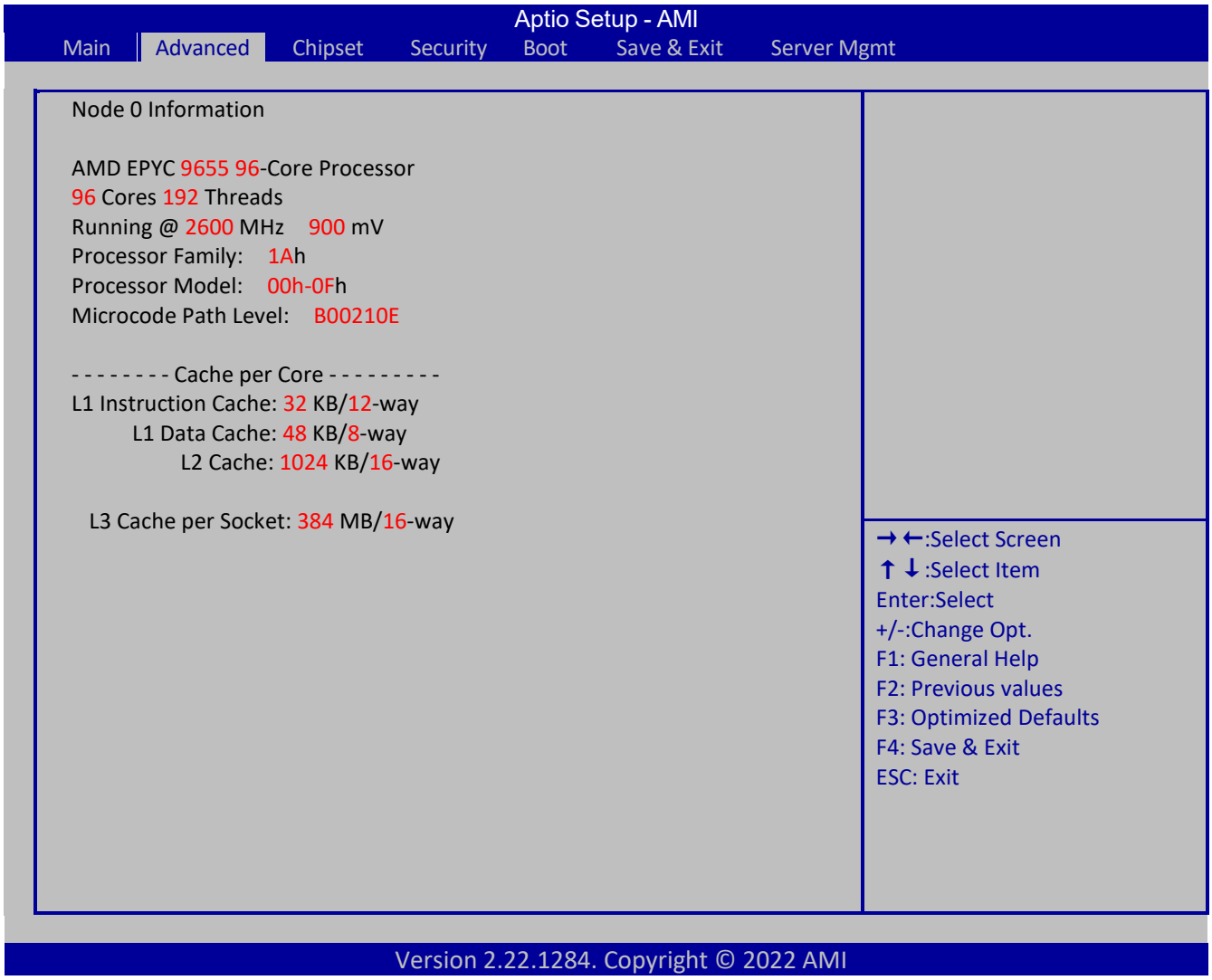
Parity EMS	None	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity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

7.2.7 CPU Configuration

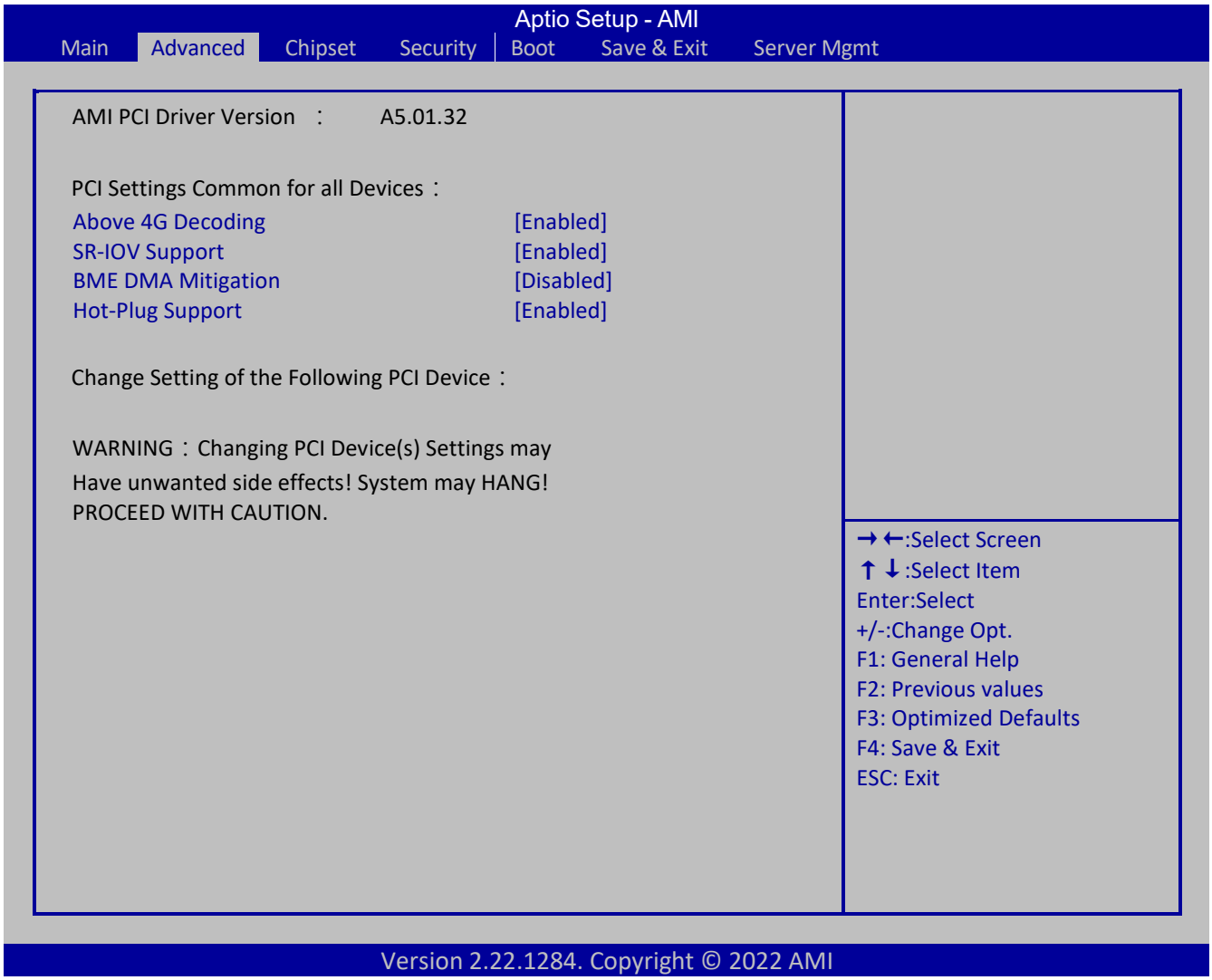


Advanced \ CPU Configuration		
Menu Fields	**Settings**	**Comments**
SVM Mode	[Disabled] **[Enabled]**	Enable/disable CPU Virtualization
Node 0 Information	Selects sub-menu	
Node 1 Information	Selects sub-menu	

7.2.7.1 Node 0 Information

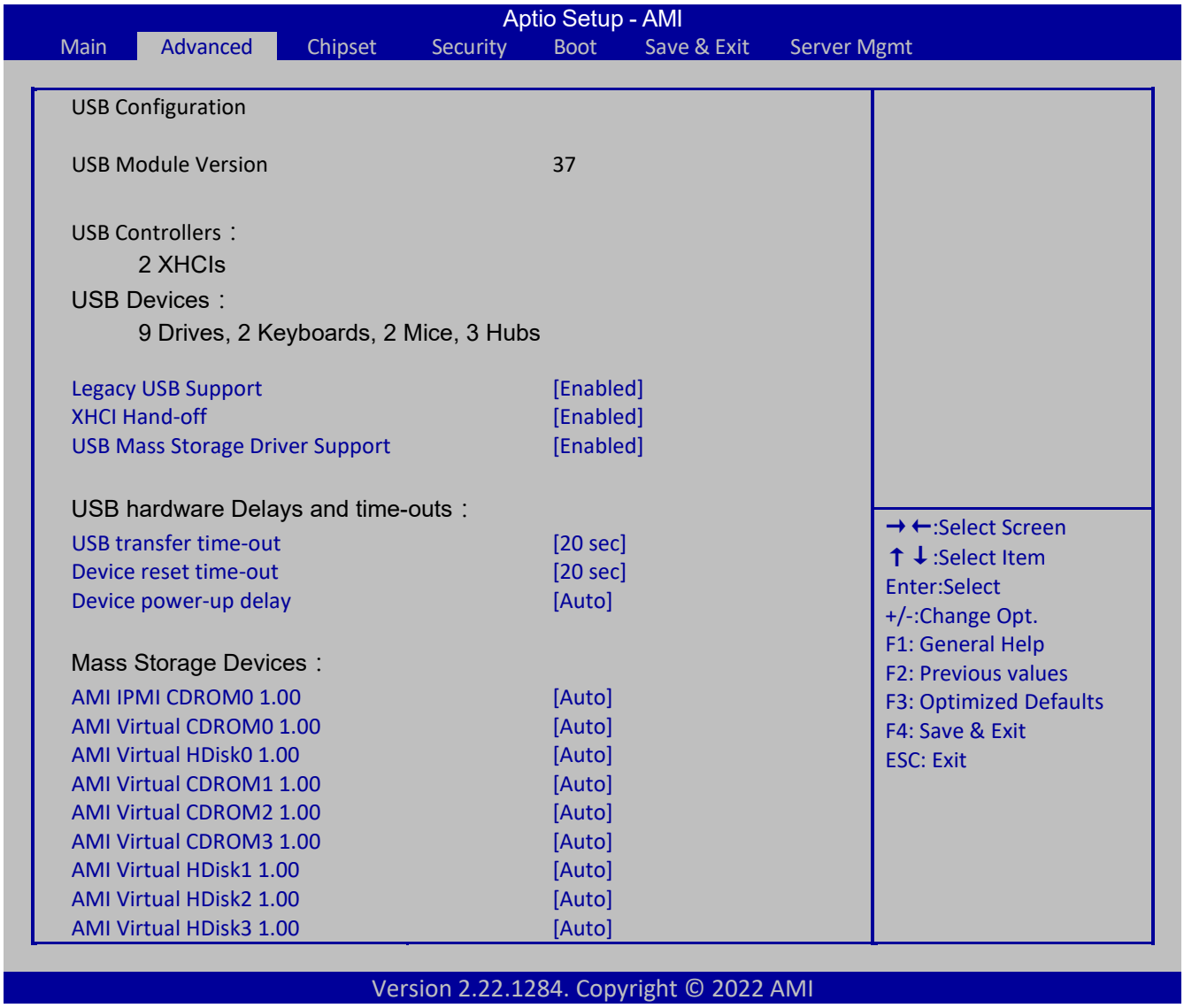


7.2.8 PCI Subsystem Settings



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

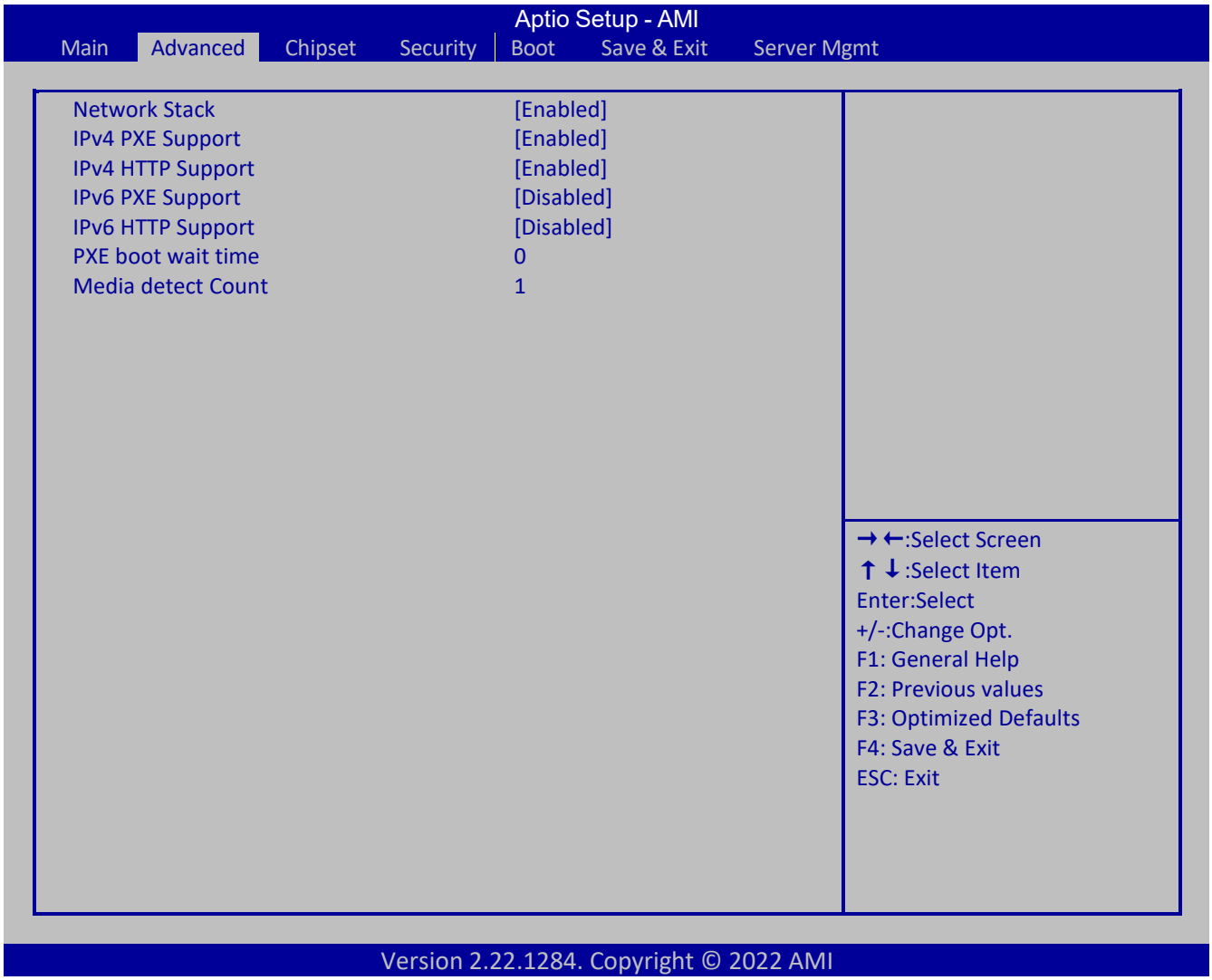
7.2.9 USB Configuration



Advanced \ USB Configuration		
Menu Fields	**Settings**	**Comments**
Legacy USB Support	**[Enabled]** [Disabled] [Auto]	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	**[Enabled]** [Disabled]	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	[Disabled] **[Enabled]**	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	[1 sec] [5 sec] [10 sec] **[20 sec]**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	[10 sec] **[20 sec]** [30 sec] [40 sec]	USB mass storage device Start Unit command time-out.

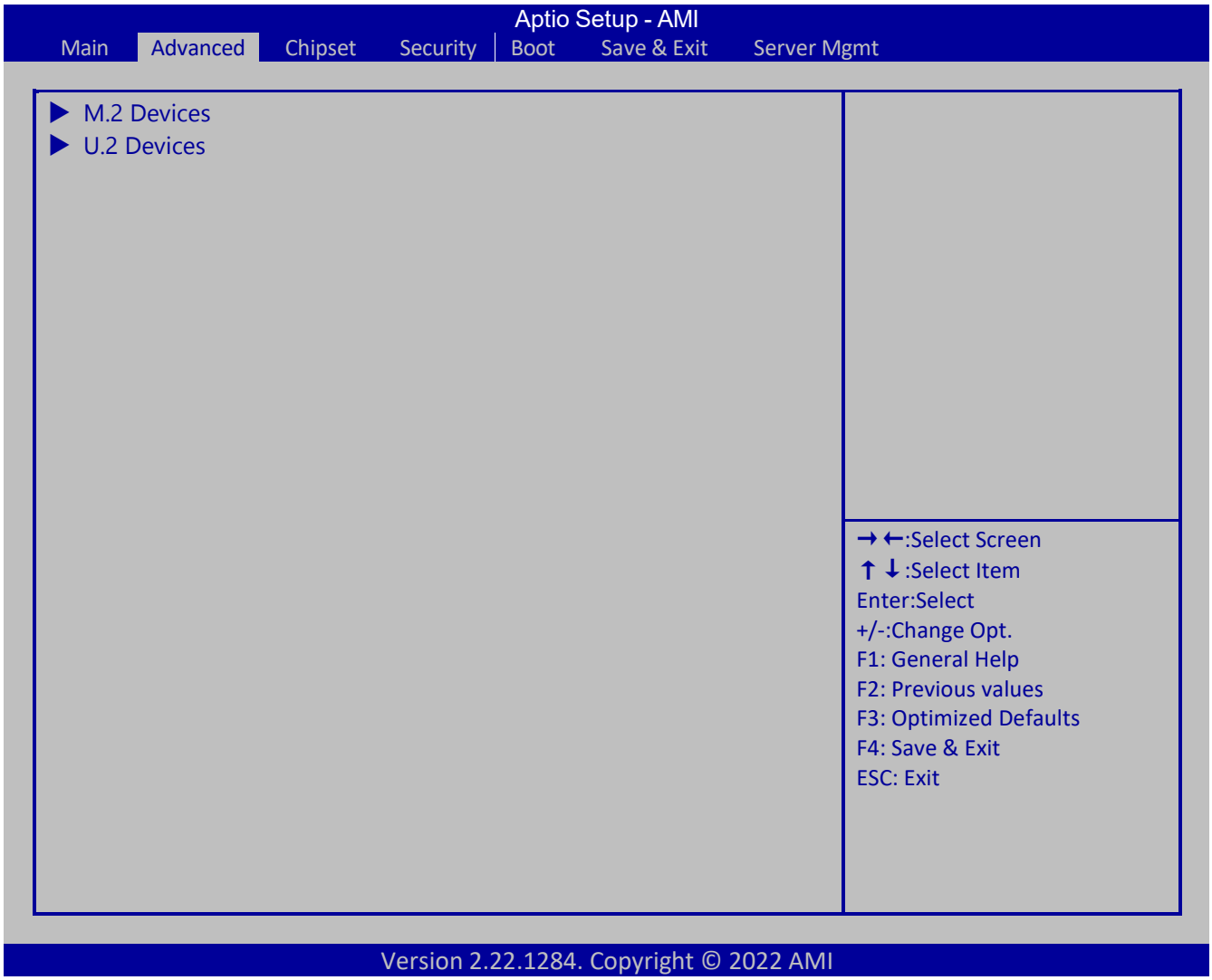
Advanced \ USB Configuration		
Menu Fields	**Settings**	**Comments**
Device power-up delay	**[Auto]** [Manual]	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub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

7.2.10 Network Stack Configuration



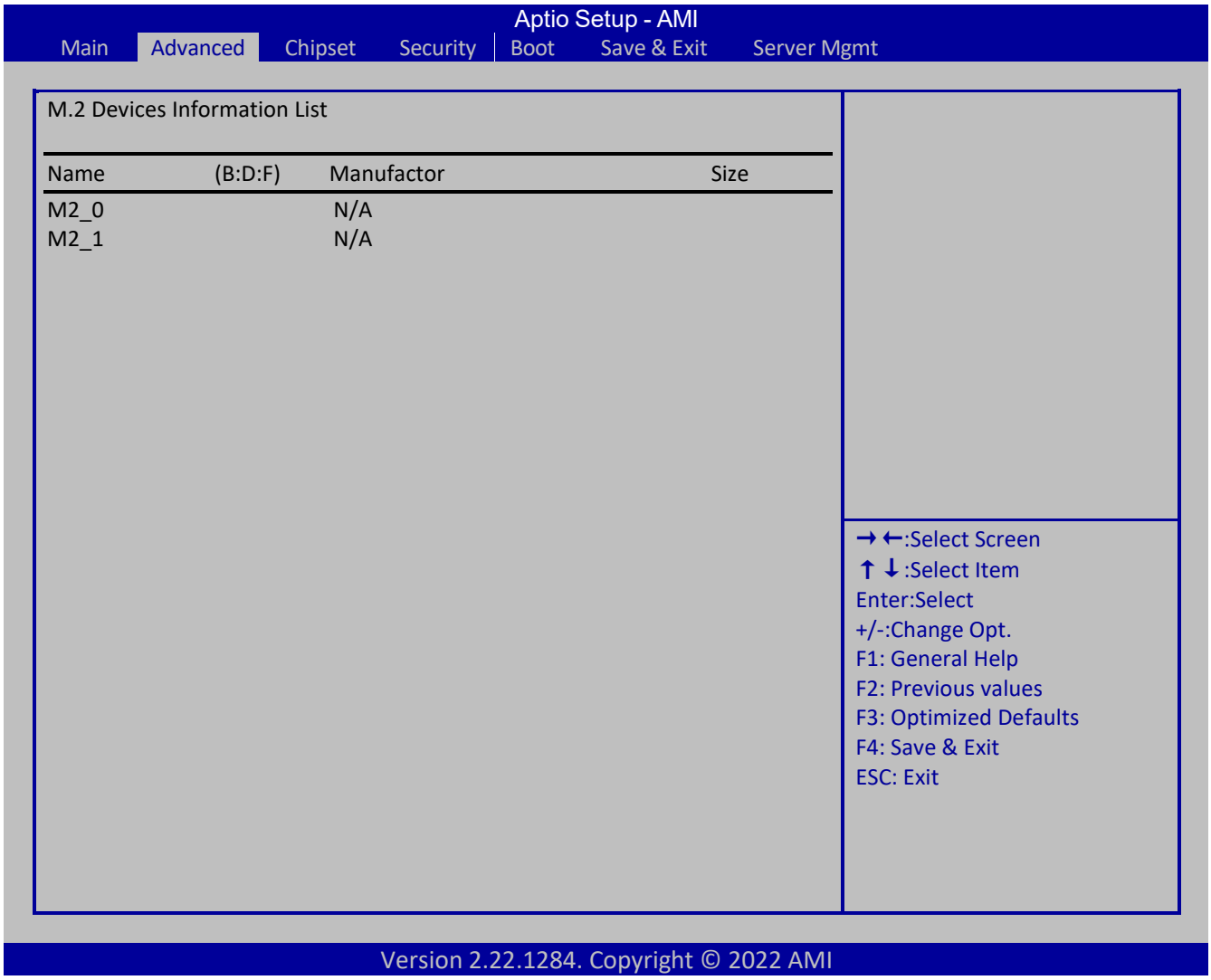
Advanced \ Network Stack Configuration		
Menu Fields	**Settings**	**Comments**
Network Stack	[Disabled] **[Enabled]**	Enable/Disable UEFI Network Stack
IPv4 PXE Support	[Disabled] **[Enabled]**	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support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

