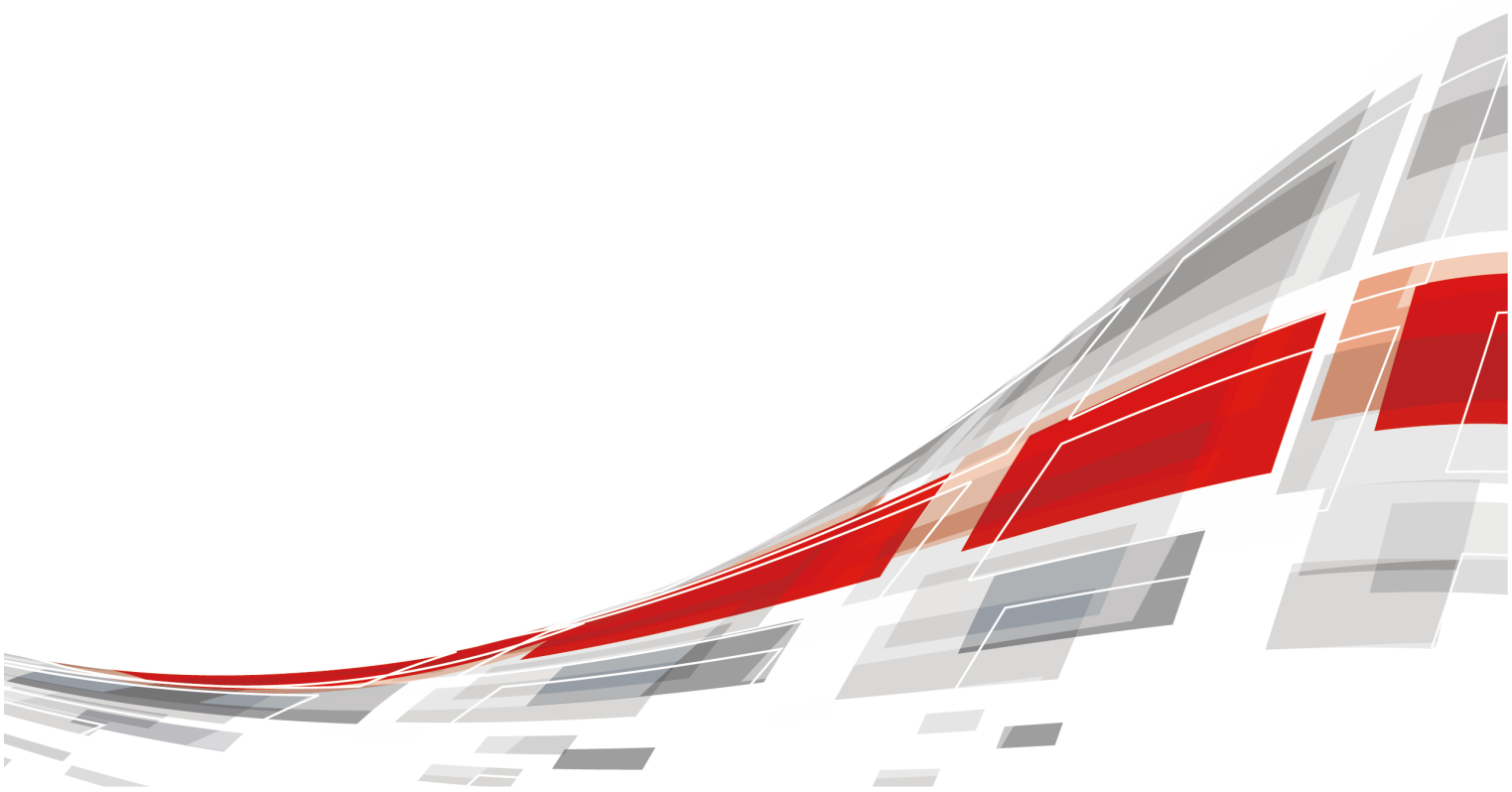
Server Eagle Stream Platform BIOS

Parameter Reference

Issue 21

Date 2025-09-30



XFUSION INTERNATIONAL PTE. LTD.

Copyright © XFUSION INTERNATIONAL PTE. LTD. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of XFUSION INTERNATIONAL PTE. LTD.

Trademarks and Permissions

XFUSION and other xFusion trademarks are trademarks of XFUSION INTERNATIONAL PTE. LTD. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between xFusion and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

XFUSION INTERNATIONAL PTE. LTD.

Website: https://www.xfusion.com

About This Document

Overview

This document describes the menus, parameters, and common tasks of the basic input/output system (BIOS) based on the Eagle Stream platform.

This document is applicable to the following products:

Rack servers:

- 1288H V7
- 2288 V7
- 2288H V7
- 2488H V7
- 5288 V7
- 5298 V7
- 5885H V7

AI servers:

- G5200 V7
- G5500 V7
- G8600 V7

This document uses the BIOS screens of the 1288H V7 server or the 5885H V7 server as an example. The BIOS screens vary depending on the server model.

Intended Audience

This document is intended for:

- Technical support engineers
- Enterprise administrators
- Enterprise device users

Symbolic Conventions

The symbols that may be found in this document are defined as follows:

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, could result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Change History

Version	Release Date	Description
21	2025-09-30	• Updated the **2 BIOS Overview**. • Added the description of the **Re-Size BAR Support** and **BAR Size** in the **5.2.5 Misc Configuration**. • Updated the description of the **TME-MT Keys** option in the **5.2.7.1 Processor Configuration**. • Updated the description of the **Memory Frequency** in the **5.2.7.4 Memory Configuration**. • Added the description of the **PSS Table Turbo Frequency** in the **5.2.7.6.1 CPU P-State Control**. • Updated the description of the **PXE Timeout Control** option in the **5.4 Boot**. • Added the description of the **Memory integrity**, **TDX Secure Arbitration Mode Loader (SEAM Loader)** and **Disable excluding Mem below 1MB** option in CMR in the **6.2.5.1 Processor Configuration**. • Updated the description of the **Total Memory Encryption (TME) Bypass**, **Total Memory Encryption Multi-Tenant (TME-MT)**, **Key stock amount**, **TME-MT key ID bits**, **TME-MT/TDX key split**, **TME-MT Keys:**, **TDX keys:** and **Trust Domain Extension (TDX)** option in the **6.2.5.1 Processor Configuration**. • Updated the description of the **Uncore Per Socket Configuration** in the **6.2.5.3 Uncore Configuration**. • Updated the description of the **Link Frequency Select** in the **6.2.5.3.1 Uncore General Configuration**. • Added the description of the **Force PPR On All Dram For UCE** and **Memory Frequency** in the **6.2.5.4 Memory Configuration**. • Updated the description of the **CPU Frequency Select** and added the description of the **PSS Table Turbo**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Version	Release Date	Description
		Frequency in the **6.2.5.6 Advanced Power Management Configuration**. • Added the description of the PCIe ACSCTL option in the **6.2.5.5.2 Intel(R) Virtualization for Directed I/O (VT-d)**. • Updated the description of the **PPD** in the **6.2.5.6.8 Memory Power & Thermal Configuration**. • Added the description of the **PCI Express Configuration** in the **6.2.7 PCH-IO Configuration**. • Added the description of the **TPM State** option in the **6.3 Security**. • Updated the description of the **PXE Timeout Control** option in the **6.4 Boot**. • Added the description of the **Hard Disk Drive**, **DVD-ROM Drive**, **PXE** and **Others** in the **6.4.1 Boot Sequence**.
20	2025-08-31	• Updated the description of the **Flow Control** option in the **5.2.11 Console Redirection Configuration**. • Added the description of the **MOR State** option in the **5.3 Security**. • Updated the description of the **PCIe SR-IOV** option in the **6.2.2.1 SR-IOV Setup Settings**. • Updated the description of the **Manual Commit S3M FW CFR** and **Manual Commit PUcode CFR** options in the **6.2.5.1.2 Processor CFR Configuration**. • Added the description of the **Legacy USB Support** option in the **6.2.7.3 USB Configuration**. • Updated the description of the **Memory SN Customization** option in the **6.2.8 Misc Configuration**.
19	2025-07-31	Added the description of the **Re-Size BAR Support** and **BAR Size** options in the **6.2.8 Misc Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Version	Release Date	Description
18	2025-06-23	• Updated the descriptions of the **Time Zone** and added the descriptions of the **Synchronize Time Zone With BMC** options in the **5.1 Main**. • Added the description of the **Memory SN Customization** option in the **5.2.5 Misc Configuration**. • Added the description of the **Memory SN Customization** option in the **B Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**.
17	2025-03-27	• Added the descriptions of the **Time Zone** and **Daylight Saving Time** options in the **5.1 Main**. • Added the descriptions of the **Memory CE Record** and **PCIe CE Record** options in the **5.2.6 System Event Log**.
16	2025-02-14	Added the description of the **Link Speed Mode** option in the **5.2.7.3.1 Uncore General Configuration**.
15	2024-11-04	Updated the description of the **MBA BW Calibration Profiles** option in the **5.2.7.3.1 Uncore General Configuration**.
14	2024-08-27	Added the descriptions of the **Memory integrity**, **TDX Secure Arbitration Mode Loader (SEAM Loader)** and **Disable excluding Mem below 1MB in CMR** options in the **5.2.7.1 Processor Configuration**.
13	2024-07-30	Added the description of the **Surprise Hot Plug Support** option in the **5.2.7.5.5 Intel(R) VMD Technology**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Version	Release Date	Description
12	2024-05-27	• Added the description of the **System Cloaking** option in the **5.2.6 System Event Log**. • Added the descriptions of the **Whea Log Memory Error**, **Whea Log Processor Error** and **Whea Log PCI Error** options in the **5.2.6.2 WHEA Setttings**. • Added the description of the **ME Seg Error Injection Support** option in the **5.2.6.3 Error Injection Settings**. • Added the description of the **Enable ADDDC Error Injection** option in the **5.2.7.4.6 Memory RAS Configuration**.
11	2024-03-29	• Added **B Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**. • Added **C Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**.
10	2023-12-30	• Updated **5.2.7.4.6 Memory RAS Configuration**. • Updated **5.2.7.5.1 SocketX Configuration**. • Updated **5.2.7.6 Advanced Power Management Configuration**. • Added **5.2.7.6.4 UCP**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Version	Release Date	Description
09	2023-11-30	• Updated **3.1.1 Accessing the Front Page**. • Updated **3.1.4 Accessing the Smart Provisioning GUI**. • Updated **4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**. • Updated **5 Description of Setup Utility (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**. • Updated **5.2.7.1 Processor Configuration**. • Added **5.2.7.1.2 In Field Scan (IFS)**. • Updated **5.2.7.3 Uncore Configuration**. • Updated **5.2.7.4.5 Memory Map**. • Updated **5.2.7.4.6 Memory RAS Configuration**. • Updated **5.2.7.5 IIO Configuration**. • Added **5.2.7.5.2 IOAT Configuration**. • Updated **5.2.7.6.1 CPU P-State Control**. • Updated **5.2.7.6.8 CPU Advanced PM Tuning**.
08	2023-10-30	• Updated **5.2.7.4.6 Memory RAS Configuration**. • Updated **5.2.7.5.4 Intel Virtualization for Directed I/O(VT-d)**. • Updated **6.2.5.4.5 Memory RAS Configuration**.
07	2023-09-20	Added information about the G5500 V7.
06	2023-08-31	• Updated **5.3.2 TLS Certificate Manager**. • Updated **6.3.2.1 CA Manager**. • Updated **6.3.2.2 CRL Manager**.
05	2023-08-03	Added information about the 2488H V7.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Version	Release Date	Description
04	2023-07-20	• Updated **3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**. • Updated **6.1 Main**. • Updated **6.2 Advanced**. • Updated **6.4 Boot**. • Added information about the 2288 V7, 5288 V7, and G5200 V7.
03	2023-06-21	Added information about the G8600 V7.
02	2023-05-24	Added information about the 5885H V7.
01	2023-04-26	This issue is the first official release.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Contents

About This Document ii
1 Before You Start 1
2 BIOS Overview 2
3 Common Operations 7
3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7) 7
3.1.1 Accessing the Front Page 7
3.1.2 Accessing the Setup Utility Screen 12
3.1.3 Accessing BIOS Using a Serial Port 12
3.1.4 Accessing the Smart Provisioning GUI 15
3.1.5 Querying CPU Information 18
3.1.6 Querying Memory Information 22
3.1.7 Querying Drive Information 26
3.1.8 Querying the BMC IP Address 30
3.1.9 Setting the BIOS System Language 34
3.1.10 Setting the BIOS System Time and Date 35
3.1.11 Setting the BIOS Password 36
3.1.11.1 Setting the BIOS Administrator Password 36
3.1.11.2 Setting the BIOS Common User Password 38
3.1.12 Setting PXE for an NIC 40
3.1.12.1 Setting PXE for an OCP NIC 40
3.1.12.2 Setting the PXE Function for a PCIe NIC 42
3.1.13 Setting the TXT Function 45
3.1.14 Setting the Fan Speed Adjustment Mode 49
3.1.15 Setting Secure Boot in UEFI Mode 53
3.1.16 Setting the Server Boot Mode 56
3.1.17 Setting the Server Boot Device 59
3.1.18 Setting the BMC User Password 63
3.1.19 Setting the BMC Network Information 67
3.1.20 Setting a PCIe Port 72
3.1.21 Setting Serial Port Redirection 77
3.1.22 Enabling Software Guard Extension 79
3.1.23 Restoring Default BIOS Settings 84

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)....87
3.2.1 Accessing the Front Page....87
3.2.2 Accessing the Setup Utility Screen....92
3.2.3 Accessing BIOS Using a Serial Port....94
3.2.4 Accessing the Smart Provisioning GUI....97
3.2.5 Querying CPU Information....100
3.2.6 Querying Memory Information....102
3.2.7 Querying the SATA Drive Information....105
3.2.8 Querying the BMC IP Address....107
3.2.9 Setting the BIOS System Language....111
3.2.10 Setting the BIOS System Time and Date....112
3.2.11 Setting the BIOS Password....113
3.2.11.1 Setting the BIOS Administrator Password....114
3.2.11.2 Setting the BIOS Common User Password....115
3.2.12 Setting PXE for a NIC....117
3.2.12.1 Setting the PXE Function for an OCP NIC....117
3.2.12.2 Setting the PXE Function for a PCIe NIC....120
3.2.13 Setting the TXT Function....123
3.2.14 Setting the Fan Speed Adjustment Mode....127
3.2.15 Setting the Server Boot Mode....130
3.2.16 Setting the Server Boot Device....133
3.2.17 Setting the BMC User Password....138
3.2.18 Setting the BMC Network Information....142
3.2.19 Setting a PCIe Port....146
3.2.20 Setting Serial Port Redirection....150
3.2.21 Restoring BIOS Factory Settings....152

4 Description of the Front Page....156

4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)....156
4.1.1 Boot Manager....159
4.1.2 Device Manager....160
4.1.3 Boot From File....162
4.1.4 Administer Secure Boot....163
4.1.4.1 PK Options....166
4.1.4.1.1 Enroll PK....167
4.1.4.1.2 Delete PK....167
4.1.4.2 DBX Options....168
4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)....170
4.2.1 Boot Manager....172
4.2.2 Device Manager....174
4.2.3 Boot From File....176
4.2.4 Administer Secure Boot....176
4.2.4.1 Custom Secure Boot Options....179

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

4.2.4.1.1 DB Options....181

5 Description of Setup Utility (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)....185

5.1 Main....185
5.2 Advanced....190
5.2.1 Platform Information....192
5.2.2 Peripheral Configuration....193
5.2.2.1 SR-IOV Setup Settings....194
5.2.2.2 SIO 1711....196
5.2.3 Video Configuration....198
5.2.4 ACPI Table or Features Control....198
5.2.5 Misc Configuration....199
5.2.6 System Event Log....202
5.2.6.1 eMCA Setttings....207
5.2.6.2 WHEA Setttings....209
5.2.6.3 Error Injection Settings....211
5.2.6.4 Memory Error Enabling....213
5.2.6.5 IIO Error Enabling....215
5.2.6.6 PCIe Error Enabling....217
5.2.6.7 Error Control Setting....219
5.2.6.8 DWR Configuration....220
5.2.7 Socket Configuration....222
5.2.7.1 Processor Configuration....223
5.2.7.1.1 Per-Socket Information....238
5.2.7.1.2 In Field Scan (IFS)....240
5.2.7.1.3 Processor CFR Configuration....241
5.2.7.2 Common RefCode Configuration....244
5.2.7.3 Uncore Configuration....246
5.2.7.3.1 Uncore General Configuration....246
5.2.7.4 Memory Configuration....256
5.2.7.4.1 fADR Configuration....265
5.2.7.4.2 Memory Channel Control....267
5.2.7.4.3 Memory Topology....268
5.2.7.4.4 Page Policy....269
5.2.7.4.5 Memory Map....270
5.2.7.4.6 Memory RAS Configuration....273
5.2.7.4.7 PMem Configuration....280
5.2.7.4.8 Memory Dfx Configuration....286
5.2.7.4.9 BSSA Configuration Menu....288
5.2.7.5 IIO Configuration....290
5.2.7.5.1 Socket*X* Configuration....293
5.2.7.5.2 IOAT Configuration....300

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.7.5.3 IIO Stack IO Resource Configuration....302
5.2.7.5.4 Intel Virtualization for Directed I/O(VT-d)....303
5.2.7.5.5 Intel(R) VMD Technology....306
5.2.7.5.6 IIO DFX Configuration....307
5.2.7.5.7 IIO Global Performance Tuning....310
5.2.7.6 Advanced Power Management Configuration....311
5.2.7.6.1 CPU P-State Control....316
5.2.7.6.2 Hardware PM State Control....321
5.2.7.6.3 Frequency Prioritization....323
5.2.7.6.4 UCP....324
5.2.7.6.5 CPU C-State Control....325
5.2.7.6.6 Package C-State Control....328
5.2.7.6.7 CPU Thermal Management....331
5.2.7.6.8 CPU Advanced PM Tuning....332
5.2.7.6.9 Memory Power & Thermal Configuration....340
5.2.8 ME Configuration....346
5.2.8.1 Server ME Configuration....347
5.2.9 PCH-IO Configuration....348
5.2.9.1 SATA And RST Configuration....348
5.2.9.1.1 Controller *X* SATA And RST Configuration....350
5.2.9.2 USB Configuration....353
5.2.10 BMC Configuration....355
5.2.10.1 BMC Configuration....356
5.2.10.1.1 Add BMC User....364
5.2.10.1.2 Delete BMC User....366
5.2.10.1.3 Change BMC User Settings....367
5.2.11 Console Redirection Configuration....370
5.2.12 PXE Configuration....374
5.2.13 NVMe Information....376
5.2.13.1 NVMe Device Information....377
5.3 Security....378
5.3.1 Weak Password Dictionary....388
5.3.2 TLS Certificate Manager....389
5.3.2.1 Import Certificate....390
5.3.2.2 Delete Certificate....391
5.4 Boot....392
5.4.1 Boot Sequence....402
5.5 Exit....403

6 Description of Setup Utility (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)....406

6.1 Main....406
6.2 Advanced....408

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.1 Platform Information....410
6.2.2 Peripheral Configuration....411
6.2.2.1 SR-IOV Setup Settings....413
6.2.2.2 SIO 1711....415
6.2.3 Video Configuration....417
6.2.4 ACPI Table or Features Control....418
6.2.5 Socket Configuration....419
6.2.5.1 Processor Configuration....420
6.2.5.1.1 Processor Information....434
6.2.5.1.2 Processor CFR Configuration....436
1. Socket1 CFR Revision Info....438
6.2.5.2 Common RefCode Configuration....439
6.2.5.3 Uncore Configuration....441
6.2.5.3.1 Uncore General Configuration....442
6.2.5.3.2 Uncore Per Socket Configuration....452
6.2.5.4 Memory Configuration....455
6.2.5.4.1 Memory Topology....463
6.2.5.4.2 Memory Channel Control....464
6.2.5.4.3 Page Policy....466
6.2.5.4.4 Memory Map....466
6.2.5.4.5 Memory RAS Configuration....467
6.2.5.4.6 PMem Configuration....472
6.2.5.4.7 Memory Dfx Configuration....479
6.2.5.4.8 BSSA Configuration Menu....480
6.2.5.5 IIO Configuration....482
6.2.5.5.1 Socket X Configuration....485
6.2.5.5.2 Intel(R) Virtualization for Directed I/O (VT-d)....492
6.2.5.5.3 IIO Stack IO Resource Configuration....495
6.2.5.5.4 Intel(R) VMD technology....495
6.2.5.5.5 IIO DFX Configuration....496
6.2.5.5.6 IIO Global Performance Tuning....500
6.2.5.6 Advanced Power Management Configuration....501
6.2.5.6.1 CPU P-State Control....507
6.2.5.6.2 Hardware PM State Control....512
6.2.5.6.3 Frequency Prioritization....514
6.2.5.6.4 CPU C-State Control....515
6.2.5.6.5 Package C-State Control....517
6.2.5.6.6 CPU Thermal Management....521
6.2.5.6.7 CPU Advanced PM Tuning....522
6.2.5.6.8 Memory Power & Thermal Configuration....525
6.2.6 BMC Configuration....532
6.2.6.1 BMC Configuration....533

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.6.1.1 Add BMC User....544
6.2.6.1.2 Delete BMC User....546
6.2.6.1.3 Change BMC User Settings....547
6.2.7 PCH-IO Configuration....549
6.2.7.1 PCI Express Configuration....550
6.2.7.1.1 PCI Express Root Port X....551
6.2.7.2 SATA And RST Configuration....552
6.2.7.2.1 Controller 1 SATA And RST Configuration....553
6.2.7.2.2 Controller 1 SATA Information....555
6.2.7.3 USB Configuration....556
6.2.8 Misc Configuration....560
6.2.9 Console Redirection Configuration....563
6.2.10 PXE Configuration....567
6.2.11 ME Configuration....571
6.2.12 NVMe Information....572
6.2.13 System Event Log....574
6.2.13.1 eMCA Settings....578
6.2.13.2 WHEA Settings....580
6.2.13.3 Error Injection Settings....581
6.2.13.4 Memory Error Enabling....582
6.2.13.5 IIO Error Enabling....584
6.2.13.6 PCIe Error Enabling....586
6.2.13.7 Error Control Setting....588
6.2.13.8 DWR Configuration....588
6.3 Security....590
6.3.1 Weak Password Dictionary....602
6.3.2 TLS Certificate Manager....604
6.3.2.1 CA Manager....604
6.3.2.1.1 Import Certificate....606
6.3.2.1.2 Delete Certificate....607
6.3.2.2 CRL Manager....609
6.3.2.2.1 Import Cert Revocation List....611
6.3.2.2.2 Delete Cert Revocation List....613
6.4 Boot....615
6.4.1 Boot Sequence....625
6.4.2 UEFI/Legacy....627
6.5 Exit....628

A FAQ....631

A.1 Restrictions on Boot Devices in Legacy Mode....631

B Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)....632

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

C Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)..... 699

D Linkage Options in Energy Efficiency Test Scenarios (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)..... 767

E Acronyms and Abbreviations.....778

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

1 Before You Start

For details, see the corresponding sections based on the server model.

- For the 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7, see the following sections:
  - **2 BIOS Overview**
  - **3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**
  - **4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**
  - **5 Description of Setup Utility (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**
- For the 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see the following sections:
  - **2 BIOS Overview**
  - **3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**
  - **4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**
  - **6 Description of Setup Utility (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

2 BIOS Overview

Introduction to BIOS

The BIOS is the most basic software loaded on a computer hardware system. It provides an abstraction layer between the computer hardware and the OS. It is used to perform hardware initialization during the boot process and provide runtime services for the OS. The BIOS can enable or disable the components integrated on the motherboard. **Figure 2-1** shows the BIOS position in the system.

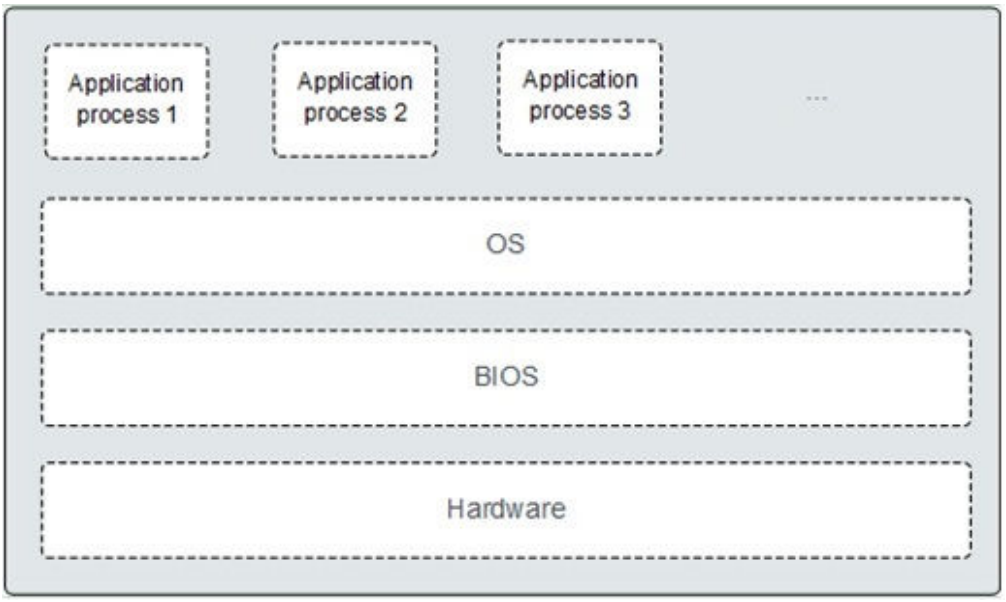
The BIOS data is stored on the Serial Peripheral Interface (SPI) flash memory. The BIOS performs a power-on, self-test (running during startup a hardware diagnostic system, including self-tests of the CPU, memory, and boot devices), initializes CPUs and memory, checks the I/O and boot devices, and finally boots the OS. This technical specification for hardware and software collaboration eliminates the need for manual configuration (such as changing jumpers or setting parameters). Upon connecting a hardware device to the computer, the system automatically detects the device, installs the required drivers, and completes configuration, enabling plug-and-play. The BIOS also provides the advanced configuration and power interface (ACPI), hot swap setting, and a management interface in Chinese, English, and Japanese.

The Eagle Stream platform BIOS complies with UEFI 2.8 and ACPI 6.3 specifications.

The Eagle Stream-based servers use the BIOS developed based on the code bases of Independent BIOS Vendors (IBVs). BIOS provides a variety of in-band and out-of-band configuration functions. It is scalable and can be easily customized to a variety of setups.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 2-1 BIOS in the system



BIOS Keyboard Operations

NOTE

The BIOS keyboard instructions apply to the 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7. For the 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see **BIOS Keyboard Operations (Only for the 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**.

You can use the mouse or keyboard to perform operations on the BIOS screen. **Table 2-1** describes the function keys on the keyboard.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 2-2 BIOS keyboard operations



Table 2-1 BIOS keyboard operations and description

Function Key	Description
F2	Alternates between the English (US), French, and Japanese keyboards.
ESC	Exits BIOS or returns to the previous screen.
↑	Moves the cursor up to select the desired parameter.
↓	Moves the cursor down to select the desired parameter.
←	• Moves the cursor to select the desired parameter on the left. • Return to the previous screen.
→	• Moves the cursor to select the desired parameter on the right. • Enters the submenu of the current parameter.

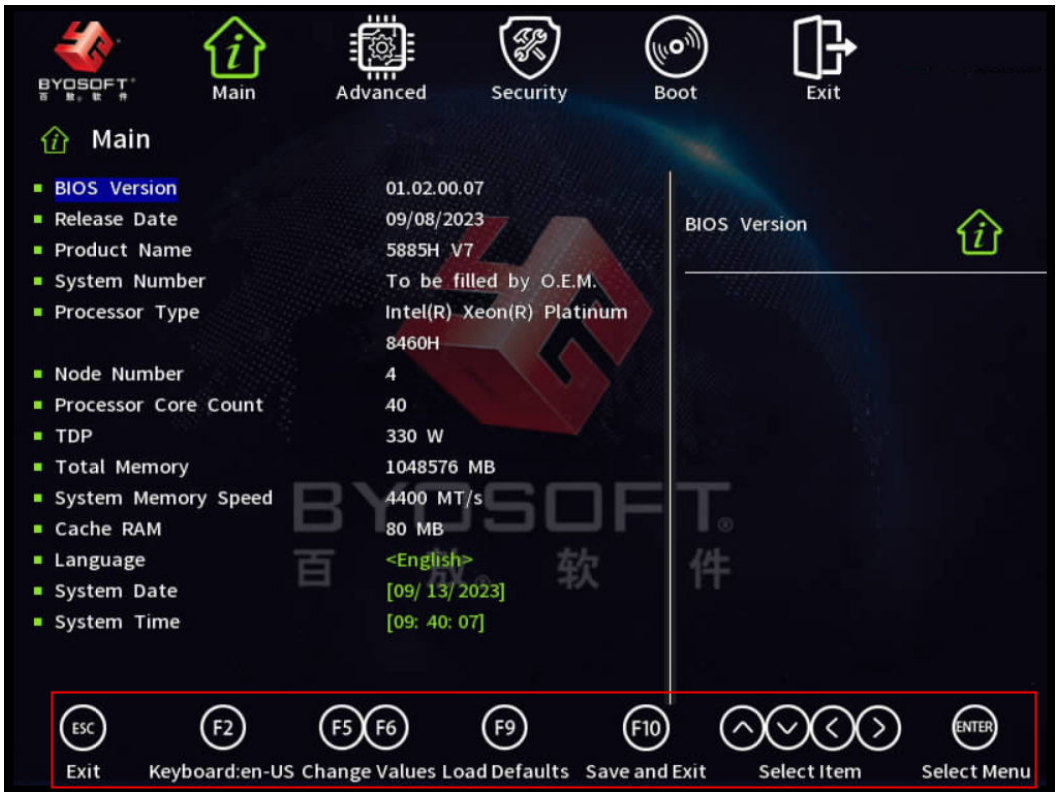
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Function Key	Description
F5	• Moves the parameter value down or increases it. • Changes the value of the selected parameter to another value.
F6	• Moves the parameter value up or decreases it. • Changes the value of the selected parameter to another value.
ENTER	Selects the current parameter or opens the submenu of the current parameter.
F9	• Restores the BIOS factory settings. • Restores the BIOS factory settings or customized settings for customized configurations.
F10	Saves the settings and exits the screen.

BIOS Keyboard Operations (Only for the 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

You can use the mouse or keyboard to perform operations on the BIOS screen. Figure 2-3 describes the function keys on the keyboard.

Figure 2-3 BIOS keyboard operations



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 2-2 BIOS keyboard operations and description

Function Key	Description
↑	Moves the cursor up to select the desired parameter.
↓	Moves the cursor down to select the desired parameter.
←	Moves the cursor to select the desired parameter on the left.
→	Moves the cursor to select the desired parameter on the right.
Enter	Selects the current parameter or opens the submenu of the current parameter.
F2	Alternates between the English (US), French, and Japanese keyboards.
F5	● Decreases a parameter value. ● Changes the value of the selected parameter to another value.
F6	● Increases a parameter value. ● Changes the value of the selected parameter to another value.
F9	● Restores the BIOS factory settings. ● Restores the BIOS factory settings or customized settings for customized configurations.
F10	Saves the settings and exits the screen.
Esc	Exits BIOS or returns to the previous screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3 Common Operations

- For the 1288H V7, 2288H V7-HE, 2288H V7, 5288 V7, 5298 V7, and G5200 V7,see **3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/ G5200 V7)**.
- For the 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see **3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/ G8600 V7)**.

3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7/2288 V8)

3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7/2288 V8)

3.1.1 Accessing the Front Page

Scenarios

Access the front page.

Procedure

Step 1 Connect a local PC with the keyboard, video, and mouse (KVM) to the server, or log in to the server using the Remote Console of the iBMC WebUI.