7.2.11 NVME Configuration

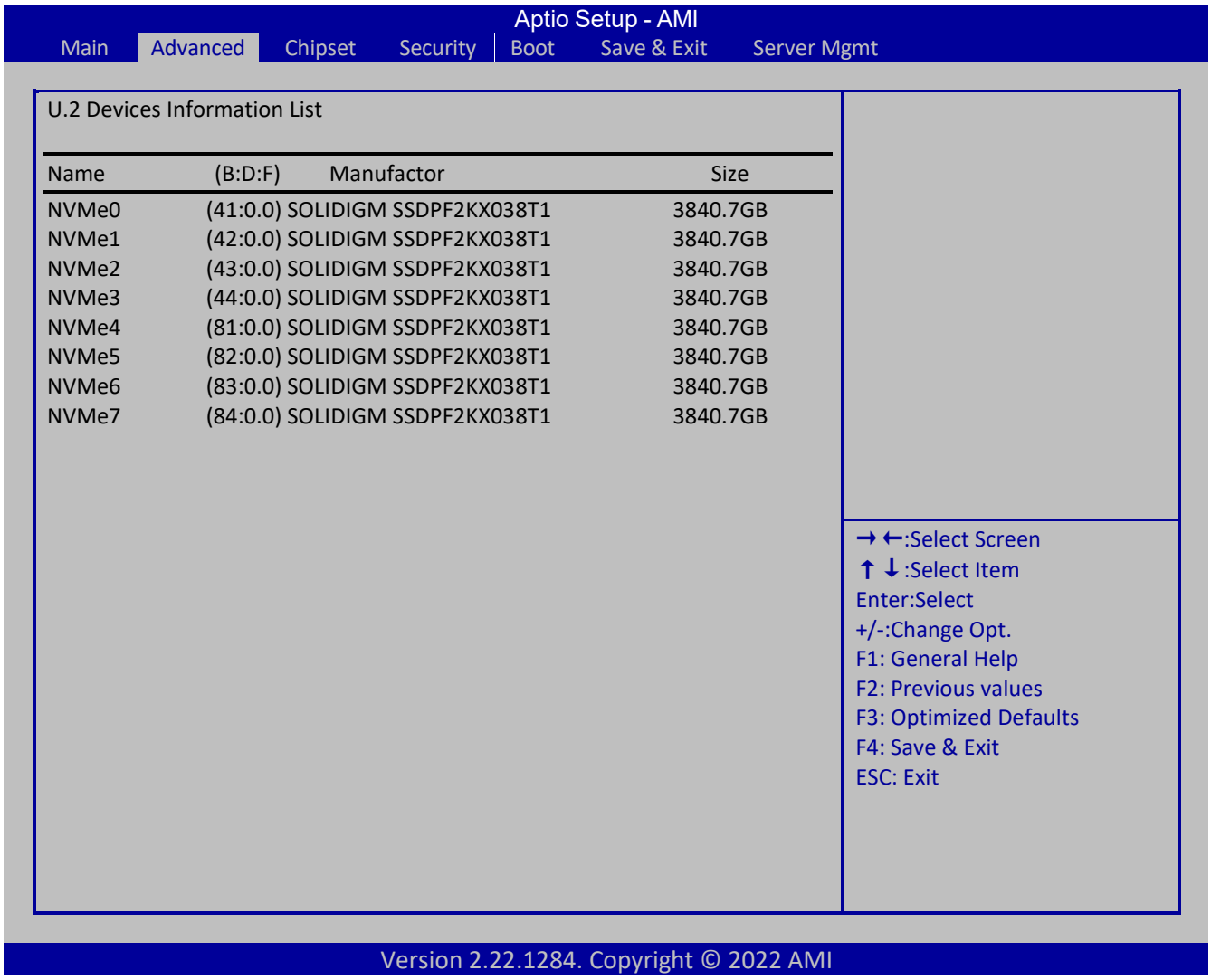


Advanced \ NVME Configuration		
Menu Fields	**Settings**	**Comments**
M.2 Devices	Selects sub-menu	
U.2 Devices	Selects sub-menu	

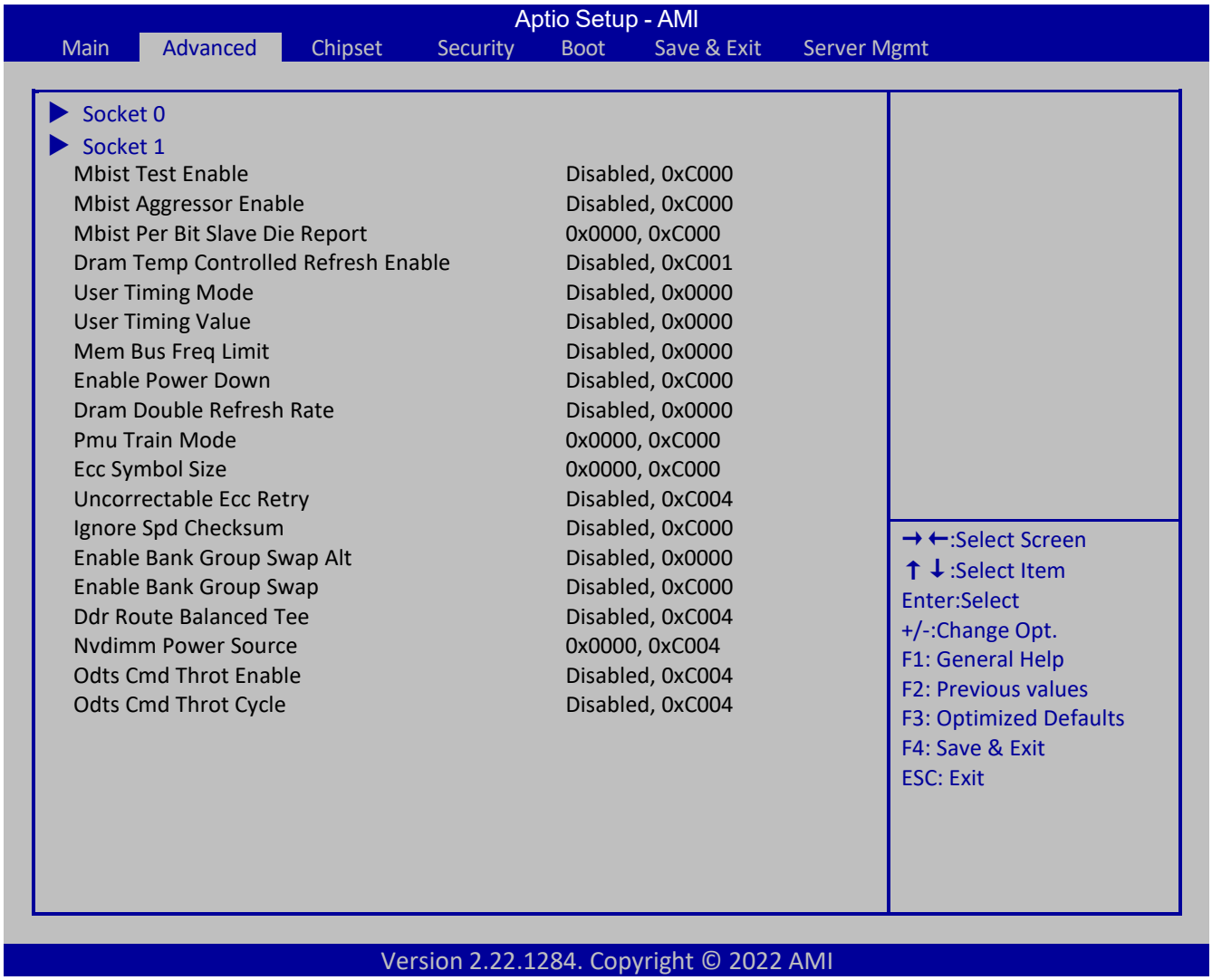
7.2.11.1 M.2 Devices



7.2.11.2 U.2 Devices

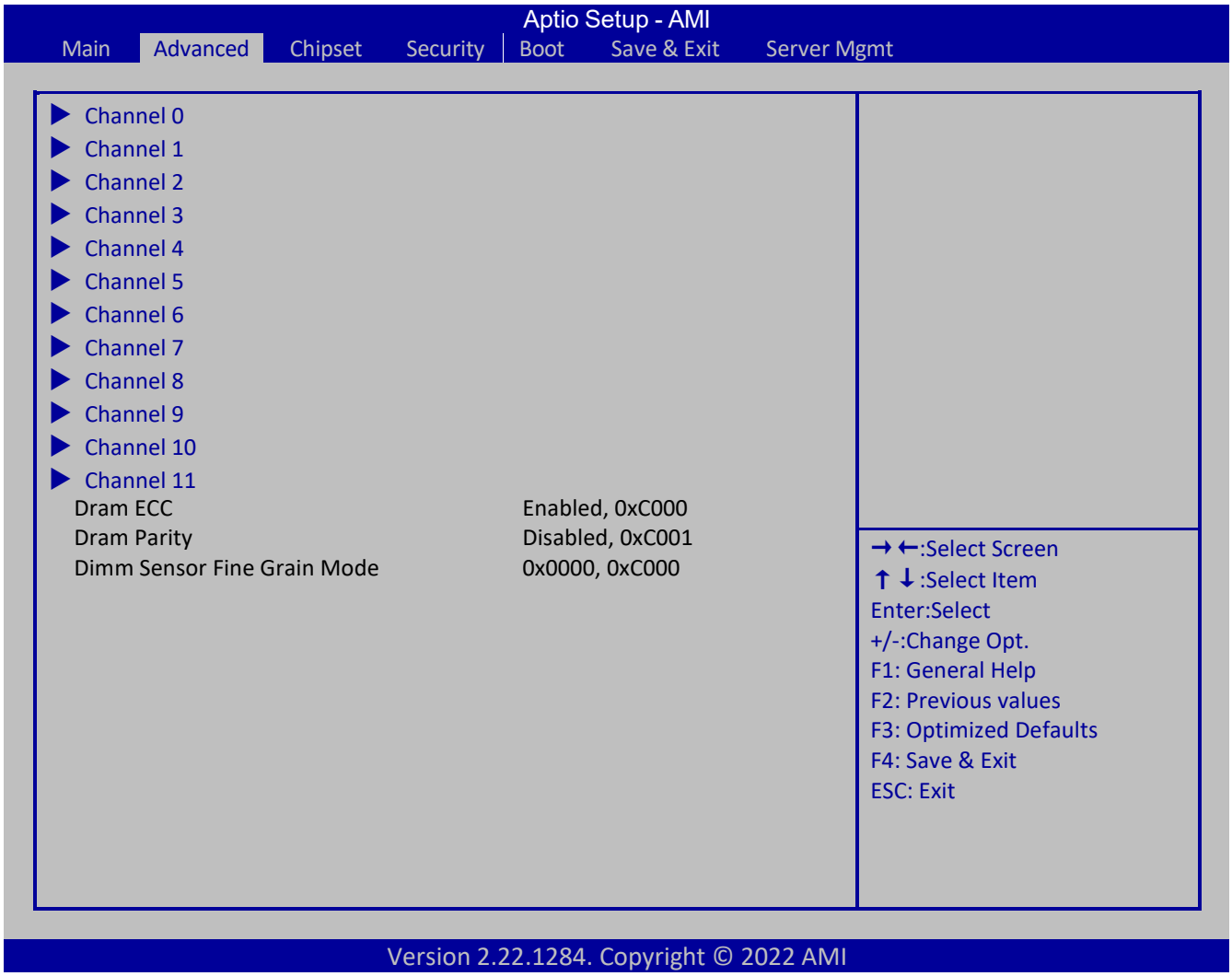


7.2.12 AMD Mem Configurations Status



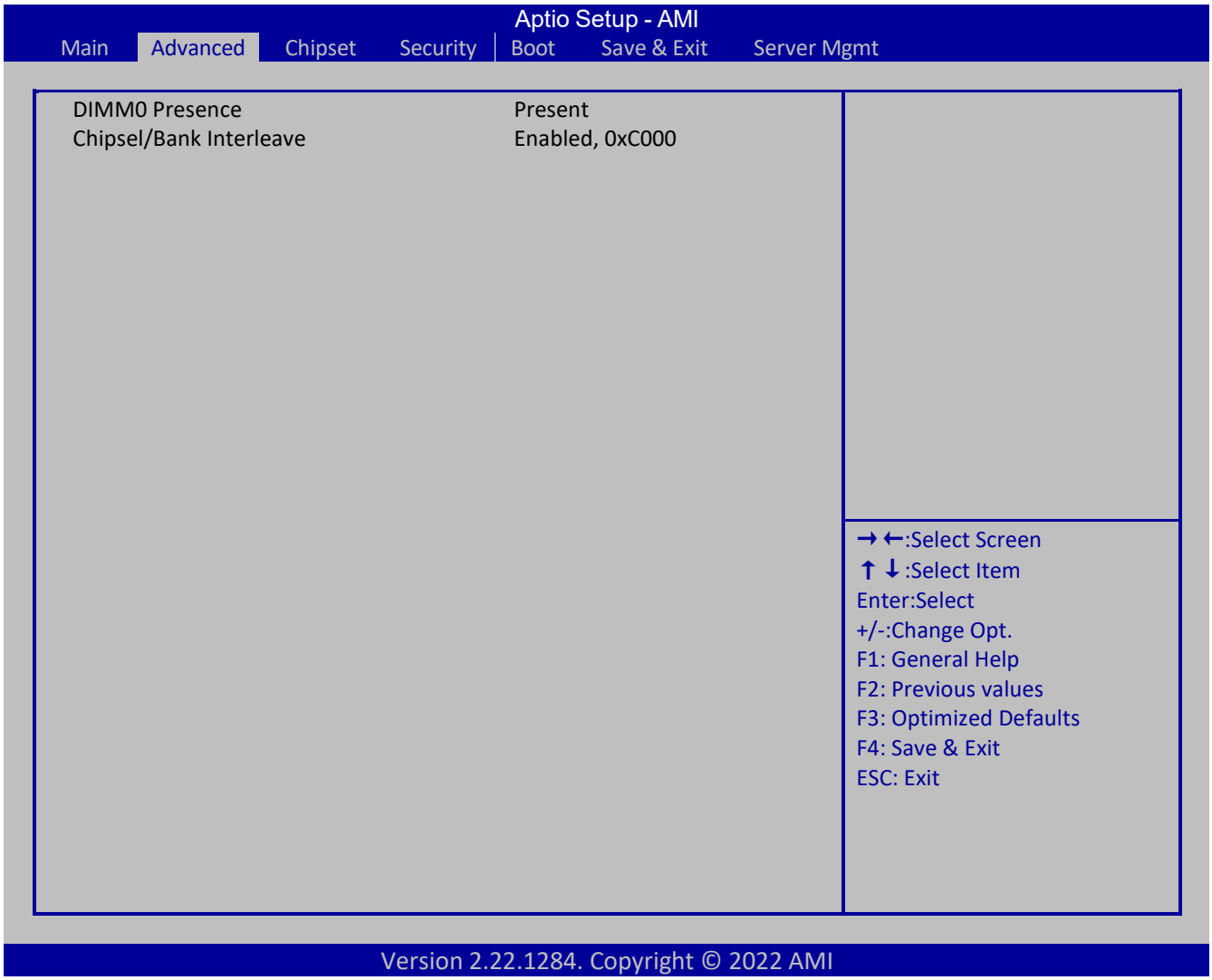
Advanced \ AMD Mem Configuration Status		
Menu Fields	**Settings**	**Comments**
Socket 0	Selects Sub-menu	
Socket 1	Selects Sub-menu	

7.2.12.1 Socket0

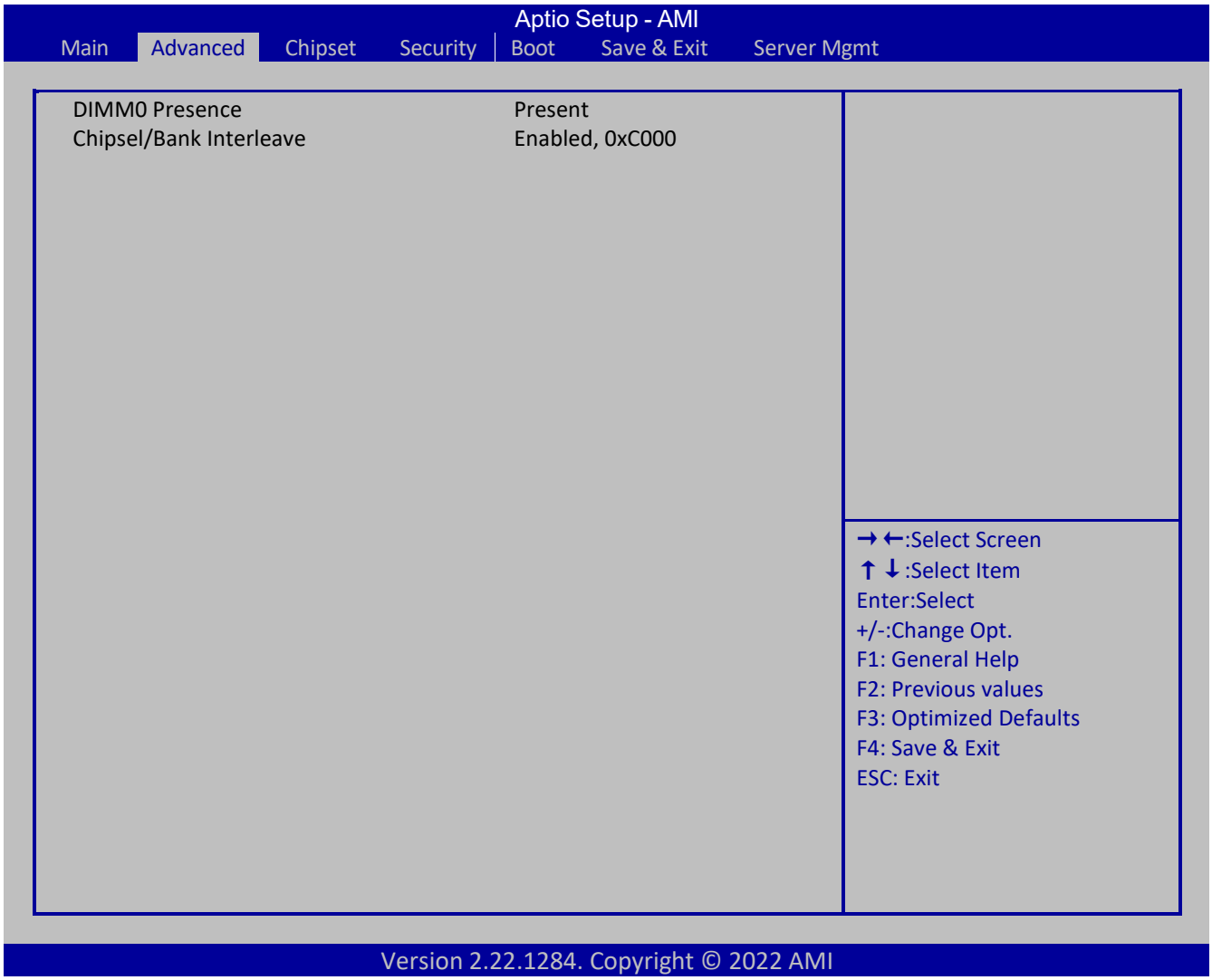


Advanced \ AMD Mem Configuration Status \ Socket 0		
Menu Fields	**Settings**	**Comments**
Channel 0	Selects Sub-menu	
Channel 1	Selects Sub-menu	
Channel 2	Selects Sub-menu	
Channel 3	Selects Sub-menu	
Channel 4	Selects Sub-menu	
Channel 5	Selects Sub-menu	
Channel 6	Selects Sub-menu	
Channel 7	Selects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

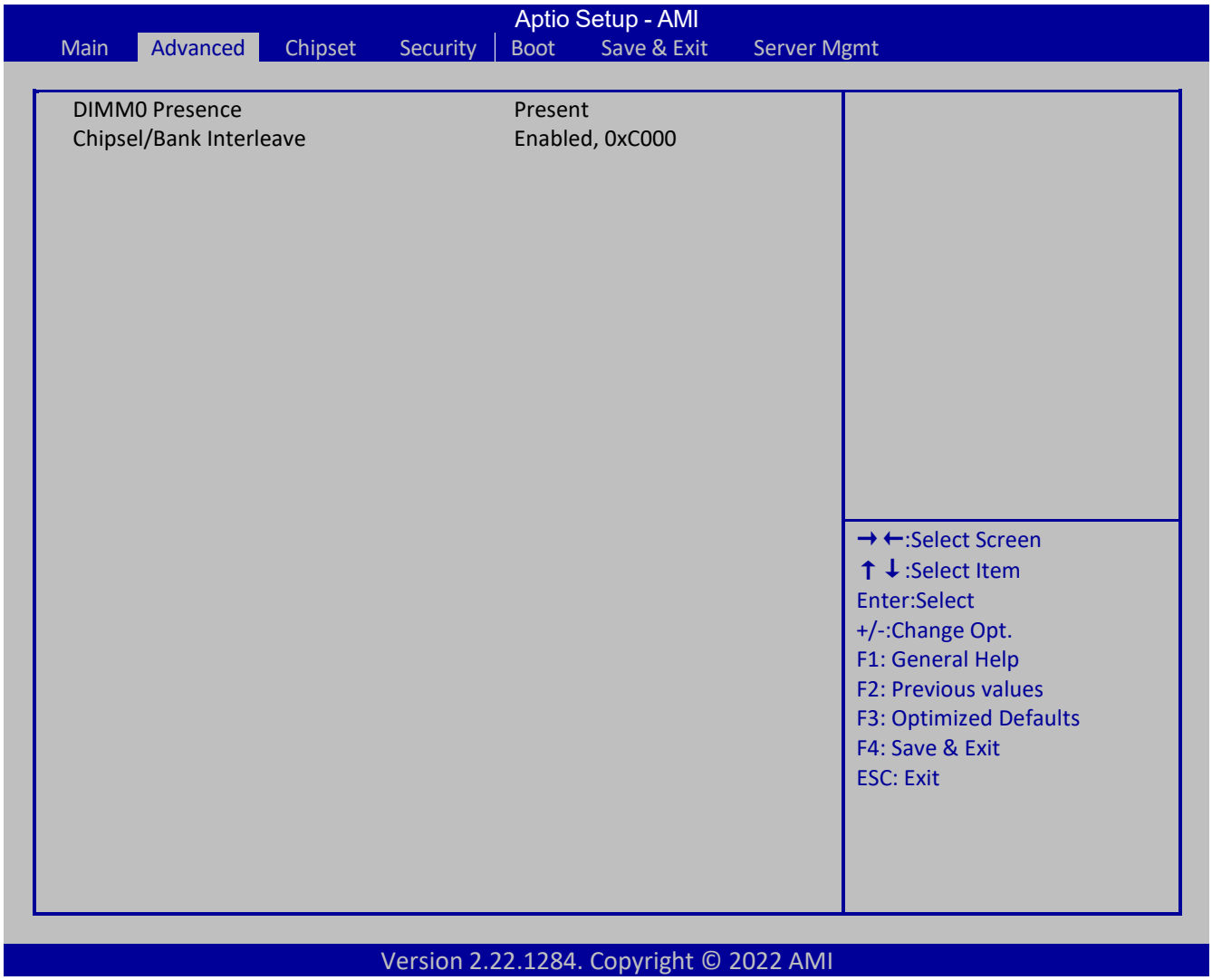
7.2.12.1.1 Channel 0



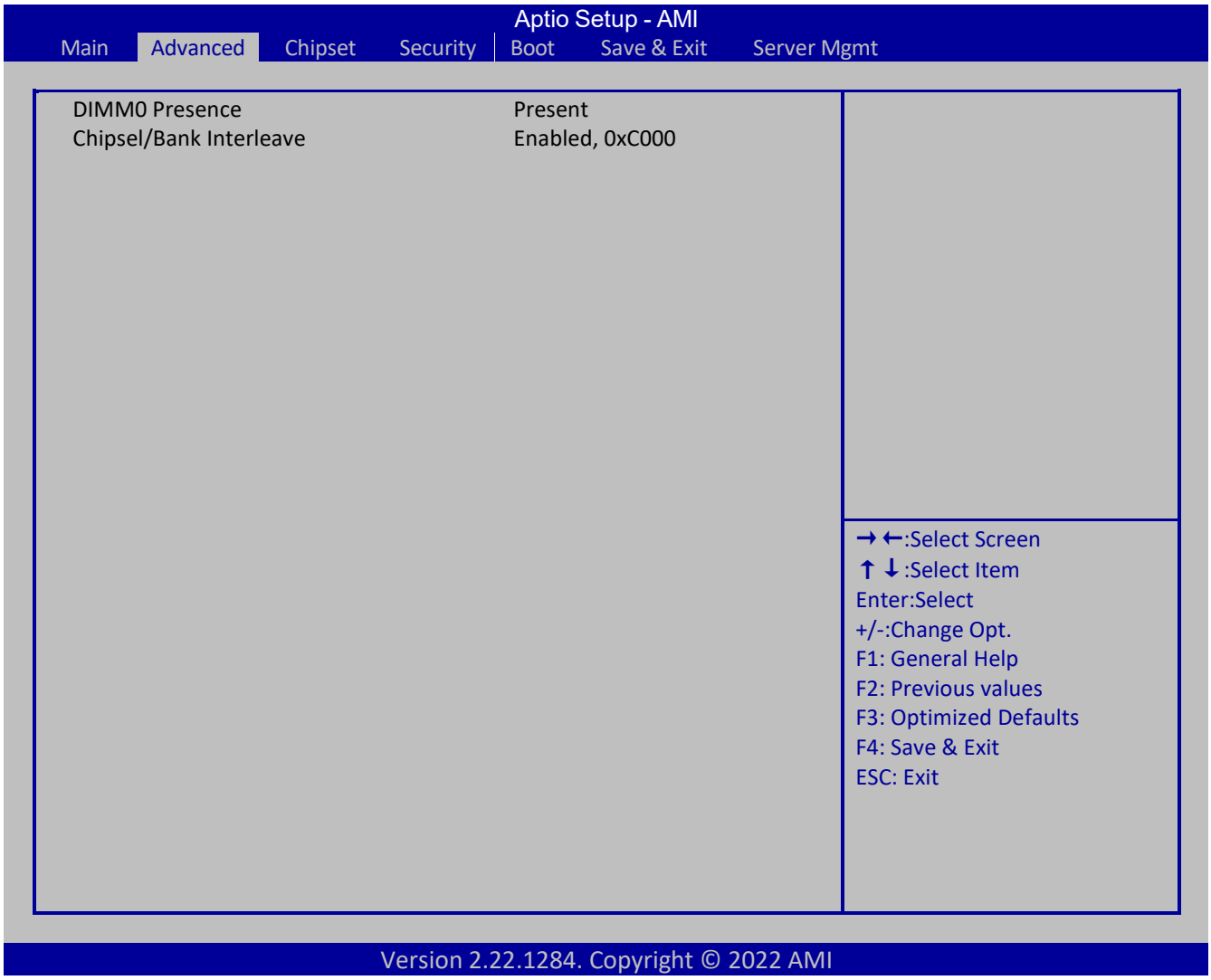
7.2.12.1.2 Channel 1



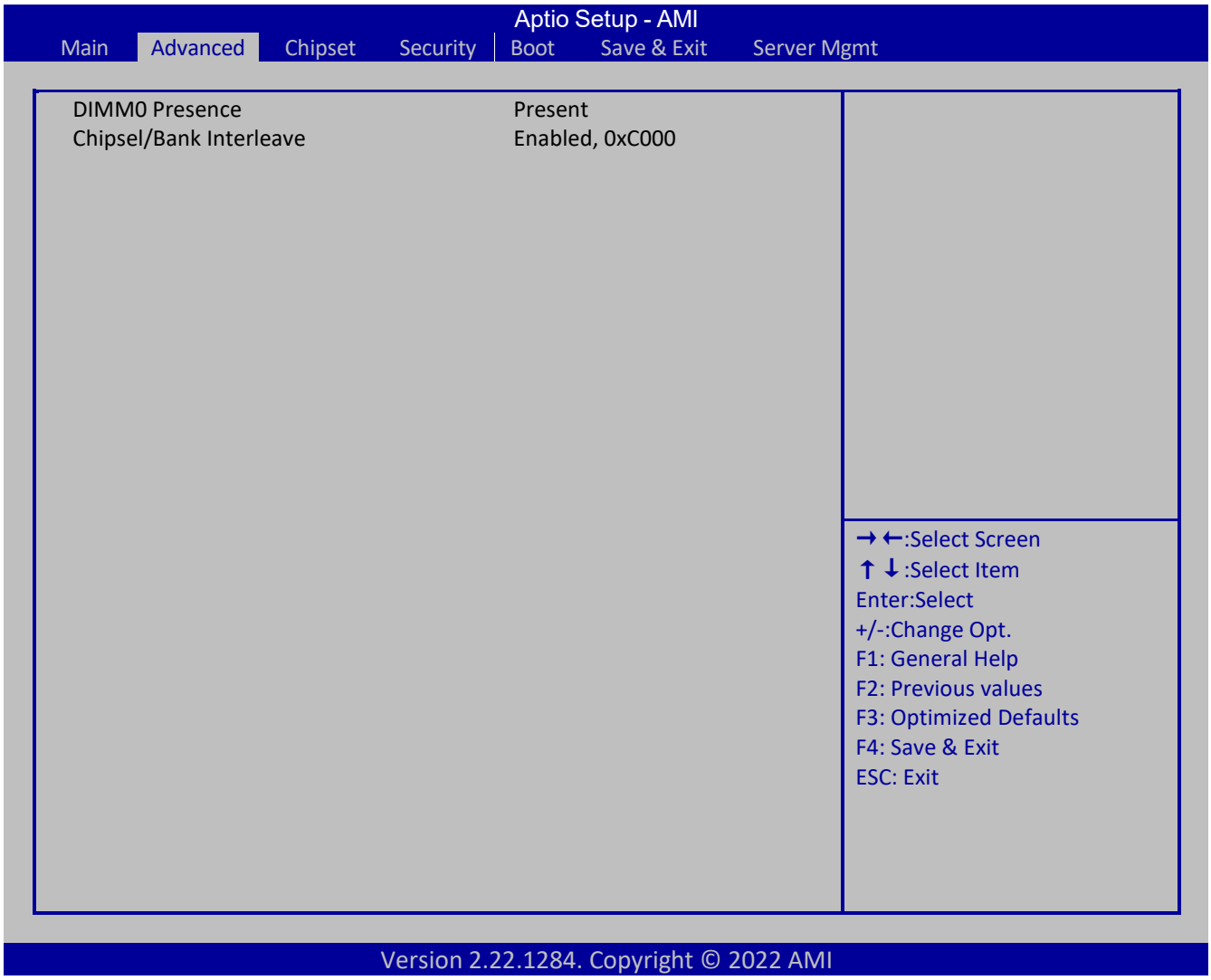
7.2.12.1.3 Channel 2



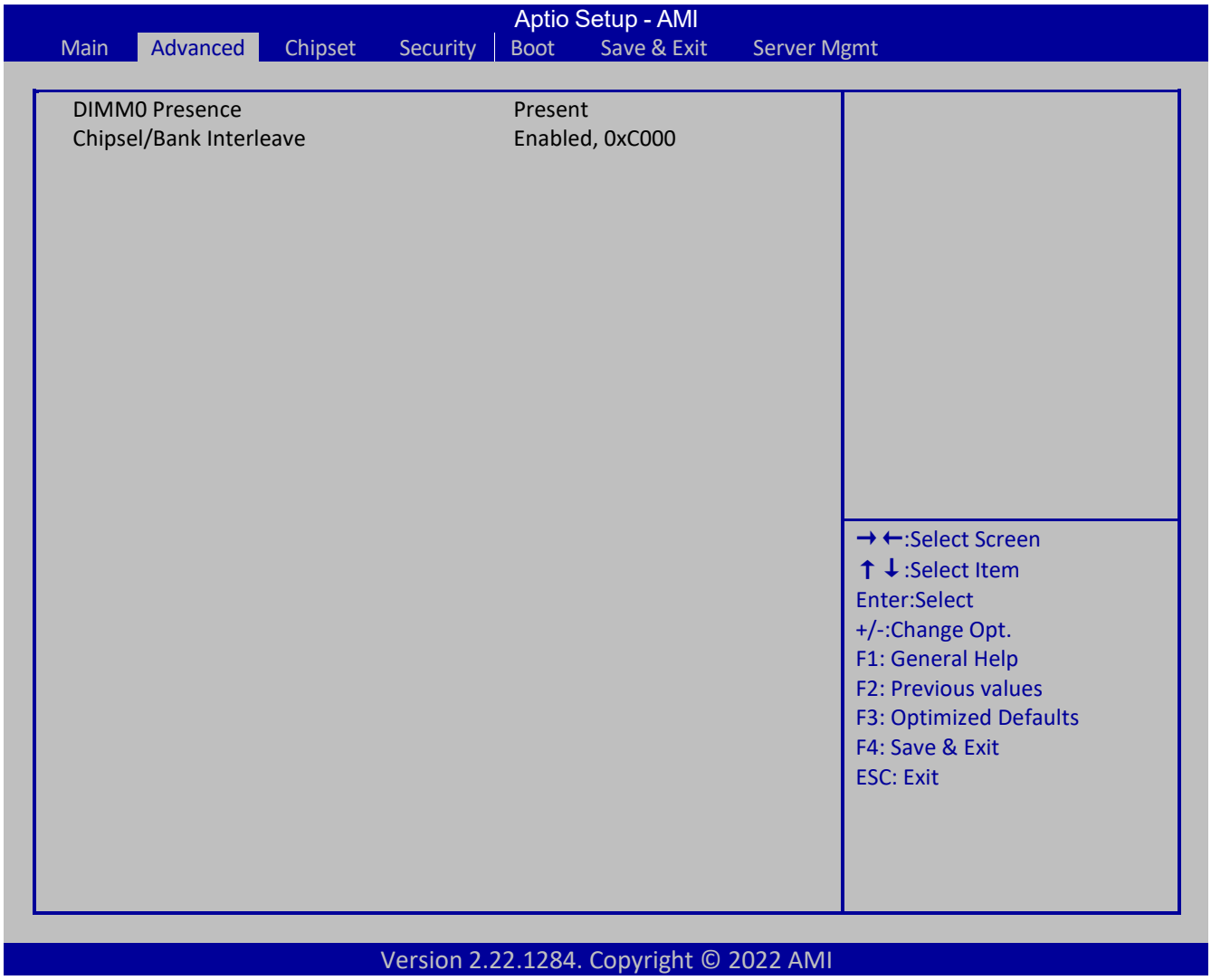
7.2.12.1.4 Channel 3



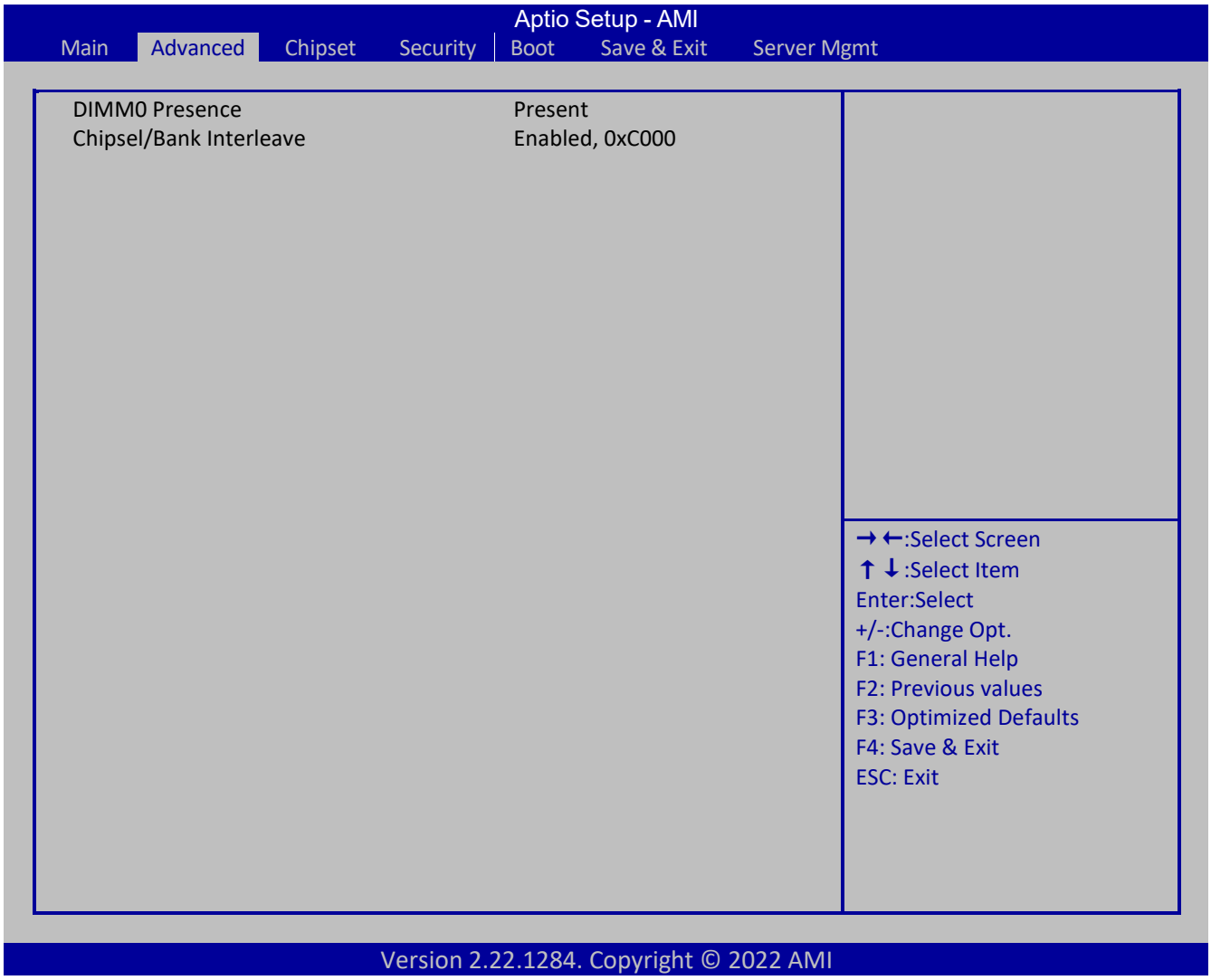
7.2.12.1.5 Channel 4



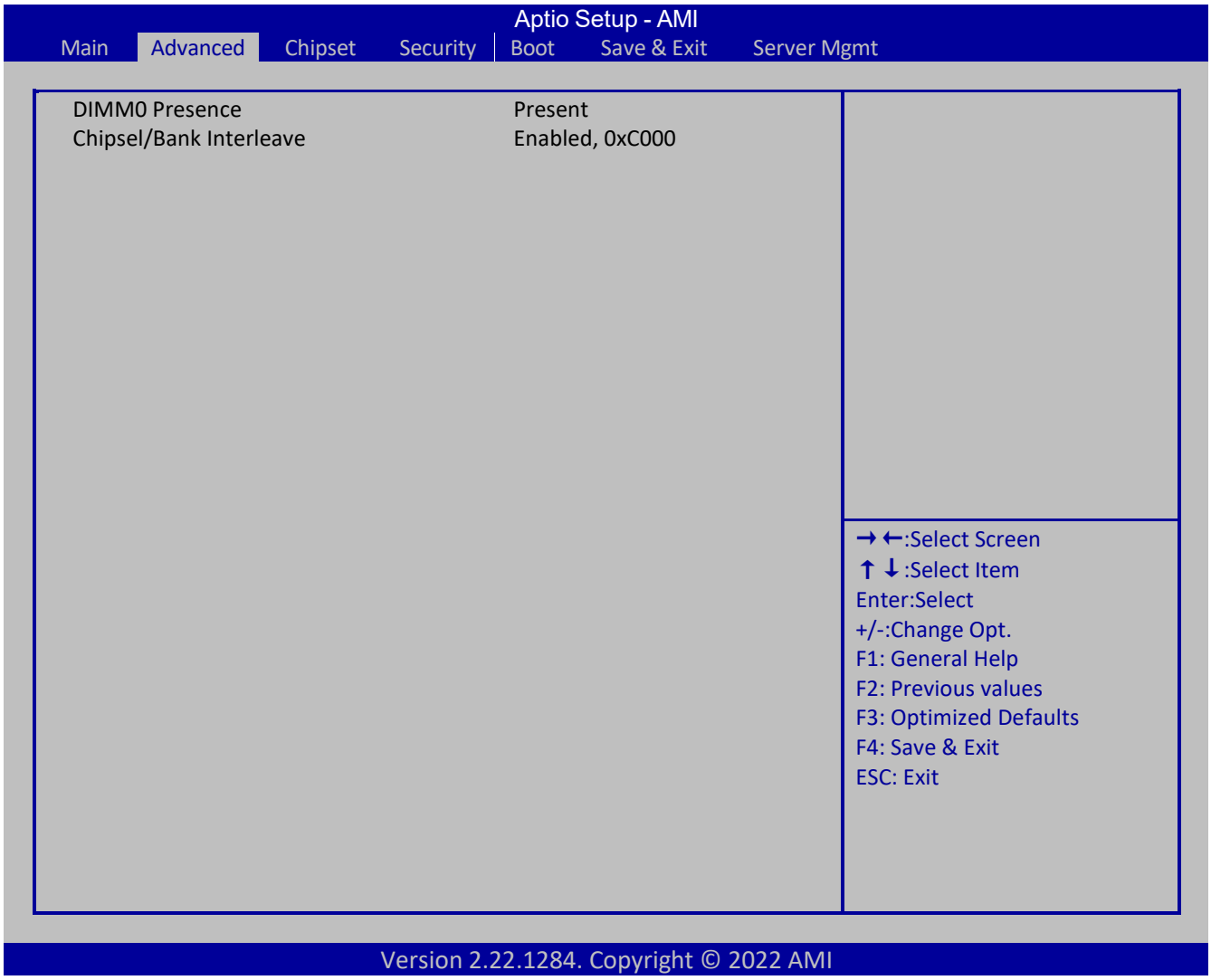
7.2.12.1.6 Channel 5



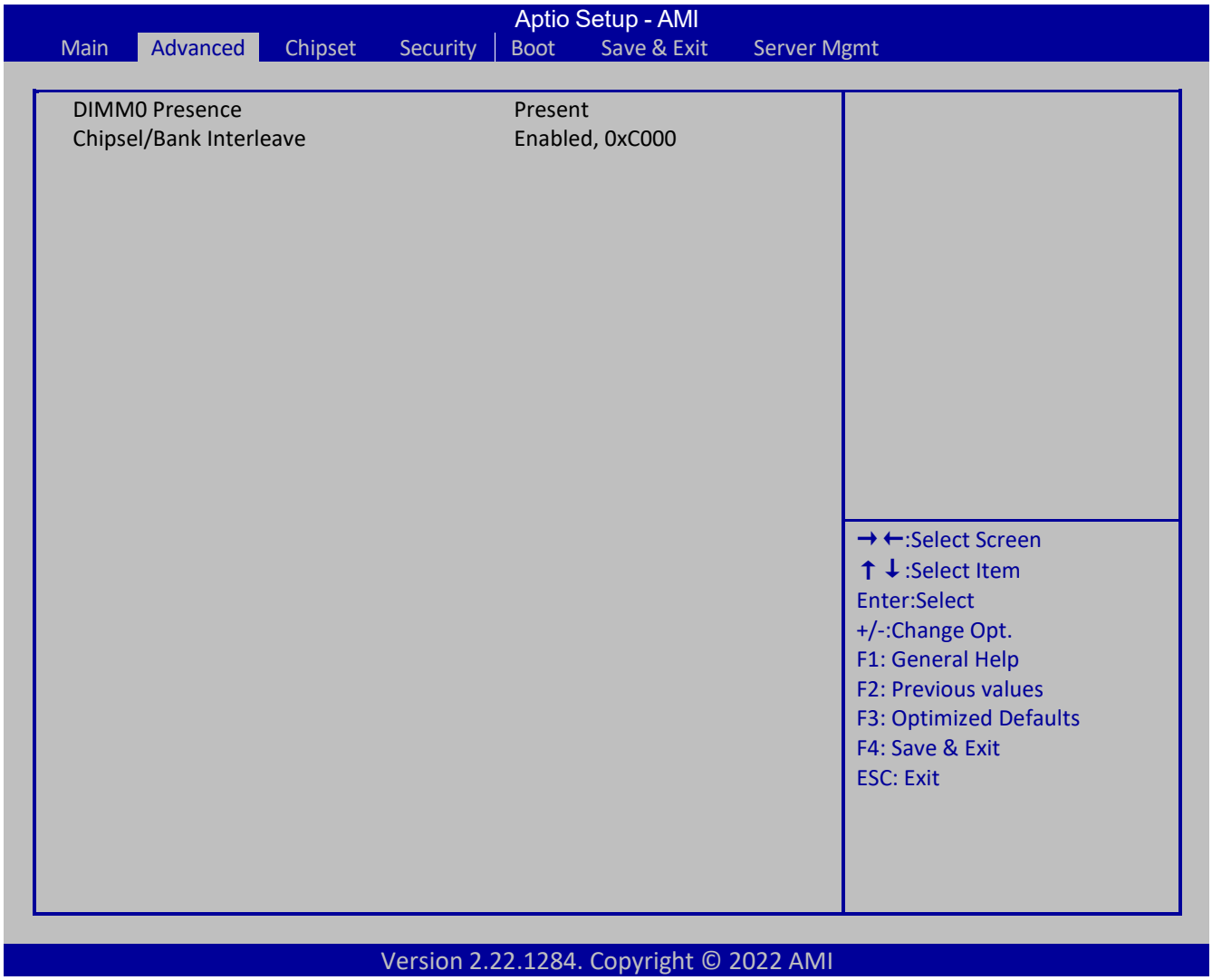
7.2.12.1.7 Channel 6



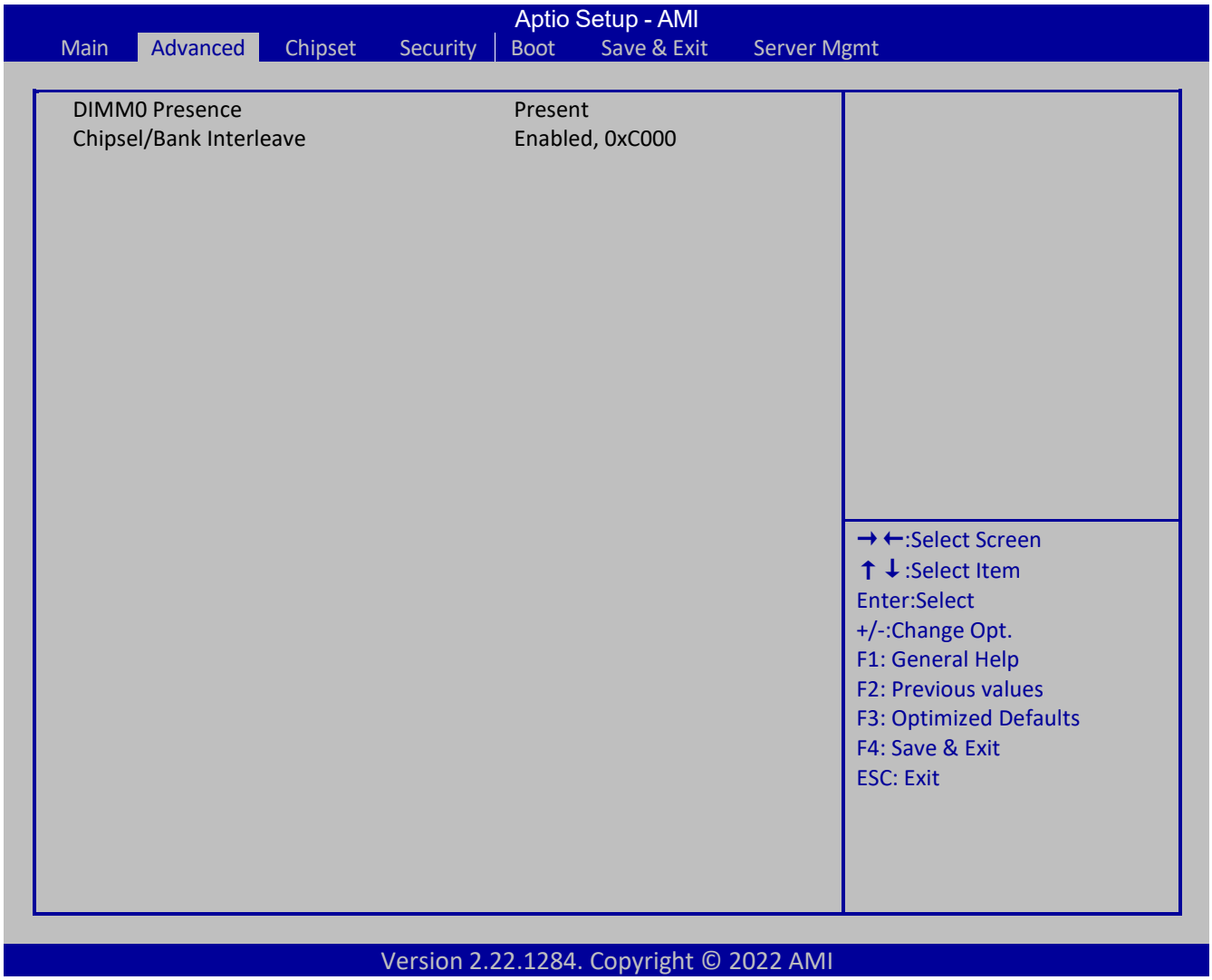
7.2.12.1.8 Channel 7



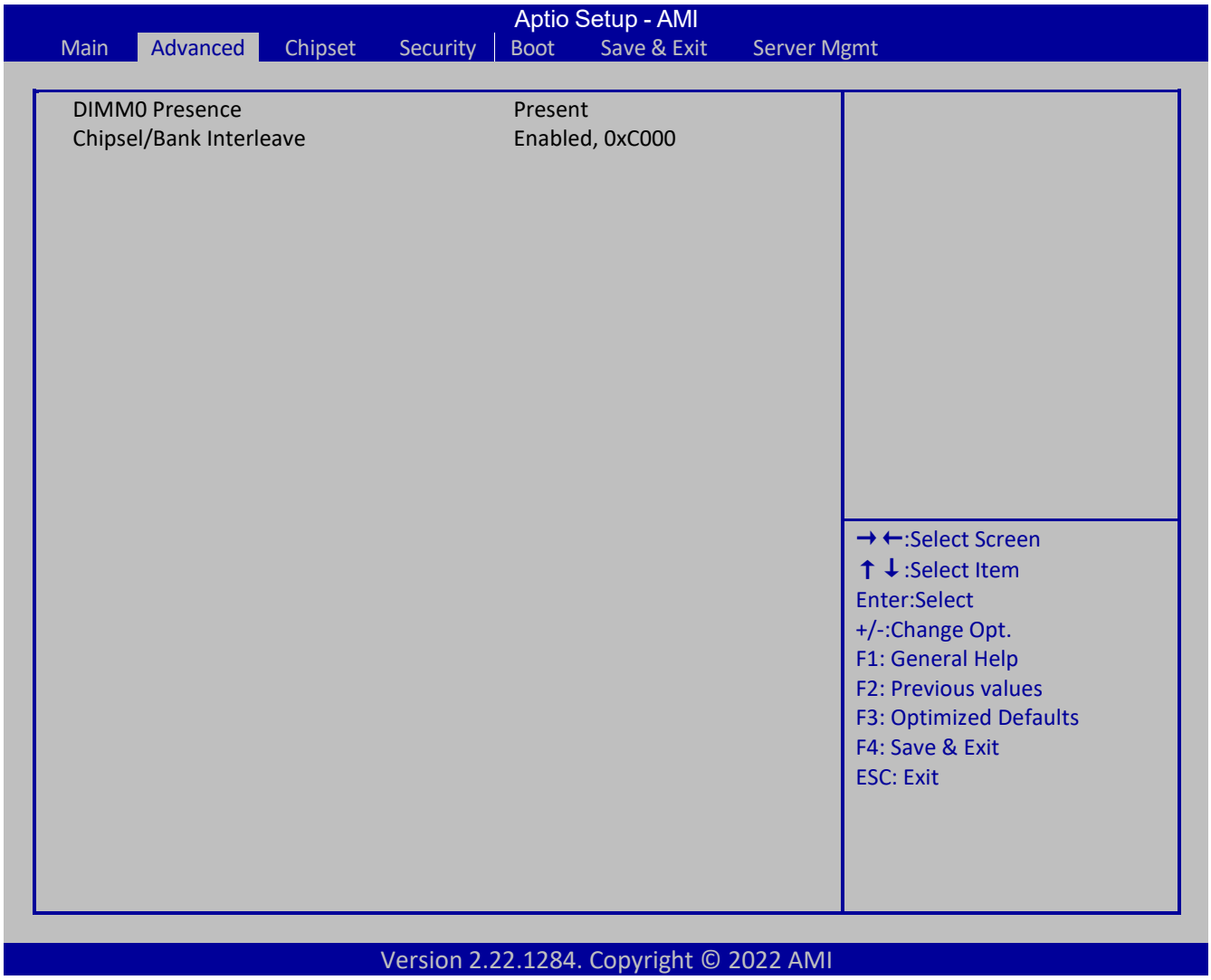
7.2.12.1.9 Channel 8



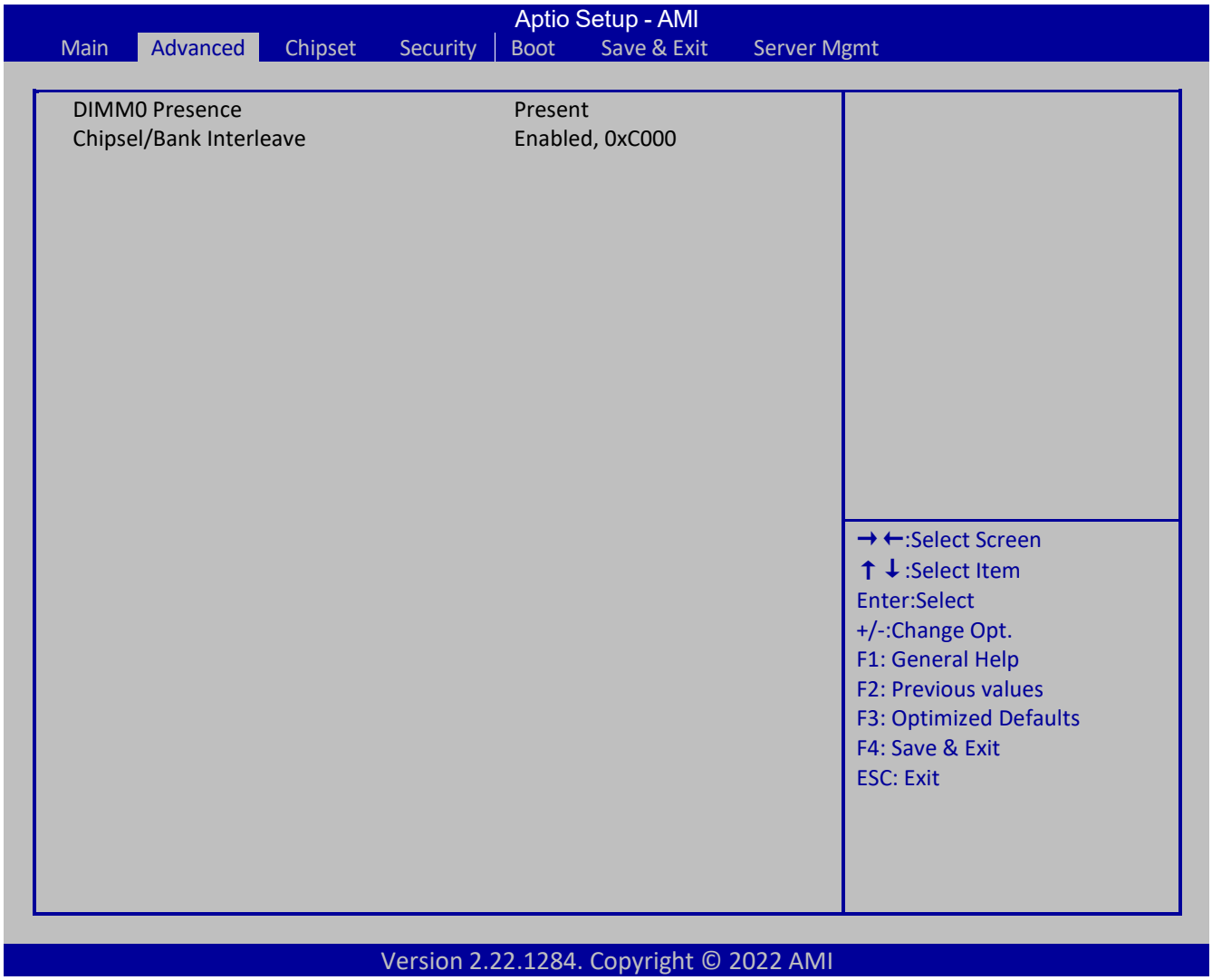