NOTE

For details about how to log in to the Remote Console screen of the iBMC WebUI, see the corresponding *iBMC User Guide*.

Step 2 Power on or restart the server.

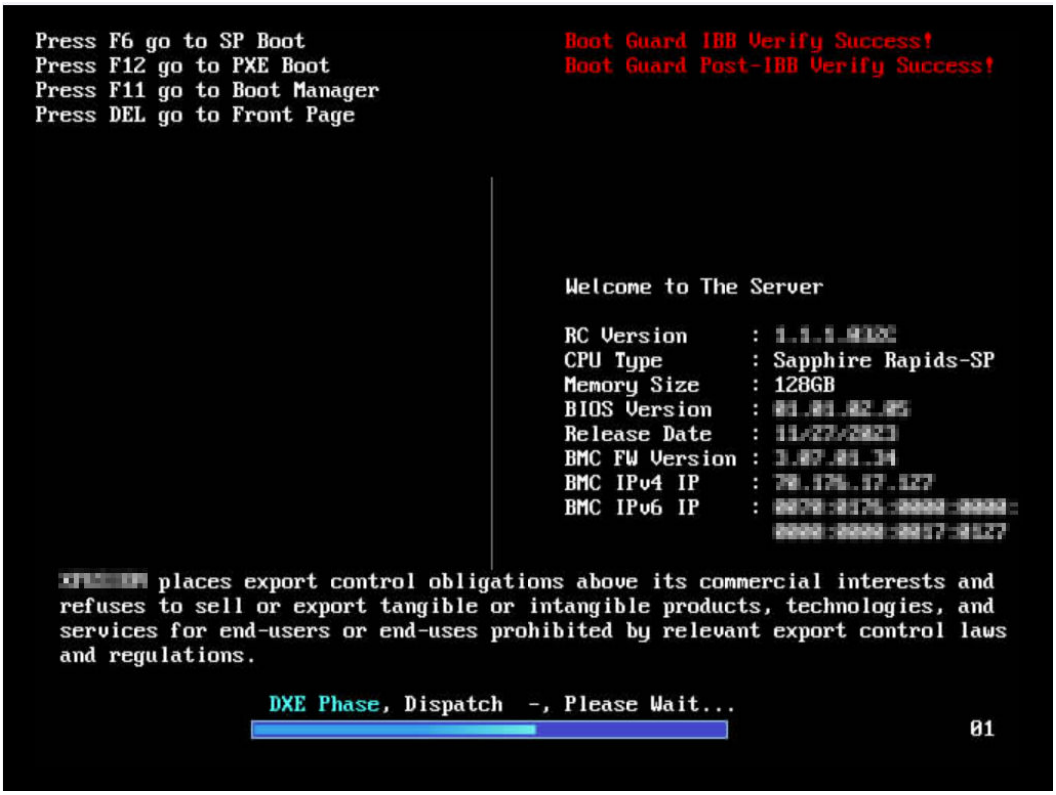
NOTE

Restarting the server will interrupt services. Exercise caution when performing this operation.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 3 Press **Del** or **Delete** when the screen shown in **Figure 3-1** is displayed.

Figure 3-1 BIOS boot screen



NOTE

- To access the Smart Provisioning GUI, press **F6**. For details, see **3.1.4 Accessing the Smart Provisioning GUI**.
- To boot from the network, press **F12**.
- To access the **Boot Manager** screen, press **F11**.
- To access the **front page**, press **Del**.

Step 4 Enter the current password.

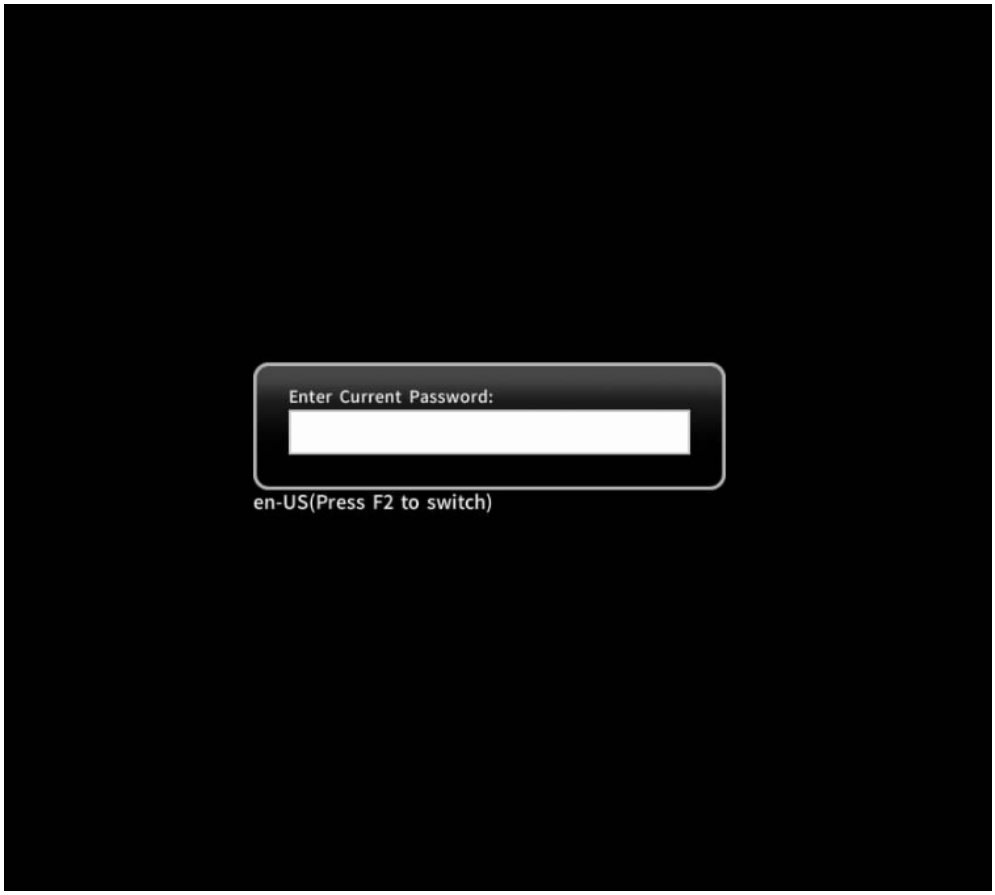
Enter the current password in the dialog box displayed if prompted, as shown in **Figure 3-2**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- The default BIOS password is **Admin@9000** (administrator password). If you use the default password to log in, the system prompts you to change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.
- For security purposes, you are advised to periodically change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.1.11.2 Setting the BIOS Common User Password**.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- Use the mouse to open the on-screen keyboard and enter the password.

Figure 3-2 Entering the current password



Step 5 After entering the password, press **Enter**.

The **front page** is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- Figure 3-3 and Figure 3-4 show the front pages displayed in different modes when you log in to the system as the administrator. The administrator can set all parameters on the Setup Utility screen and use shortcut keys **F10** (save and exit) and **F9** (restore defaults).
- Figure 3-5 shows the front page displayed when you log in to the system as a common user. In this case, only the **Continue** and **Setup Utility** menus are displayed. On the **Setup Utility** screen, common users can only view menu options, set or change their own passwords (that is, editing the **Set User Password** option on the 5.3 Security screen), set parameters (except **Load Defaults**) on the 5.5 Exit screen, and press **F10** to save the settings and exit. Other options are all grayed out and cannot be edited, and the **F9** shortcut function is unavailable.

Figure 3-3 Front page (UEFI mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-4 Front page (legacy mode)



Figure 3-5 Front page (login as a common user)



----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.1.2 Accessing the Setup Utility Screen

Scenarios

Access the Setup Utility screen when you need to set system boot parameters and query system data.

Procedure

Step 1 Access the front page.

For details, see **3.1.1 Accessing the Front Page**.

Step 2 On the front page, select **Setup Utility** and press **Enter**.

The **Main** screen is displayed, as shown in **Figure 3-6**.

Figure 3-6 Main screen 1



----End

3.1.3 Accessing BIOS Using a Serial Port

Scenarios

Use a serial port to access the front page. This section uses a Windows OS as an example.

Prepare the following data and software tools in advance:

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

- BMC IP address of the server to be accessed
- BMC administrator's user name and password of the server to be accessed
- IPMItool: third-party software that is prepared by yourself

NOTE

- The IP address of the Windows client must be reachable from the BMC management network port.
- IPMItool is used as an example here.

Procedure

Step 1 Place the IPMItool tool package in the root directory of the drive on a Windows client. Use drive D as an example.

Step 2 Log in to the Remote Console of the iBMC WebUI.

NOTE

For details about how to log in to the Remote Console screen of the iBMC WebUI, see the corresponding *iBMC User Guide*.

Step 3 Power on the server.

Step 4 Access the command line interface (CLI) of the OS.

- On the Windows OS, enter **cmd** in the search box of the **Start** menu and press **Enter**.
- For other OSs, refer to the methods provided on the OS official websites.

NOTE

The Windows OS is used as an example. For commands on other OSs, see the OS official websites.

Step 5 Run the **D:** command to access drive D.

Step 6 Run the **cd ipmitool** command to access the directory where IPMItool is located.

Step 7 Run the **ipmitool -I lanplus -H *192.168.2.100* -U *Administrator* -P *Admin@9000* sol activate** command to access BIOS through the serial port.

NOTE

Change the IP address, user name, and password in this command as needed.

- **192.168.2.100** indicates the BMC IP address.
- **Administrator** indicates the BMC user name.
- **Admin@9000** indicates the BMC Password.

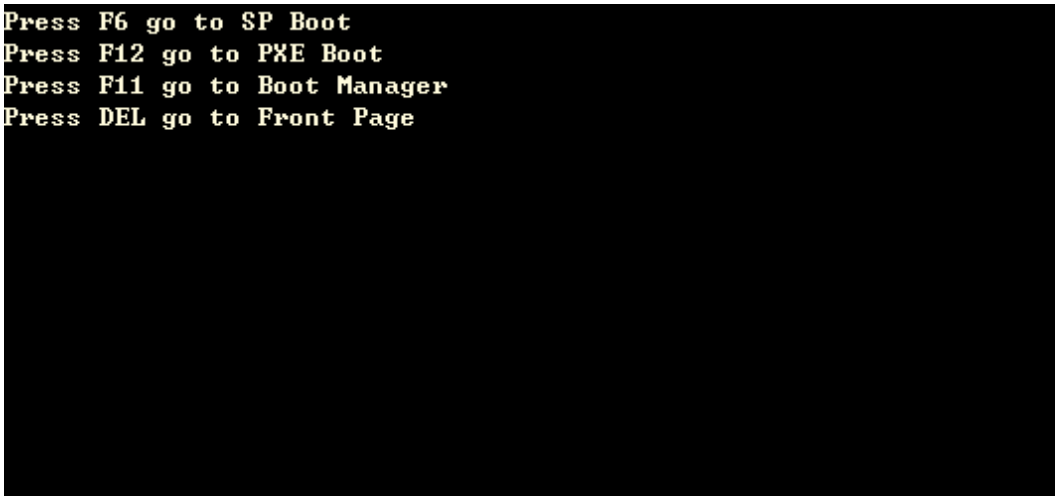
```
D:\ipmitool>ipmitool -I lanplus -H 192.168.2.100 -U Administrator -P Admin@9000 sol activate
[SOL Session operational.  Use ~? for help]
```

Step 8 Restart the server.

Step 9 When the BIOS boot screen shown in **Figure 3-7** is displayed, press **Del** or **Delete**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-7 BIOS boot screen



NOTE

- To access the Smart Provisioning GUI, press **F6**. For details, see **3.1.4 Accessing the Smart Provisioning GUI**.
- To boot from the network, press **F12**.
- To access the **Boot Manager** screen, press **F11**.
- To access the front page, press **DEL**.

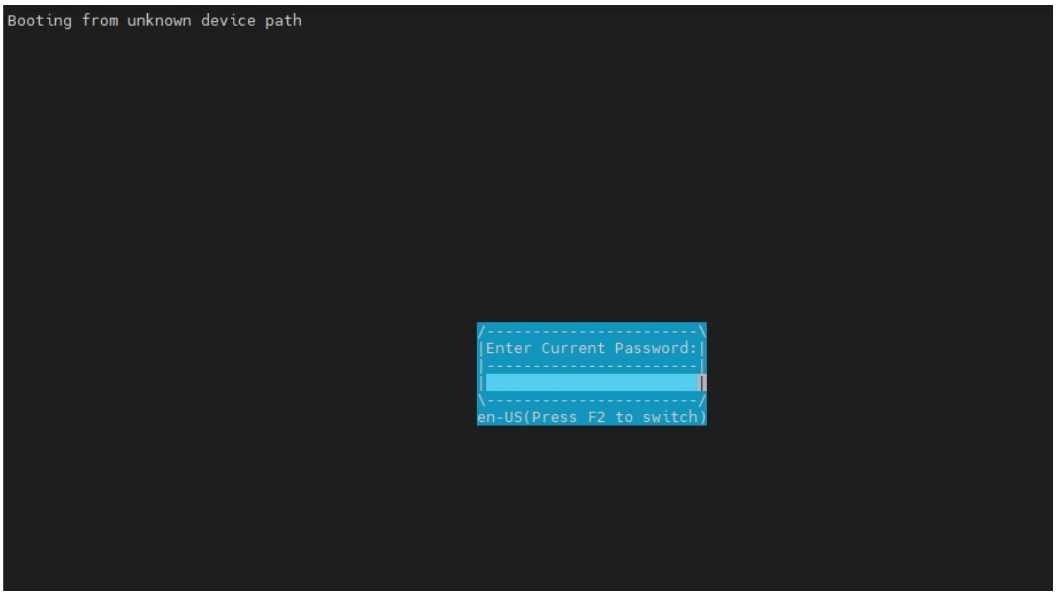
Step 10 In the displayed dialog box, enter the password and press **Enter**, as shown in **Figure 3-8**.

NOTE

- The default BIOS password is **Admin@9000** (administrator password). If you use the default password to log in, the system prompts you to change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.
- For security purposes, you are advised to periodically change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.1.11.2 Setting the BIOS Common User Password**.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- Use the mouse to open the on-screen keyboard and enter the password.

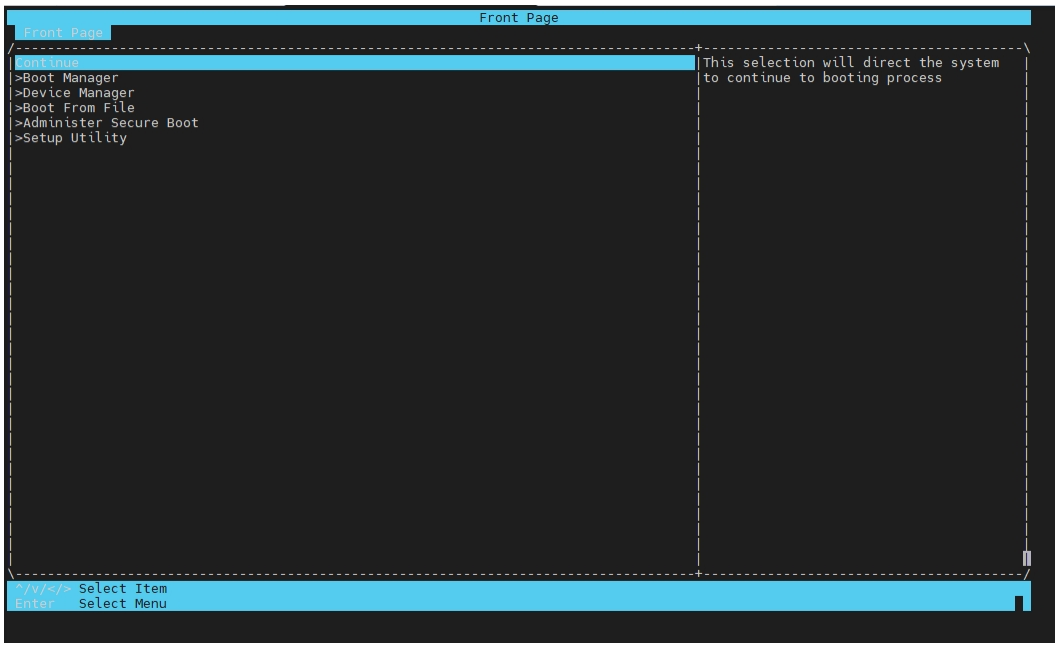
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-8 Entering the current password



The front page shown in **Figure 3-9** is displayed.

Figure 3-9 Front page



----End

3.1.4 Accessing the Smart Provisioning GUI

Scenarios

Log in to the Smart Provisioning GUI.

When the server is installed with the Smart Provisioning tool and the Smart Provisioning tool is enabled, you can enter the Smart Provisioning GUI.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

Step 1 Connect a local PC with the keyboard, video, and mouse (KVM) to the server, or log in to the server using the Remote Console of the iBMC WebUI.

NOTE

For details about how to log in to the Remote Console screen of the iBMC WebUI, see the corresponding *iBMC User Guide*.

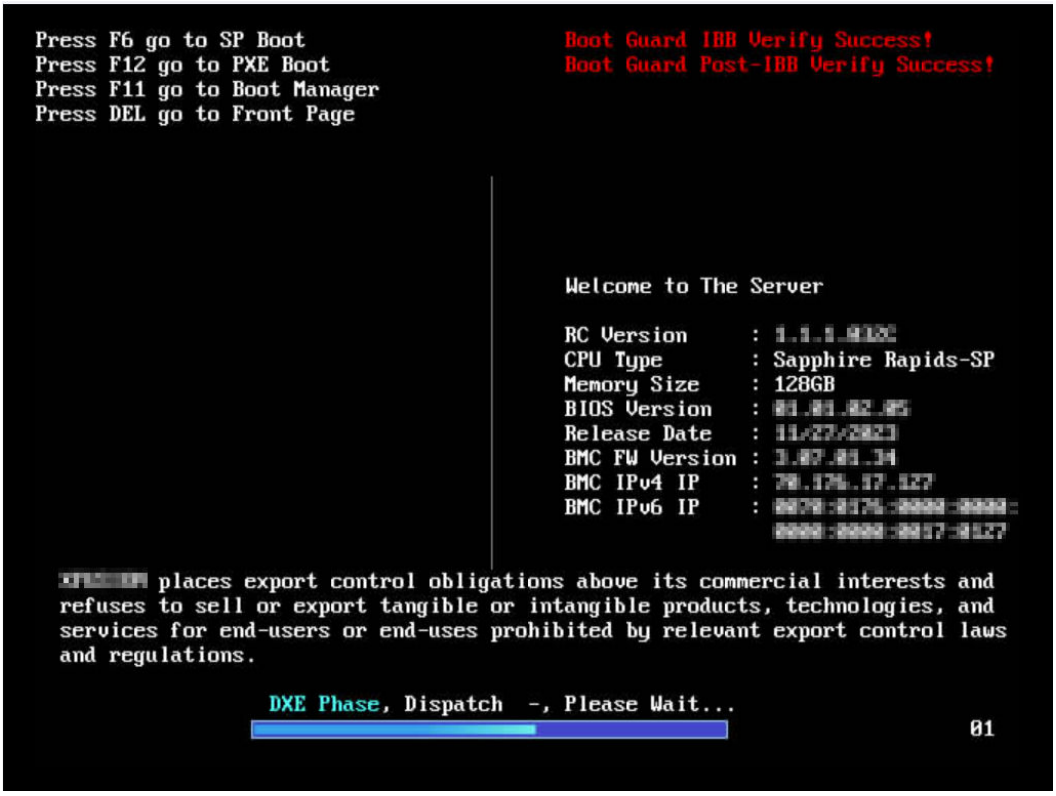
Step 2 Power on or restart the server.

NOTE

Restarting the server will interrupt services. Exercise caution when performing this operation.

Step 3 Press **F6**, when the screen shown in **Figure 3-10** is displayed.

Figure 3-10 BIOS boot screen



Step 4 Enter the password in the dialog box as prompted during startup, and press **Enter**.

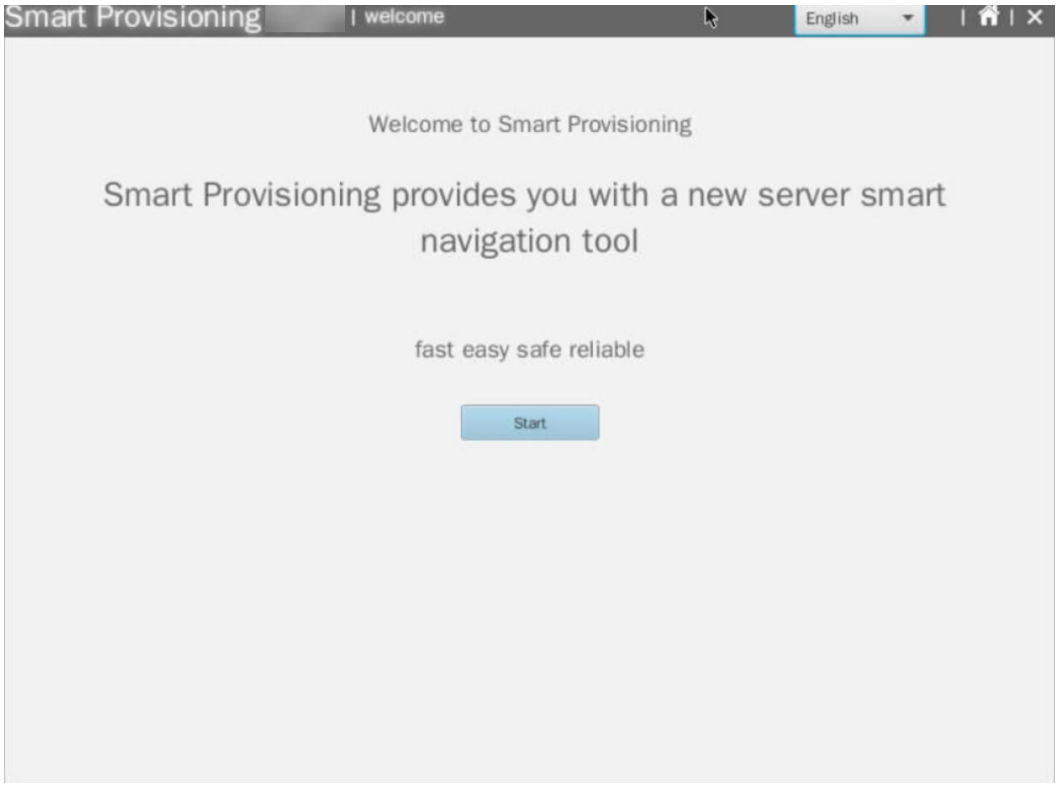
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- The default BIOS password is **Admin@9000** (administrator password). If you use the default password to log in, the system prompts you to change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**.
- For security purposes, you are advised to periodically change the administrator password. For details, see **3.1.11.1 Setting the BIOS Administrator Password**.
- You can change the password only when you log in to the system using the administrator password.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- Use the mouse to open the on-screen keyboard and enter the password.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.

The Smart Provisioning welcome window is displayed, as shown in **Figure 3-11**.

Figure 3-11 Smart Provisioning welcome screen



Step 5 Click **Start**.

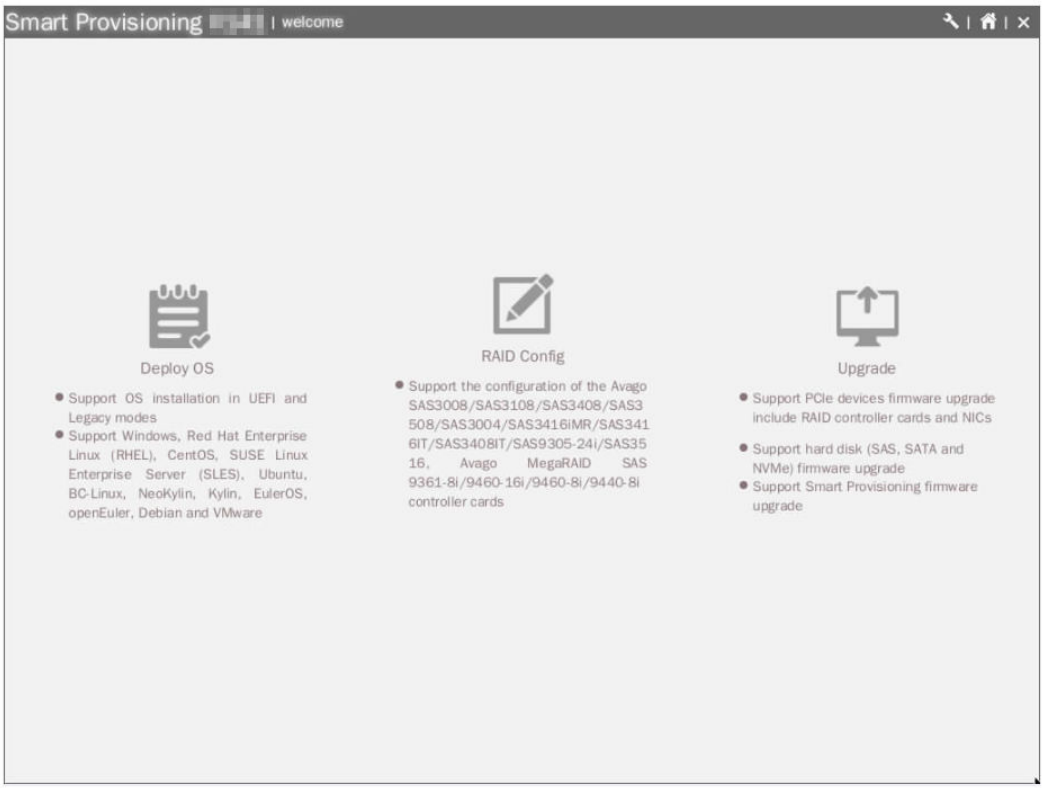
Access the Smart Provisioning main screen, as shown in **Figure 3-12**.

NOTE

- The information displayed on the screen varies depending on the version of Smart Provisioning.
- When using Smart Provisioning, you can click  in the upper right corner to return to the main screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-12 Smart Provisioning main screen



----End

3.1.5 Querying CPU Information

Scenarios

Query the CPU information about a server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

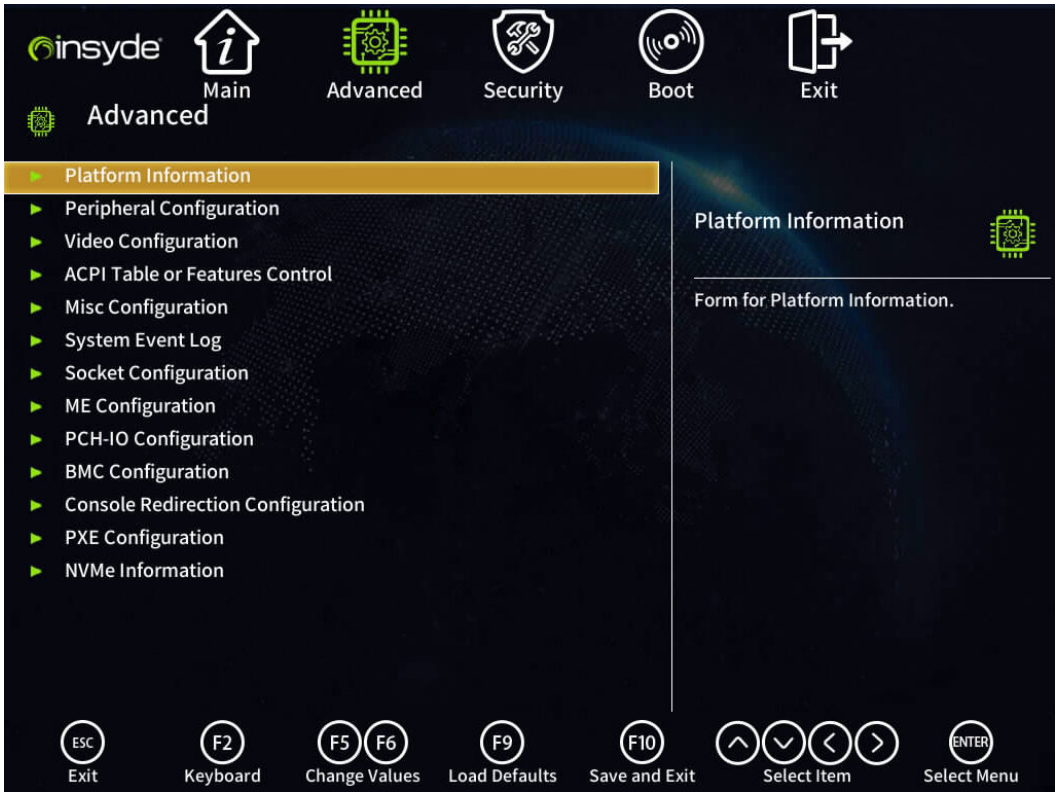
For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-13**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-13 Advanced screen

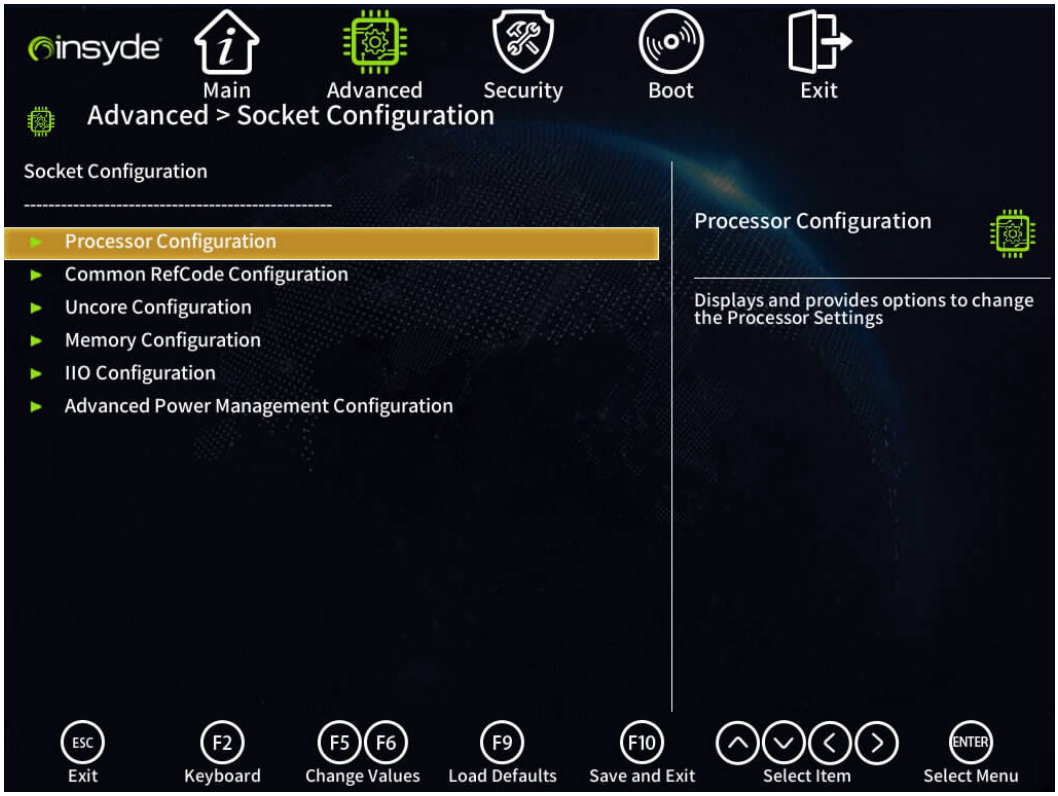


Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-14**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-14 Socket Configuration screen



Step 4 Select **Processor Configuration** and press **Enter**.

The **Processor Configuration** screen is displayed, as shown in **Figure 3-15**.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-15 Processor Configuration screen



Step 5 Select **Per-Socket Information** and press **Enter**.

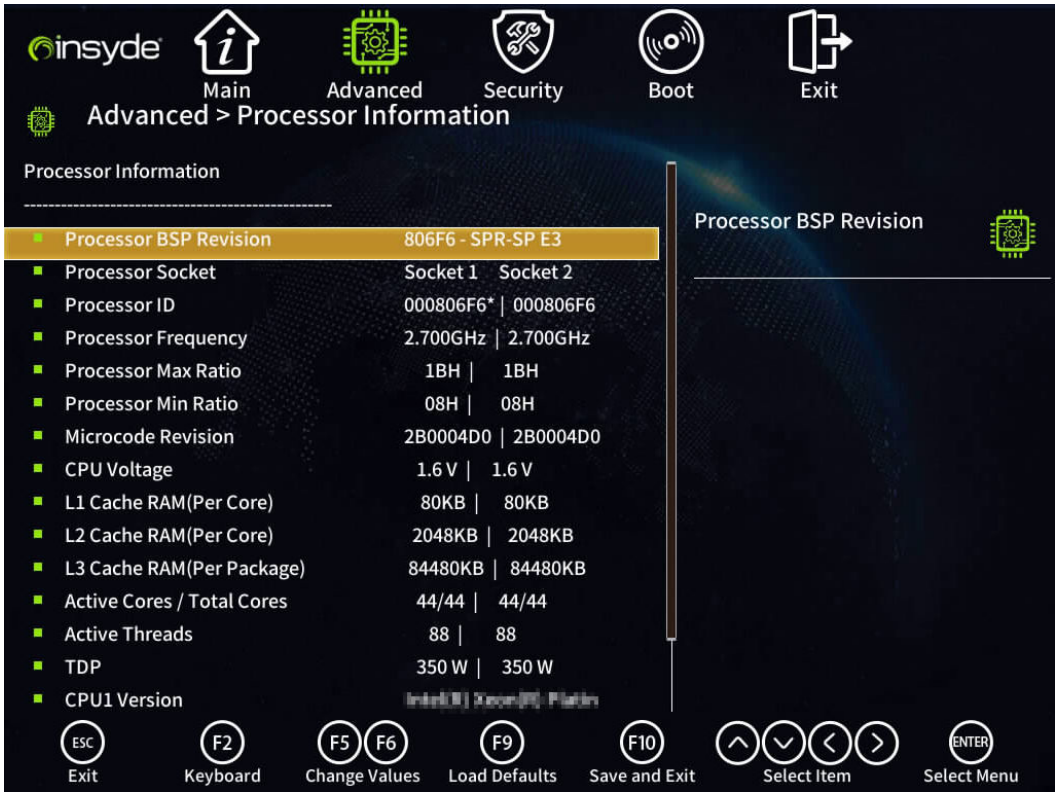
The **Per-Socket Information** screen is displayed, as shown in **Figure 3-16**. View the required CPU information. For details about parameters, see **5.2.7.1.1 Per-Socket Information**.

NOTE

The displayed screen varies depending on the CPU model of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-16 Per-Socket Information screen



----End

3.1.6 Querying Memory Information

Scenarios

Query the memory information about a server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

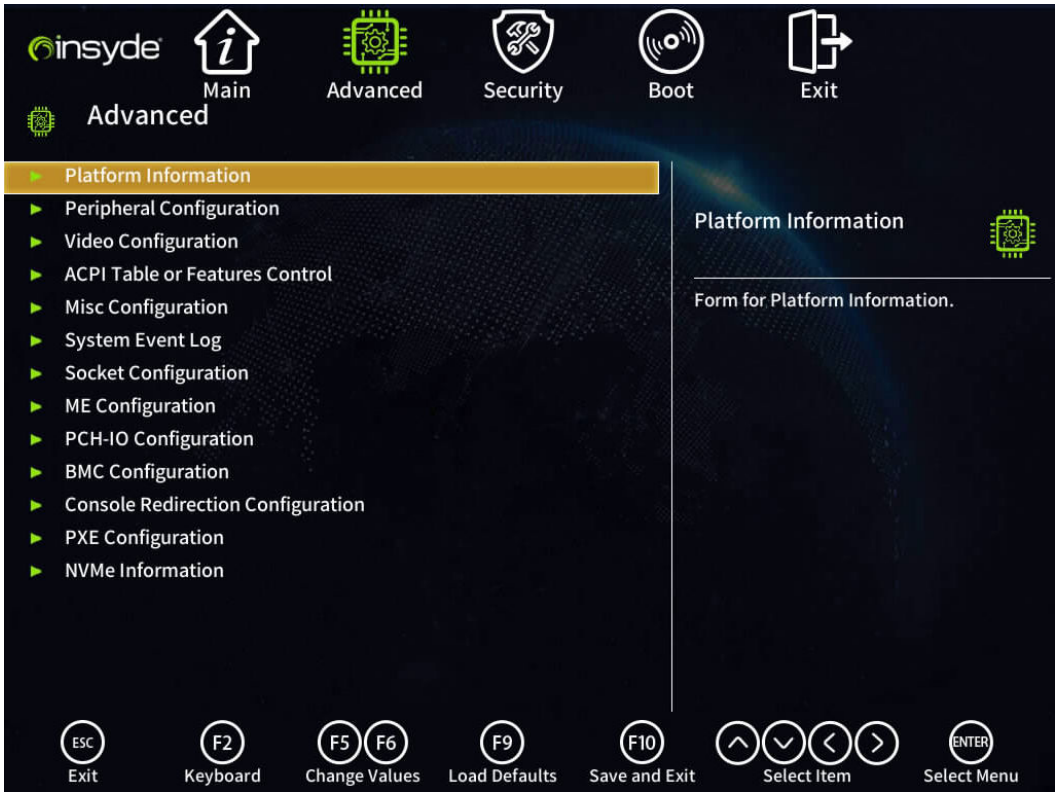
For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-17**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-17 Advanced screen

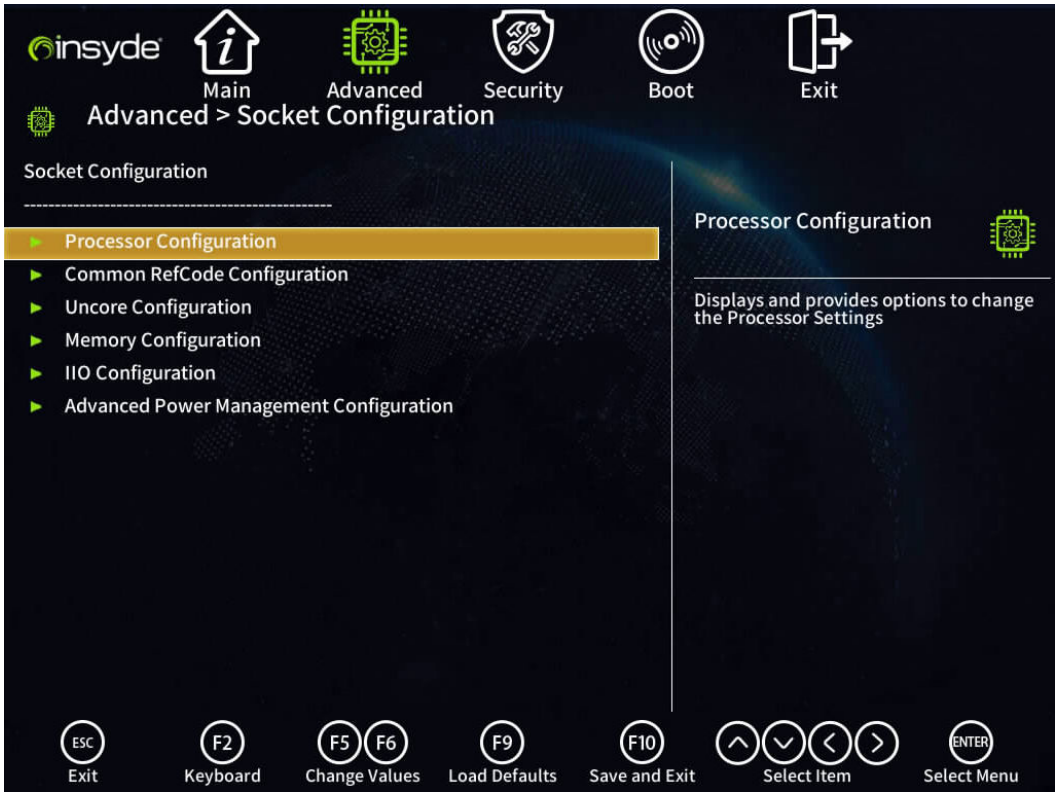


Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-18**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-18 Socket Configuration screen



Step 4 Select **Memory Configuration** and press **Enter**.

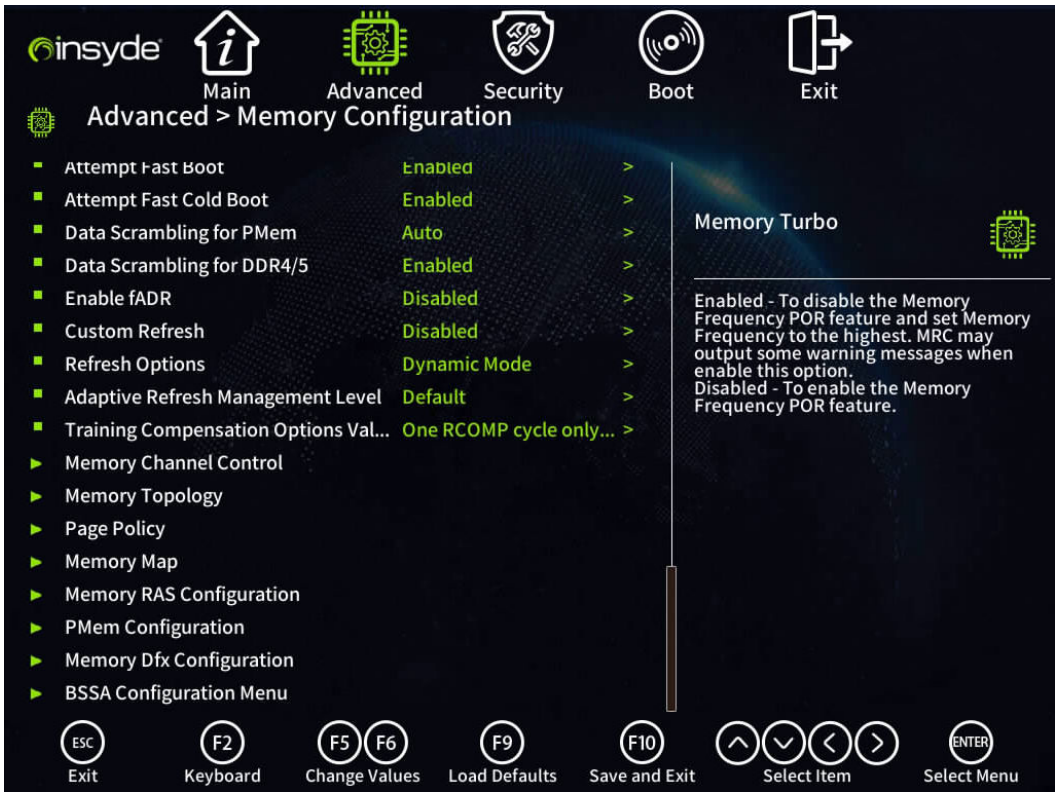
The **Memory Configuration** screen is displayed, as shown in **Figure 3-19** and **Figure 3-20**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-19 Memory Configuration screen 1



Figure 3-20 Memory Configuration screen 2



Step 5 Select **Memory Topology** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Memory Topology** screen is displayed, as shown in **Figure 3-21**.

View the memory information. For details about parameters, see **5.2.7.4.3 Memory Topology**.

NOTE

- The information displayed on the screen varies depending on the configuration of the server.
- **DIMM***xyz*: indicates the DIMM numbered *z*+1 in the channel numbered *y*+1 of the CPU numbered *x*+1.

Figure 3-21 Memory Topology screen



----End

3.1.7 Querying Drive Information

Scenarios

Query the information about the server Platform Controller Hub (PCH) pass-through drives or M.2 SSDs on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Advanced** screen is displayed, as shown in **Figure 3-22**.

Figure 3-22 Advanced screen



Step 3 Select **PCH-IO Configuration** and press **Enter**.

The **PCH-IO Configuration** screen is displayed, as shown in **Figure 3-23**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-23 PCH-IO Configuration screen



Step 4 Select **SATA And RST Configuration** and press **Enter**.

The **SATA And RST Configuration** screen is displayed, as shown in **Figure 3-24**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-24 SATA And RST Configuration screen



Step 5 Select **Controller** *X* **SATA And RST Configuration** (**Controller 1 SATA And RST Configuration** is used as an example) and press **Enter**.

The **Controller 1 SATA And RST Configuration** screen is displayed, as shown in **Figure 3-25**.

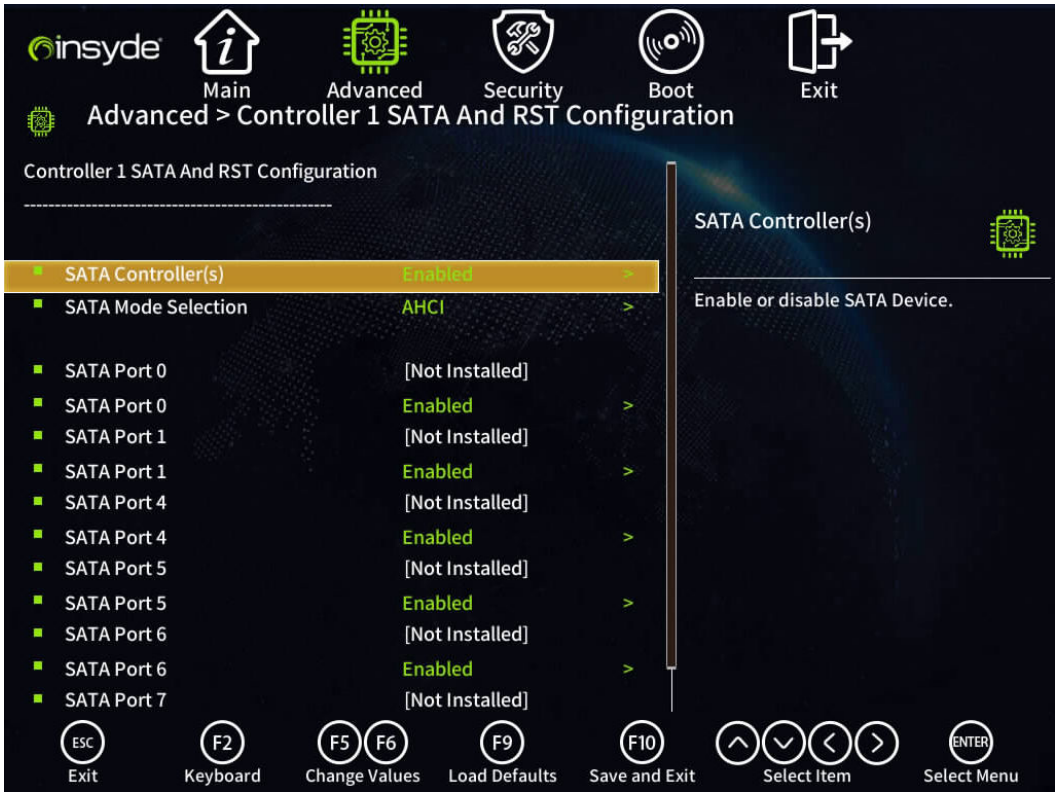
View the required drive status. For details about parameters, see **5.2.9.1.1 Controller X SATA And RST Configuration**.

NOTE

- In **SATA Port *x***, ***x*** indicates the drive port number, which starts from 0.
- For more details about the slot numbers of the drives, see the user guide of the server you use.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-25 Controller 1 SATA And RST Configuration screen



----End

3.1.8 Querying the BMC IP Address

Scenarios

Query the IP address of the BMC management port of the server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

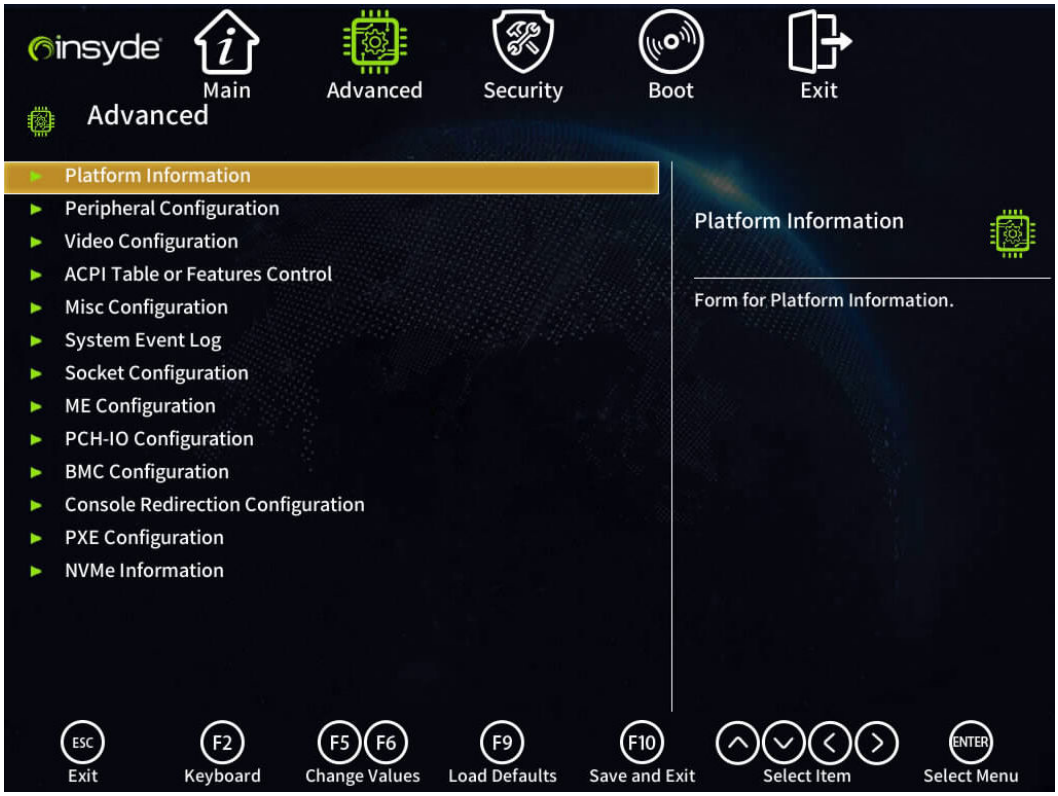
For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-26**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-26 Advanced screen

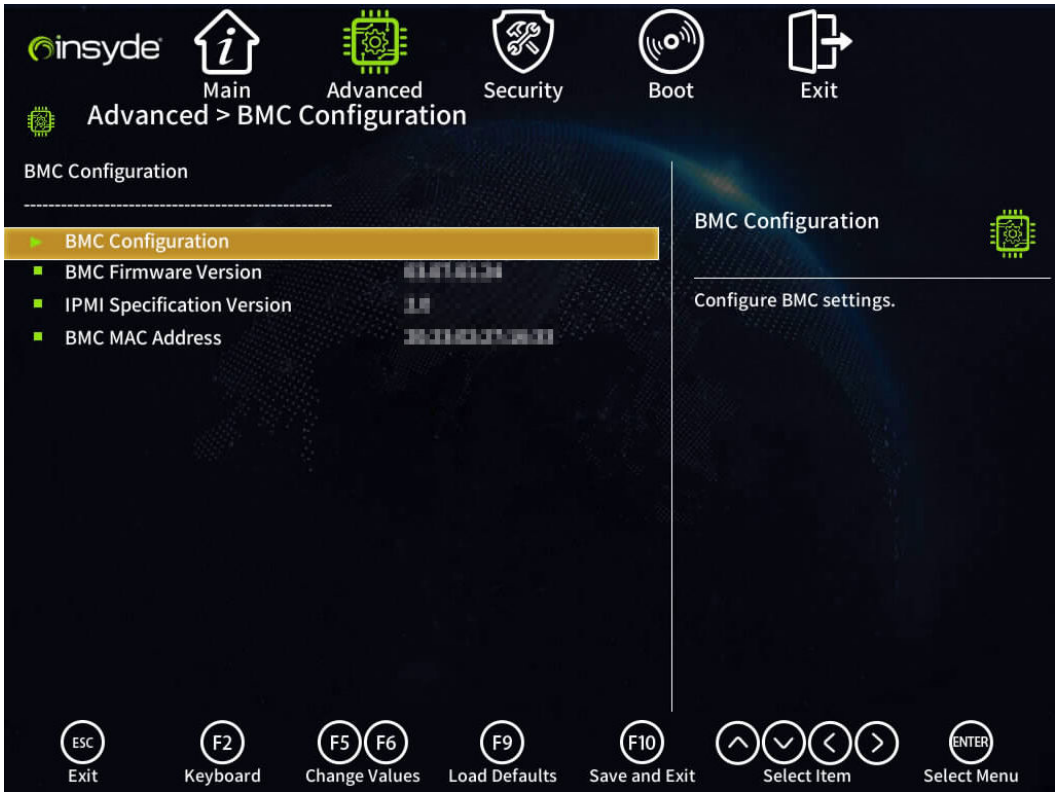


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-27**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-27 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-28** and **Figure 3-29**.

Check the BMC IP address. For details about parameters, see **5.2.10.1 BMC Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-28 BMC Configuration screen 1



Figure 3-29 BMC Configuration screen 2



----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.1.9 Setting the BIOS System Language

Scenarios

Set the BIOS language.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Main** tab.

The **Main** screen is displayed, as shown in **Figure 3-30**.

Figure 3-30 Main screen 1



Step 3 Select **Language** and press **Enter**.

The dialog box for setting a language is displayed,

Step 4 Select the target language (English, Chinese, or Japanese) and press **Enter**.

Step 5 Use any of the following methods to save the settings.

- Method 1: Press **F10**. The **Exit Saving Changes** dialog box is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Select **Yes** and press **Enter** to save the settings. The server automatically restarts for the settings to take effect.

- Method 2: Select **Exit** to enter the **Exit** screen.

  Select **Save Changes Without Exiting**, select **Yes**, and press **Enter** to save the settings. The settings automatically take effect.

----End

3.1.10 Setting the BIOS System Time and Date

Scenarios

Set the BIOS system time and date.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Main** tab.

The **Main** screen is displayed, as shown in **Figure 3-31**.

Figure 3-31 Main screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 3 Set the system time.

1. Select **System Time** and press **Enter**.

   The window for setting the system time is displayed.

   The system time is in the format of *HH:MM:SS* in the 24-hour system. To switch among the hour, minute, and second, press **Enter**. To change the time, use the following methods:

   – Press **+** to increase the value by 1.
   – Press **-** to decrease the value by 1.
   – Press a number to change the value directly.

2. After the setting is complete, click **Yes**.

   The setting takes effect immediately.

Step 4 Set the system date.

1. Select **System Date** and press **Enter**.

   The window for setting the system date is displayed.

   The system date is in the format of *YYYY/MM/DD*. To switch among the year, month, and day, press **Enter**. To change the date, use the following methods:

   – Press **+** to increase the value by 1.
   – Press **-** to decrease the value by 1.
   – Press a number to change the value directly.

2. After the setting is complete, click **Yes**.

   The setting takes effect immediately.

----End

NOTE

BIOS does not support setting time zone. Windows and Linux are different in time management. In Windows, the CMOS time is the local time. In Linux, the CMOS time is the Greenwich Mean Time (GMT).

3.1.11 Setting the BIOS Password

3.1.11.1 Setting the BIOS Administrator Password

Scenarios

Set the BIOS administrator password on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 2 Select the **Security** tab.

The **Security** screen is displayed, as shown in **Figure 3-32**.

Figure 3-32 Security screen



Step 3 Select **Set Supervisor Password** and press **Enter**.

The **Set Supervisor Password** dialog box is displayed.

Step 4 Enter the old BIOS administrator password and the new password, confirm the new password, and click **Yes**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- Before changing the BIOS administrator password, you need to enter the current BIOS administrator password. If you enter incorrect passwords for three consecutive times, the server will be locked. You can restart the server to unlock it.
- The password complexity requirements are as follows:
  - The password must contain 8 to 16 characters.
  - The password must contain at least two types of the following characters: uppercase letters, lowercase letters, and digits.
  - The password must contain at least one space or one of the following special characters:

    `~!@#$^&*%()-_=+\|[{}];:'",<.>/?
  - A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10.
  - The new password must contain at least two different characters from the old password.
  - The administrator password cannot be the same as a common user.
- If **Simple Password** is set to **Enabled**, the system does not verify the password complexity, but the password must contain 8 to 16 characters. Enabling the simple password function will reduce system security. Exercise caution when enabling this function.

Step 5 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 6 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the settings to take effect.

----End

3.1.11.2 Setting the BIOS Common User Password

Scenarios

Set the BIOS common user password on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported when you access the Setup Utility screen using the BIOS administrator password or common user password.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Security** tab.

The **Security** screen is displayed, as shown in **Figure 3-33**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-33 Security screen



Step 3 Select **Set User Password** and press **Enter**.

The **Set User Password** dialog box is displayed.

Step 4 Enter the password and confirm password of the common user, and click **Yes**.

NOTE

- If you log in using the administrator password, you can directly set a new common user password without verification of the original common user password. If you log in using a common user password, you need to verify the original common user password before setting a new common user password.
- The password complexity requirements are as follows:
  - The password must contain 8 to 16 characters.
  - The password must contain at least two types of the following characters: uppercase letters, lowercase letters, and digits.
  - The password must contain at least one space or one of the following special characters:

    `~!@#$^&*%()-_=+\|[{}];:'",<.>/?
  - A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10.
  - The new password must contain at least two different characters from the old password.
  - The administrator password cannot be the same as a common user.
- If **Simple Password** is set to **Enabled**, the system does not verify the password complexity, but the password must contain 8 to 16 characters. Enabling the simple password function will reduce system security. Exercise caution when enabling this function.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 5 When a dialog box prompts you to save the setting to make it take effect, click **Ok**.

Step 6 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 7 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.12 Setting PXE for an NIC

3.1.12.1 Setting PXE for an OCP NIC

Scenarios

Enable or disable the PXE function for a OCP NIC on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

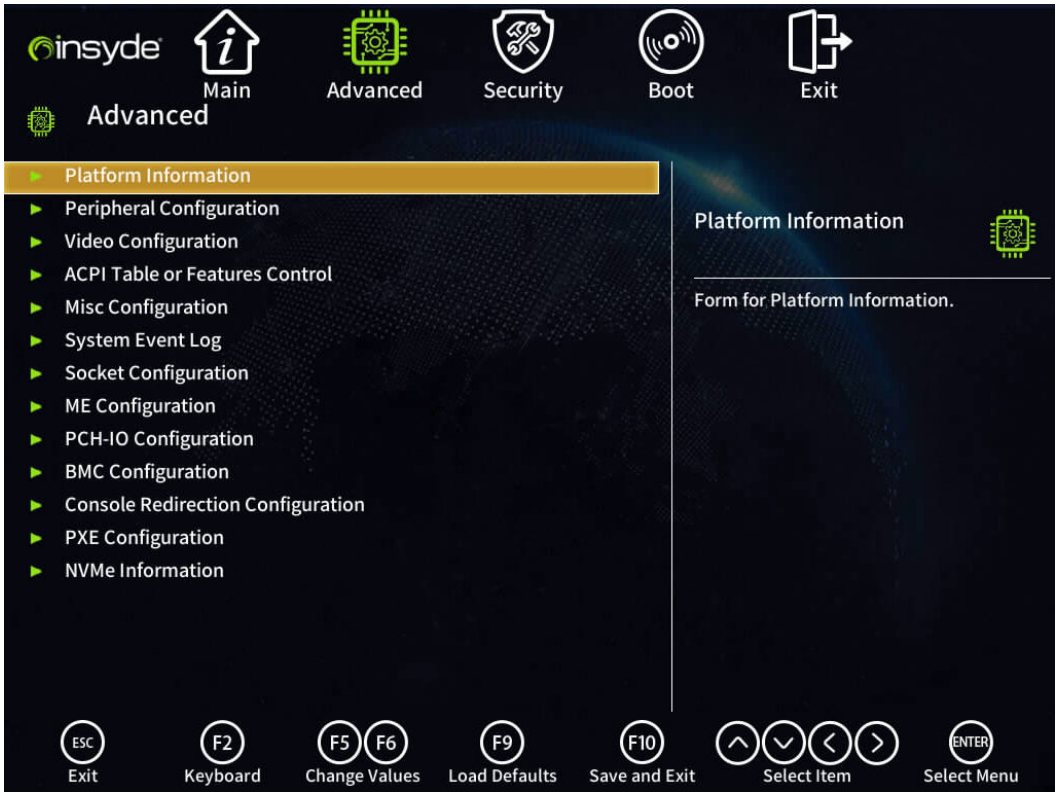
For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-34**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-34 Advanced screen



Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 3-35**.

NOTE

- The parameters displayed on this screen vary according to actual server NIC configuration.
- For details about the OCP NICs supported by each server, see the user guide of the corresponding server.
- In UEFI mode, the default values are **Enabled** for all network ports.
- In legacy mode, only the first network port of each NIC is enabled by default. That is, the default value is **Enabled** for FLEX IO 1 Port1 and **Disabled** for FLEX IO 1 Port2.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-35 PXE Configuration screen



Step 4 Select the OCP NIC port to be configured, for example, **FLEX IO 2 Port 1**, and press **Enter**.

Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enable the PXE function for the network port.
- **Disabled**: Disable the PXE function for the network port.

Step 6 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 7 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.12.2 Setting the PXE Function for a PCIe NIC

Scenarios

Enable or disable the PXE function for a PCIe NIC on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

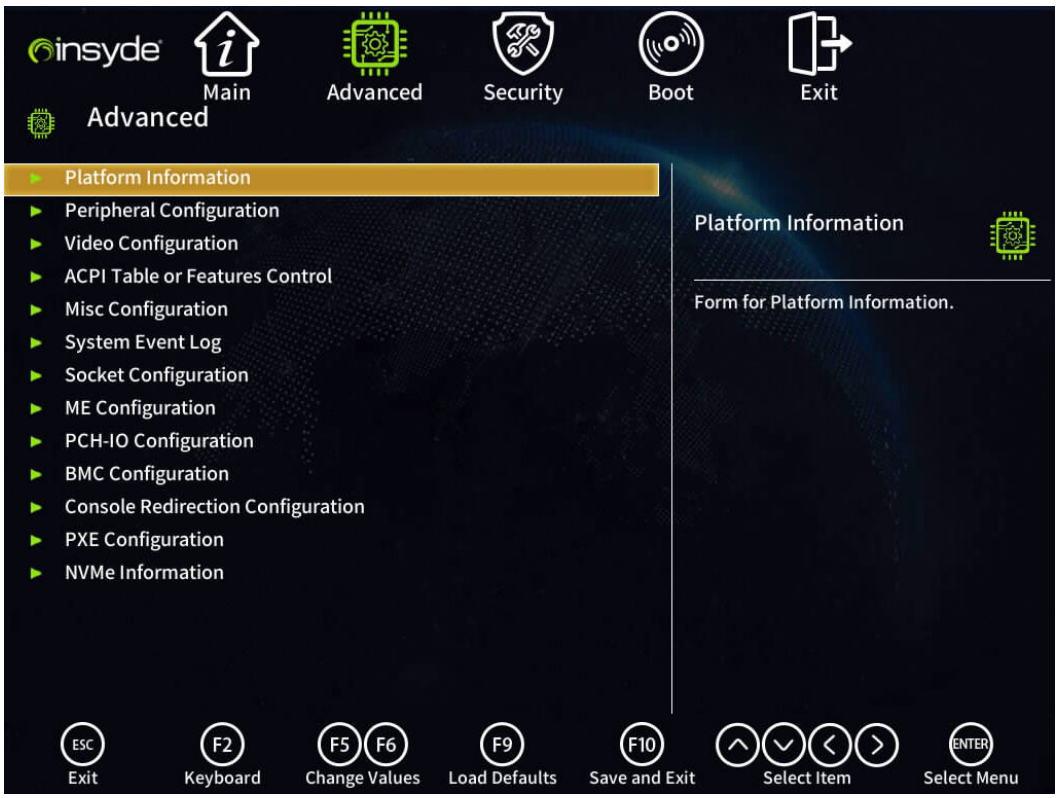
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-36**.