7.2.12.1.10 Channel 9



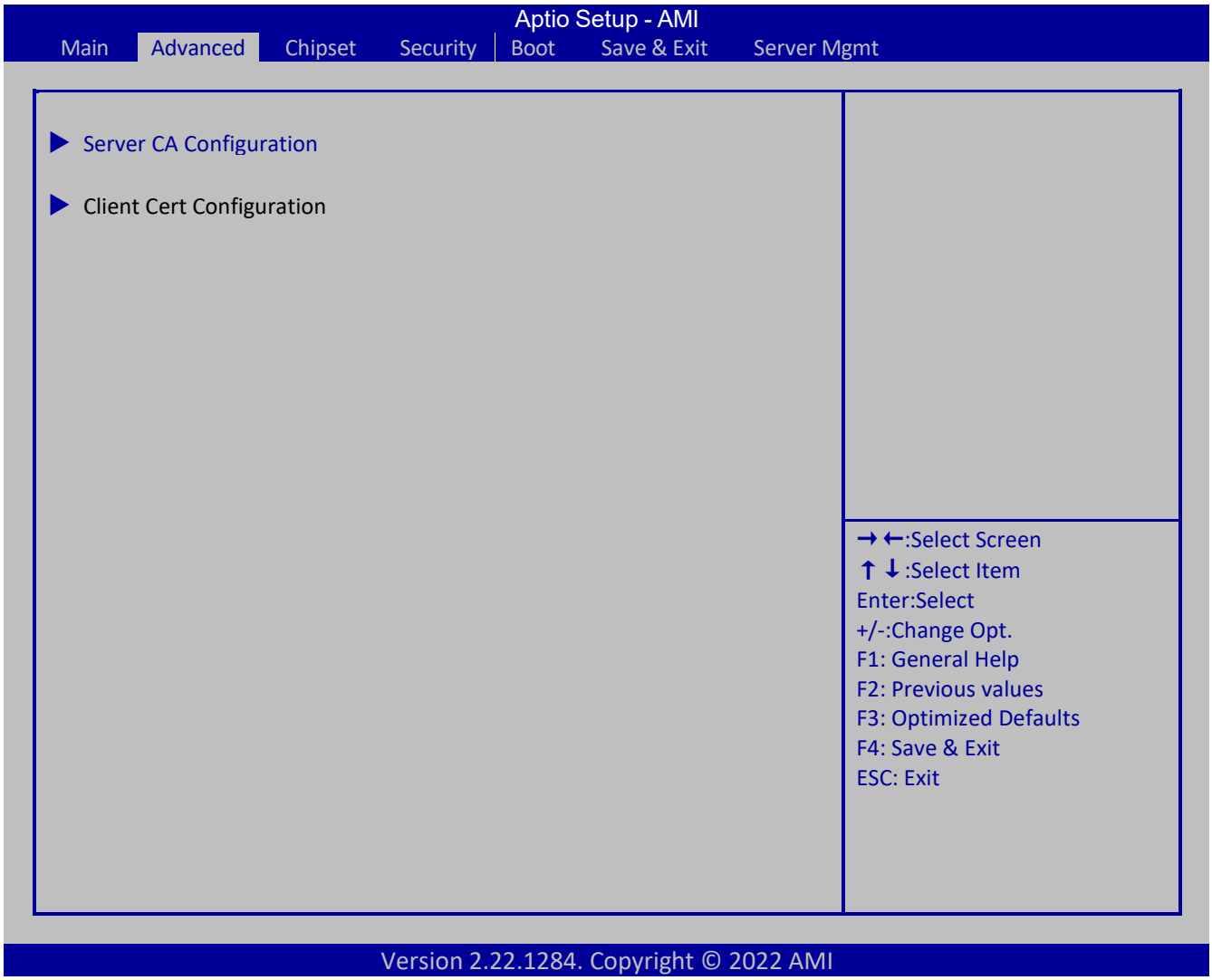
7.2.12.1.11 Channel 10



7.2.12.1.12 Channel 11

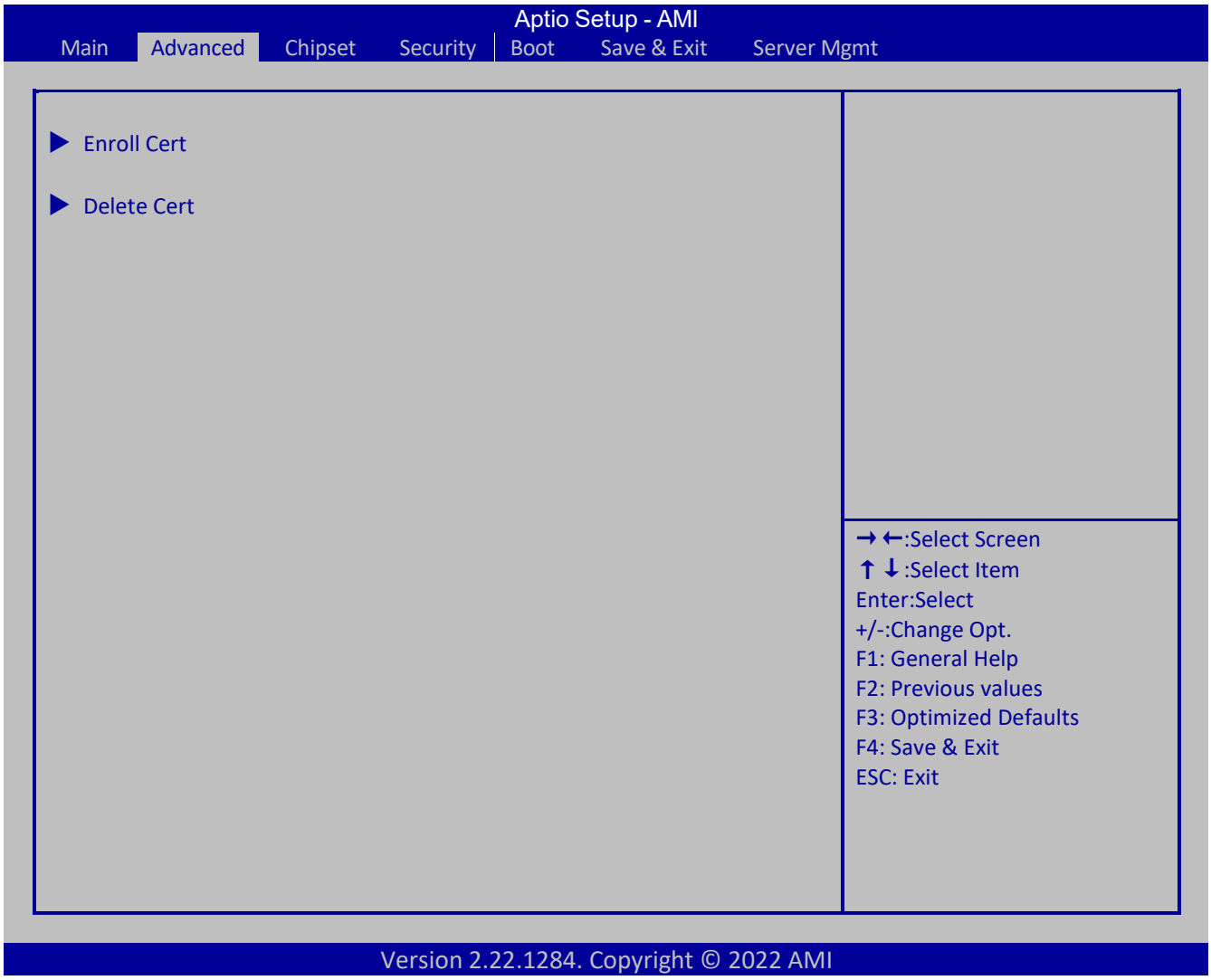


7.2.13 Tls Auth Configuration



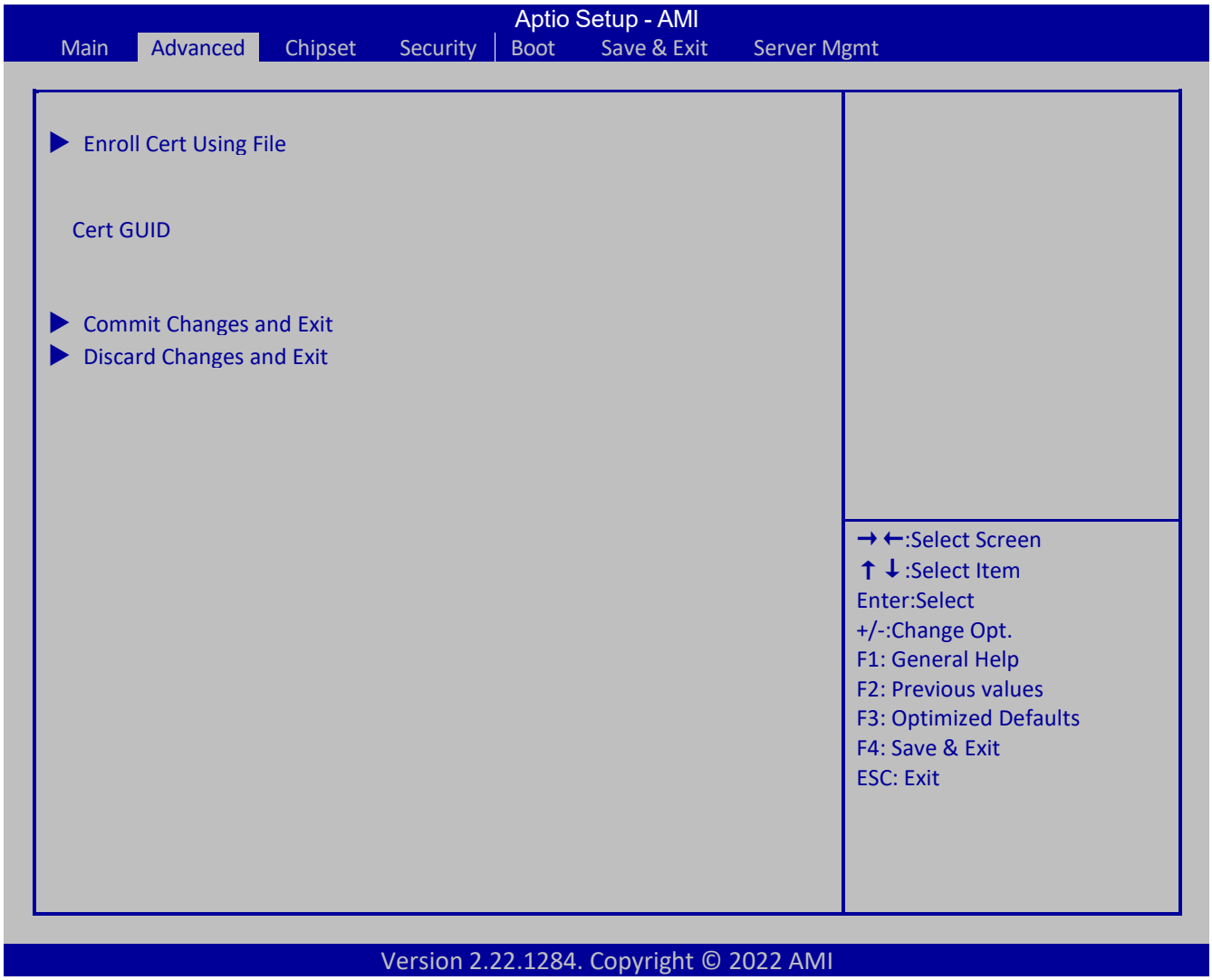
Advanced \ Tls Auth Configuration		
Menu Fields	**Settings**	**Comments**
Server CA Configuration	Selects Sub-menu	
Client Cert Configuration	Selects Sub-menu	

7.2.13.1 Server CA Configuration



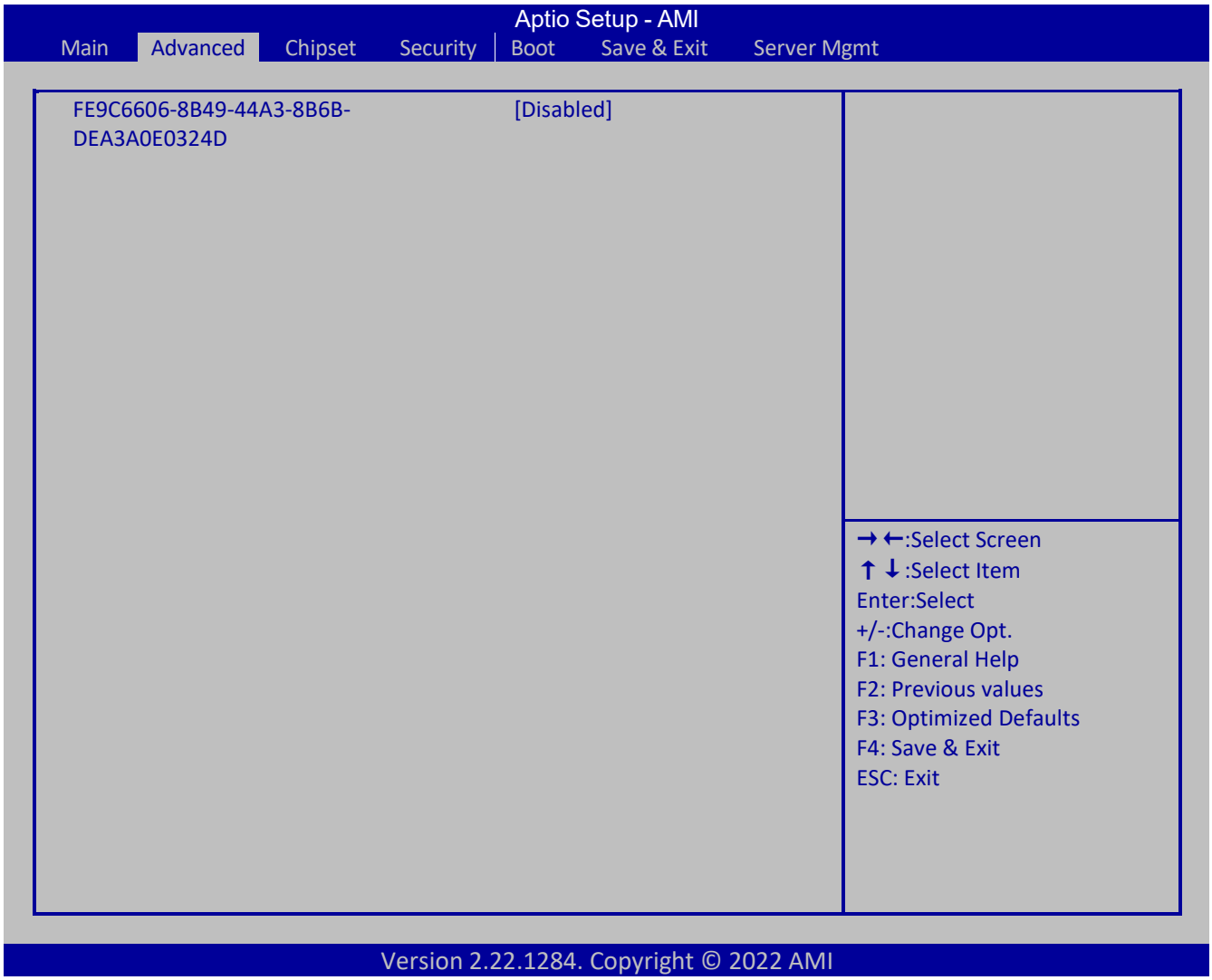
Advanced \ Tls Auth Configuration \ Server CA Config		
Menu Fields	**Settings**	**Comments**
Enroll Cert	Selects Sub-menu	
Delete Cert	Selects Sub-menu	