Figure 3-36 Advanced screen



Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 3-37**.

NOTE

The parameters displayed on this screen vary according to actual server NIC configuration.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-37 PXE Configuration screen



Step 4 Select **Slot PXE Control** and press **Enter**.

Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enable the PXE function for the PCIe NIC.

  NOTE

  After the PXE function is enabled for a PCIe NIC, you can enable or disable the PXE function for a specific PCIe NIC network port, for example, **CPU1 First Slot Port 1**.

- **Disabled**: Disable the PXE function for the PCIe NIC.

  NOTE

  After the PXE function of the PCIe NIC is disabled, the PXE function setting menu of a single PCIe NIC port is hidden and cannot be configured.

Step 6 Select a PCIe NIC port, for example, **CPU1 First Slot Port 1**, and press **Enter**.

Step 7 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enable the PXE function for the network port.
- **Disabled**: Disable the PXE function for the network port.

Step 8 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 9 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.1.13 Setting the TXT Function

Scenarios

Enable or disable the TXT function using the BIOS.

TXT is a security feature of the Intel processor and must be used together with the (Trusted Platform Module) TPM.

NOTE

- The server must be installed with the CPU and TPM.
- If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Check whether a TPM is installed on the server.

1. Select the **Security** tab.

   The **Security** screen is displayed, as shown in **Figure 3-38**.
2. Check whether related TPM parameters are properly displayed.
   - If yes, a TPM is installed on the server.
   - If no, check whether the TPM is properly installed. For details, see section "Installing the TPM" in the server maintenance and service guide.

Figure 3-38 Security screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 3 Check whether the required number of CPUs has been installed on the server.

1. Select the **Main** tab.

   The **Main** screen is displayed, as shown in **Figure 3-39**.

2. Check whether the value of **Node Number** is **1** or **2**.
   - If yes, the required number of CPUs has been installed on the server.
   - If no, check whether the CPU is properly installed. For details, see section "Installing a Processor" in the server maintenance and service guide.

Figure 3-39 Main screen 1

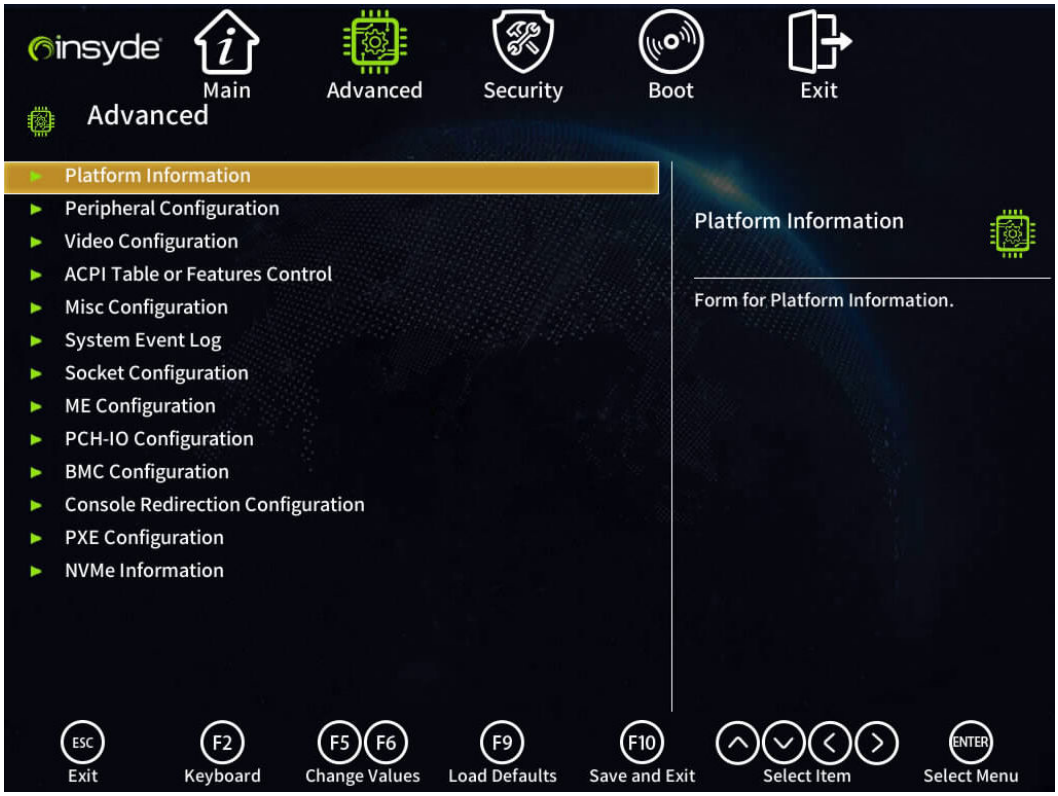


Step 4 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-40**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-40 Advanced screen

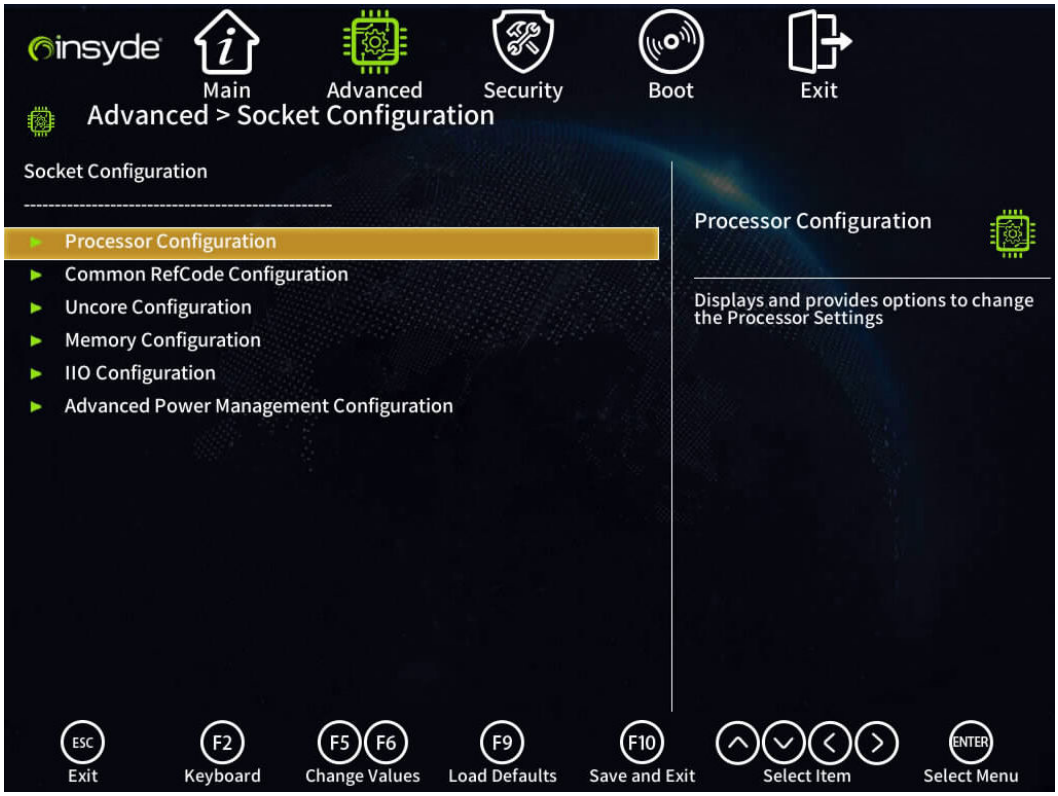


Step 5 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-41**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-41 Socket Configuration screen



Step 6 Select **Processor Configuration** and press **Enter**.

The **Processor Configuration** screen is displayed, as shown in **Figure 3-42**.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-42 Processor Configuration screen



Step 7 Select **Intel (R) TXT** and press **Enter**.

Step 8 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enables the TXT function.
- **Disabled**: Disables the TXT function.

Step 9 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 10 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the settings to take effect.

----End

3.1.14 Setting the Fan Speed Adjustment Mode

Scenarios

Set the fan speed adjustment mode on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

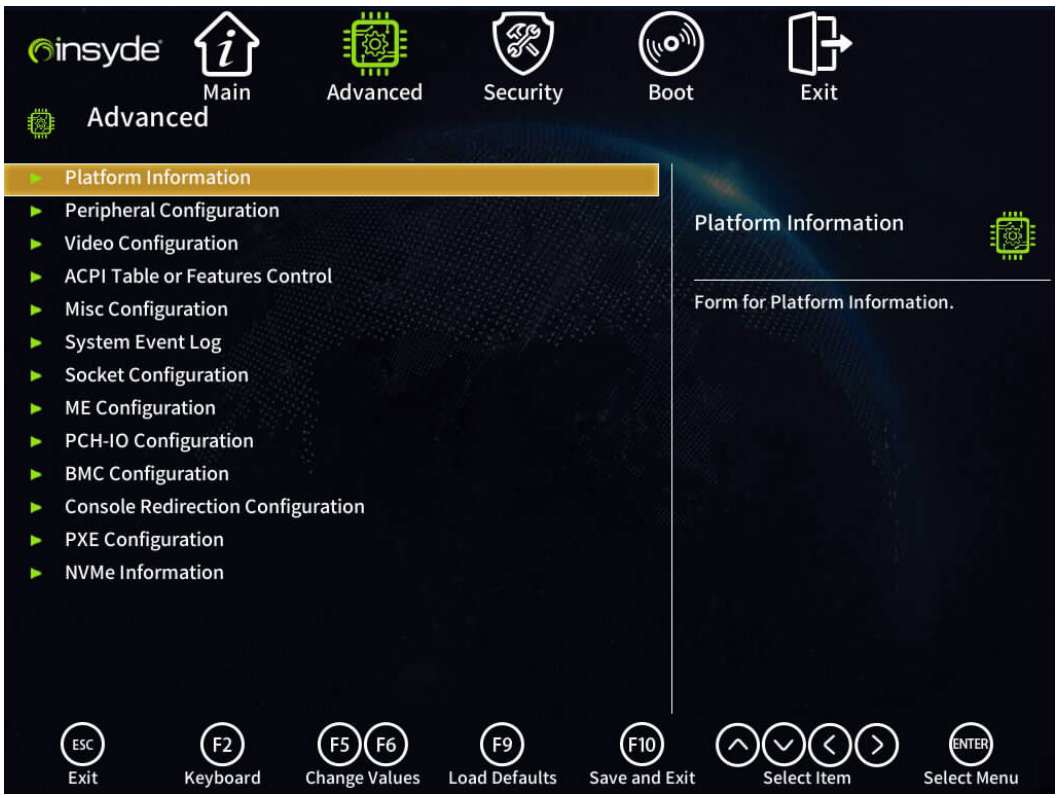
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-43**.

Figure 3-43 Advanced screen

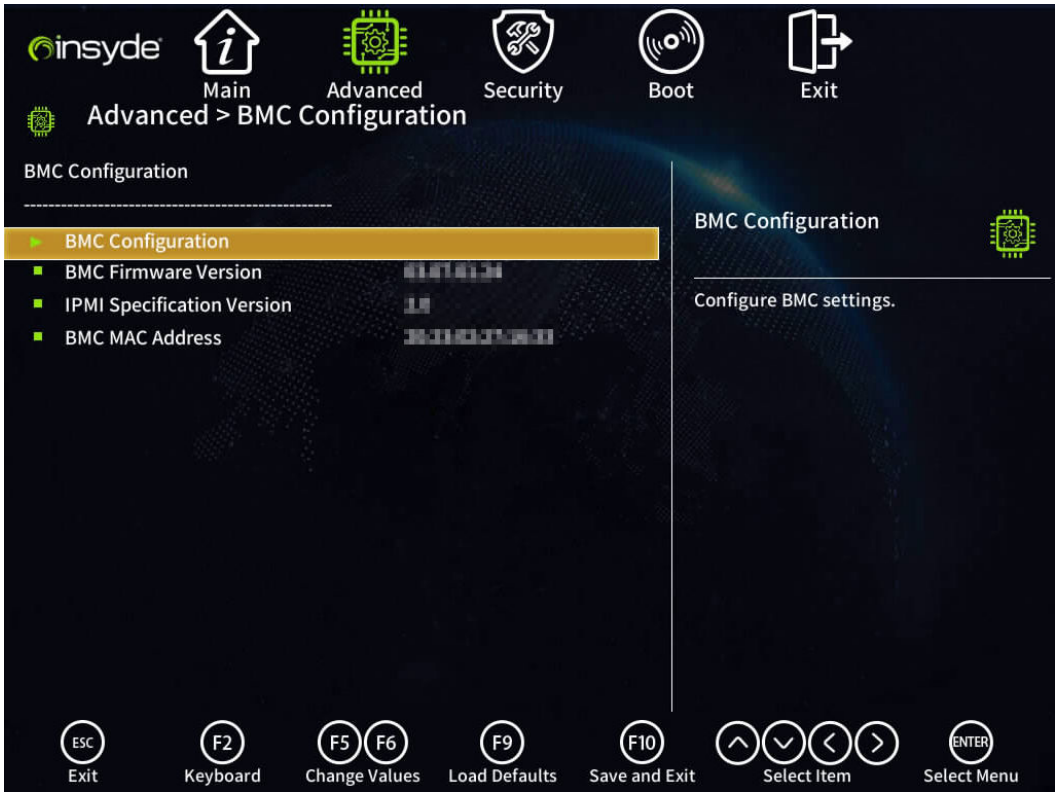


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-44**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-44 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-45** and **Figure 3-46**.

Check the BMC IP address. For details about parameters, see **5.2.10.1 BMC Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-45 BMC Configuration screen 1



Figure 3-46 BMC Configuration screen 2



Step 5 Select **BMC Smart Cooling** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 6 In the displayed dialog box, select a mode as required and press **Enter**.

- **Energy saving mode**: Evaluates the current load and heat dissipation of the system, controls the fan speed at a balanced point, and keeps the system power consumption at the lowest level.
- **Low noise mode**: Minimizes the fan speed and reduces noise while meeting heat dissipation requirements.
- **High performance mode**: Increases the fan speed and ensures the heat dissipation for key components to maintain low temperature for highest performance.
- **Custom Mode**: Provides a custom interface. You can set the target CPU temperature and the fan speed corresponding to each temperature area of the air intake vent.

Step 7 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 8 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.15 Setting Secure Boot in UEFI Mode

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Scenarios

Set Secure Boot in UEFI mode using the BIOS.

Secure Boot is defined by the UEFI specification to ensure the security of the boot environment. Before installing OS, third-party driver, or cards on a server, check whether they support digital signature. If digital signature is not supported, disable Secure Boot to ensure normal use. If digital signature is supported, enable Secure Boot to ensure system security.

Procedure

Step 1 Check the status of Secure Boot.

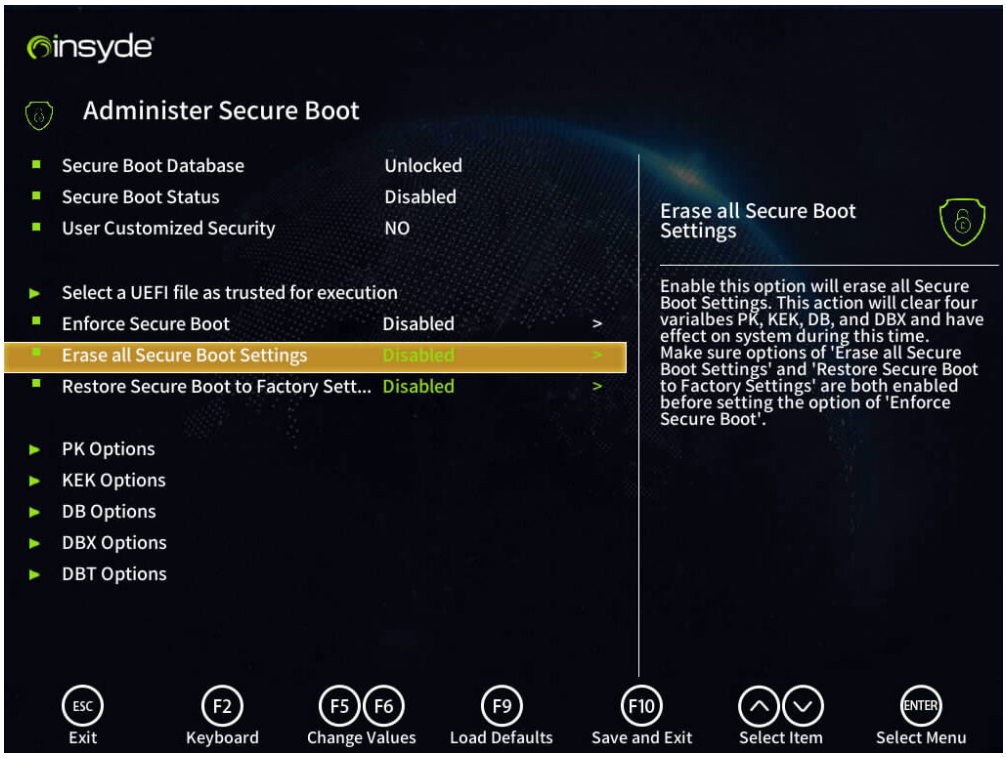
1. Access the front page.

   For details, see **3.1.1 Accessing the Front Page**.
2. Select **Administer Secure Boot** and press **Enter**.

   The **Administer Secure Boot** screen is displayed, as shown in **Figure 3-47**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-47 Administer Secure Boot screen



3. Check the status of **Secure Boot Database**.
   – If the status is **Installed and Locked**, the Secure Boot certificate database has been installed. Check the value of **Secure Boot Status**.
     - **Enabled**: Secure Boot is enabled. For details about how to disable Secure Boot, see **Step 3**.
     - **Disabled**: Secure Boot is disabled. For details about how to enable Secure Boot, see **Step 2**.
   – If the status is **Unlocked**, the Secure Boot certificate database is not installed. In this case, Secure Boot is disabled. For details about how to enable Secure Boot, see **Step 2**.

Step 2 (Optional) Enable Secure Boot.

- When the value of **Secure Boot Database** is **Installed and Locked** and the value of **Secure Boot Status** is **Disabled**:
  a. On the **Administer Secure Boot** screen, select **Enforce Secure Boot** and press **Enter**.
  b. Select **Enabled** from the menu that pops up.
  c. Press **F10**.
     The **Exit Saving Changes** dialog box is displayed.
  d. Select **Yes** and press **Enter** to save the settings.
     The server automatically restarts.
  e. Repeat **Step 1.1** to **Step 1.2** to access the **Administer Secure Boot** screen again.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The value of **Secure Boot Database** is **Installed and Locked** and the value of **Secure Boot Status** is **Enabled**, indicating that Secure Boot is enabled.

- When the value of **Secure Boot Database** is **Unlocked**:
  a. On the **Administer Secure Boot** screen, select **Restore Secure Boot to Factory Settings** and press **Enter**.
  b. Select **Enabled** from the menu that pops up.
  c. Press **F10**.
     The **Exit Saving Changes** dialog box is displayed.
  d. Select **Yes** and press **Enter** to save the settings.
     The server automatically restarts.
  e. Repeat **Step 1.1** to **Step 1.2** to access the Administer Secure Boot screen again.
  f. Check the value of **Secure Boot Status**.
     - **Enabled**: Secure Boot is enabled. The operation is completed.
     - **Disabled**: Secure Boot is disabled. In this case, go to **Step 2.g**.
  g. Set the value of **Enforce Secure Boot** to **Enabled**.
  h. Press **F10**.
     The **Exit Saving Changes** dialog box is displayed.
  i. Select **Yes** and press **Enter** to save the settings.
     The server automatically restarts.
  j. Repeat **Step 1.1** to **Step 1.2** to access the **Administer Secure Boot** screen again.
     The value of **Secure Boot Database** is **Installed and Locked** and the value of **Secure Boot Status** is **Enabled**, indicating that Secure Boot is enabled.

Step 3 (Optional) Disable Secure Boot.

- Using the **Enforce Secure Boot** parameter:
  a. On the **Administer Secure Boot** screen, select **Enforce Secure Boot** and press **Enter**.
  b. Select **Disabled** from the menu that pops up.
  c. Press **F10**.
     The **Exit Saving Changes** dialog box is displayed.
  d. Select **Yes** and press **Enter** to save the settings.
     The server automatically restarts.
  e. Repeat **Step 1.1** to **Step 1.2** to access the Administer Secure Boot screen again.
     The value of **Secure Boot Database** is **Installed and Locked** and the value of **Secure Boot Status** is **Disabled**, indicating that Secure Boot is disabled.
- Using the **Erase all Secure Boot Settings** parameter:

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

a. On the **Administer Secure Boot** screen, select **Erase all Secure Boot Settings** and press **Enter**.

b. Select **Enabled** from the menu that pops up to clear the security configuration.

c. Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

d. Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

e. Repeat **Step 1.1** to **Step 1.2** to access the Administer Secure Boot screen again.

The value of **Secure Boot Database** is **Unlocked** and the value of **Secure Boot Status** is **Disabled**, indicating that Secure Boot is enabled.

NOTE

Using the **Enforce Secure Boot** parameter to disable Secure Boot only disables Secure Boot but does not clear other configured Secure Boot settings. Using the **Erase all Secure Boot Settings** parameter to disable Secure Boob and clears all Secure Boot settings. Select a disabling mode as required.

----End

3.1.16 Setting the Server Boot Mode

Scenarios

Set the boot mode and sequence.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Boot** tab.

The **Boot** screen is displayed, as shown in **Figure 3-48** and **Figure 3-49**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-48 Boot screen (UEFI mode)



Figure 3-49 Boot screen (legacy mode)



Step 3 Set the BIOS boot mode.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

1. Select **Boot Type** and press **Enter**.
2. In the displayed dialog box, select **Legacy Boot Type** or **UEFI Boot Type**, and press **Enter**.

NOTE

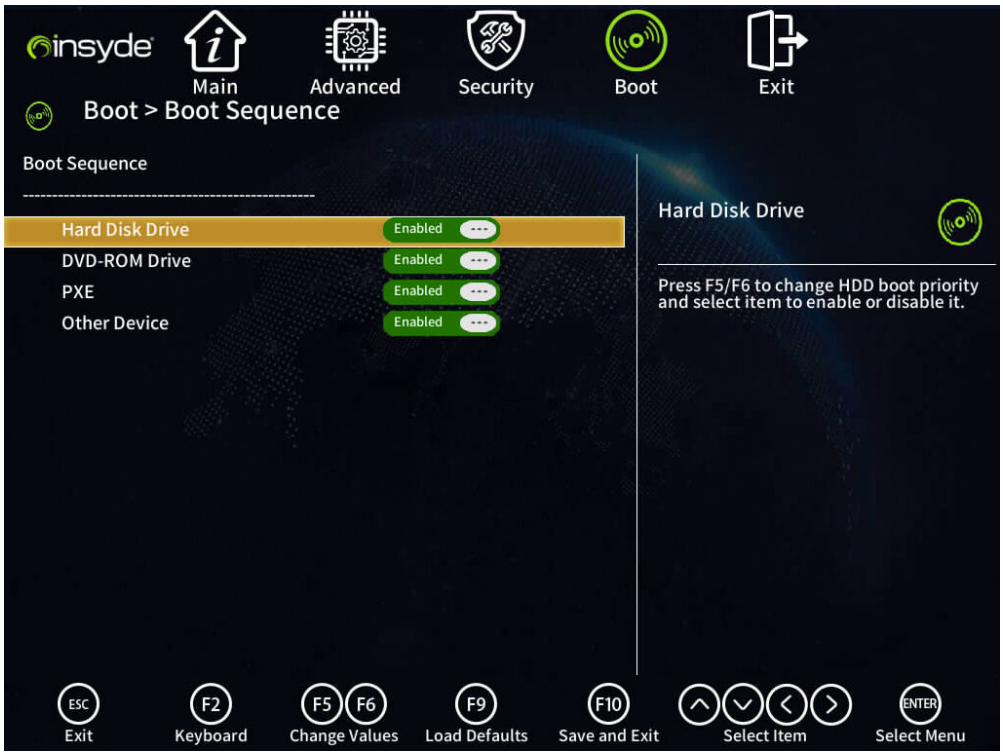
- The default boot mode is UEFI mode.
- After the Secure Boot function is enabled in UEFI mode, **Boot Type** is grayed out (that is, it cannot be set to **Legacy Boot Type**).
- For some OSs, if the capacity of the drive or the RAID array for installing the OS is greater than 2 TB, use the UEFI mode. For details, see the release notes of the OS.
- If the OS is to be installed on an NVMe drive, you can set **Boot Type** to only **UEFI Boot**.
- The UEFI mode supports more boot devices than legacy mode. If a server is configured with multiple boot devices, some devices may fail to start in legacy mode. In this case, the UEFI boot mode is recommended. If you need to use legacy mode, you are advised to disable the serial port redirection function or NIC PXE function based on the actual service scenario to ensure that the OS can be started properly. For details, see **3.1.12 Setting PXE for an NIC** and **3.1.21 Setting Serial Port Redirection**.

Step 4 Set the boot sequence.

1. Select **Boot Sequence** and press **Enter**.

   The **Boot Sequence** screen is displayed, as shown in **Figure 3-50**.

Figure 3-50 Boot Sequence screen



2. Select the target boot option and press **F5** or **F6** to change the boot sequence.
   - Press **F5** to move a boot option down.
   - Press **F6** to move a boot option up.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- The server boots in the sequence specified on this screen.
- The default boot sequence is **Hard Disk Drive** > **DVD-ROM Drive** > **PXE** > **Other Device**.
- You can enable or disable a boot option by dragging the button on the right of the boot option.

Step 5 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 6 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the settings to take effect.

----End

3.1.17 Setting the Server Boot Device

Scenarios

Set the device from which the server is booted on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Boot** tab.

The **Boot** screen is displayed, as shown in **Figure 3-51** and **Figure 3-52**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-51 Boot screen (UEFI mode)



Figure 3-52 Boot screen (legacy mode)



Step 3 Set the BIOS boot mode.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

1. Select **Boot Type** and press **Enter**.
2. In the displayed dialog box, select **Legacy Boot Type** or **UEFI Boot Type**, and press **Enter**.

   NOTE

   – The default boot mode is UEFI mode.
   – After the Secure Boot function is enabled in UEFI mode, **Boot Type** is grayed out (that is, it cannot be set to **Legacy Boot Type**).
   – For some OSs, if the capacity of the drive or the RAID array for installing the OS is greater than 2 TB, use the UEFI mode. For details, see the release notes of the OS.
   – If the OS is to be installed on an NVMe drive, you can set **Boot Type** to only **UEFI Boot**.
   – The UEFI mode supports more boot devices than legacy mode. If a server is configured with multiple boot devices, some devices may fail to start in legacy mode. In this case, the UEFI boot mode is recommended. If you need to use legacy mode, you are advised to disable the serial port redirection function or NIC PXE function based on the actual service scenario to ensure that the OS can be started properly. For details, see **3.1.12 Setting PXE for an NIC** and **3.1.21 Setting Serial Port Redirection**.

Step 4 Set the first boot device.

- To set a drive or RAID controller card as the first boot device, perform the following steps:

  a. On the **Boot Sequence** screen, set **Hard Disk Drive** as the first boot option, as shown in **3.1.16 Setting the Server Boot Mode**.

  b. In the **UEFI** or **Legacy** area of the **Boot** screen, select **Hard Disk Drive** and press **Enter**.

     NOTE

     ▪ **UEFI** is displayed in UEFI mode. **Legacy** is displayed in legacy mode.

     ▪ If no boot device is configured or boot devices do not support UEFI/Legacy boot, the boot type is not displayed in the UEFI/Legacy information area. For example, if the server is configured with a DVD-ROM drive, PXE, or USB device but no drive is configured, **Hard Disk Drive** is not displayed below the UEFI/Legacy information area.

  c. Select the boot device to be adjusted.

  d. Press **F5** (downwards) or **F6** (upwards) to set the corresponding drive or RAID controller card as the first boot device. That is, move it to the first row.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- You can enable or disable a boot device by dragging the button on the right of the boot device.
- In legacy mode, if the server is configured with a RAID controller card or physical drive that supports the legacy boot mode, the **Hard Disk Drive** list displays the information about the RAID controller card or physical drive. You can adjust the position of the RAID controller card or physical drive in the boot device list to adjust the boot device.
- In UEFI mode:
  - If no OS is installed on the drives of the server, there is no boot device in the **Hard Disk Drive** list. The drive selected to install the OS during the OS installation will be the boot drive.
  - If an OS has been installed on the drives of the server, the OS version will be displayed in the **Hard Disk Drive** list. You can set the boot device by adjusting the OS sequence.

- **To set the DVD-ROM drive as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **DVD-ROM Drive** as the first boot option, as shown in **3.1.16 Setting the Server Boot Mode**.
  b. Return to the **UEFI** or **Legacy** area on the **Boot** screen, select **DVD-ROM Drive**, and press **Enter**.
  c. Select the boot device to be adjusted.
  d. Press **F5** (downwards) or **F6** (upwards) to set the DVD-ROM drive as the first boot device. That is, move the DVD-ROM drive to the first row.

  NOTE

  You can enable or disable a boot device by dragging the button on the right of the boot device.

- **To set PXE as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **PXE** as the first boot option, as shown in **3.1.16 Setting the Server Boot Mode**.
  b. Return to the **UEFI** or **Legacy** area on the **Boot** screen, select **Other Device**, and press **Enter**.
  c. Select the boot device to be adjusted.
  d. Press **F5** (downwards) or **F6** (upwards) to set the PXE boot option as the first boot device. That is, move the PXE boot option to the first row.

  NOTE

  You can enable or disable a boot device by dragging the button on the right of the boot device.

- **To set a USB device as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **Other Device** as the first boot option, as shown in **3.1.16 Setting the Server Boot Mode**.
  b. Return to the **UEFI** or **Legacy** area on the **Boot** screen, select **Other Device**, and press **Enter**.
  c. Select the boot device to be adjusted.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

d. Press **F5** (downwards) or **F6** (upwards) to set the USB device as the first boot device. That is, move the USB device to the first row.

NOTE

You can enable or disable a boot device by dragging the button on the right of the boot device.