7.2.13.1.1 Enroll Cert



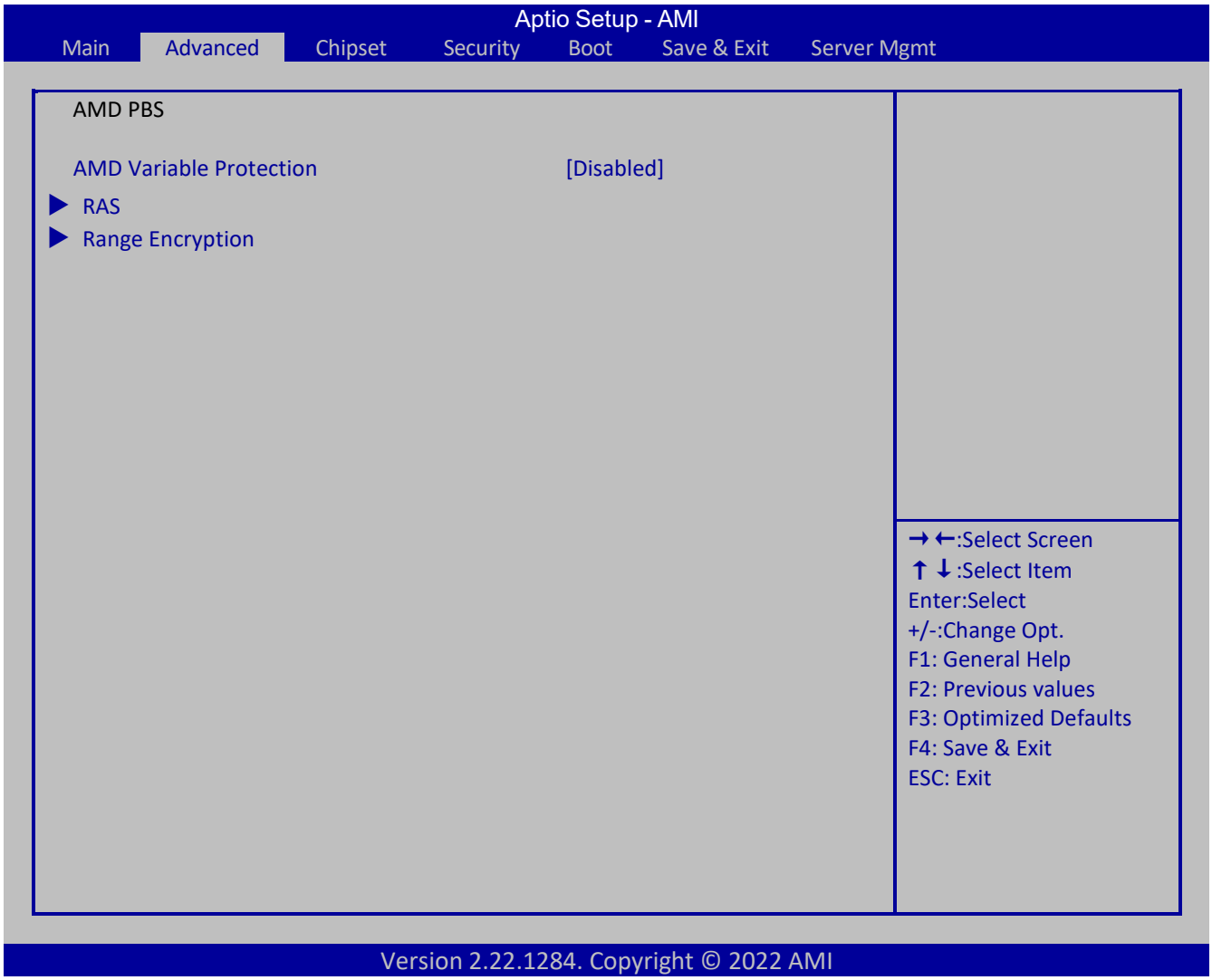
Advanced \ Tls Auth Configuration \ Server CA Config		
Menu Fields	**Settings**	**Comments**
Enroll Cert Using File	Select Storage Device	Enroll Cert Using File
Cert GUID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Input digit character in 11111111-2222-3333-44444-1234567890ab format.
Commit Changes and Exit		Commit Changes and Exit
Discard Changes and Exit		Discard Changes and Exit

7.2.13.1.2 Delete Cert



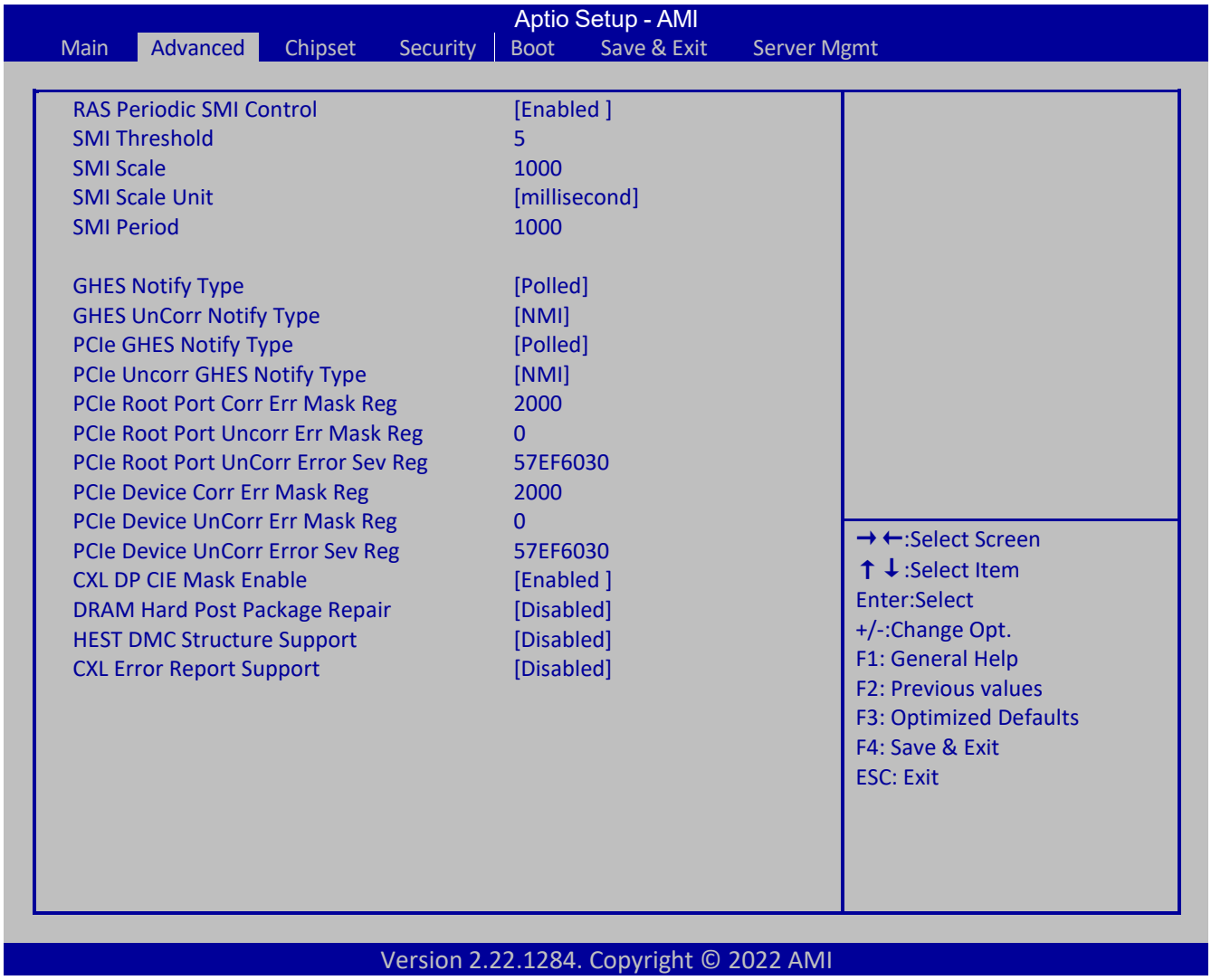
Advanced \ Tls Auth Configuration		
Menu Fields	**Settings**	**Comments**
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	**[Disabled]** [Enabled]	GUID for CERT

7.2.14 AMD PBS



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

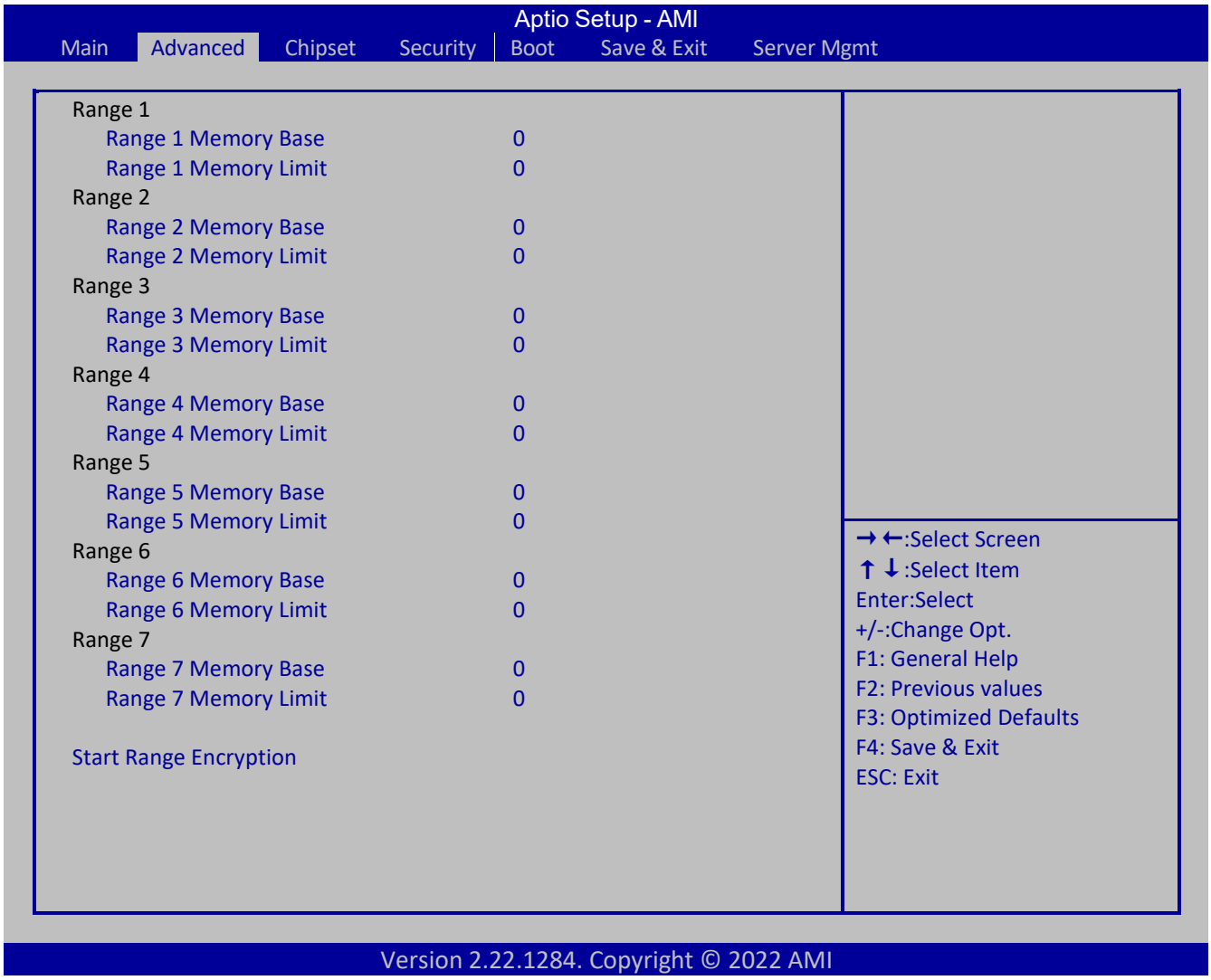
7.2.14.1 RAS



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

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

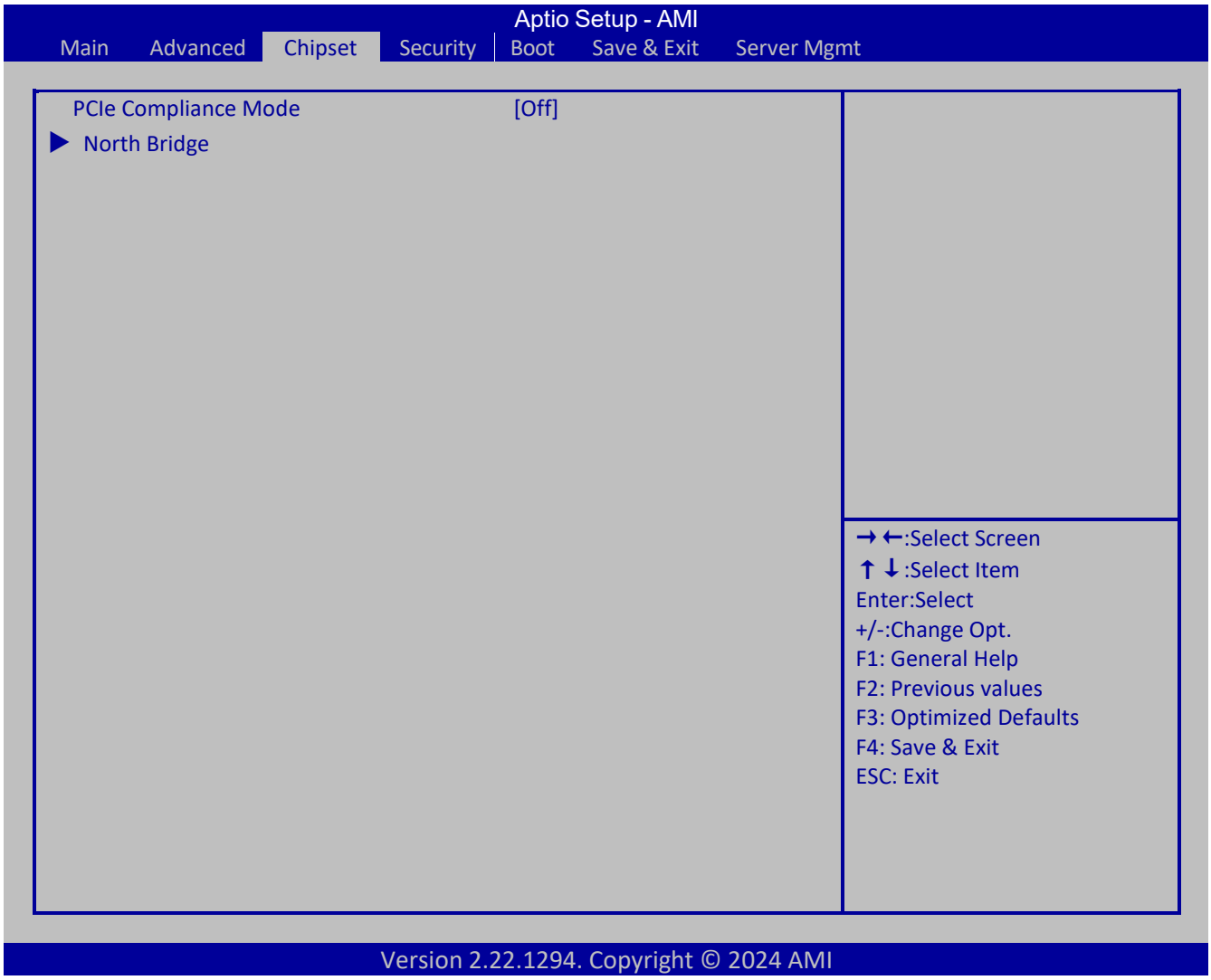
7.2.14.2 Range Encryption



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

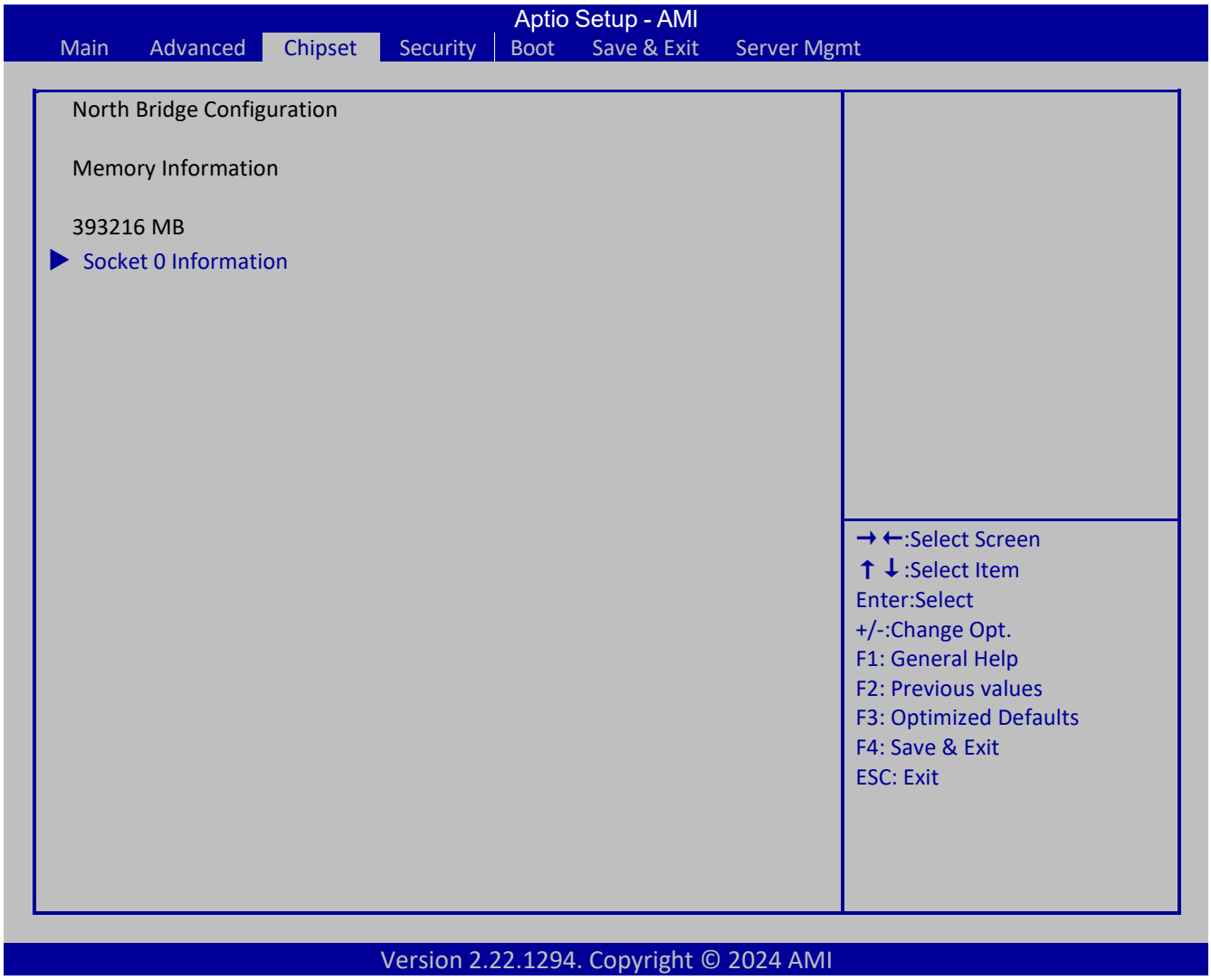
Advanced \ AMD PBS \ Range Encryption		
Menu Fields	**Settings**	**Comments**
Range 7 Memory Base	X	Entry memory range base address and limit address
Range 7 Memory Limit	X	Entry memory range base address and limit address
Start Range Encryption	Executable item	Start to encrypt all memory ranges.

7.3 CHIPSET



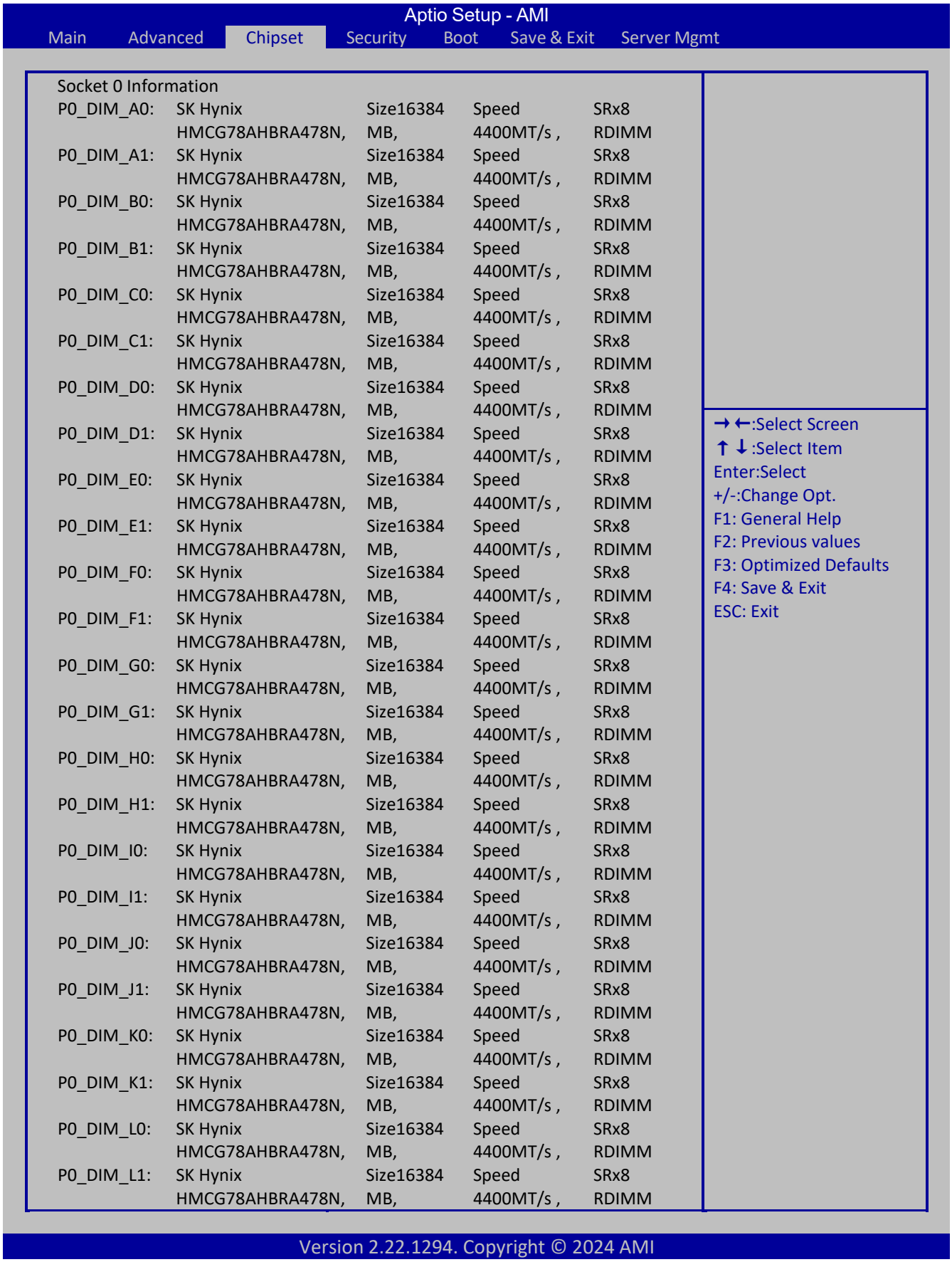
Chipset		
Menu Fields	**Settings**	**Comments**
PCIe Compliance Mode	[Off] [On]	PCIe Link Compliance Mode.
North Bridge	Selects Sub-menu	North Bridge Paramters