Step 5 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 6 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.18 Setting the BMC User Password

Scenarios

Set the user password for logging in to the BMC of a server using the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

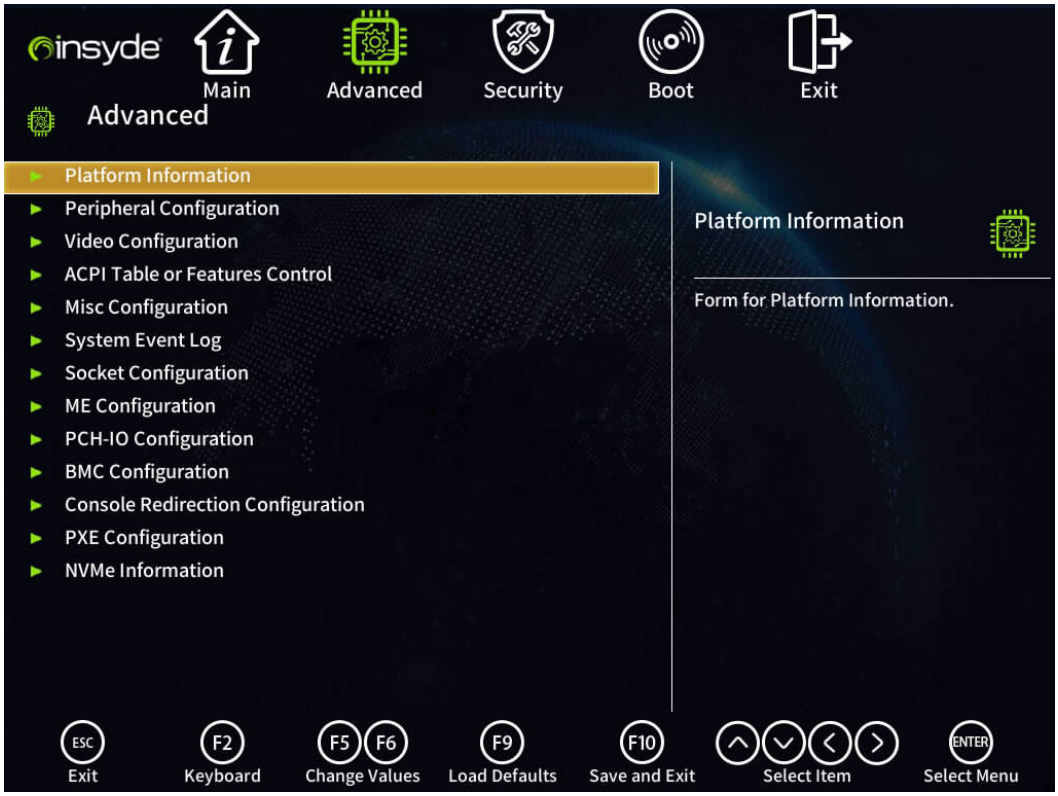
For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-53**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-53 Advanced screen

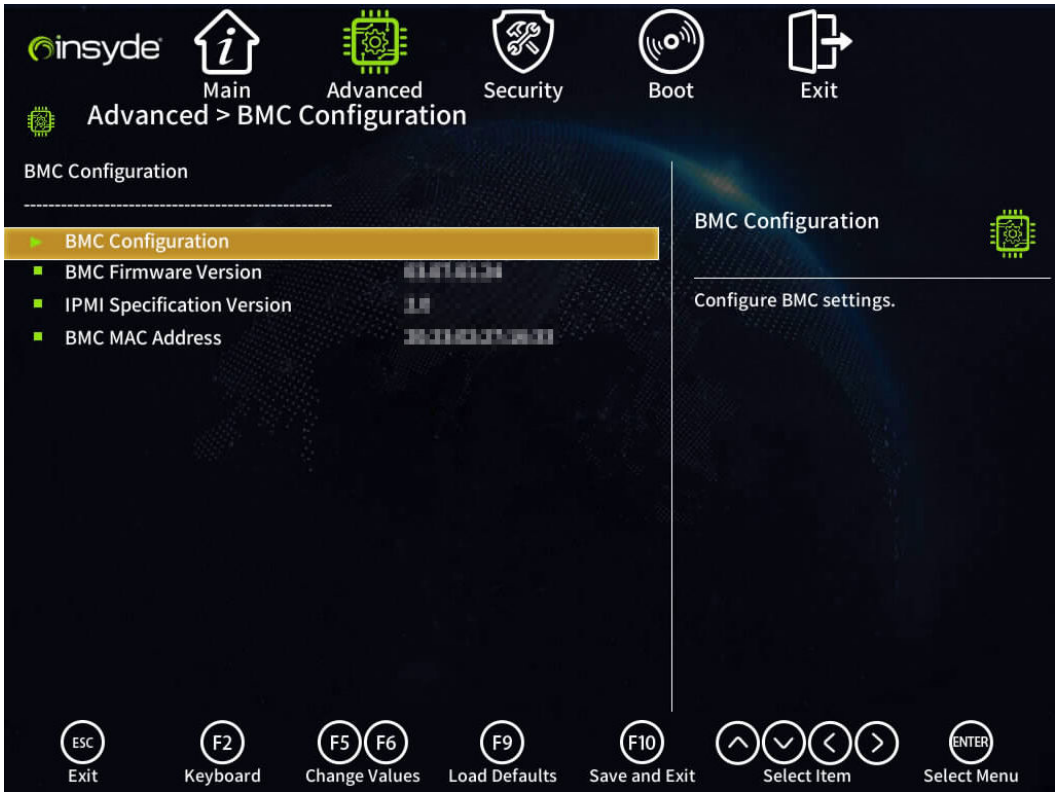


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-54**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-54 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-55** and **Figure 3-56**.

Check the BMC IP address. For details about parameters, see **5.2.10.1 BMC Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-55 BMC Configuration screen 1



Figure 3-56 BMC Configuration screen 2



Step 5 Select **Change BMC User Settings** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 6 Select **Reset BMC User Password** and press **Enter**.

The **Reset BMC User Password** dialog box is displayed.

Step 7 Enter and confirm the new password of the BMC user.

- If password complexity check is disabled, the password length cannot be zero or exceed 20 characters.
- If password complexity check is enabled, the password must meet the following requirements:
  - The password is a string of 8 to 20 characters.
  - The password must contain at least one space or one of the following special characters:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - The password must also contain at least two types of the following characters:
    - Uppercase letters A to Z
    - Lowercase letters a to z
    - Digits 0 to 9
  - The password must be different from the user name or the user name in reverse order.
- If the weak password dictionary authentication is enabled, the password must be different from passwords contained in the weak password dictionary.

NOTE

- Run the **ipmcset -t user -d weakpwddic -v export** command to obtain the weak password dictionary.
- For details about how to set the password check function and query the weak password dictionary, see the corresponding *iBMC User Guide*.

Step 8 After the setting is complete, click **Yes**.

After you disconnect the BMC and log in to the BMC again, a message is displayed indicating that the password is successfully set.

Step 9 Click **OK**.

The password is set successfully.

----End

3.1.19 Setting the BMC Network Information

Scenarios

Set the BMC network information, including the mode for obtaining the BMC IP address, subnet mask, and gateway address.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

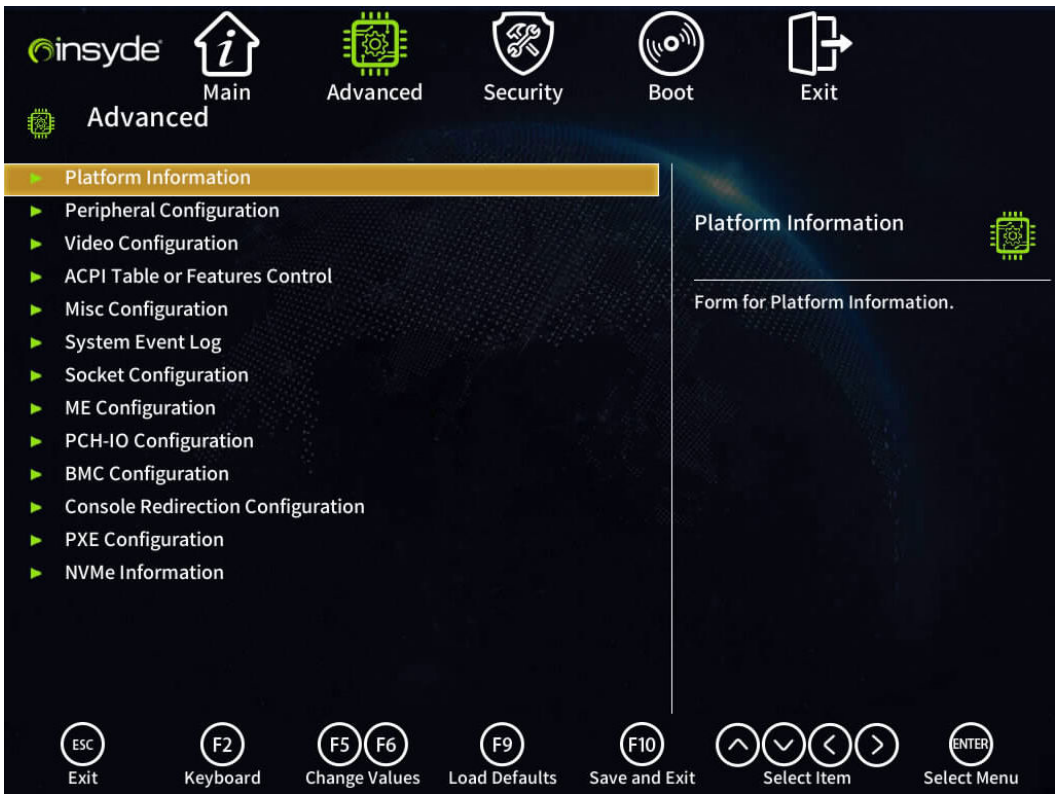
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-57**.

Figure 3-57 Advanced screen

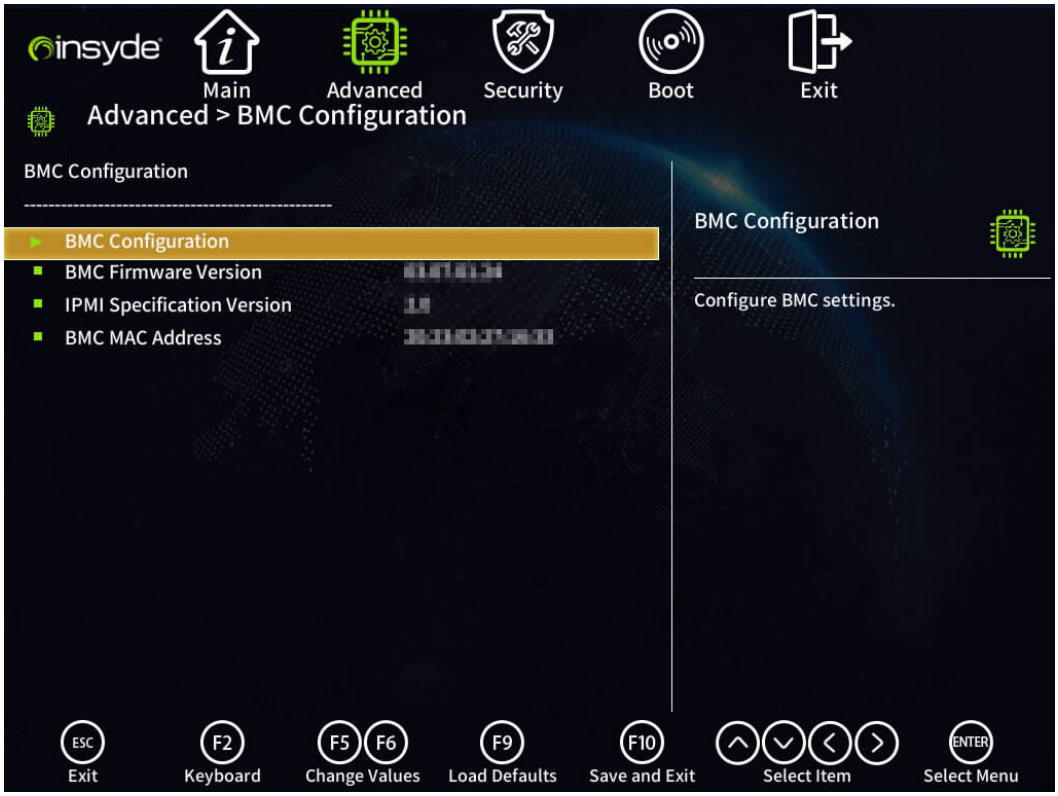


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-58**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-58 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-59** and **Figure 3-60**.

Check the BMC IP address. For details about parameters, see **5.2.10.1 BMC Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-59 BMC Configuration screen 1



Figure 3-60 BMC Configuration screen 2



Step 5 (Optional) Set the BMC network port mode.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

1. Select **BMC Network Mode** and press **Enter**.

   NOTE

   The menu options of this parameter vary with the server configuration.

2. In the displayed dialog box, select the network mode and press **Enter**. The network mode can be any of the following:
   - **Dedicated**: Dedicated mode. You can access the BMC only through the management network port.
   - **Auto**: Auto-negotiation mode. You can access the BMC through the management network port or the NCSI service network port of the server.
   - **PCIe Shared**: PCIe NIC sharing mode. You can access the BMC only through the NCSI network port of the PCIe NIC.
   - **OCP1 Shared**: OCP1 NIC sharing mode. You can access the BMC only through the network port of the OCP1 NIC.
   - **OCP2 Shared**: OCP2 NIC sharing mode. You can access the BMC only through the network port of the OCP2 NIC.

   NOTE

   - When this parameter is set to **PCIe Shared**, the **Vlan Id** and **NCSI PCIe Port Select** options are displayed, which are used to set the BMC VLAN ID and the service network port.
   - When this parameter is set to **OCP*x* Shared**, the **Vlan Id** and **NCSI OCP Port Select** options are displayed, which are used to set the BMC VLAN ID and service network port.
   - When this parameter is set to **Auto**, the **Vlan Id** option is displayed, which is used to set the BMC VLAN ID.

Step 6 (Optional) Set the BMC IPv4 network information.

- Manually configure the IP address as follows:
  a. Select **IPv4 Configuration** and press **Enter**.
  b. In the displayed dialog box, select **Static** and press **Enter**.
  c. Select **IPv4 IP Address** and press **Enter**.
     The **IPv4 IP Address** dialog box is displayed.
  d. Enter the BMC IPv4 address and click **Yes**.
  e. Select **IPv4 Subnet Mask** and press **Enter**.
     The **IPv4 Subnet Mask** dialog box is displayed.
  f. Enter the BMC IPv4 subnet mask and click **Yes**.
  g. Select **IPv4 Gateway Address** and press **Enter**.
     The **IPv4 Gateway Address** dialog box is displayed.
  h. Enter the BMC IPv4 gateway and click **Yes**.
     The BMC network is configured.
- Dynamically assign an IP address as follows:
  a. Select **IPv4 Configuration** and press **Enter**.
  b. In the displayed dialog box, select **DHCP** and press **Enter**.
     The configuration of dynamically obtaining the BMC network information through the DHCP protocol is completed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

The IP addresses listed below are reserved addresses and cannot be set by users.

- 0.0.0.0/8
- 10.0.0.0/8
- 100.64.0.0/10
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12
- 192.0.0.0/24
- 192.0.2.0/24
- 192.88.99.0/24
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/4
- 233.252.0.0/24
- 240.0.0.0/4
- 255.255.255.255/32

Step 7 (Optional) Set the BMC IPv6 network information.

NOTE

You can set the BMC IPv6 network information in the same way of setting the BMC IPv4 network information.

The IP addresses listed below are reserved addresses and cannot be set by users.

- ::/128
- ::1/128
- fe80::/10
- ff00::/8

Step 8 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 9 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.20 Setting a PCIe Port

Scenarios

Enable or disable a PCIe port using the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

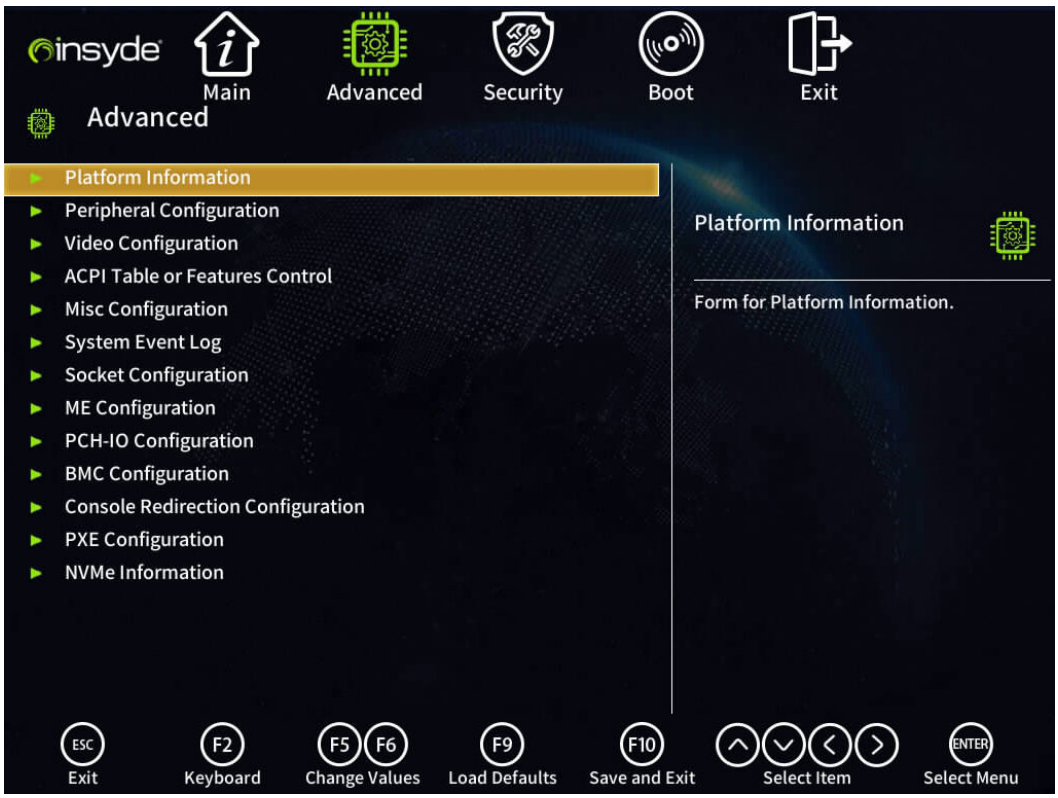
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-61**.

Figure 3-61 Advanced screen

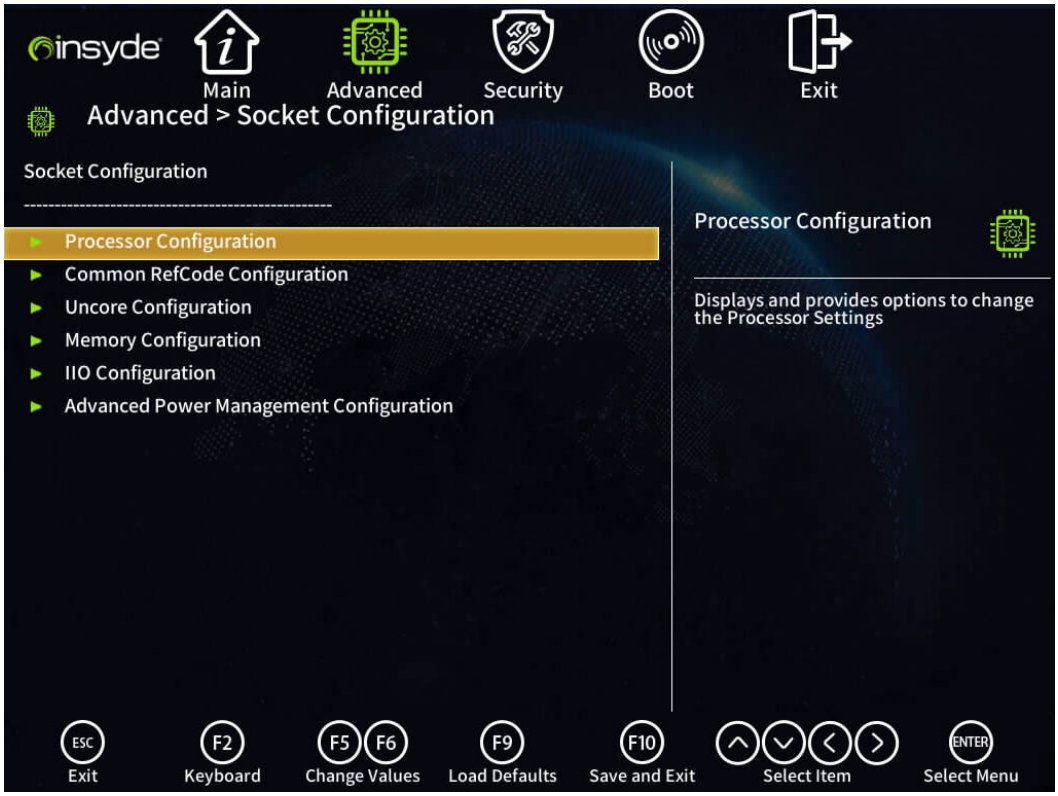


Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-62**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-62 Socket Configuration screen



Step 4 Select **IIO Configuration** and press **Enter**.

The **IIO Configuration** screen is displayed, as shown in **Figure 3-63**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-63 IIO Configuration screen



Step 5 Select a socket configuration screen, for example, **Socket1 Configuration**, and press **Enter**.

The **Socket1 Configuration** screen is displayed, as shown in **Figure 3-64**.

NOTE

The parameters on the displayed screen vary depending on the bandwidth configuration and used port of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-64 Socket1 Configuration screen



Step 6 Select a port, for example, **Port 1A**, and press **Enter**.

The **Port 1A** screen is displayed, as shown in **Figure 3-65**.

NOTE

For details about the mapping between ports and PCIe components, see "Hardware Description" > "I/O Expansion" in the server user guide.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-65 Port 1A screen



Step 7 Select **PCIe Port** and press **Enter**.

Step 8 In the displayed dialog box, select **Enabled**, **Disabled**, or **Auto** as required, and press **Enter**.

- **Enabled/Auto**: Enable the PCIe port.
- **Disabled**: disables the PCIe port.

Step 9 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 10 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.1.21 Setting Serial Port Redirection

Scenarios

Enable or disable serial port redirection using the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

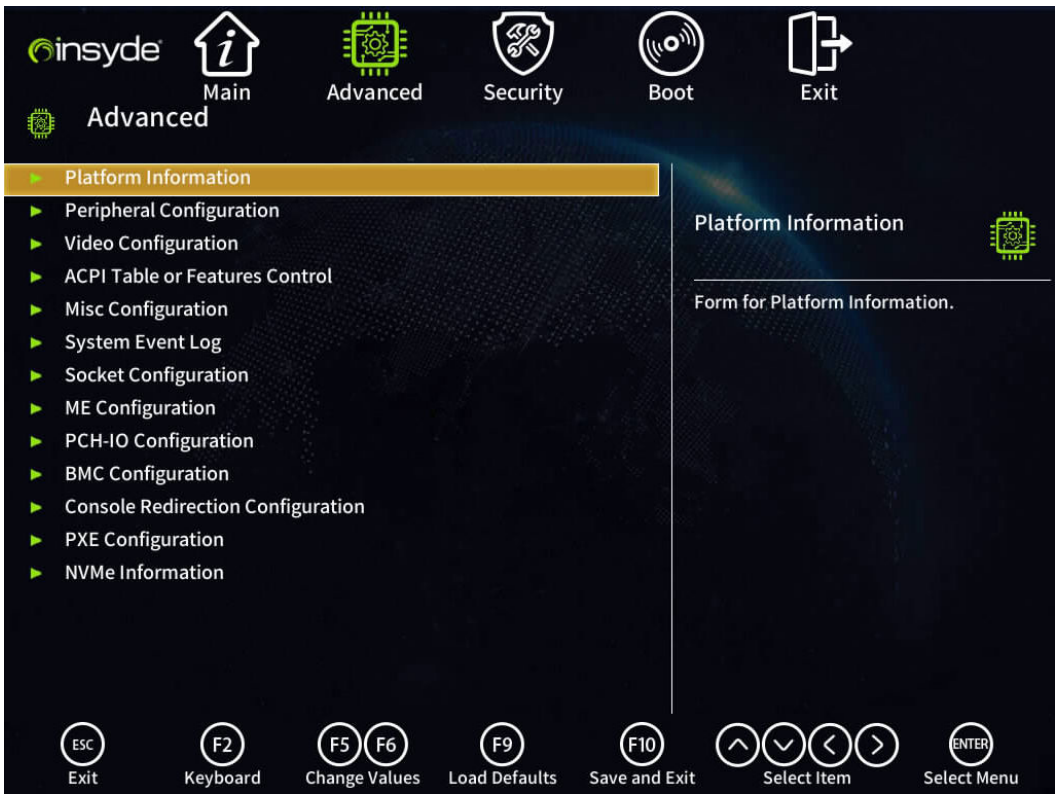
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

The **Advanced** screen is displayed, as shown in **Figure 3-66**.

Figure 3-66 Advanced screen



Step 3 Select **Console Redirection** and press **Enter**.

The **Console Redirection** screen is displayed, as shown in **Figure 3-67**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-67 Console Redirection Configuration screen



Step 4 Select **Console Serial Redirect** and press **Enter**.

Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: enables serial port redirection.
- **Disabled**: disables serial port redirection.

Step 6 Press **F10**.

The **Exit Saving Changes?** dialog box is displayed.

Step 7 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the settings to take effect.

----End

3.1.22 Enabling Software Guard Extension

Scenarios

Enable the Software Guard Extension (SGX) function on the BIOS.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- Before enabling SGX, set related options. For details, see **Procedure**.
- Memory DIMM requirements: A DIMM is installed in channel slot 1. The models and capacities of all DIMMs in all channel slots 1 are the same.
- If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.
- Check the processor specifications on Intel's official website to confirm whether the processor supports SGX.
- The BIOS checks whether the SGX Flexible Launch Control feature is supported based on the CPU ID. If the feature is supported, the BIOS enables the feature by default.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab.

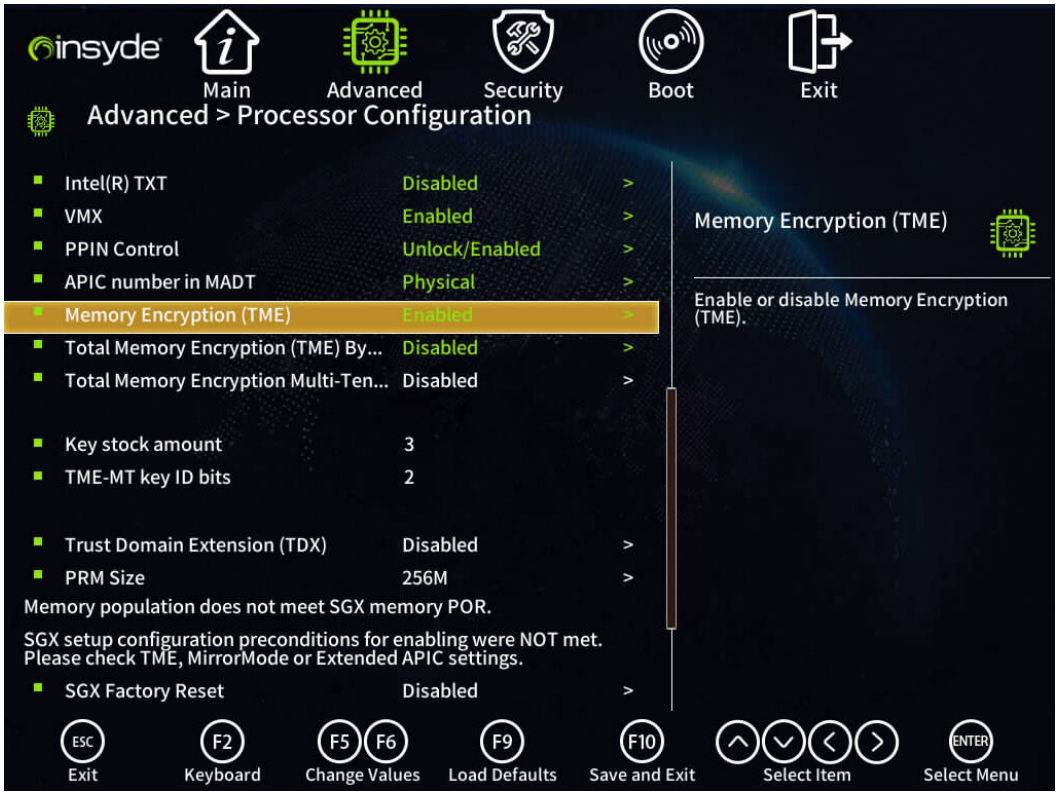
The **Advanced** screen is displayed.

Step 3 Select **Socket Configuration** > **Processor Configuration**.

The **Processor Configuration** screen is displayed.

Step 4 Set Memory Encryption (TME) to Enabled, as shown in **Figure 3-68**.

Figure 3-68 Setting Memory Encryption (TME)



Step 5 Press Esc to return to the **Socket Configuration** screen and select **Common RefCode Configuration**.

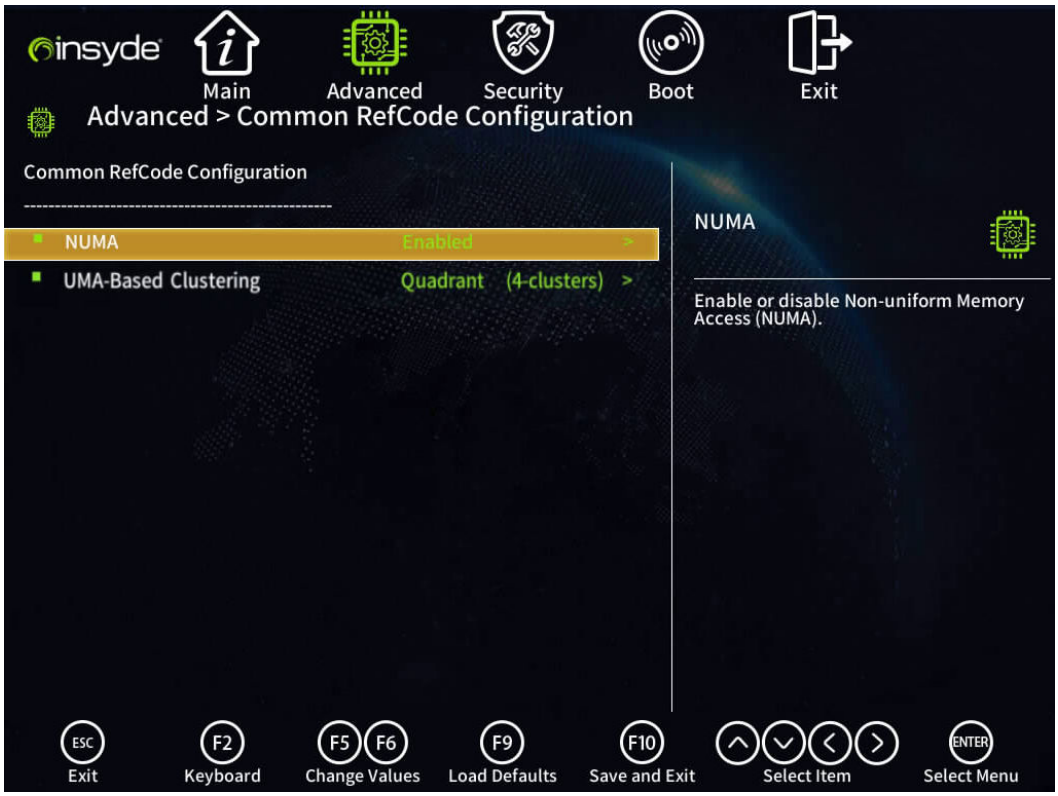
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Common RefCode Configuration** screen is displayed.

Step 6 Set the following parameters, as shown in **Figure 3-68**.

1. Set **NUMA** to **Enabled**.
2. Set **UMA-Based Clustering** to **Disabled (All2All)**.

Figure 3-69 Common RefCode Configuration screen



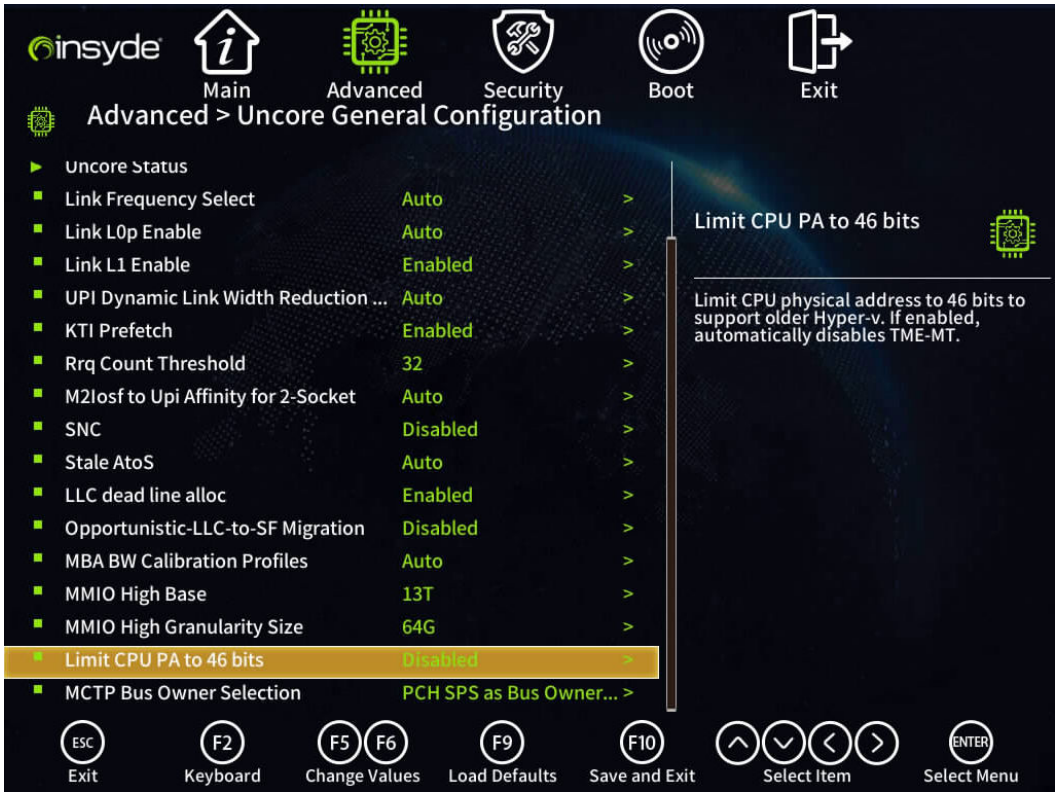
Step 7 Press Esc to return to the **Socket Configuration** screen and select **Uncore Configuration** > **Uncore General Configuration**.