7.3.1 North Bridge

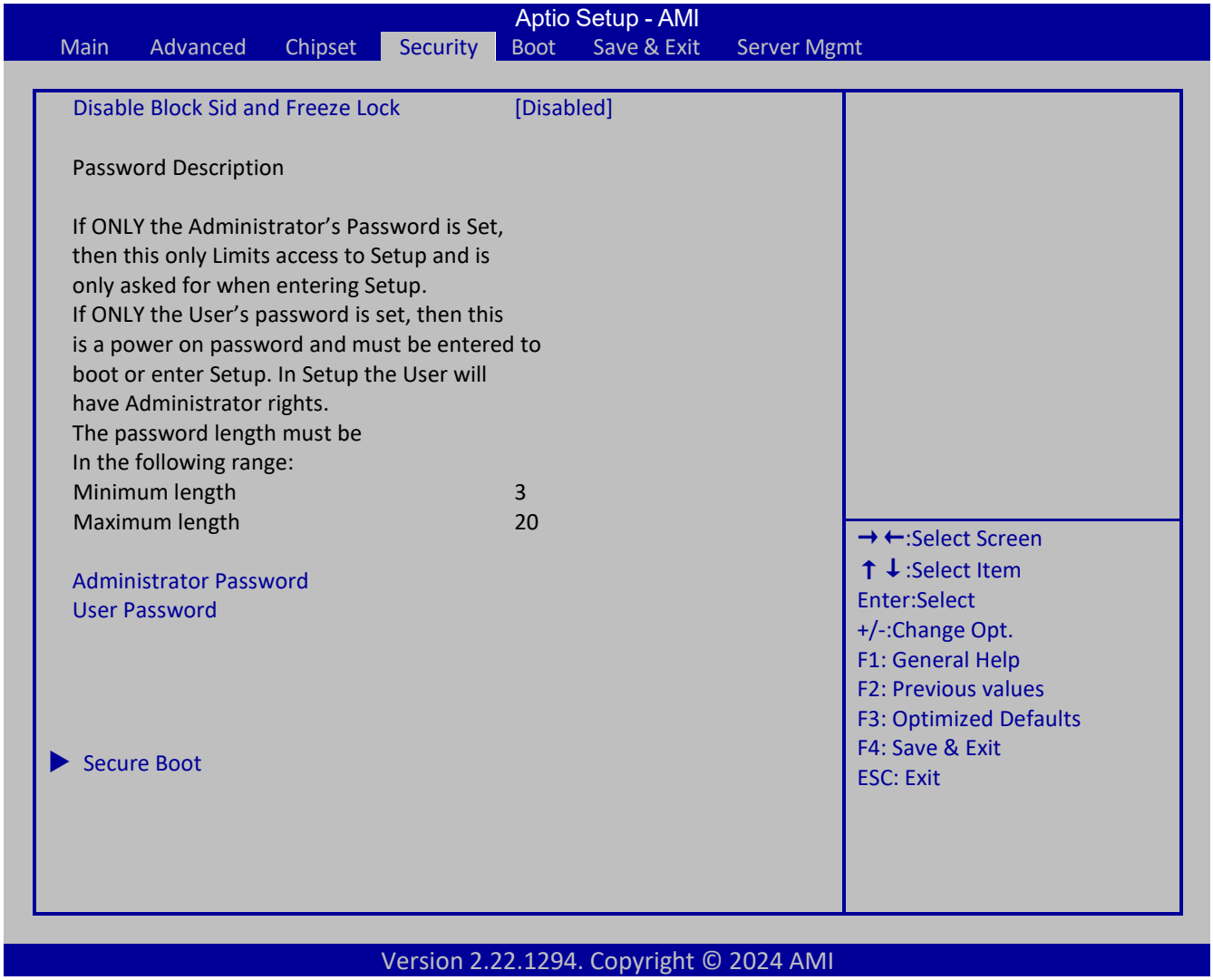


Chipset \ North Bridge		
Menu Fields	**Settings**	**Comments**
Socket 0 Information	Selects Sub-menu	
Socket 1 Information	Selects Sub-menu	

7.3.1.1 Socket 0 Information

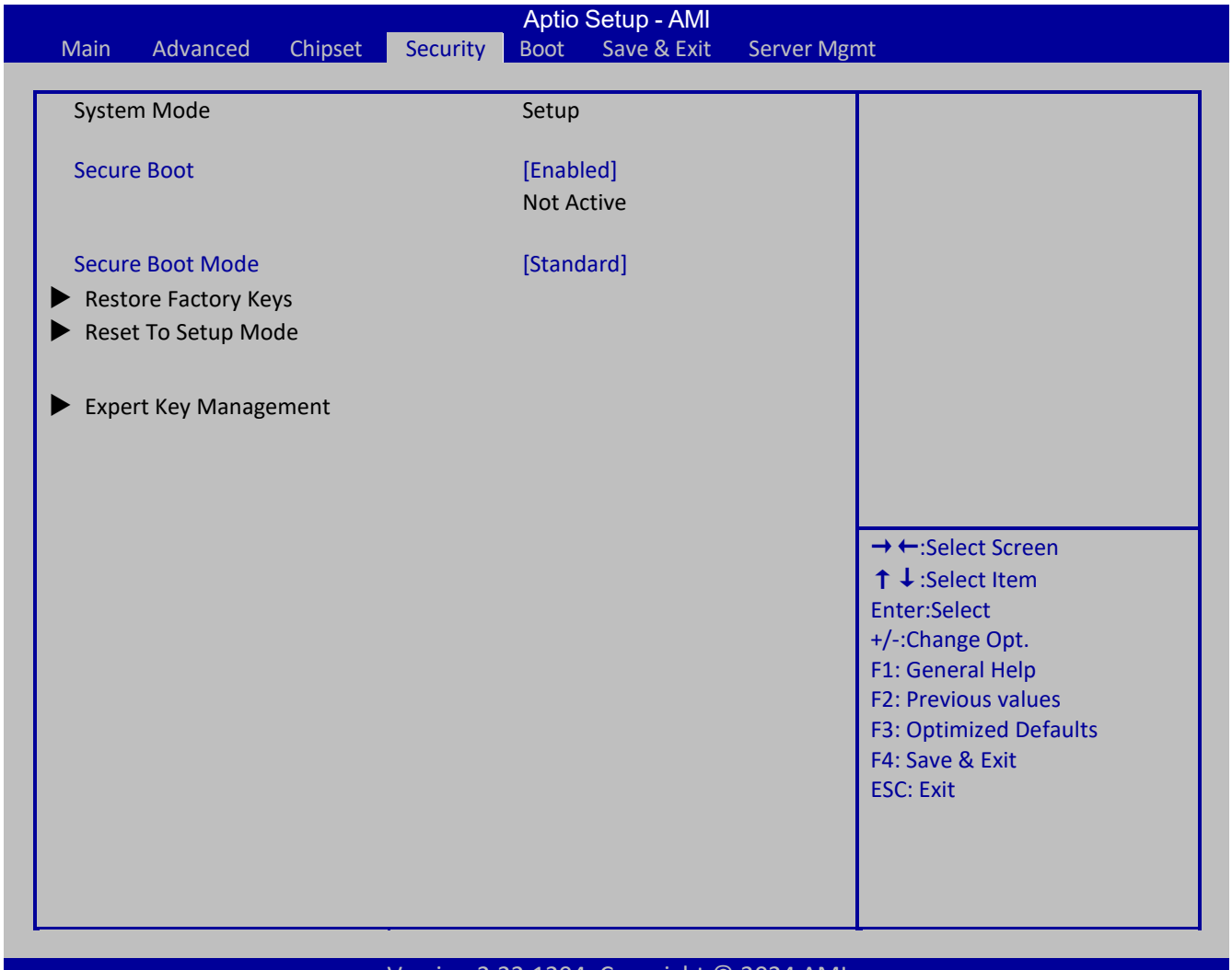


7.4 SECURITY


Aptio Setup - AMI
Main
Advanced
Chipset
Security
Boot
Save & Exit
Server Mgmt
Disable Block Sid and Freeze Lock
[Disabled]
Password Description
If ONLY the Administrator's Password is Set, then this only Limits access to Setup and is only asked for when entering Setup.
If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.
The password length must be
In the following range:
Minimum length
3
Maximum length
20
Administrator Password
User Password
Secure Boot
→←:Select Screen
↑↓:Select Item
Enter:Select
+/-:Change Opt.
F1: General Help
F2: Previous values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1294. Copyright © 2024 AMI

Security		
Menu Fields	**Settings**	**Comments**
Disable Block Sid and Freeze Lock	**[Disabled]** [Enabled]	Override to allow SID authentication of TCG Storage device and to skip freeze lock command for SAT3 device. Modified value will be applicable only for next boot.
Administrator Password	Executable item	Set Administrator Password
User Password	Executable item	Set User Password
Secure Boot	Selects Sub-menu	

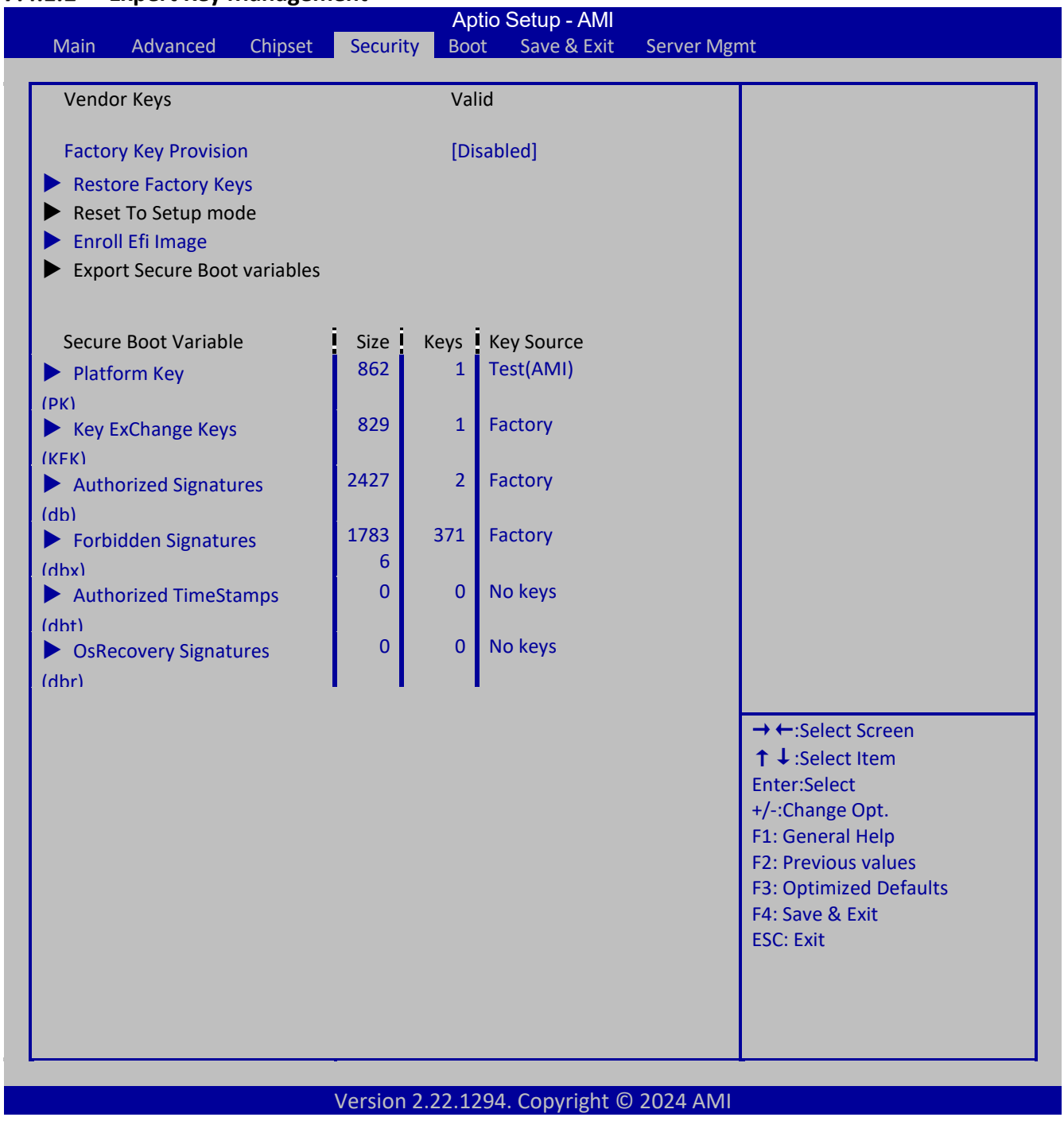
7.4.1 Secure Boot



Security \ Secure Boot		
Menu Fields	**Settings**	**Comments**
Secure Boot	[Disabled] [Enabled]	Secure Boot feature is Active if secure boot is enabled. Platform Key (PK) is enrolled and the System is in User mode. The mode change require platform reset.
Secure Boot Mode	[Standard] [Custom]	Secure boot mode option: Standard or Custom.

Security \ Secure Boot		
Menu Fields	**Settings**	**Comments**
		In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys	Executable item	Force System to User Mode. Install factory default Secure Boot key databases.
Expert Key Management	Selects sub-menu	Enable expert users to modify Secure Boot Policy variables without variable authentication.

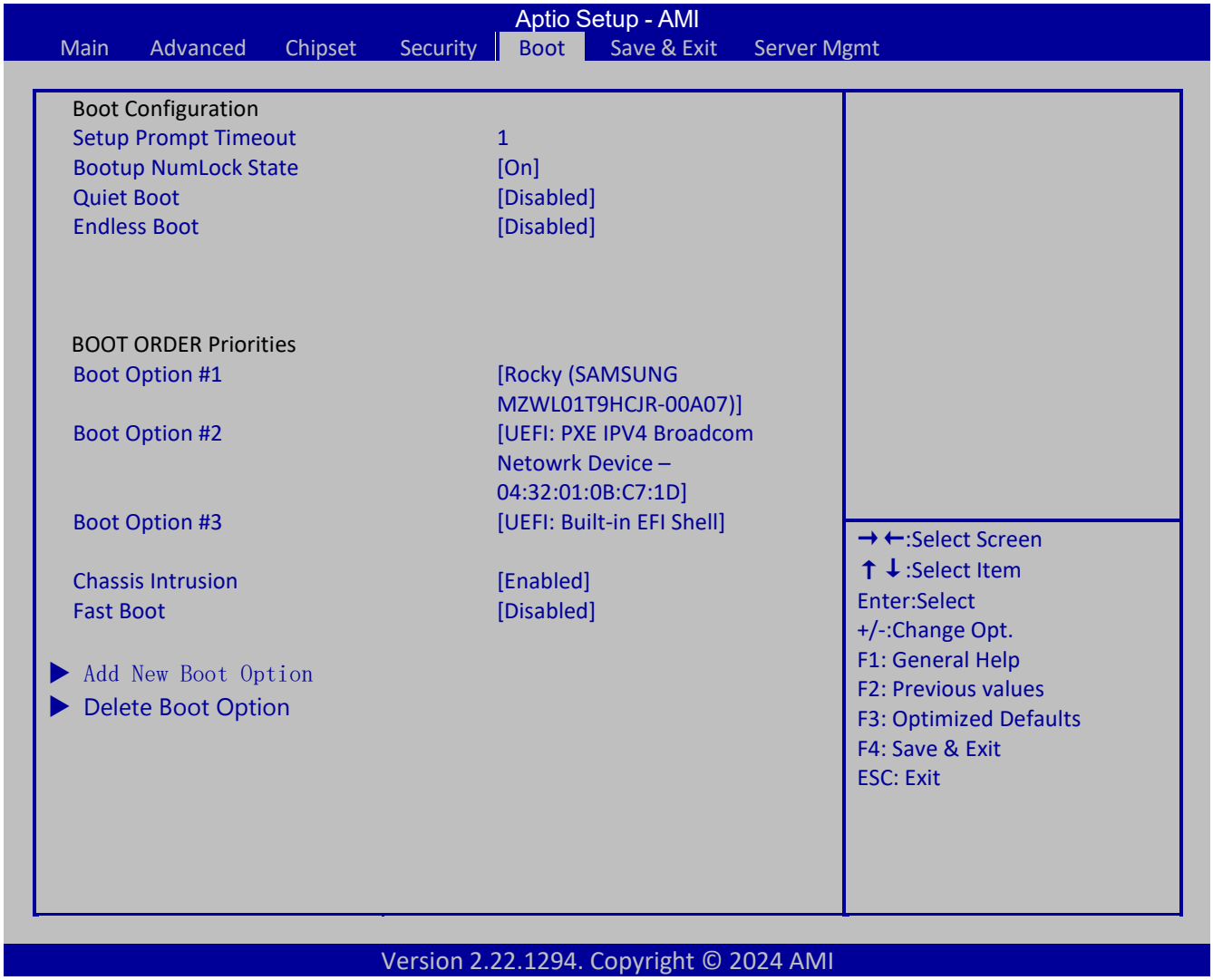
7.4.1.1 Expert Key Management



Security \ Secure Boot		
Menu Fields	**Settings**	**Comments**
Factory Key Provision	**[Disabled]** [Enabled]	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Restore Factory Keys	Executable item	Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode	Executable item	Delete all Secure Boot key databases from NVRAM
Enroll Efi Image	Executable item	Allow Efi image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
Export Secure Boot Variables	Executable item	Save NVRAM content of Secure Boot variable to a file
Platform Key (PK)	[Update]	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
Key ExChange Keys (KEK)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Authorized Signatures (db)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Forbidden Signatures (dbx)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
Authorized TimeStamps (dbt)	[Update] [Append]	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST

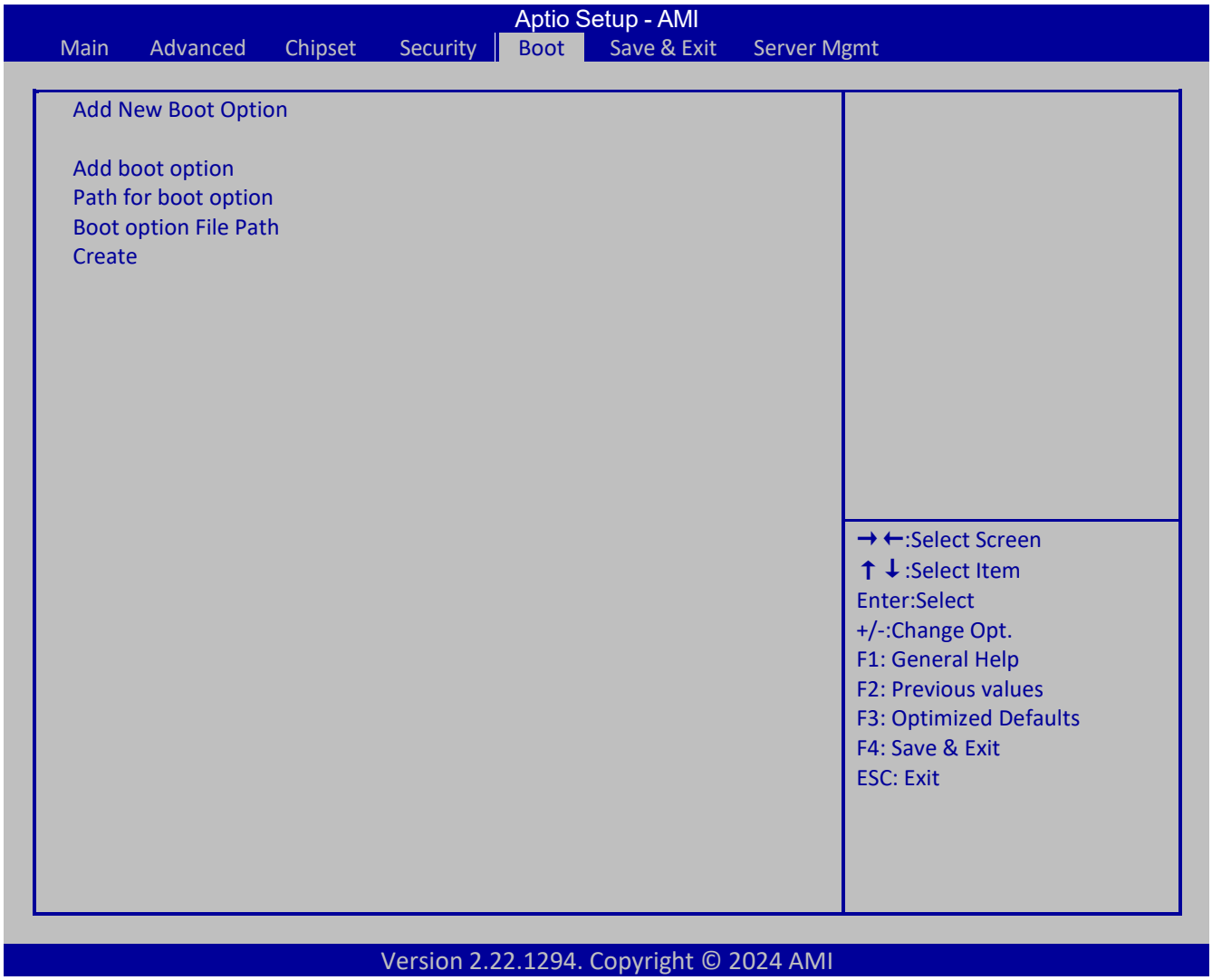
Security \ Secure Boot		
Menu Fields	**Settings**	**Comments**
		b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory,Modified,Mixed
OsRecovery Signatures (dbr)	[Update] [Append]	Enroll Factory Defaults or load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

7.5 BOOT



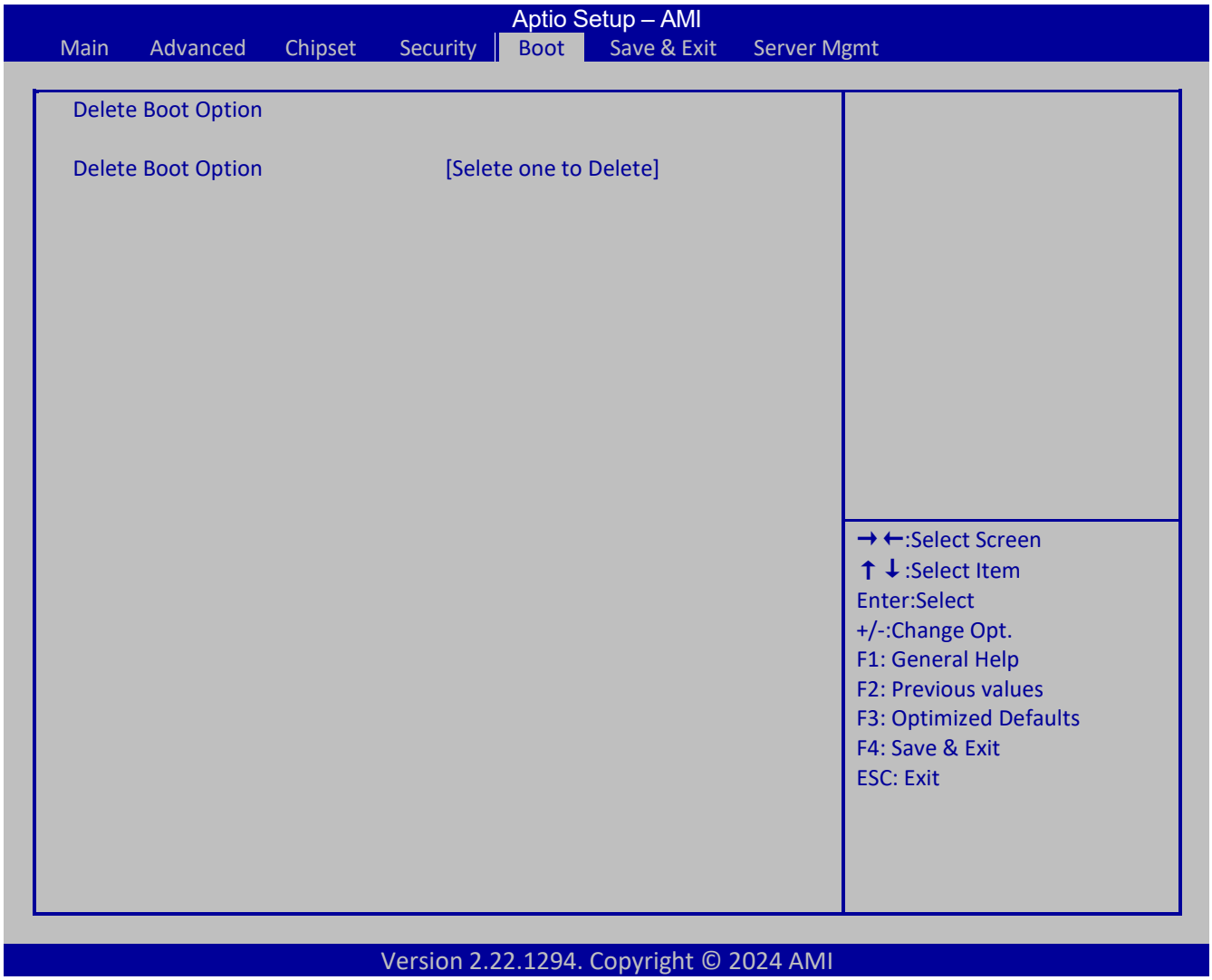
Boot		
Menu Fields	**Settings**	**Comments**
Setup Prompt Timeout	X	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**[On]** [Off]	Select the keyboard NumLock state
Quiet Boot	[**Disabled**] **[**Enabled**]**	Enables or disables Quiet Boot option
Endless Boot	**[Disabled]** [Enabled]	Enabled: BIOS try bootable devices constantly in loop until finding a bootable device(Excluding Built-in EFI Shell)
Boot Option #1	Executable item	Sets the system boot order
Boot Option #2	Executable item	Sets the system boot order
Boot Option #3	Executable item	Sets the system boot order
Boot Option #4	Executable item	Sets the system boot order
Boot Option #5	Executable item	Sets the system boot order
Boot Option #6	Executable item	Sets the system boot order
Boot Option #7	Executable item	Sets the system boot order
Chassis Intrusion	**[**Disabled**]** [**Enabled**]	Chassis Intrusion
Fast Boot	**[Disabled]** [Enabled]	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
Add New Boot Option	**Selete sub menu**	Add a new EFI boot option to the boot order
Delete Boot Opion	**Selete sub menu**	Delete a new EFI boot option to the boot order

7.5.1 Add New Boot option



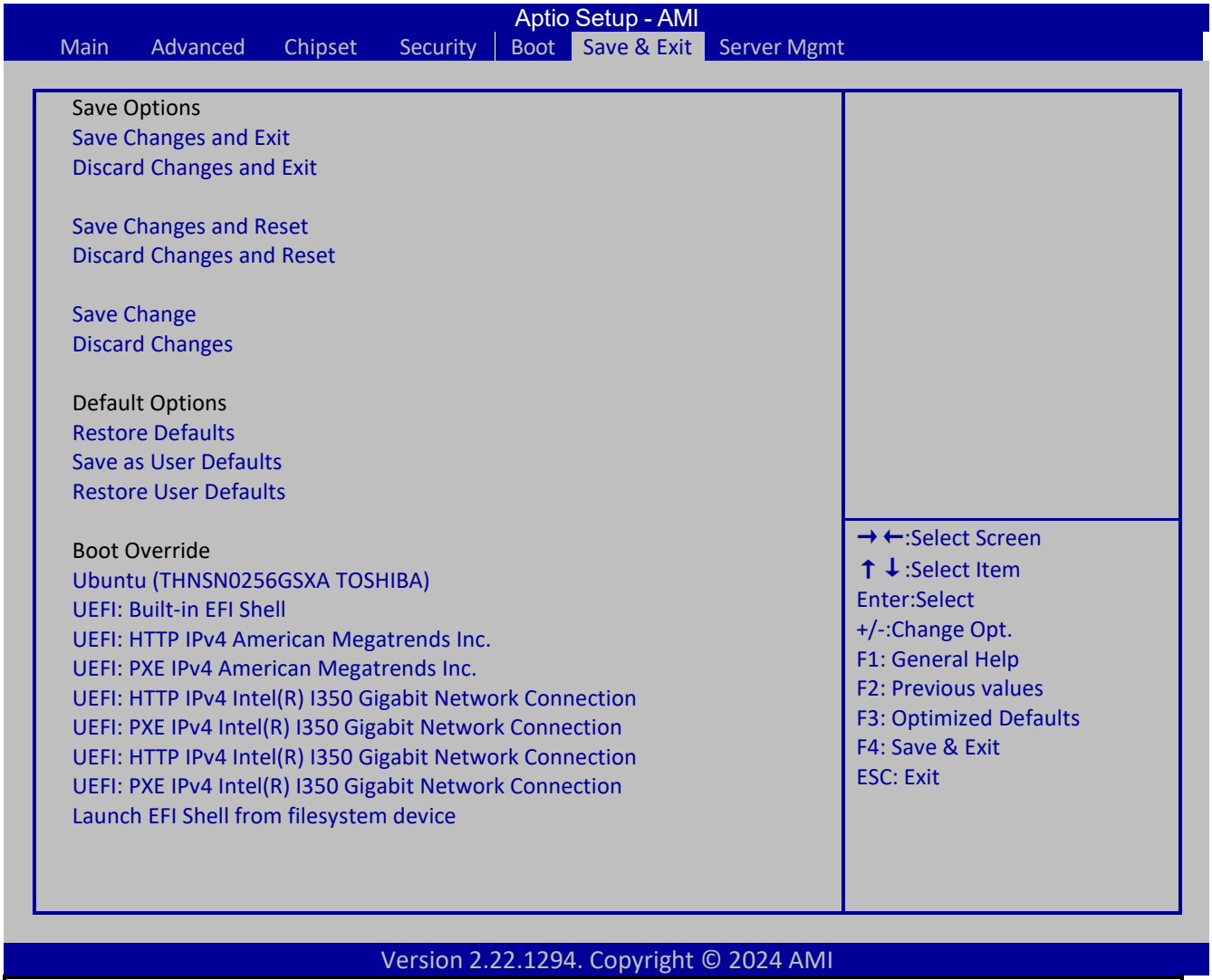
Boot \Add New Boot Option		
Menu Fields	**Settings**	**Comments**
Add boot option	Executable item	Specify name for new boot option
Path for boot option	Executable item	Enter the path to the boot option in the format fsx:\path\filename.efi
Create	Executable item	Creae the newly formed boot option

7.5.2 Delete Boot option



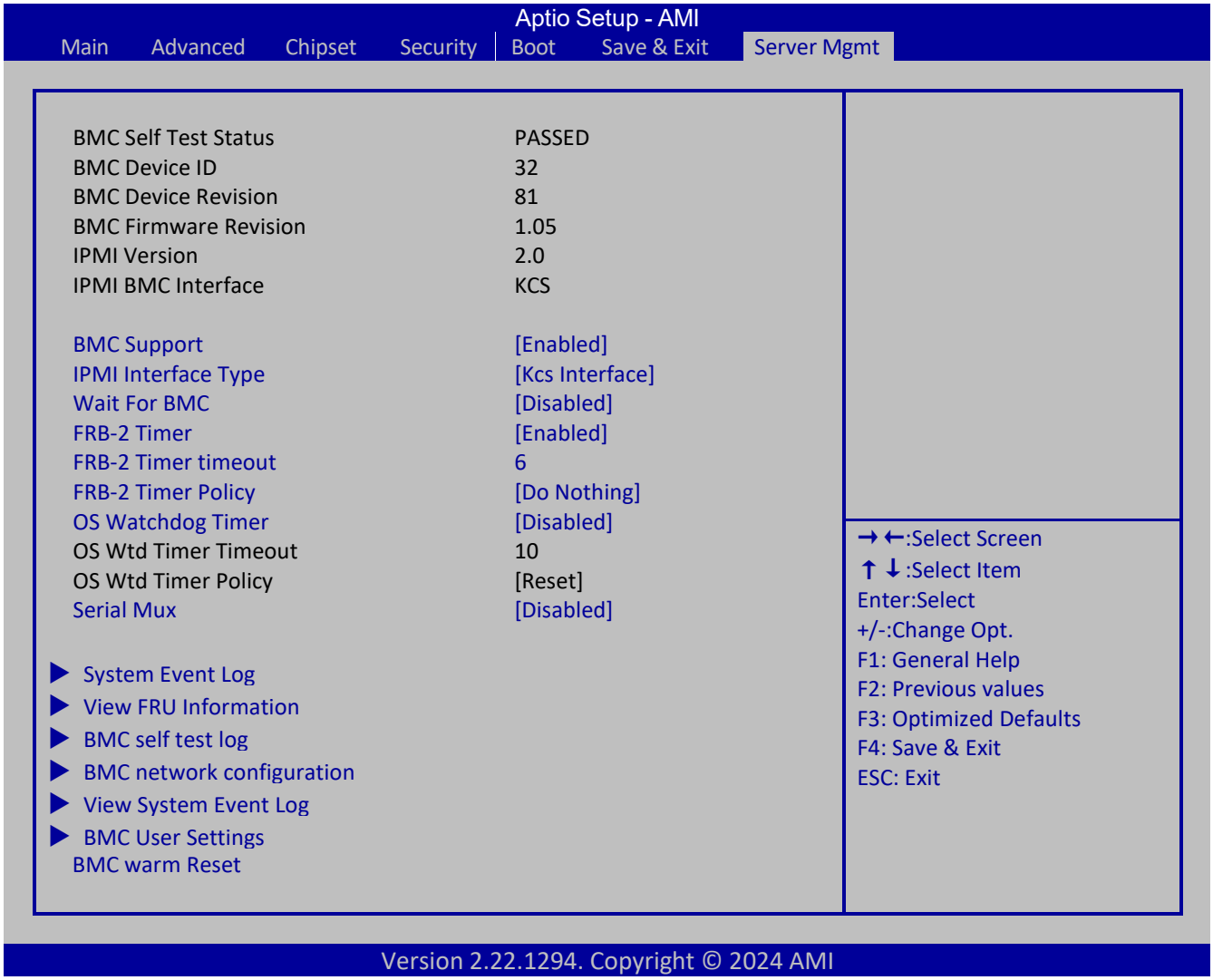
Boot \ Delete Boot Option		
Menu Fields	**Settings**	**Comments**
Delete Boot Option	Executable item	Remove an EFI boot option from the boot order

7.6 SAVE & EXIT



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

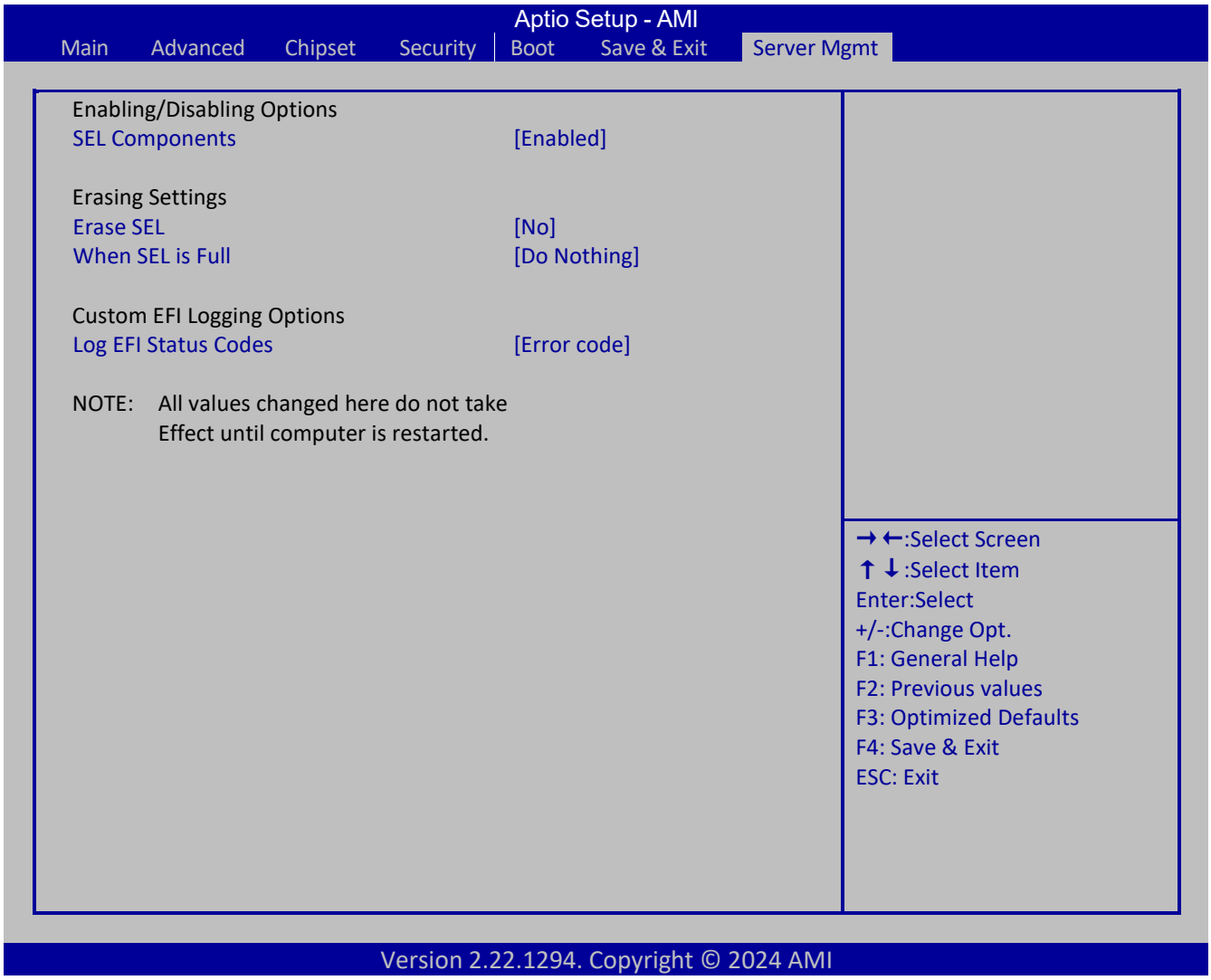
7.7 SERVER MGMT



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

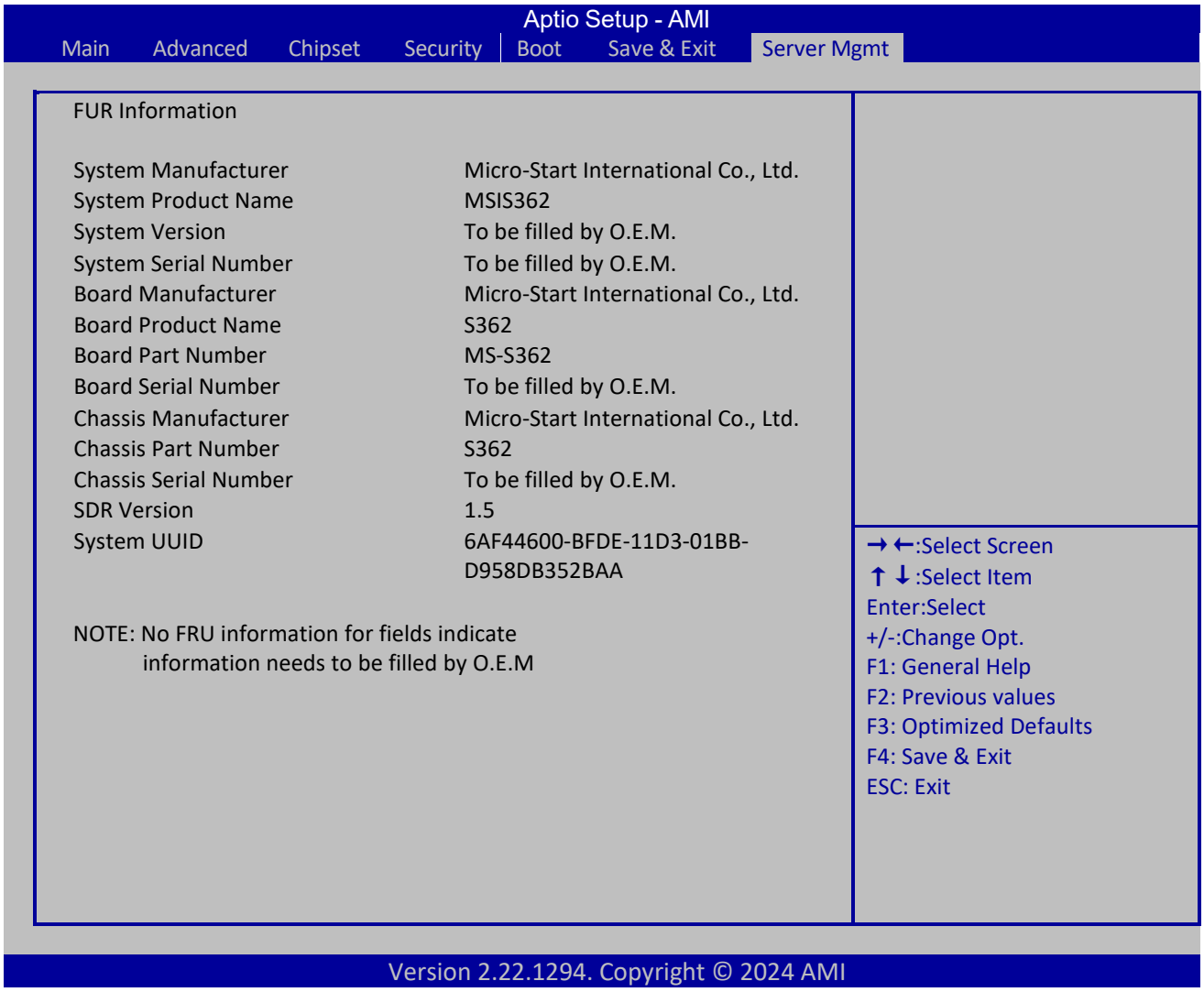
Advanced		
Menu Fields	**Settings**	**Comments**
OS Watchdog Timer	[Enabled] **[Disabled]**	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS success fully loaded or follows the OS Boot Watchdog Timer policy.
OS Wtd Timer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

7.7.1 System Event Log

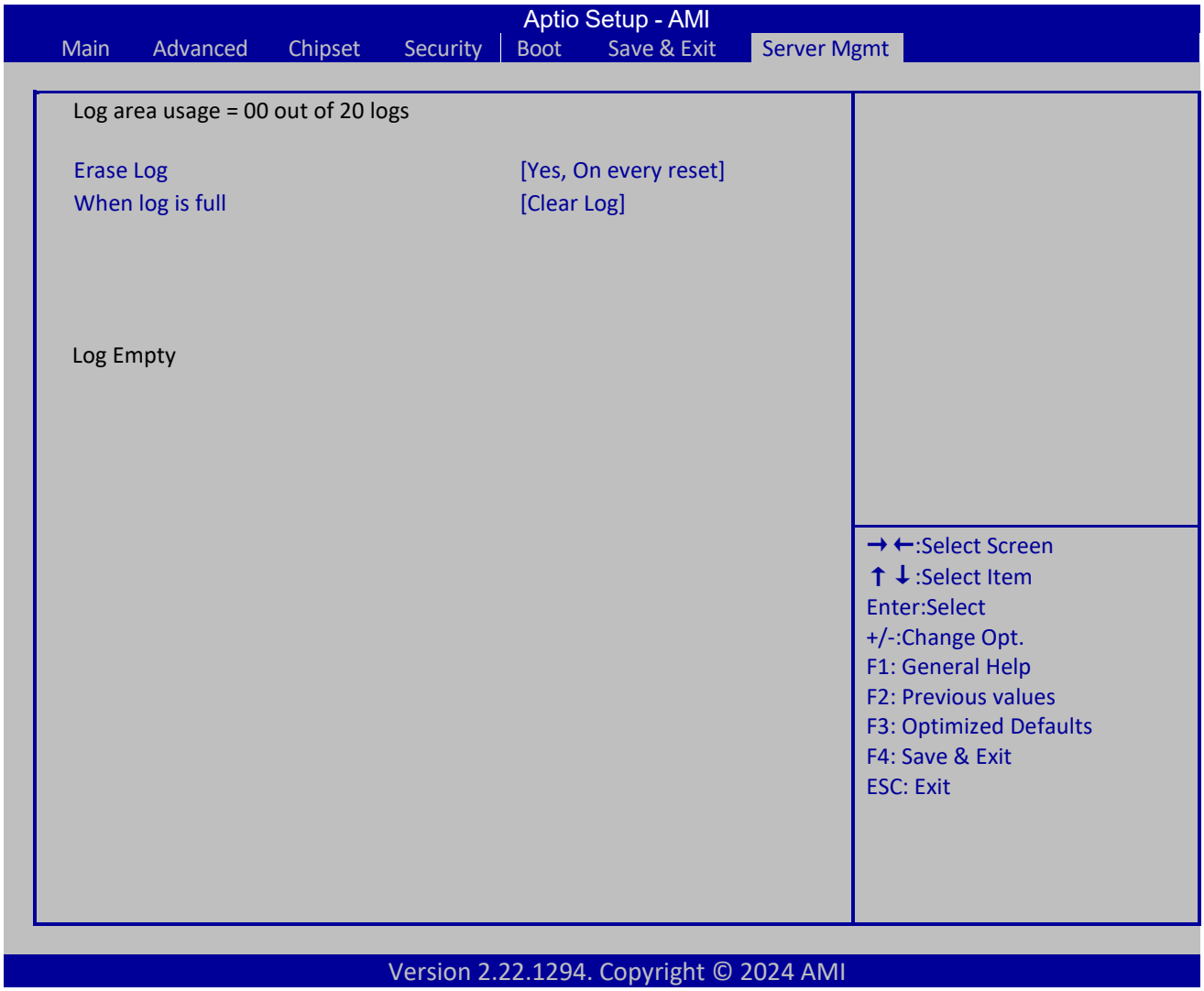


Advanced		
Menu Fields	**Settings**	**Comments**
SEL Components	[Disabled] **[Enabled]**	Change this to enabled or disable event logging for error/progress codes during boot.
Erase SEL	**[No]** [Yes, On next reset] [Yes, On every reset]	Choose options for erasing SEL.
When SEL is Full	**[Do Nothing]**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

7.7.2 View FRU information

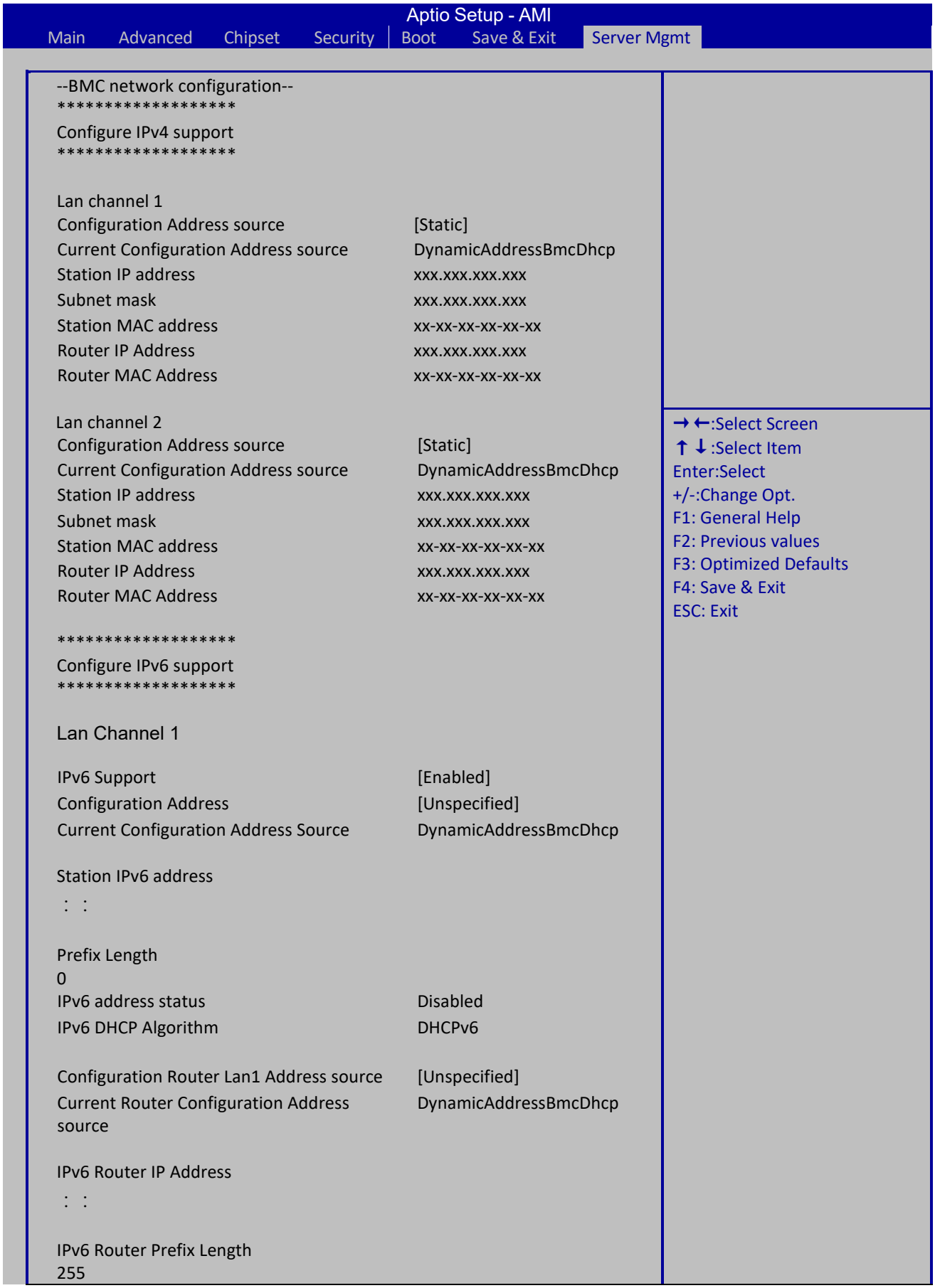


7.7.3 Bmc Self Test log



Advanced		
Menu Fields	**Settings**	**Comments**
Erase Log	**[Yes, On every reset]** [No]	Erase Log Options
When log is full	**[Clear Log]** [Do not log any more]	Select the action to be taken when log is full