The **Uncore General Configuration** screen is displayed.

Step 8 Set **Limit CPU PA to 46 bits** to **Disabled**, as shown in **Figure 3-70**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-70 Setting Limit CPU PA to 46 bits



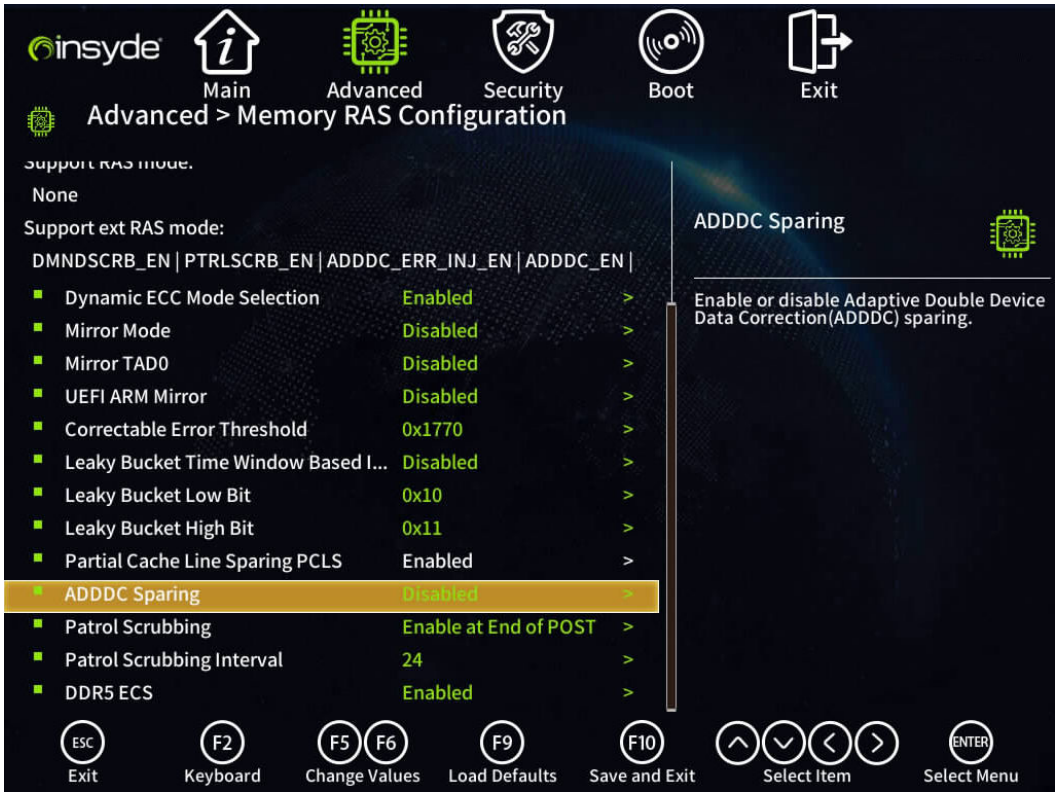
Step 9 Press Esc to return to the **Socket Configuration** screen and select **Memory Configuration** > **Memory RAS Configuration**.

The **Memory RAS Configuration** screen is displayed.

Step 10 Set **ADDDC Sparing** to **Disabled**, as shown in **Figure 3-71**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-71 Setting ADDDC Sparing



Step 11 Press **Esc** to return to the **Socket Configuration** screen and select **Processor Configuration**.

The **Processor Configuration** screen is displayed.

Step 12 Set **SW Guard Extensions (SGX)** to **Enabled**, as shown in **Figure 3-72**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-72 Enabling Software Guard Extension (SGX)



----End

3.1.23 Restoring Default BIOS Settings

Scenarios

Restore the BIOS factory settings of the server.

NOTE

- If the configurations are customized, press **F9** to restore the customized configurations or BIOS factory settings.
- This task is supported only when you access the Setup Utility screen as the BIOS administrator.
- Except for the following information that cannot be restored, the other BIOS parameters will be restored to default values of the current BIOS version. Modify related parameters again if the service requires special configurations on the BIOS parameters.
  - Date and time information on the **Main** screen
  - BIOS password and BIOS startup logo
  - All parameters (except watchdog-related parameters) on the **BMC Configuration** screen under the **Advanced** screen
  - All parameters on the **Device Manager** and **Administer Secure Boot** screens in UEFI mode
- For details about how to restore the default BIOS settings using the BMC CLI, see the corresponding *iBMC User Guide*.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Method 1

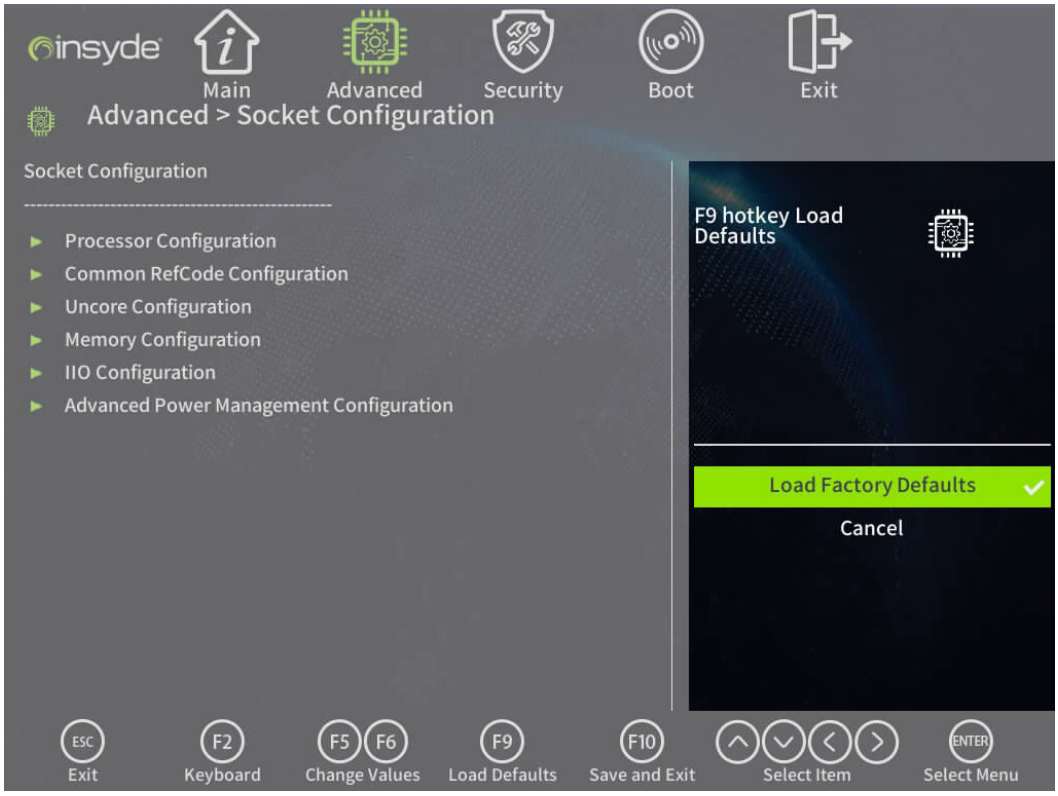
Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Press **F9**.

The **Load Factory Defaults** dialog box is displayed, as shown in **Figure 3-73**.

Figure 3-73 Load Factory Defaults dialog box



Step 3 Select **Yes** and press **Enter**.

Step 4 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 5 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

Method 2

Step 1 Access the Setup Utility screen.

For details, see **3.1.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Exit** tab.

The **Exit** screen is displayed, as shown in **Figure 3-74**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-74 Exit screen

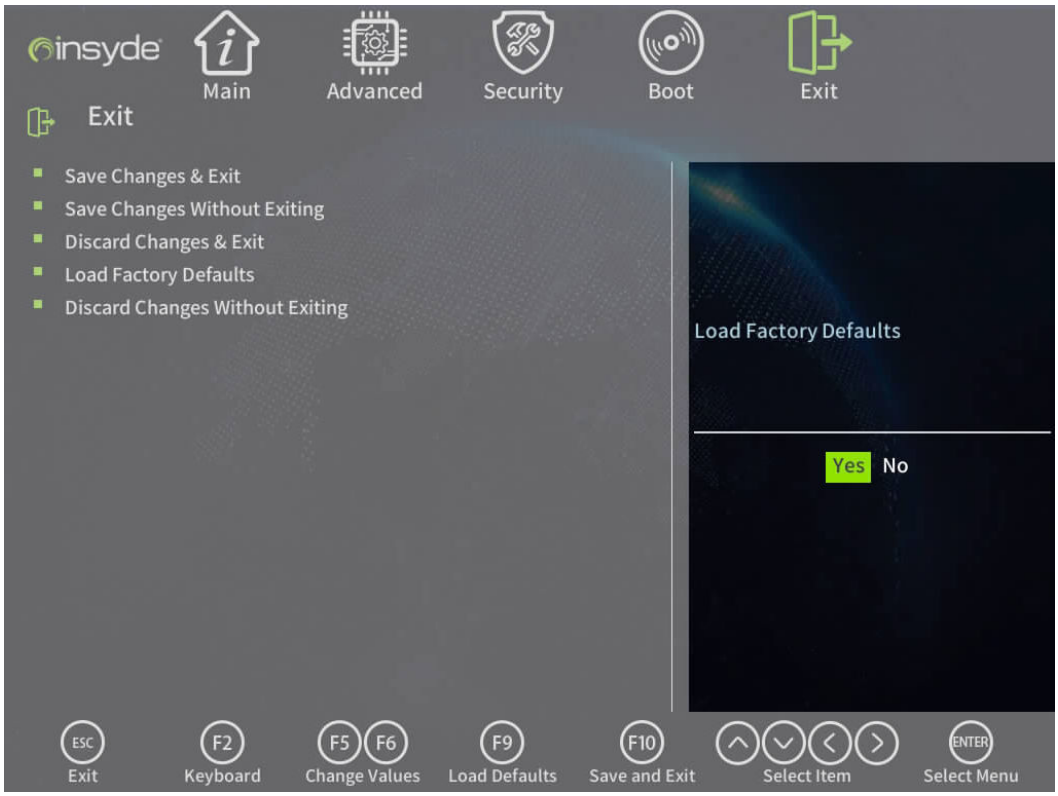


Step 3 Select **Load Factory Defaults** and press **Enter**.

The **Load Factory Defaults** dialog box is displayed, as shown in **Figure 3-75**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-75 Load Factory Defaults dialog box



Step 4 Click **Yes**.

Step 5 Press **F10**.

The **Exit Saving Changes** dialog box is displayed.

Step 6 Select **Yes** and press **Enter** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2 Common Operations (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

NOTE

This section applies to the 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7. For common operations of 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7, see **3.1 Common Operations (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**.

3.2.1 Accessing the Front Page

Scenarios

Access the front page.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

Step 1 Connect a local PC with the keyboard, video, and mouse (KVM) to the server, or log in to the server using the Remote Console of the iBMC WebUI.

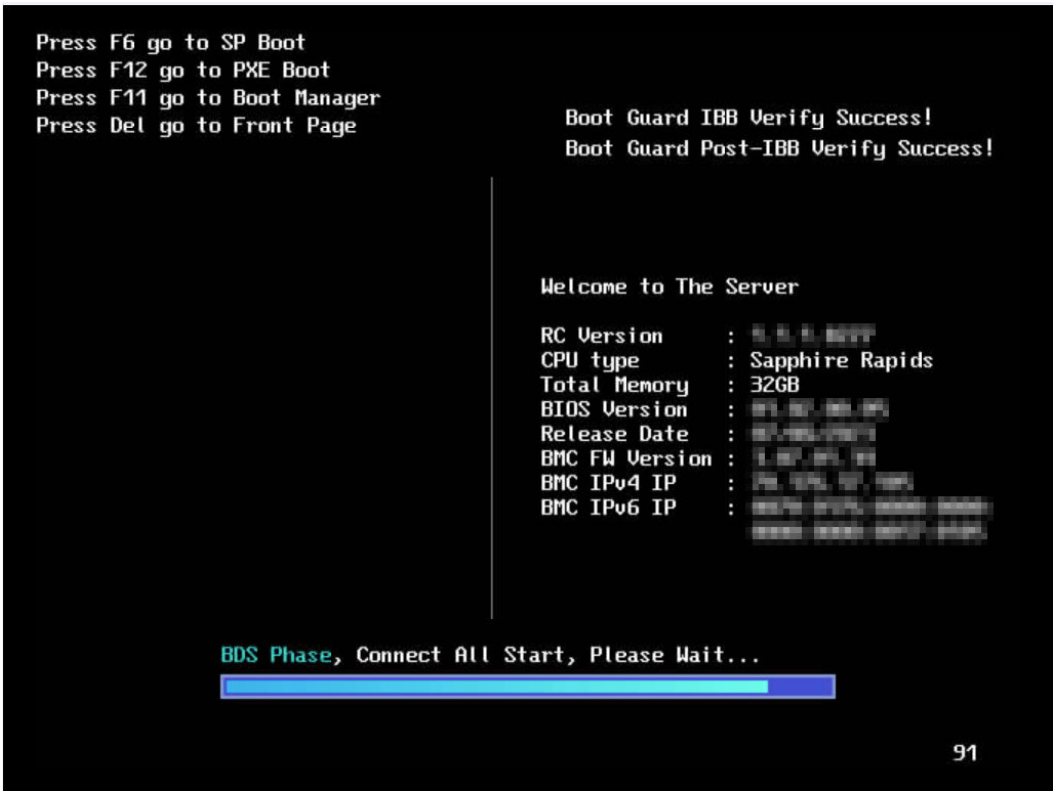
Step 2 Power on or restart the server.

NOTE

Restarting the server will interrupt services. Exercise caution when performing this operation.

Step 3 When the screen shown in **Figure 3-76** is displayed, press **Del** or **Delete**.

Figure 3-76 BIOS boot screen



NOTE

- To access the Smart Provisioning GUI, press **F6**. For details, see **3.2.4 Accessing the Smart Provisioning GUI**.
- To boot from the network, press **F12**.
- To access the **Boot Manager** screen, press **F11**.
- To access the front page, press **DEL**.

Step 4 Enter the current password.

Enter the current password in the dialog box displayed if prompted, as shown in **Figure 3-77**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- The default BIOS password is **Admin@9000**. If you use the default password to log in, the system prompts you to change the administrator password. For details, see **3.2.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.2.11.2 Setting the BIOS Common User Password**. For security purposes, you are advised to periodically change the administrator password.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.

Figure 3-77 Entering the current password



Step 5 After entering the password, press **Enter**.

The front page is displayed, as shown in **Figure 3-78** or **Figure 3-79**.

NOTE

- **Figure 3-78** and **Figure 3-80** show the front pages displayed in different modes when you log in to the system as the administrator. The administrator can set all parameters on the Setup Utility screen and use shortcut keys **F10** (save and exit) and **F9** (restore defaults).
- **Figure 3-79** and **Figure 3-81** show the front pages displayed in different modes when you log in to the system as a common user. In this case, only the **Continue** and **Setup Utility** menus are configurable. Other menus are grayed out and cannot be edited. On the Setup Utility screen, a common user can only view menu options, set or change their own password (that is, editing the **Set User Password** option on the **6.3 Security** screen and the **Save Changes & Exit** option on the **6.5 Exit** screen). Other options are grayed out and cannot be edited.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-78 Front page 1 (login as the administrator in UEFI mode)



Figure 3-79 Front page 2 (login as a common user in UEFI mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-80 Front page 3 (login as the administrator in legacy mode)



Figure 3-81 Front page 4 (login as a common user in legacy mode)



----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.2.2 Accessing the Setup Utility Screen

Scenarios

Access the Setup Utility screen when you need to set system boot parameters and query system data.

Procedure

Step 1 Connect a local PC with the keyboard, video, and mouse (KVM) to the server, or log in to the server using the Remote Console of the iBMC WebUI.

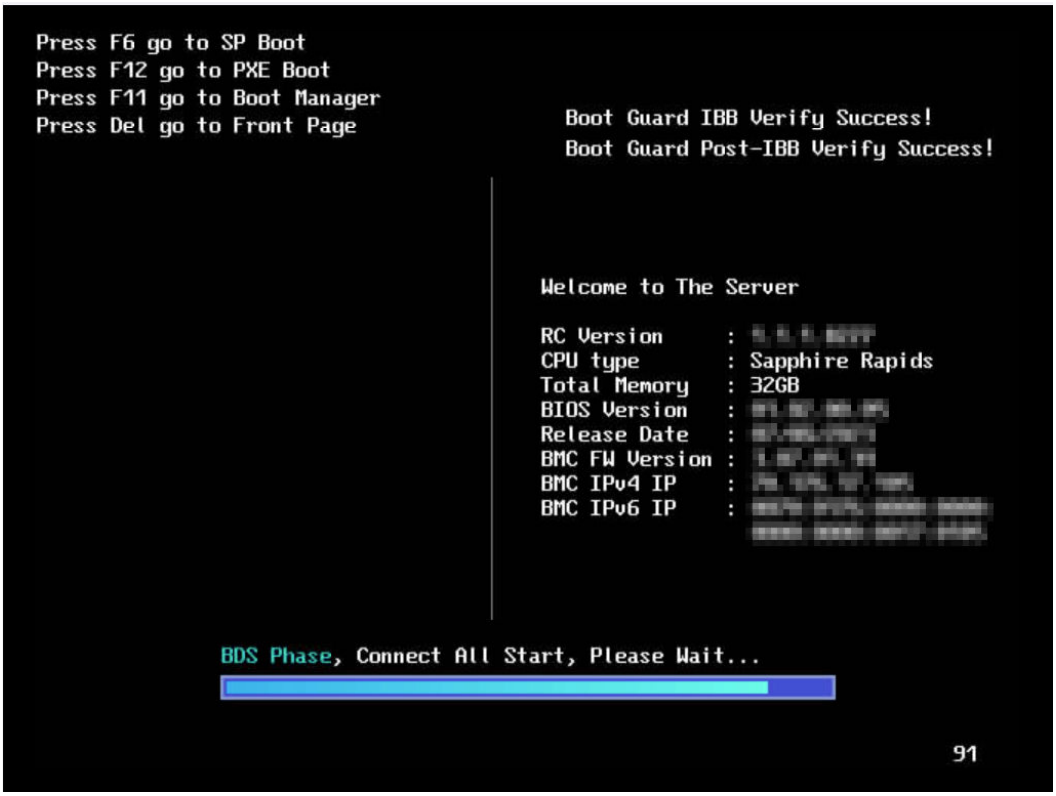
Step 2 Power on or restart the server.

NOTE

Restarting the server will interrupt services. Exercise caution when performing this operation.

Step 3 When the screen shown in **Figure 3-82** is displayed, press **Del** or **Delete**.

Figure 3-82 BIOS boot screen



NOTE

- To access the Smart Provisioning GUI, press **F6**. For details, see **3.2.4 Accessing the Smart Provisioning GUI**.
- To boot from the network, press **F12**.
- To access the **Boot Manager** screen, press **F11**.
- To access the front page, press **DEL**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Enter the current password.

Enter the current password in the dialog box displayed if prompted, as shown in **Figure 3-83**.

NOTE

- The default BIOS password is **Admin@9000**. If you use the default password to log in, the system prompts you to change the administrator password. For details, see **3.2.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.2.11.2 Setting the BIOS Common User Password**. For security purposes, you are advised to periodically change the administrator password.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.

Figure 3-83 Entering the current password



Step 5 On the front page, select **Setup Utility** and press **Enter**.

The **Main** screen is displayed, as shown in **Figure 3-84**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-84 Main screen



----End

3.2.3 Accessing BIOS Using a Serial Port

Scenarios

Use a serial port to access the Setup Utility screen. This section uses a Windows OS as an example.

Prepare the following data and software tools in advance:

- BMC IP address of the server to be accessed
- BMC administrator's user name and password of the server to be accessed
- IPMItool: third-party software that is prepared by yourself

NOTE

- The IP address of the Windows client must be reachable from the BMC management network port.
- IPMItool is used as an example here.

Procedure

Step 1 Place the IPMItool tool package in the root directory of the drive on a Windows client. Use drive D as an example.

Step 2 Log in to the Remote Console of the iBMC WebUI.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 3 Power on the server.

Step 4 Access the command line interface (CLI) of the OS.

- On the Windows OS, enter **cmd** in the search box of the **Start** menu and press **Enter**.
- For other OSs, refer to the methods provided on the OS official websites.

NOTE

The Windows OS is used as an example. For commands on other OSs, see the OS official websites.

Step 5 Run the **D:** command to access drive D.

Step 6 Run the **cd D:\ipmitool** command to access the directory where IPMItool is located.

Step 7 Run the **ipmitool -I lanplus -H *192.168.2.101* -U *Administrator* -P *Admin@9000* sol activate** command to access BIOS through the serial port.

NOTE

Change the IP address, user name, and password in this command as needed.

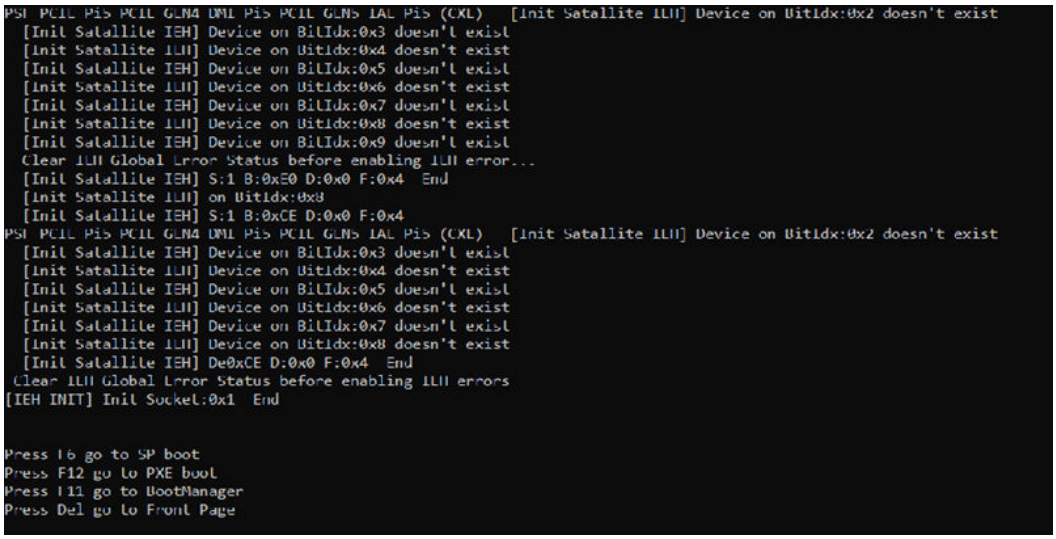
- *192.168.2.101* indicates the BMC IP address.
- *Administrator* indicates the BMC user name.
- *Admin@9000* indicates the BMC Password.

```
D:\ipmitool>ipmitool -I lanplus -H 192.168.2.101 -U Administrator -P Admin@9000
sol activate
[SOL Session operational.  Use ~? for help]
```

Step 8 Manually restart the server.

Step 9 When the BIOS boot screen shown in **Figure 3-85** is displayed, press **Del** or **Delete**.

Figure 3-85 BIOS boot screen



NOTE

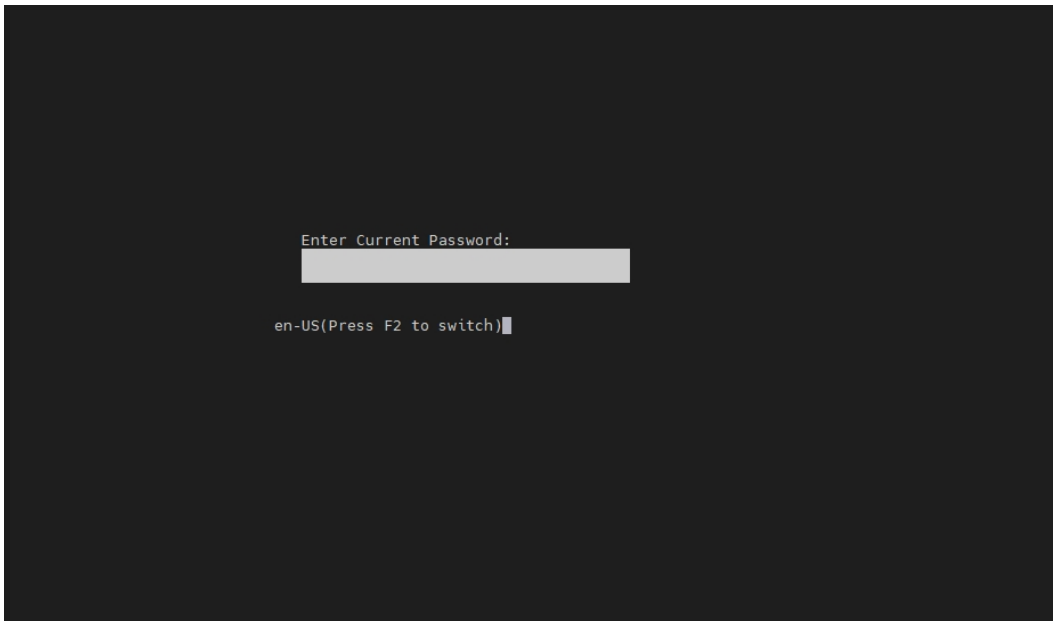
- To access the **Boot Manager** screen, press **F11**.
- To boot from the network, press **F12**.
- To access the Smart Provisioning GUI, press **F6**. For details, see **3.2.4 Accessing the Smart Provisioning GUI**.

Step 10 In the displayed dialog box, enter the password and press **Enter**, as shown in **Figure 3-86**.

NOTE

- The default BIOS password is **Admin@9000**. After the first login, you are advised to set an administrator password immediately. For details, see **3.2.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.2.11.2 Setting the BIOS Common User Password**. For security purposes, you are advised to periodically change the administrator password.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.

Figure 3-86 Entering the current password



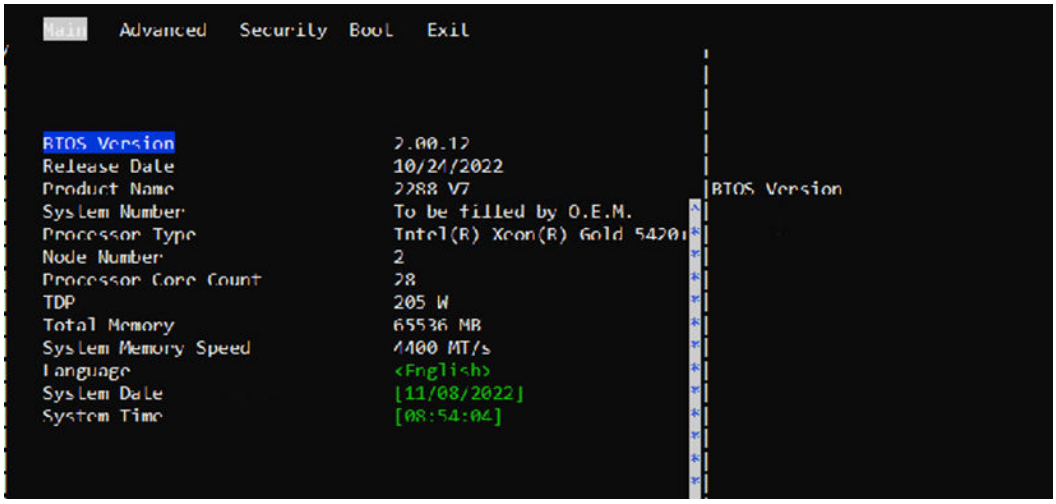
The **Main** screen is displayed, as shown in **Figure 3-87**.

NOTE

Figure 3-87 shows the screen displayed when you use the administrator password to log in to the system. If you log in to the system using a common user password, the access is restricted. On the Setup Utility screen, a common user can only view menu options, set or change the password of the common user (that is, editing the **Set User Password** option on the **6.3 Security** screen and the **Save Changes & Exit** option on the **6.5 Exit** screen). Other options are grayed out and cannot be edited.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-87 Main screen



----End

3.2.4 Accessing the Smart Provisioning GUI

Scenarios

Log in to the Smart Provisioning GUI. The following uses Smart Provisioning V132 as an example.

When the server is installed with the Smart Provisioning tool and the Smart Provisioning tool is enabled, you can enter the Smart Provisioning GUI.

Procedure

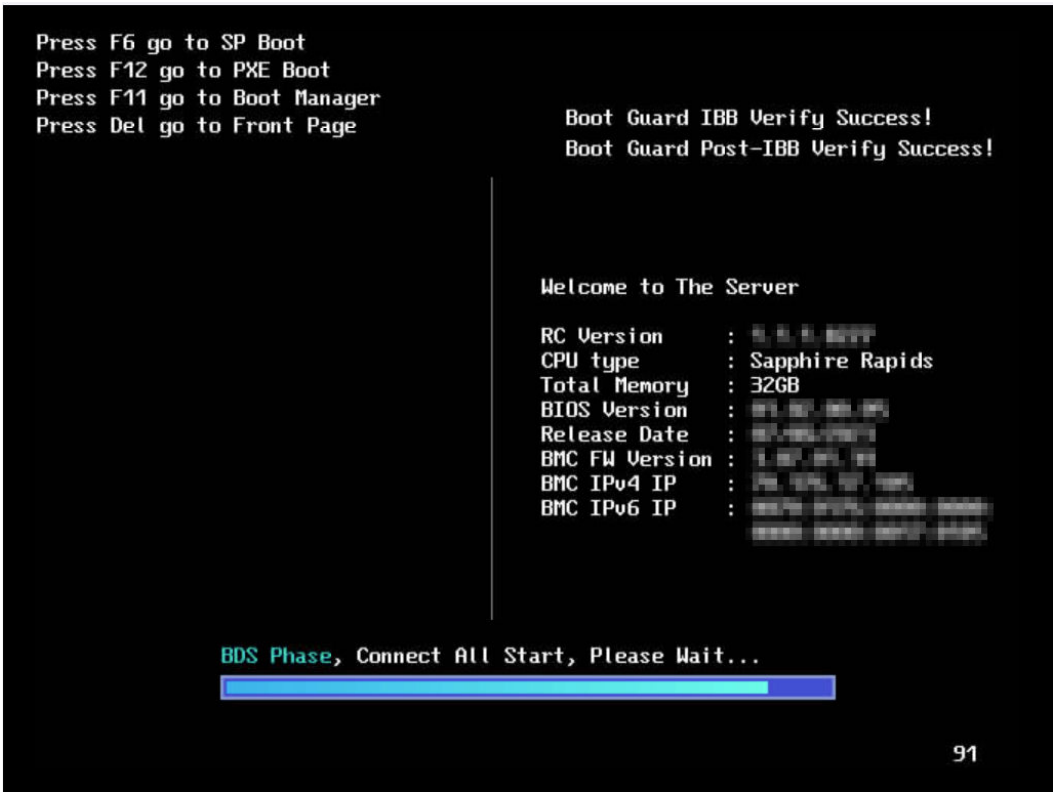
Step 1 Connect a local PC with the keyboard, video, and mouse (KVM) to the server, or log in to the server using the Remote Console of the iBMC WebUI.