7.7.4 BMC network Configuration



IPv6 Router Prefix Value
: :

Lan Channel 2

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

Station IPv6 address
: :

Prefix Length
0

IPv6 address status	Disabled]
IPv6 DHCP Algorithm	DHCPv6

Configuration Router Lan2 Address source	[Unspecified]

Current Router Configuration Address source	DynamicAddressBmcDhcp

IPv6 Router IP Address
: :

IPv6 Router Prefix Length
255

IPv6 Router Prefix Value
: :

****
Configure VLAN support
****

Lan channel 1

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

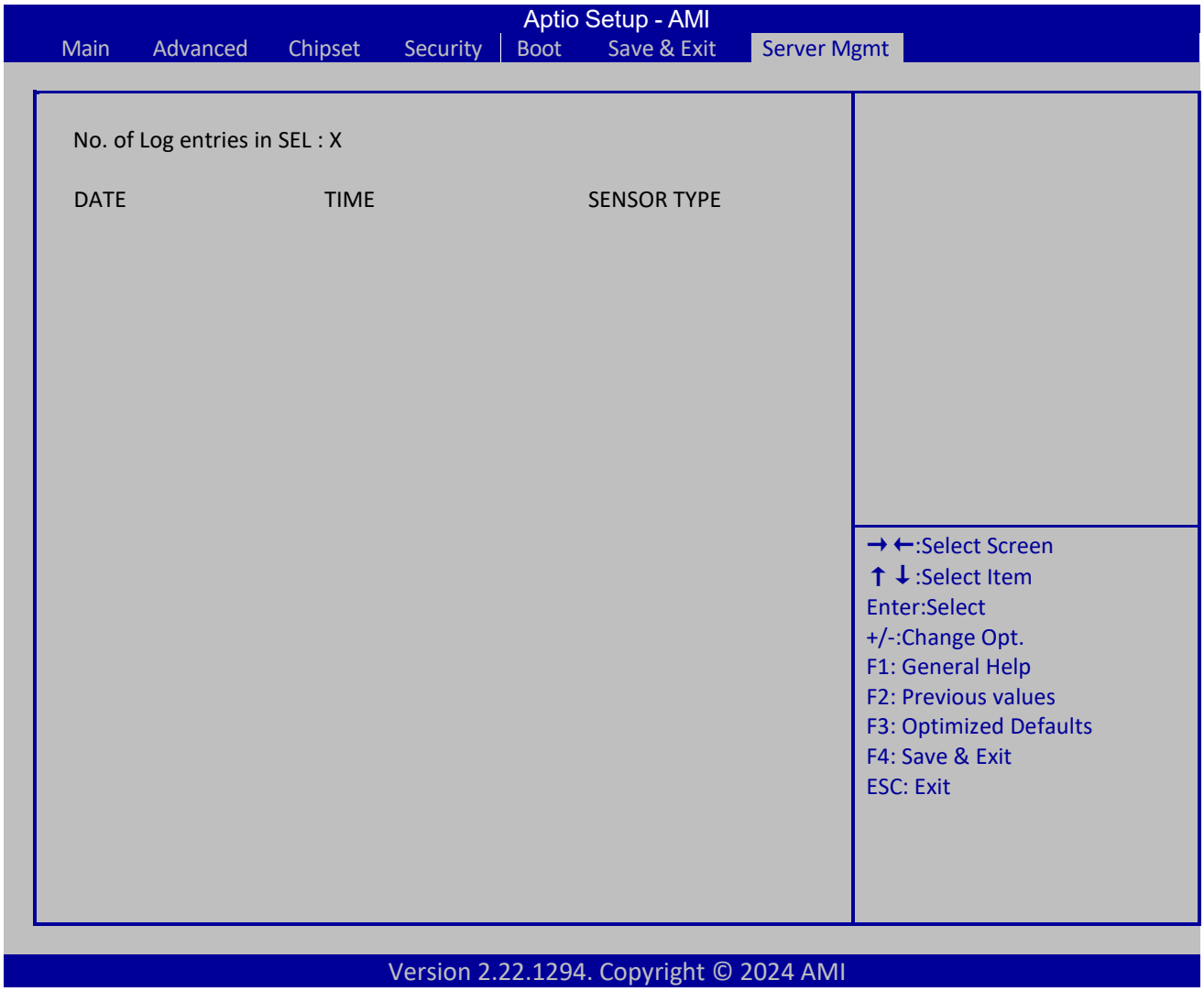
Lan channel 2

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

Advanced		
Menu Fields	**Settings**	**Comments**
**********		
Configure IPv4 support		
**********		
Configuration Address source	**[Unspecified]** [Static] [DynamicBmcDhcp] [DynamicBmcNonDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
Current Configuration Address source	DynamicAddressBmcDhcp	Current LAN Configuration statically or dynamically(by BIOS or BMC). Unspecified for not Configured address space
Station IP address	Executable item	Enter station IP address
Subnet mask	Executable item	Enter subnet
Station MAC address	xx-xx-xx-xx-xx-xx	Station MAC address from BMC
Router IP Address	Executable item	Enter router IP address
Router MAC Address	Executable item	Enter router MAC address
**********		
Configure IPv6 support		
**********		
IPv6 Support	**[Enabled]** [Disabled]	Enable or Disable Lan IPv6 Support
Configuration Address	**[Unspecified]** [Static] [DynamicBmcDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
Current Configuration Address Source	DynamicAddressBmcDhcp	Current LAN Configuration statically or dynamically(by BIOS or BMC). Unspecified for not Configured address space
Station IPv6 address	Executable item	Enter Station IPv6 address
Prefix Length	Executable item	Change the prefix length
Configuration Router Lan Address Source	**[Unspecified]** [Static] [DynamicBmcDhcp]	Select to configure Lan channel Parameters Statically or dynamically (by BIOS or BMC). Unspecified option will not modify and BMC network parameters during BIOS phase.
IPv6 Router IP Address	Executable item	Change the IPv6 Router IP Address
IPv6 Router Prefix Length	Executable item	Change the IPv6 Router Prefix Length
IPv6 Router Prefix Value	Executable item	Change the IPv6 Router Prefix Value
**********		
Configure VLAN support		
**********		
VLAN Support	[Enabled] [Disabled] **[Unspecified]**	Enabled VLAN Support to Specify the 802.1q VLAN ID.

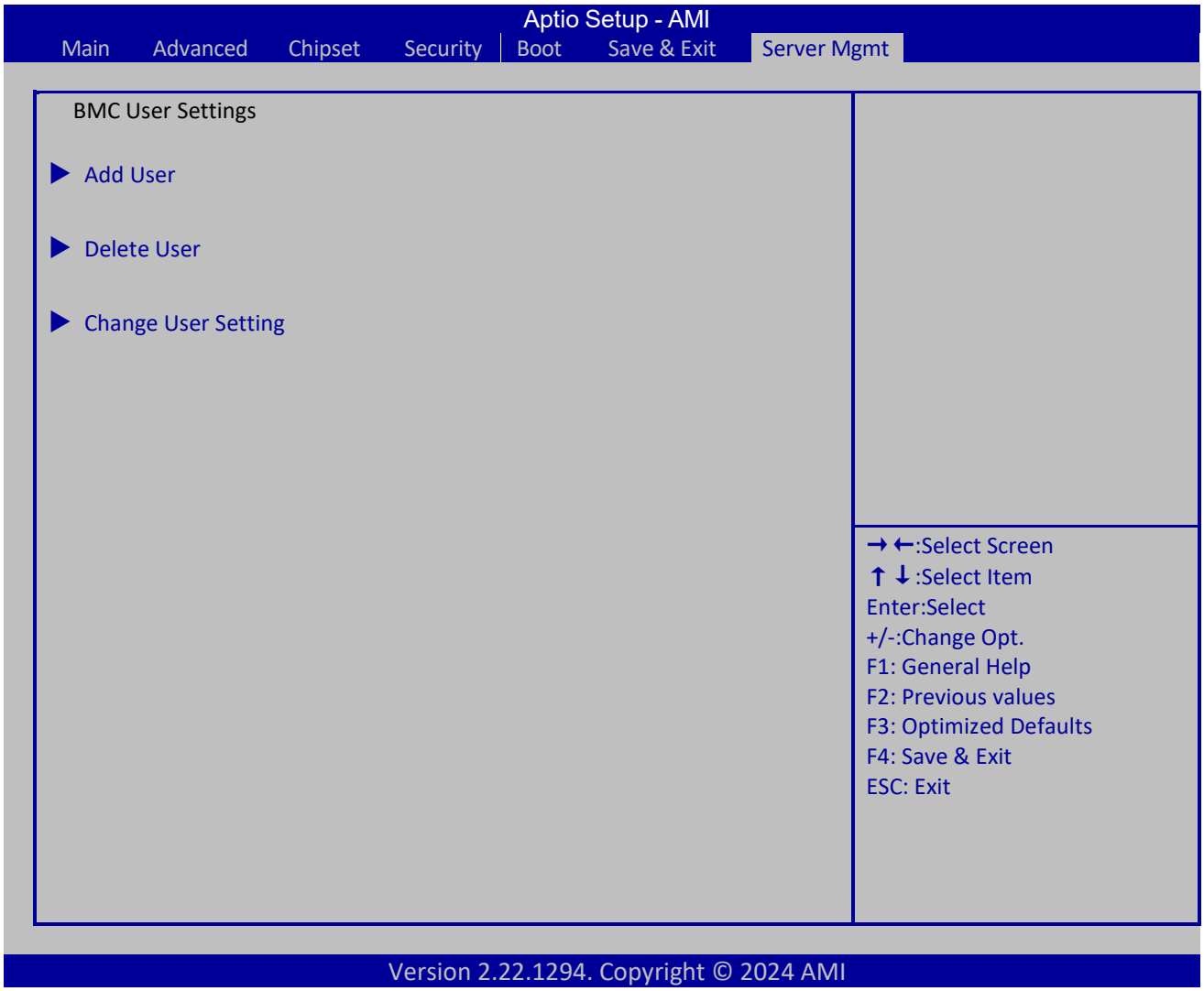
Advanced		
Menu Fields	**Settings**	**Comments**
VLAN ID	Executable item	VLAN ID Range is from 1-4094. VLAN ID 0 & 4095 are reserved VALN ID's
VLAN Priority	Executable item	Value ranges from 0 to 7. 7is the highest priority for VLAN.

7.7.5 View System Event Log



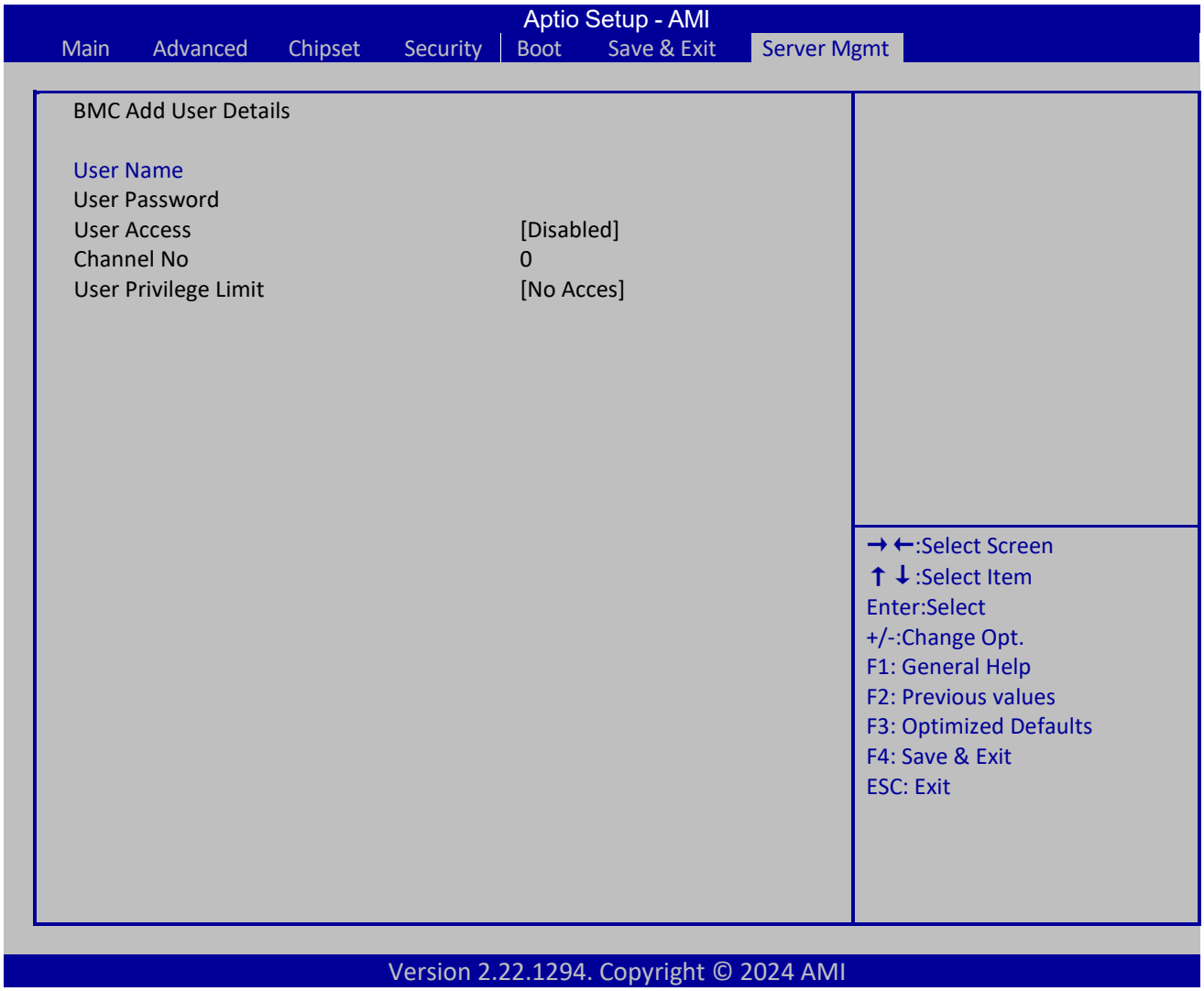
Advanced		
Menu Fields	**Settings**	**Comments**
Erase Log	**[Yes, On every reset]** [No]	Erase Log Options
When log is full	**[Clear Log]** [Do not log any more]	Select the action to be taken when log is full

7.7.6 BMC User Settings



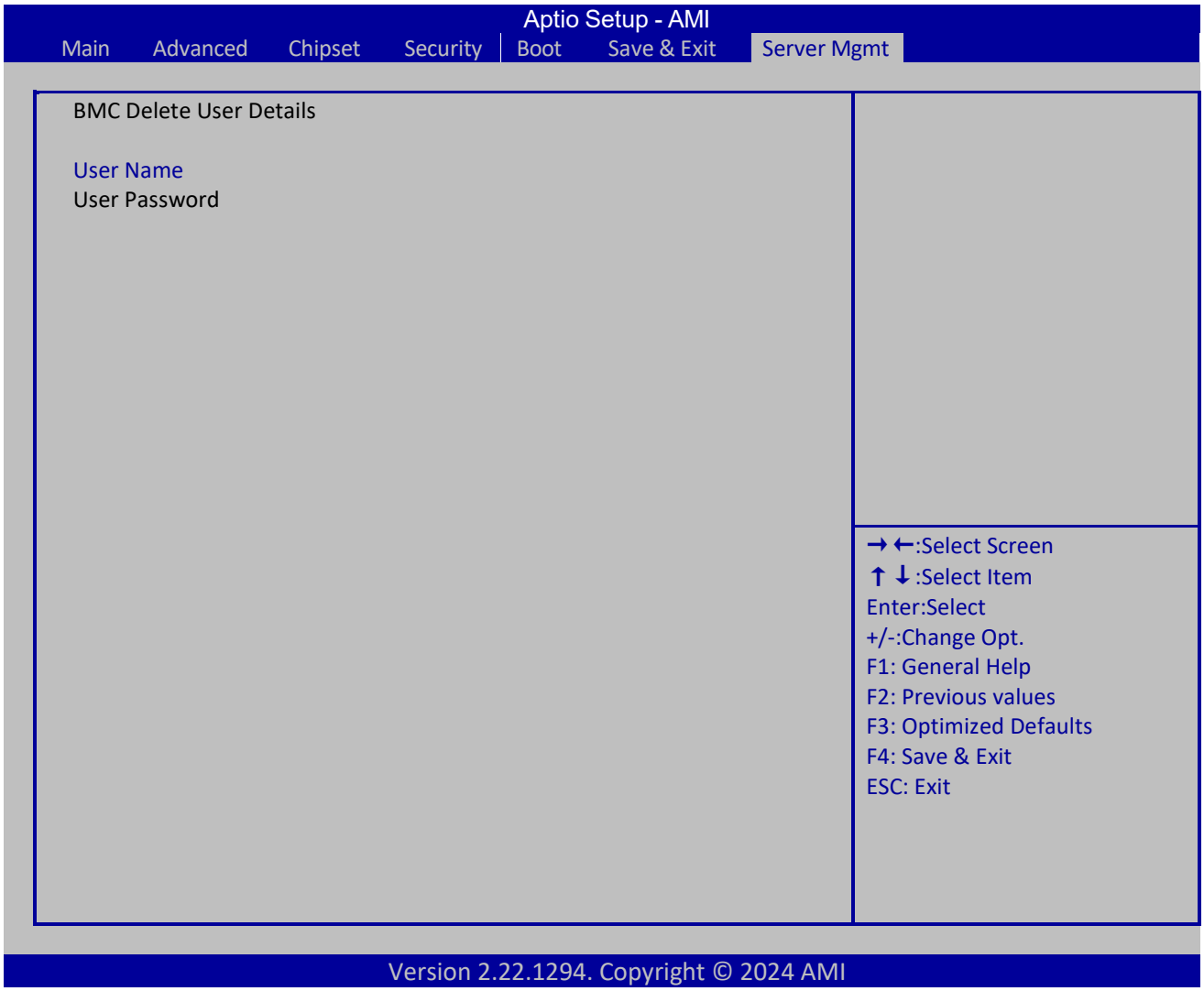
Advanced		
Menu Fields	**Settings**	**Comments**
Add User	Selects sub-menu	
Delete User	Selects sub-menu	
Change User Settings	Selects sub-menu	

7.7.6.1 Add User



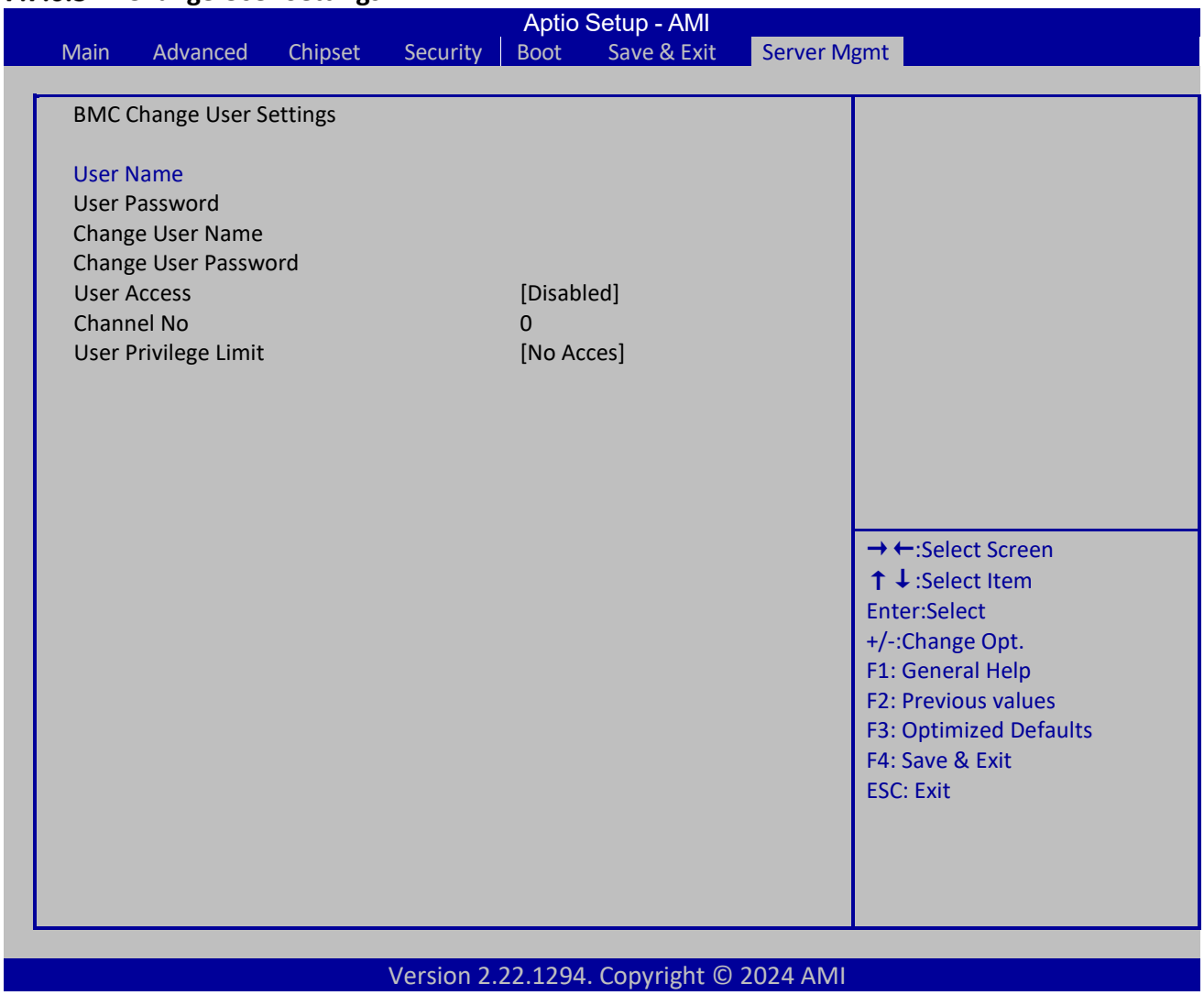
Server Mgmt \ BMC User Settings \ Add User		
Menu Fields	**Settings**	**Comments**
BMC Add User Details		
User Name		Enter BMC User Name
User Password		Enter BMC User Password
User Access	[Enabled] **[Disabled]**	Enable/Disable the BMC User's Access.
Channel No	**0**	Enter BMC Channel Number
User Privilege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

7.7.6.2 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

7.7.6.3 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

8 STATUS CODES LIST

8.1 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.

8.1.1 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

8.1.2 PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)

0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	

0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future 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
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

8.1.3 DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization

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

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