Step 2 Power on or restart the server.

Step 3 When the screen shown in **Figure 3-88** is displayed, press **F6**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-88 BIOS boot screen



Step 4 Enter the password in the dialog box as prompted during startup, and press **Enter**.

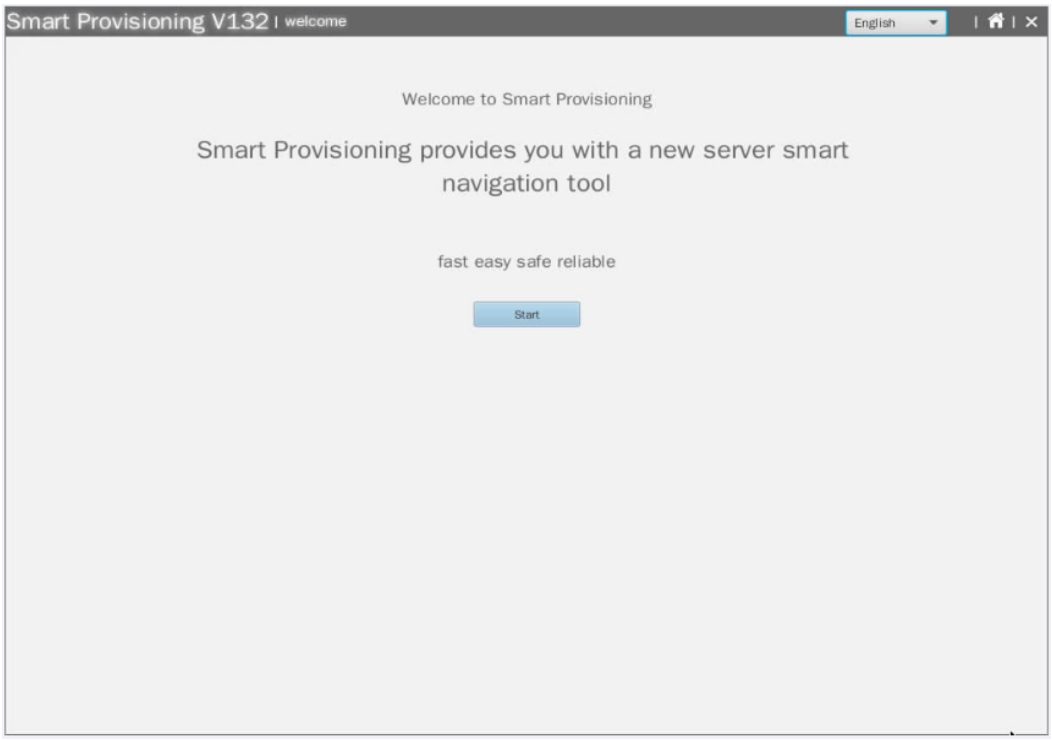
The Smart Provisioning welcome window is displayed, as shown in **Figure 3-89**.

NOTE

- The default BIOS password is **Admin@9000**. After the first login, you are advised to set an administrator password immediately. For details, see **3.2.11.1 Setting the BIOS Administrator Password**. For details about how to set the password of a common user, see **3.2.11.2 Setting the BIOS Common User Password**. For security purposes, you are advised to periodically change the administrator password.
- You can change the password only when you log in to the system using the administrator password.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- If you enter incorrect passwords for three consecutive times, the system will be locked. You can restart the server to unlock the system.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

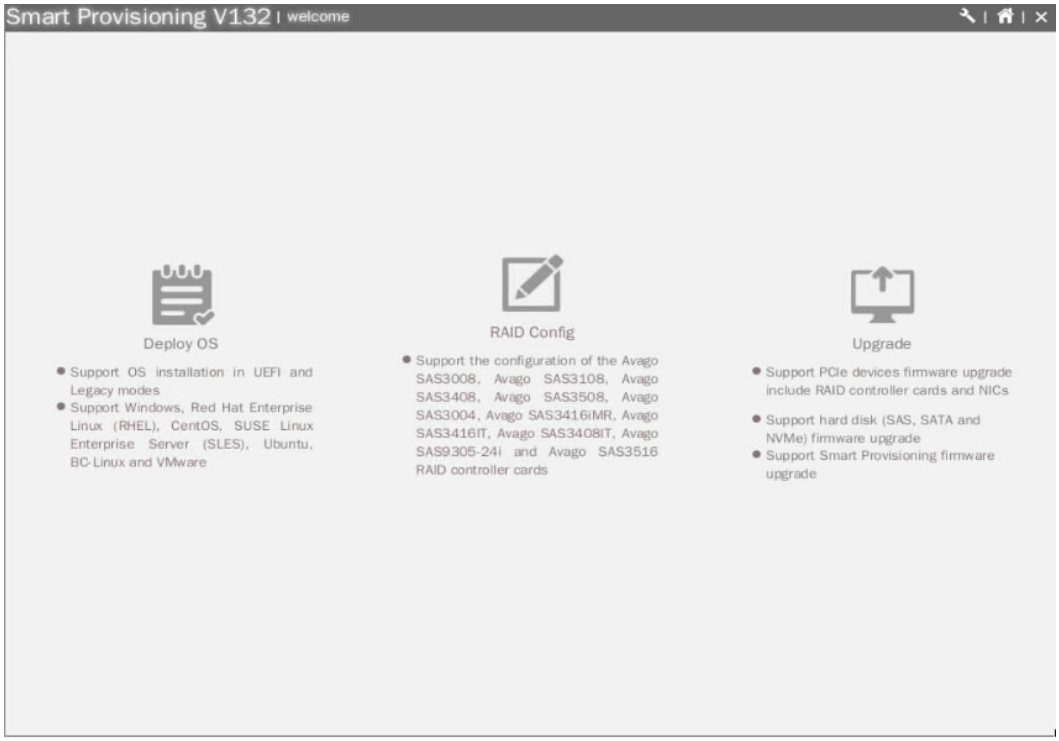
Figure 3-89 Smart Provisioning welcome screen



Step 5 Click **Start**.

Access the Smart Provisioning main screen, as shown in **Figure 3-90**.

Figure 3-90 Smart Provisioning main screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

When using Smart Provisioning, you can click  in the upper right corner to return to the main screen.

----End

3.2.5 Querying CPU Information

Scenarios

Query the CPU information about a server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab  .

The **Advanced** screen is displayed, as shown in **Figure 3-91**.

Figure 3-91 Advanced screen



Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-92**.

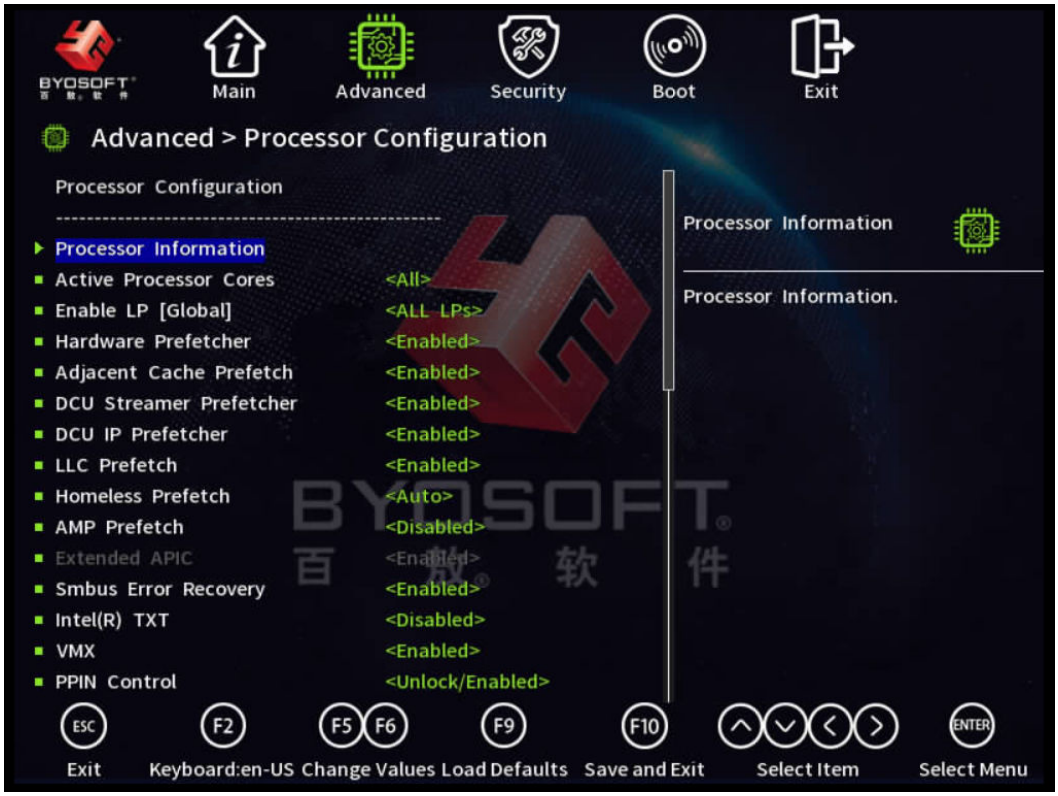
Figure 3-92 Socket Configuration screen



Step 4 Select **Processor Configuration** and press **Enter**.

The **Processor Configuration** screen is displayed, as shown in **Figure 3-93**.

Figure 3-93 Processor Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 5 Select **Processor Information** and press **Enter**.

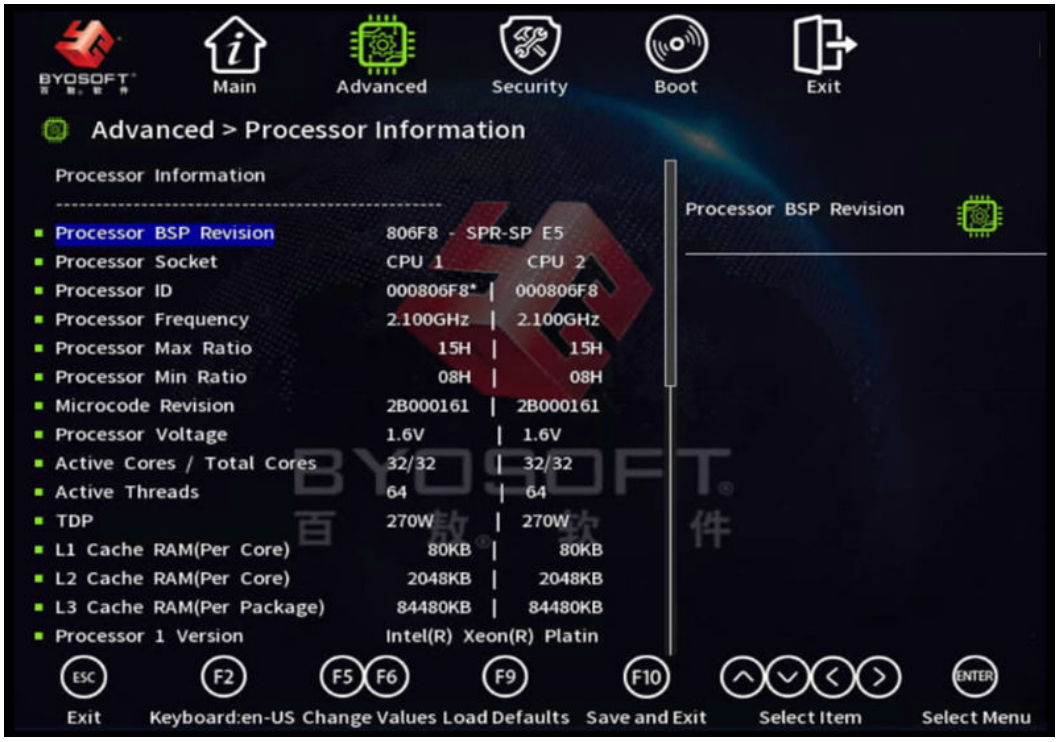
The **Processor Information** screen is displayed, as shown in **Figure 3-94**.

View the required CPU information. For details about parameters, see **6.2.5.1.1 Processor Information**.

NOTE

The displayed information varies according to the CPU model of the server.

Figure 3-94 Processor Information screen



----End

3.2.6 Querying Memory Information

Scenarios

Query the memory information about a server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-95**.

Figure 3-95 Advanced screen



Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-96**.

Figure 3-96 Socket Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Select **Memory Configuration** and press **Enter**.

The **Memory Configuration** screen is displayed, as shown in **Figure 3-97** and **Figure 3-98**.

Figure 3-97 Memory Configuration screen 1

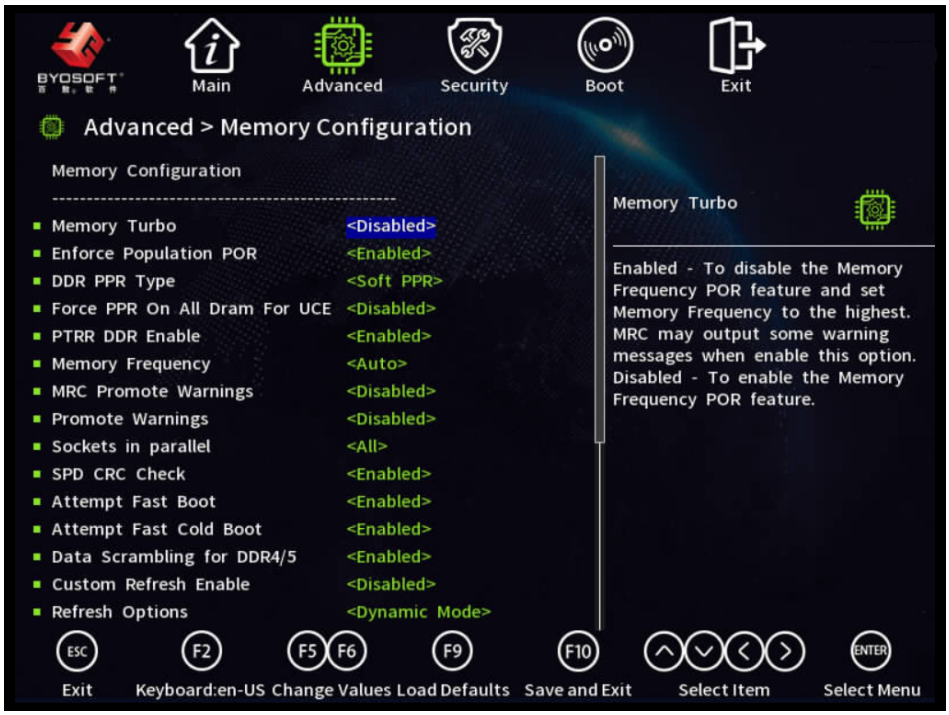
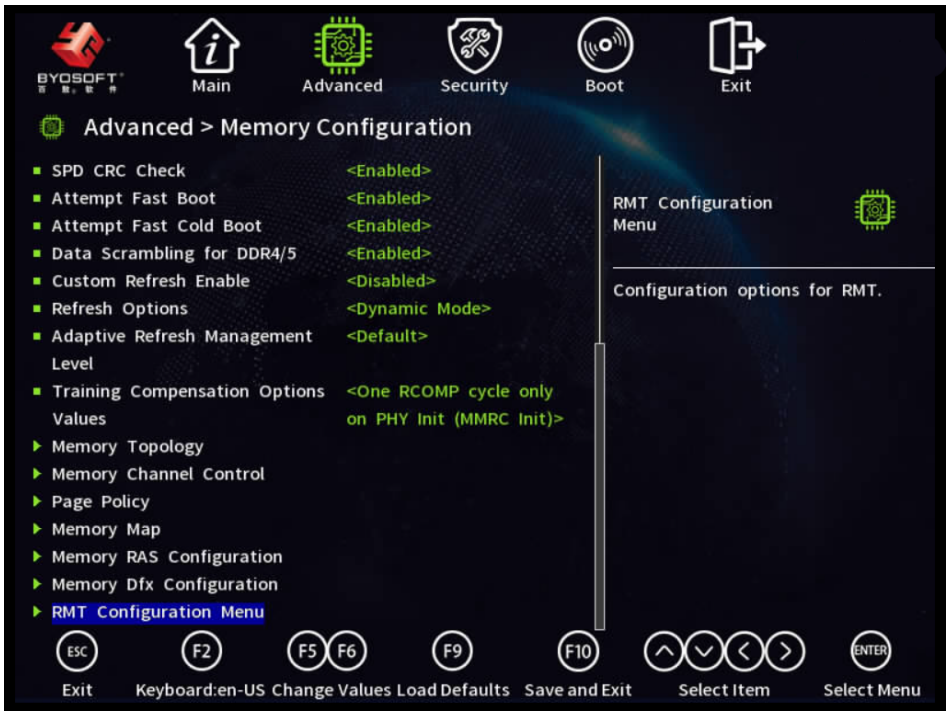


Figure 3-98 Memory Configuration screen 2



Step 5 Select **Memory Topology** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

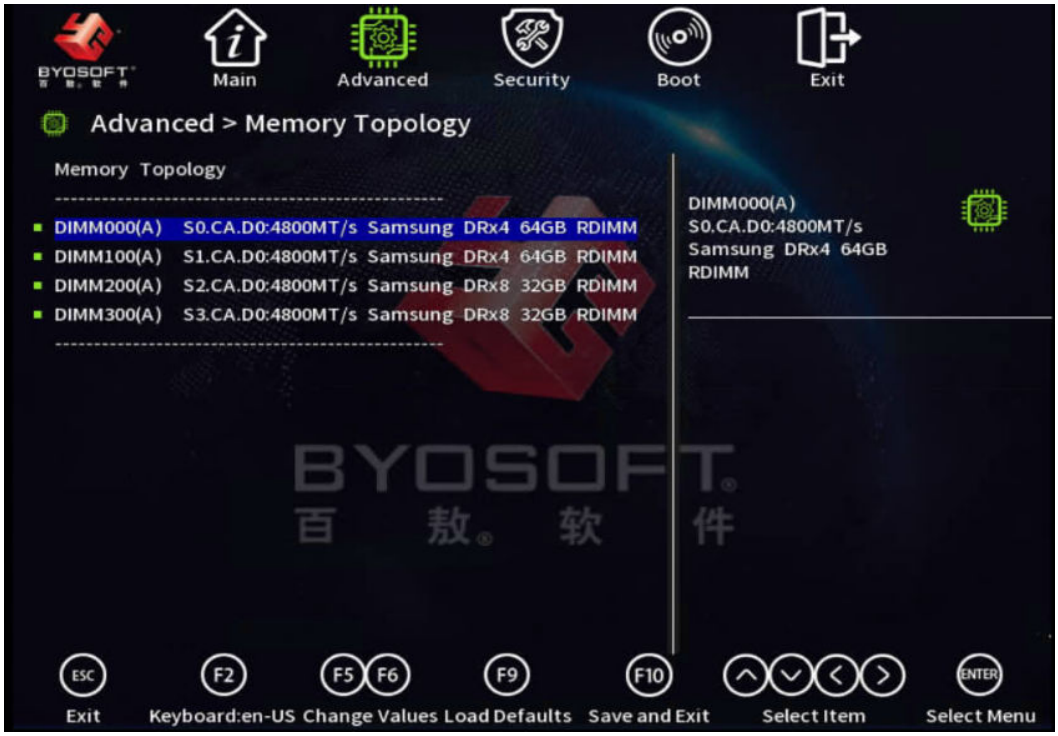
The **Memory Topology** screen is displayed, as shown in **Figure 3-99**.

View the memory information.

NOTE

- The information displayed on the screen varies depending on the configuration of the server.
- **DIMM***xyz*: indicates the DIMM numbered *z* in the channel numbered *y* of the CPU numbered *x*+1.
- If no DIMM is installed in the slot, no slot information is displayed.

Figure 3-99 Memory Topology screen



----End

3.2.7 Querying the SATA Drive Information

Scenarios

Query information about the server drives on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-100**.

Figure 3-100 Advanced screen



Step 3 Select **PCH-IO Configuration** and press **Enter**.

The **PCH-IO Configuration** screen is displayed, as shown in **Figure 3-101**.

Figure 3-101 PCH-IO Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Select **SATA And RST Configuration** and press **Enter**.

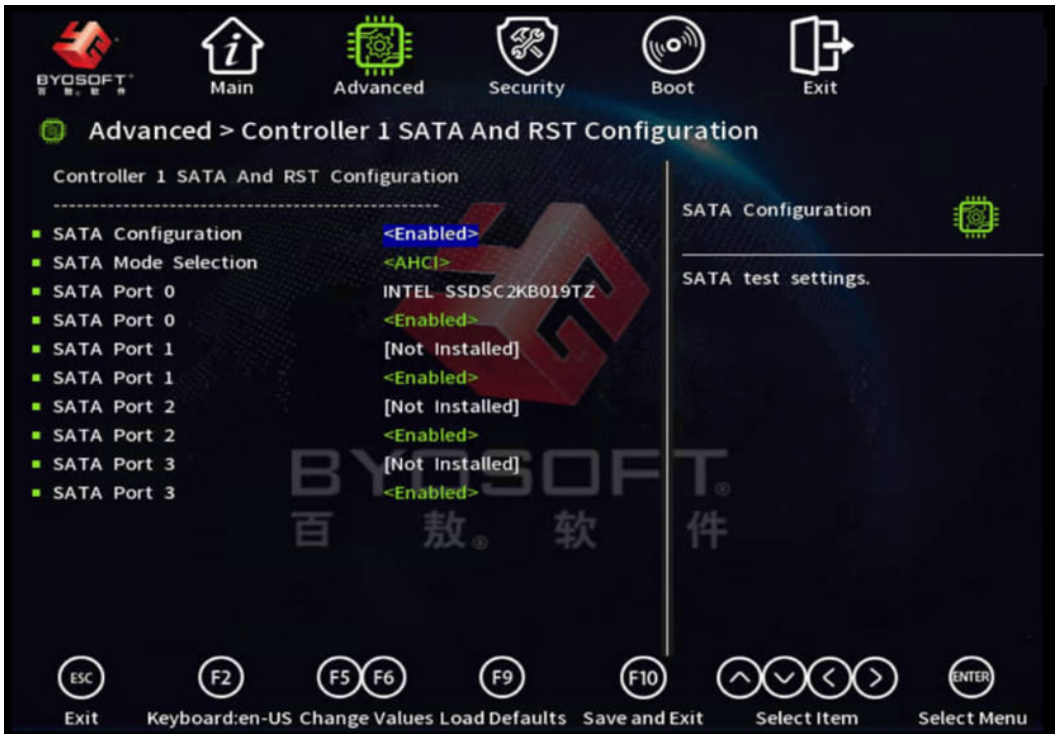
The **Controller** X **SATA And RST Configuration** screen is displayed (for example, **Controller 1 SATA And RST Configuration**), as shown in **Figure 3-102**.

View the required drive information. For details about parameters, see **6.2.7.2.1 Controller 1 SATA And RST Configuration**.

NOTE

- In SATA Port *X*, *X* indicates the drive port number, which starts from **0**.
- The number of displayed ports is subject to the actual situation.
- For more details about the slot numbers of the drives, see the user guide of the server you use.

Figure 3-102 Controller 1 SATA And RST Configuration screen



----End

3.2.8 Querying the BMC IP Address

Scenarios

Query the IP address of the BMC management port of the server on the BIOS Setup Utility.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-103**.

Figure 3-103 Advanced screen

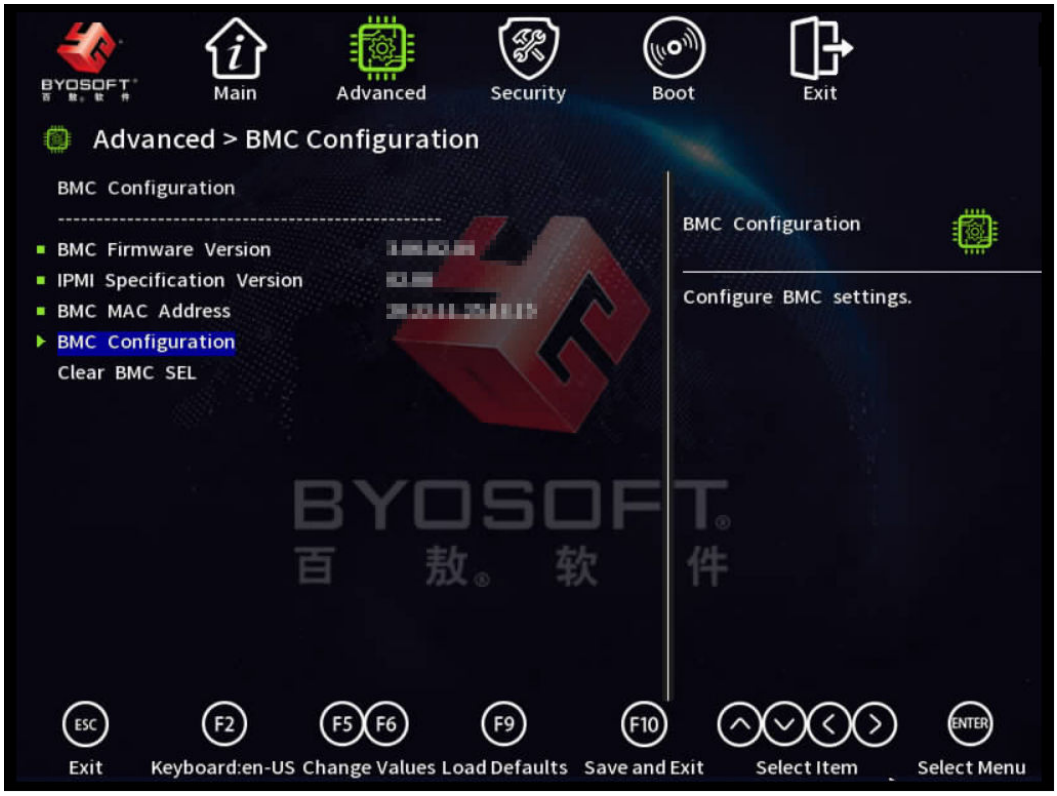


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-104**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-104 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-105** and **Figure 3-106**.

Check the BMC IP address. For details about parameters, see **6.2.6 BMC Configuration**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-105 BMC Configuration screen 1

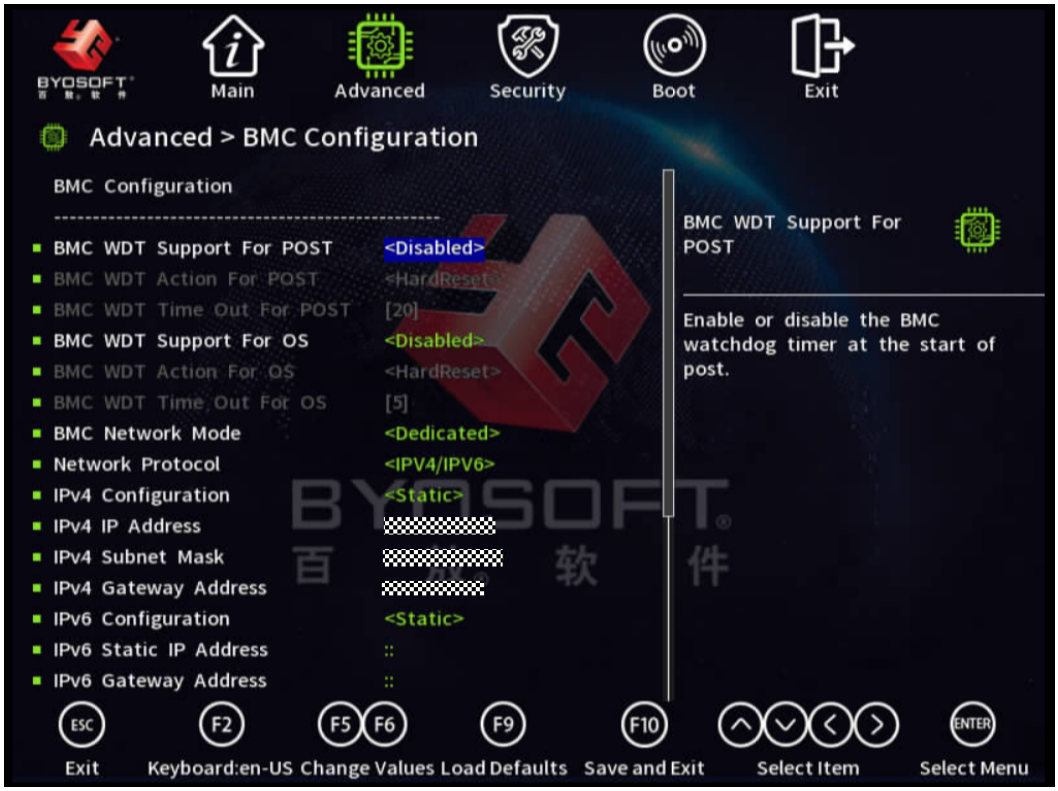
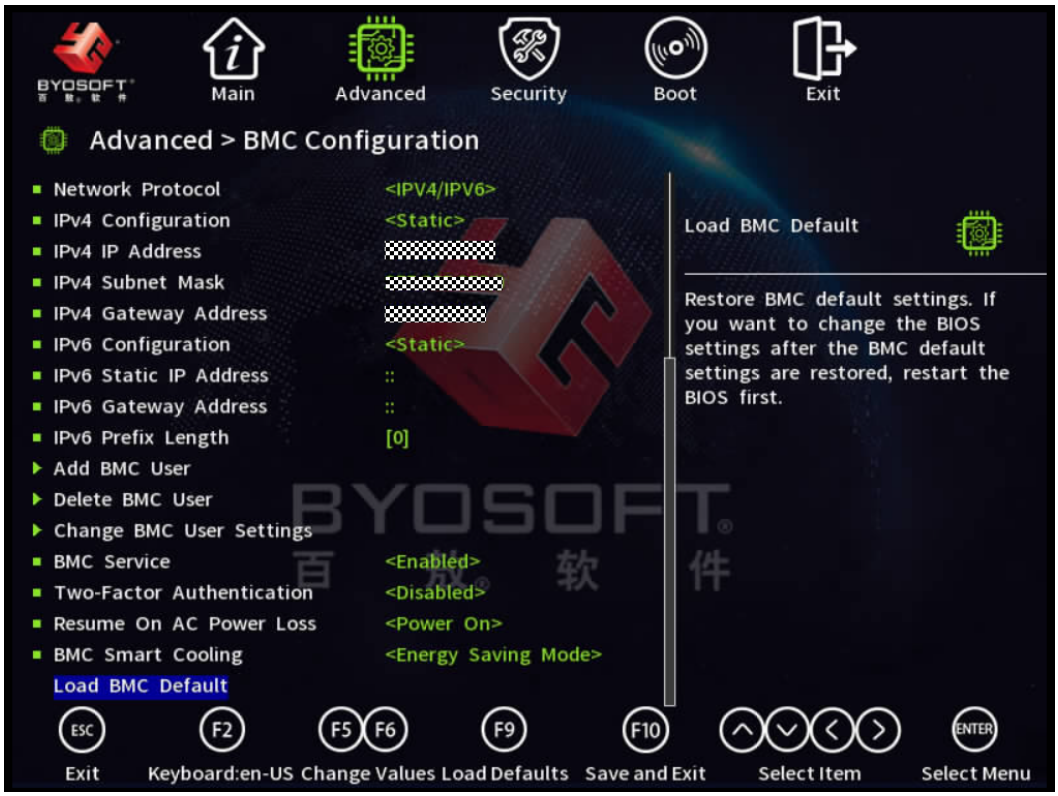


Figure 3-106 BMC Configuration screen 2



----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.2.9 Setting the BIOS System Language

Scenarios

Set the BIOS language.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

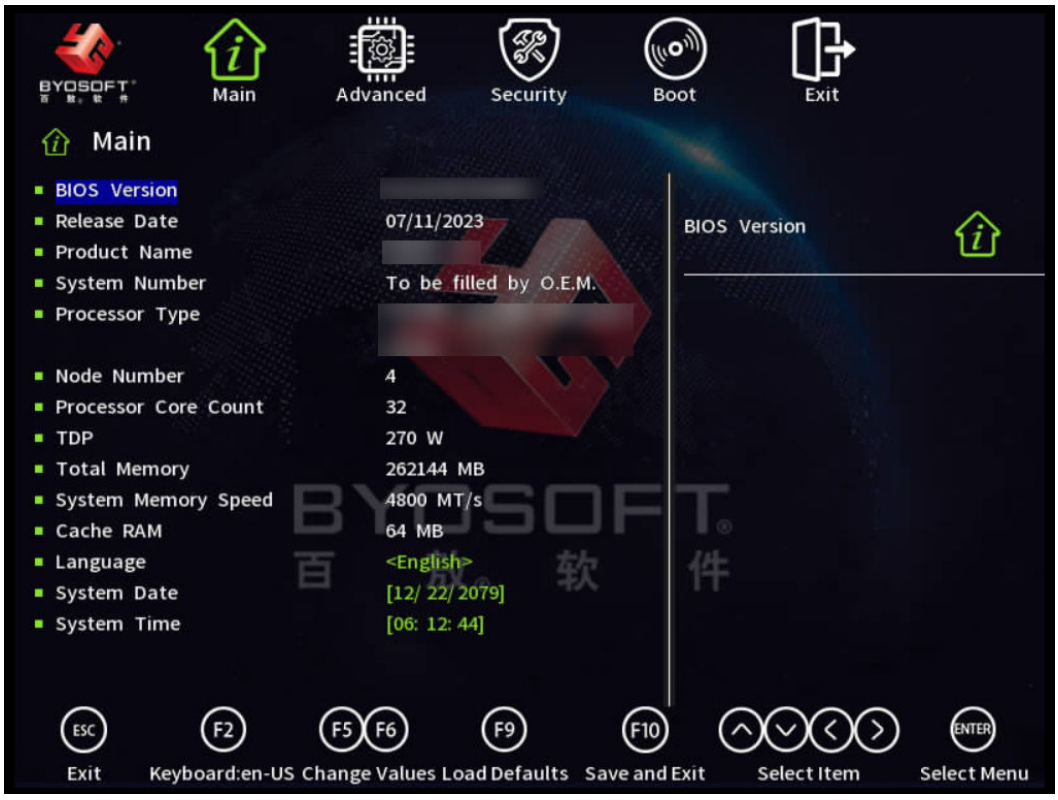
Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Main** tab .

The **Main** screen is displayed, as shown in **Figure 3-107**.

Figure 3-107 Main screen



Step 3 Select **Language** and press **Enter**.

Step 4 In the displayed dialog box, select the target language (English, Chinese, or Japanese) and press **Enter**.

Step 5 Use any of the following methods to save the settings.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

- Method 1: Press F10. The "Save configuration changes?" is displayed. **Press 'Y' to confirm, 'N'/'ESC' to ignore.** dialog box is displayed.

  Click **Yes** or press **Y** to save the settings. The server automatically restarts for the settings to take effect.
- Method 2: Select **Exit** to enter the **Exit** screen.

  Select **Save Changes Without Exiting**, select **Yes**, and press **Enter** to save the settings. The settings automatically take effect.

----End

3.2.10 Setting the BIOS System Time and Date

Scenarios

Set the BIOS system time and date.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Main** tab .

The **Main** screen is displayed, as shown in **Figure 3-108**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-108 Main screen



Step 3 Select **System Time**.

The system time is in the format of *HH:MM:SS* in the 24-hour system. Select the hour, minute, or second and press **Enter**. Enter the hour, minute, or second to be set and press **Enter**.

Step 4 Select **System Date**.

The system date is in the format of *mm/dd/yyyy*. Select the month, day, or year and press **Enter**. Enter the month, day, or year to be set and press **Enter**.

Step 5 Press **F10** when the setting is completed.

The **Save configuration changes? Press 'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 6 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

NOTE

BIOS does not support setting time zone. Windows and Linux are different in time management. In Windows, the CMOS time is the local time. In Linux, the CMOS time is the Greenwich Mean Time (GMT).

----End

3.2.11 Setting the BIOS Password

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.2.11.1 Setting the BIOS Administrator Password

Scenarios

Set the BIOS administrator password on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Security** tab .

The **Security** screen is displayed, as shown in **Figure 3-109**.

Figure 3-109 Security screen



Step 3 Select **Set Supervisor Password** and press **Enter**.

The **Please type in your password** dialog box is displayed.

Step 4 Enter the password of the current BIOS administrator and press **Enter**.

The **Please type in your new password** dialog box is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

Before changing the BIOS administrator password, you need to enter the old BIOS administrator password. If you enter incorrect passwords for three consecutive times, the server will be locked. You can restart the server to unlock it.

Step 5 Enter the new BIOS administrator password and press **Enter**.

The **Please confirm your new password** dialog box is displayed.

NOTE

- The password must contain at least 8 to 16 characters, including at least two types of the following characters: uppercase letters, lowercase letters, and digits, as well as at least one space or one special character.
- A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10.
- After you set **Delete Password Support** to **Enabled**, the **Delete Supervisor Password** parameter is displayed, which can be used to delete the BIOS administrator password. Exercise caution when you perform this operation because deleting the administrator password will reduce system security.
- If **Simple Password** is set to **Enabled**, the system does not verify the password complexity, but the password must contain 8 to 16 characters. Enabling the simple password function will reduce system security. Exercise caution when enabling this function.

Step 6 Enter the new password again and press **Enter**.

Step 7 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 8 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.11.2 Setting the BIOS Common User Password

Scenarios

Set the BIOS common user password on the BIOS.

NOTE

If the BIOS password is enabled, operations in this section can be performed when you access the Setup Utility screen using the BIOS administrator password or common user password.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Security** tab  .

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Security** screen is displayed, as shown in **Figure 3-110**.

Figure 3-110 Security screen



Step 3 Select **Set User Password** and press **Enter**.

The **Please type in your new password** dialog box is displayed.

NOTE

- If a common BIOS user password is used for login, the **Please type in your password** dialog box is displayed. In the displayed dialog box, enter the common BIOS user password and press **Enter**. Then, the dialog box for entering a new password is displayed.
- The system will be locked if you enter incorrect password for three times. You can restart the server to unlock the system.

Step 4 Enter the new password of the BIOS common user and press **Enter**.

The **Please confirm your new password** dialog box is displayed.

NOTE

- The password must contain at least 8 to 16 characters, including at least two types of the following characters: uppercase letters, lowercase letters, and digits, as well as at least one space or one special character.
- A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10.
- After you set **Delete Password Support** to **Enabled**, the **Delete User Password** parameter is displayed, which can be used to delete the BIOS common user password.

Step 5 Enter the new password again and press **Enter**.

Step 6 Press **F10**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 7 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.12 Setting PXE for a NIC

3.2.12.1 Setting the PXE Function for an OCP NIC

Scenarios

Enable or disable the PXE function of an OCP NIC on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-111**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-111 Advanced screen



Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 3-112**. Select an OCP NIC and press **Enter**. The **FlexIO 1 PXE Configuration** screen is displayed, as shown in **Figure 3-113**.

NOTE

- The displayed screen varies depending on the NIC configuration.
- The 5885H V7, 2488H V7, 2288 V7, and G8600 V7 servers support a maximum of one OCP NIC (a maximum of two network ports) and the G5500 V7 server supports a maximum of three OCP NICs.
- In UEFI mode, the default values are **Enabled** for all network ports.
- In legacy mode, only the first network port of the OCP NIC is enabled by default. That is, the default value of **FLEX IO 1 Port1** is **Enabled** and the default value of **FLEX IO 1 Port2** is **Disabled**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-112 PXE Configuration screen

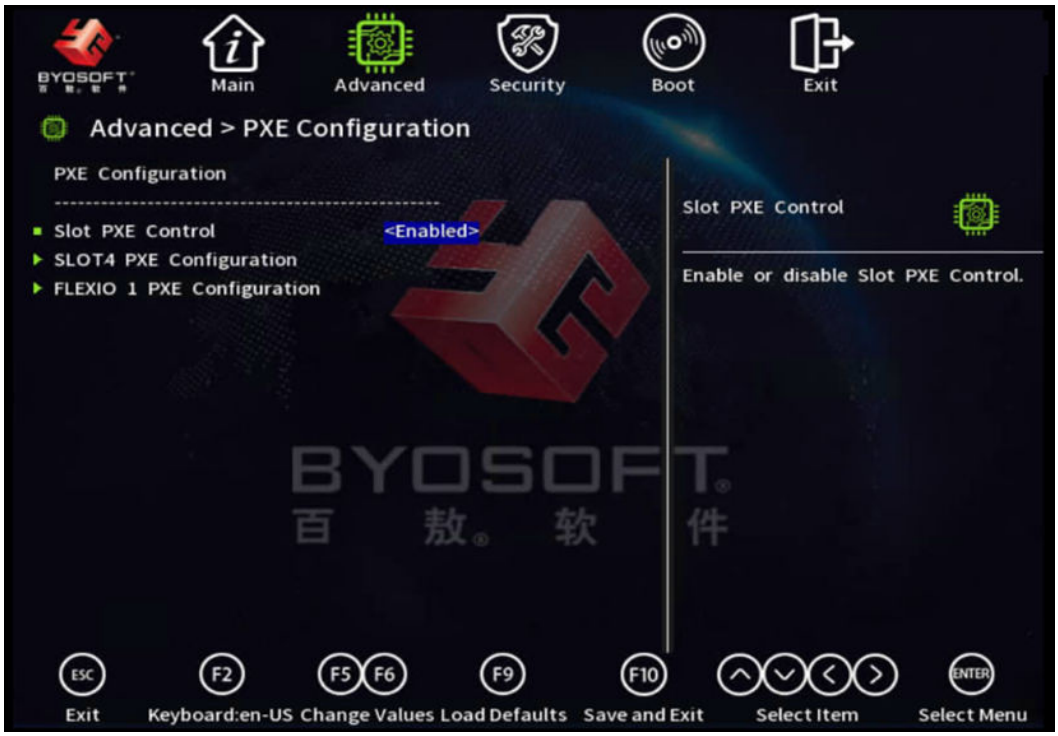


Figure 3-113 FlexIO 1 PXE Configuration screen



Step 4 Select the OCP NIC network port (for example, **Port 1 PXE Enabled**) to be set and press **Enter**.

Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

- **Enabled**: Enable the PXE function for the network port.
- **Disabled**: Disable the PXE function for the network port.

Step 6 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 7 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.12.2 Setting the PXE Function for a PCIe NIC

Scenarios

Enable or disable the PXE function for a PCIe NIC on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-114**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-114 Advanced screen



Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 3-115**.

NOTE

The displayed screen varies depending on the NIC configuration.

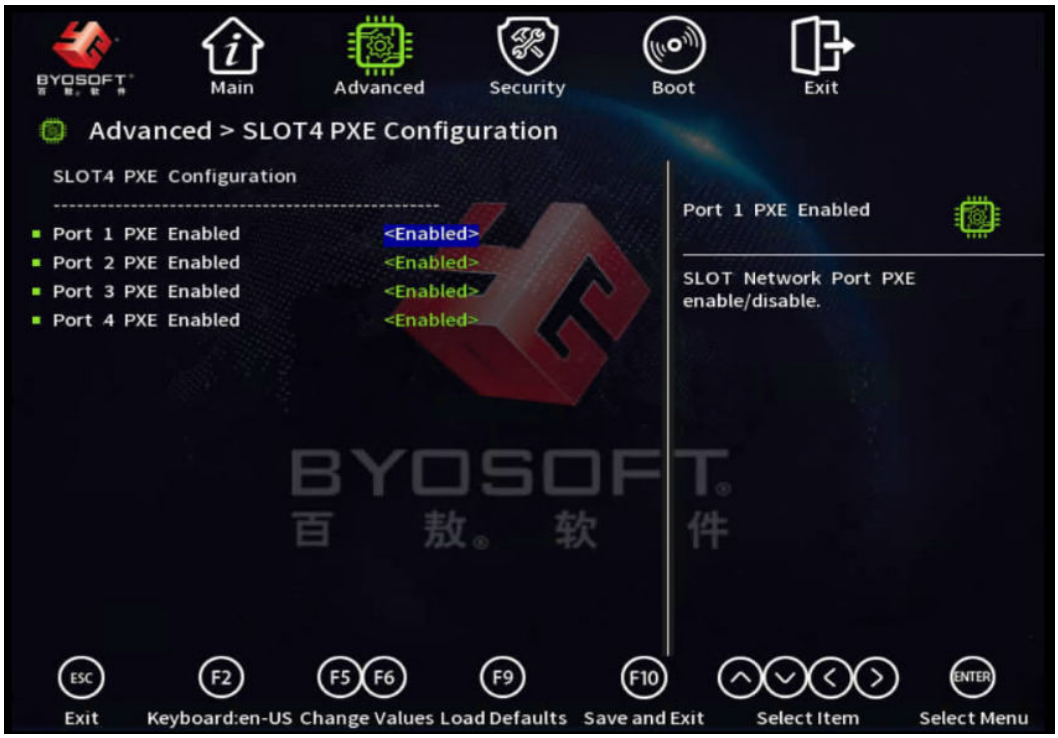
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-115 PXE Configuration screen



Step 4 Select **SLOT4 PXE Configuration** and press **Enter**. The **SLOT4 PXE Configuration** screen is displayed, as shown in **Figure 3-116**. Select a PCIe NIC network port (for example, **Port 1 PXE Enabled**), and press **Enter**.

Figure 3-116 Slot4 PXE Configuration screen



Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

- **Enabled**: Enable the PXE function for the PCIe NIC.

  NOTE

  After the PXE function is enabled for a PCIe NIC, you can enable or disable the PXE function for a specific PCIe NIC network port.

- **Disabled**: Disable the PXE function for the PCIe NIC.

  NOTE

  After the PXE function is disabled, you cannot configure the PXE function for a specific PCIe NIC network port.

Step 6 Select a PCIe NIC port (for example, **CPU1 First Slot Lan Port1 PXE**) and press **Enter**.

Step 7 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enable the PXE function for the network port.
- **Disabled**: Disable the PXE function for the network port.

Step 8 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 9 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.13 Setting the TXT Function

Scenarios

Enable or disable the TXT function using the BIOS.

TXT is a security feature of the Intel processor and must be used together with the TPM or Trusted Cryptography Module (TCM).

NOTE

- The server must be installed with the TPM/TCM and CPUs.
- If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Check whether the server is installed with a TPM or TCM.

1. Select the **Security** tab .

   The **Security** screen is displayed, as shown in **Figure 3-117** or **Figure 3-118**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

2. Check whether the TPM or TCM parameters are properly displayed.
   – If yes, the server is installed with a TPM or TCM.
   – If no, check whether the TPM or TCM is properly installed. For details, see section "Installing the TPM" in the server maintenance and service guide.

Figure 3-117 Security screen 1



Figure 3-118 Security screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 3 Check whether CPUs have been installed for the server.

1. Select the **Main** tab .
   The **Main** screen is displayed, as shown in **Figure 3-119**.
2. Check whether the value of **CPU Number** is **2** or **4**.
   – If yes, the required number of CPUs has been installed on the server.
   – If no, check whether the CPU is properly installed. For details, see section "Installing the TPM" in the server maintenance and service guide.

Figure 3-119 Main screen



Step 4 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-120**.

Figure 3-120 Advanced screen



Step 5 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-121**.

Figure 3-121 Socket Configuration screen

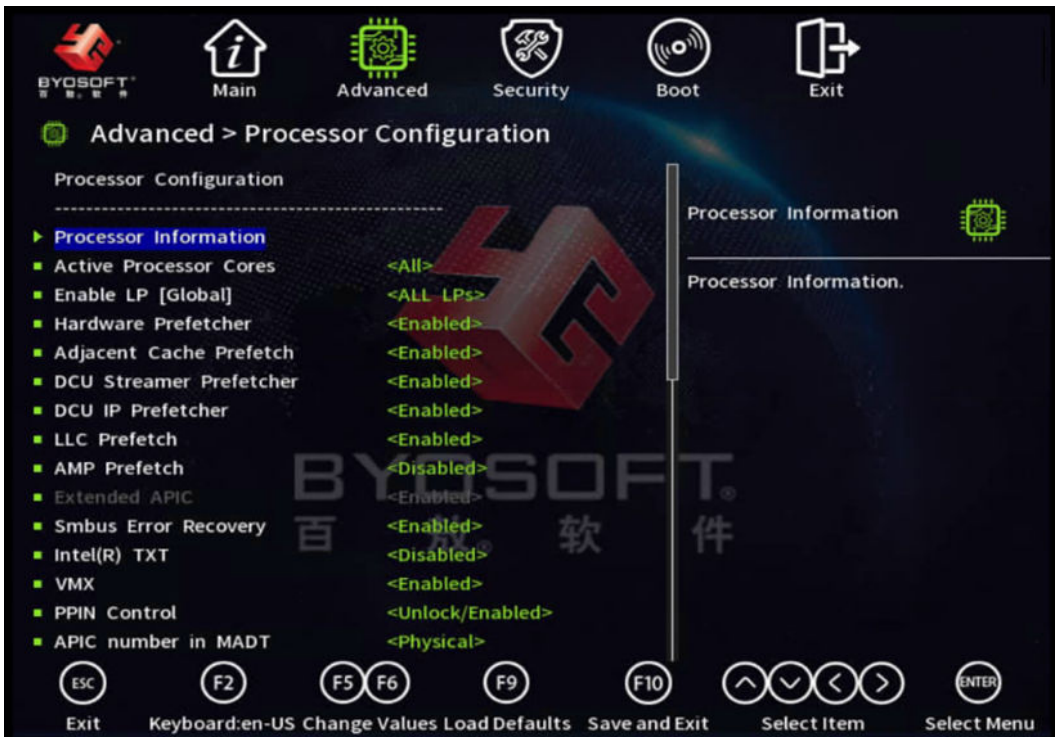


 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 6 Select **Processor Configuration** and press **Enter**.

The **Processor Configuration** screen is displayed, as shown in **Figure 3-122**.

Figure 3-122 Processor Configuration screen



Step 7 Select **Intel(R) TXT** and press **Enter**.

Step 8 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: Enable the TXT function.
- **Disabled**: Disable the TXT function.

Step 9 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 10 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.14 Setting the Fan Speed Adjustment Mode

Scenarios

Set the fan speed adjustment mode on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-123**.

Figure 3-123 Advanced screen

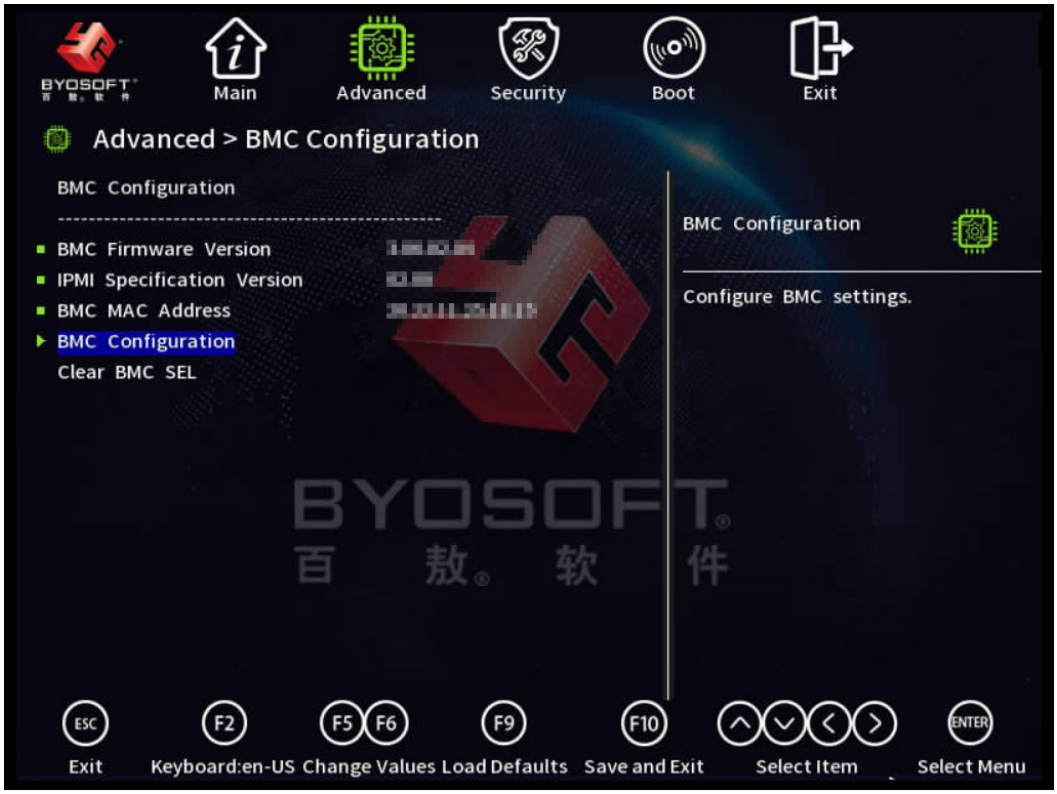


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-124**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-124 BMC Configuration screen



Step 4 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-125**.

Figure 3-125 BMC Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 5 Select **BMC Smart Cooling** and press **Enter**.

Step 6 In the dialog box displayed, select **Energy Saving Mode**, **Low Noise Mode**, **High Performance Mode**, or **Custom Mode**, and press **Enter**.

The option descriptions are as follows:

- **Low Noise Mode**: The fan rotates at a low speed. You are advised to select this mode when the server generates little heat to reduce noise.
- **Energy Saving Mode**: The fan rotates at a medium speed.
- **High Performance Mode**: The fan run rotates at a high speed. Select this value for heat dissipation when the server generates a lot of heat.
- **Custom Mode**: If you select this option, the parameters about the CPU temperature and fan speed are available.

Step 7 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 8 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.15 Setting the Server Boot Mode

Scenarios

Set the boot mode and sequence.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Boot** tab.

The **Boot** screen is displayed, as shown in **Figure 3-126Figure 3-126** and **Figure 3-127**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-126 Boot screen (UEFI mode)



Figure 3-127 Boot screen (legacy mode)



Step 3 Set the BIOS boot mode.

1. Select **Boot Type** and press **Enter**.
2. In the displayed dialog box, select **LegacyBoot** or **UEFIBoot**, and press **Enter**.

NOTE

- The default boot mode is UEFI mode.
- For some OSs, if the capacity of the drive or the RAID array for installing the OS is greater than 2 TB, use the UEFI mode. For details, see the release notes of the OS.
- The UEFI mode supports more boot devices than the legacy mode. If a server is configured with multiple boot devices, some devices may fail to start in the legacy mode. In this case, the UEFI boot mode is recommended. If you need to use the legacy mode, you are advised to disable the NIC PXE function based on the actual service scenario to ensure that the OS can be started properly. For details, see **3.2.12 Setting PXE for a NIC** and **3.2.20 Setting Serial Port Redirection**.

Step 4 Set the boot sequence.

1. Select **Boot Sequence** and press **Enter**.

   The **Boot Sequence** screen is displayed, as shown in **Figure 3-128**.

   Figure 3-128 Boot Sequence screen



2. Select the target boot option and press **F5** or **F6** to change the boot sequence.
   - Press **F5** to move a boot option down.
   - Press **F6** to move a boot option up.

   NOTE

   - The server boots in the order specified on this screen.
   - The default boot sequence is **Hard Disk Drive** > **DVD-ROM Drive** > **PXE** > **Others**.

Step 5 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 6 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.16 Setting the Server Boot Device

Scenarios

Set the device from which the server is booted on the BIOS.

NOTE

- If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.
- If **Hard Disk Drive**, **DVD-ROM Drive**, **PXE**, and **Others** all contain only one boot device, you can skip this section and perform only operations in **3.2.16 Setting the Server Boot Device**.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Boot** tab.

The **Boot** screen is displayed, as shown in **Figure 3-129Figure 3-129** and **Figure 3-130**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-129 Boot screen (UEFI mode)



Figure 3-130 Boot screen (legacy mode)



Step 3 Set the BIOS boot mode.

1. Select **Boot Type** and press **Enter**.
2. In the displayed dialog box, select **LegacyBoot** or **UEFIBoot**, and press **Enter**.

NOTE

- The default boot mode is UEFI mode.
- For some OSs, if the capacity of the drive or the RAID array for installing the OS is greater than 2 TB, use the UEFI mode. For details, see the release notes of the OS.
- The UEFI mode supports more boot devices than the legacy mode. If a server is configured with multiple boot devices, some devices may fail to start in the legacy mode. In this case, the UEFI boot mode is recommended. If you need to use the legacy mode, you are advised to disable the NIC PXE function based on the actual service scenario to ensure that the OS can be started properly. For details, see **3.2.12 Setting PXE for a NIC** and **3.2.20 Setting Serial Port Redirection**.

Step 4 Set the first boot device.

- To set a drive or RAID controller card as the first boot device, perform the following steps:
  a. On the **Boot Sequence** screen, set **Hard Disk Drive** as the first boot option, as shown in **3.2.15 Setting the Server Boot Mode**.

     NOTE

     Hard Disk Drive is the first boot option by default. If the first boot option is not modified, skip this step.

  b. On the **Boot** screen, select **UEFI** or **Legacy** and press **Enter**.

     The **UEFI** or **Legacy** screen is displayed, as shown in **Figure 3-131** or **Figure 3-132**.

     NOTE

     - **UEFI** is displayed in UEFI mode. **Legacy** is displayed in legacy mode.
     - If the server does not have boot devices such as drives, NICs, CD/DVD-ROM drives, or images, the **UEFI** or **Legacy** screen does not display the corresponding boot items. The boot items displayed on the screen are subject to the actual situation.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-131 UEFI screen

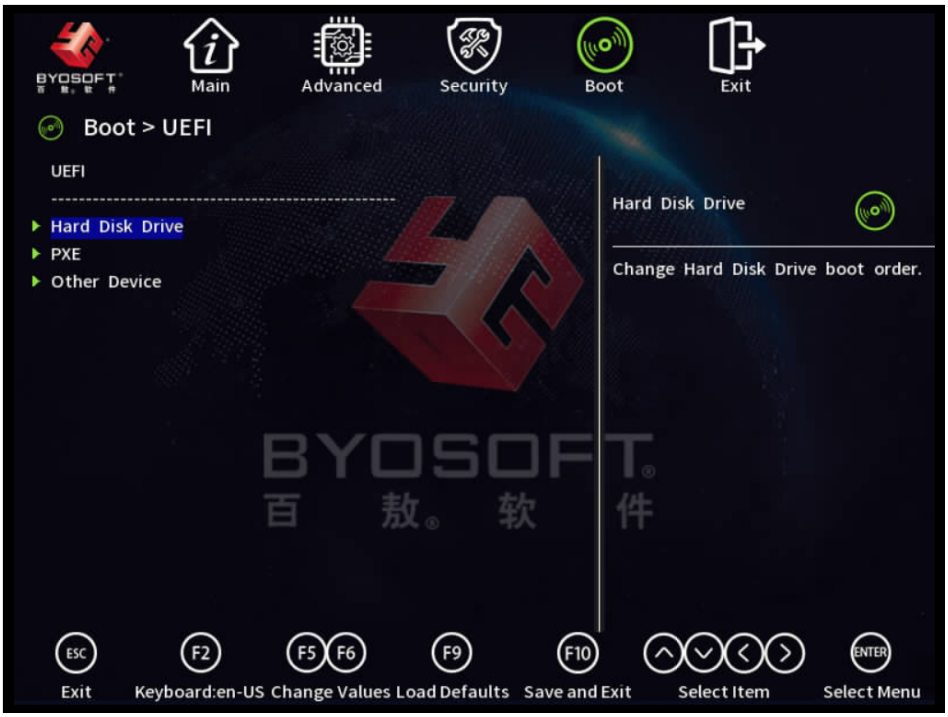
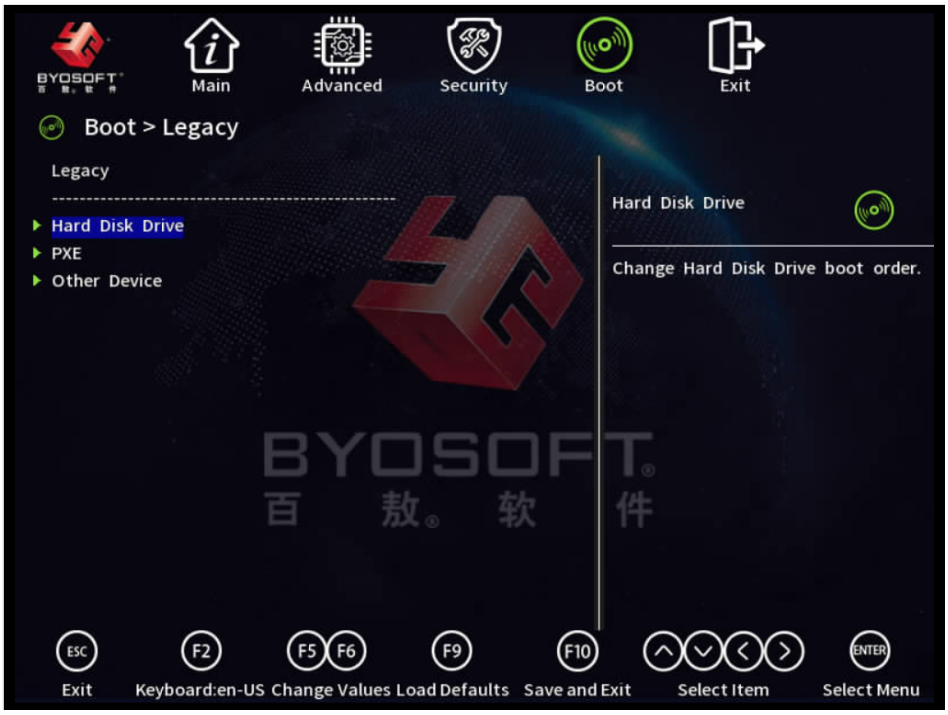


Figure 3-132 Legacy screen



c. Select **Hard Disk Drive** and press **Enter**.

d. Select the boot device to be adjusted.

e. Press **F5** (downwards) or **F6** (upwards) to set the corresponding drive or RAID controller card as the first boot device. That is, move it to the first row.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- In legacy mode, if the server is configured with a RAID controller card or physical drive that supports the legacy boot mode, the **Hard Disk Drive** list displays the information about the RAID controller card or physical drive. You can adjust the position of the RAID controller card or physical drive in the boot device list to adjust the boot device.
- In UEFI mode:
  - If no OS is installed on the drives of the server, there is no boot device in the **Hard Disk Drive** list. The drive selected to install the OS during the OS installation will be the boot drive.
  - If an OS has been installed on the server drive, the OS name is displayed in the **Hard Disk Drive** list. You can adjust the order of the OS to set the first boot device.

- **To set the DVD-ROM drive as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **DVD-ROM Drive** as the first boot option, as shown in **3.2.15 Setting the Server Boot Mode**.
  b. On the **UEFI** or **Legacy** screen, select **DVD-ROM Device** and press **Enter**.
  c. Select the boot device to be adjusted.
  d. Press **F5** (downwards) or **F6** (upwards) to set the DVD-ROM drive as the first boot device. That is, move the DVD-ROM drive to the first row.
- **To set PXE as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **PXE** as the first boot option, as shown in **3.2.15 Setting the Server Boot Mode**.
  b. On the **UEFI** or **Legacy** screen, select **PXE** and press **Enter**.
  c. Select the boot device to be adjusted.
  d. Press **F5** (downwards) or **F6** (upwards) to set the PXE boot option as the first boot device. That is, move the PXE boot option to the first row.
- **To set a USB device as the first boot device, perform the following steps:**
  a. On the **Boot Sequence** screen, set **Others** as the first boot option, as shown in **3.2.15 Setting the Server Boot Mode**.
  b. On the **UEFI** or **Legacy** screen, select **Others** and press **Enter**.
  c. Select the boot device to be adjusted.
  d. Press **F5** (downwards) or **F6** (upwards) to set the USB device as the first boot device. That is, move the USB device to the first row.

Step 5 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 6 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3.2.17 Setting the BMC User Password

Scenarios

Set the user password for logging in to the BMC of a server using the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-133**.

Figure 3-133 Advanced screen

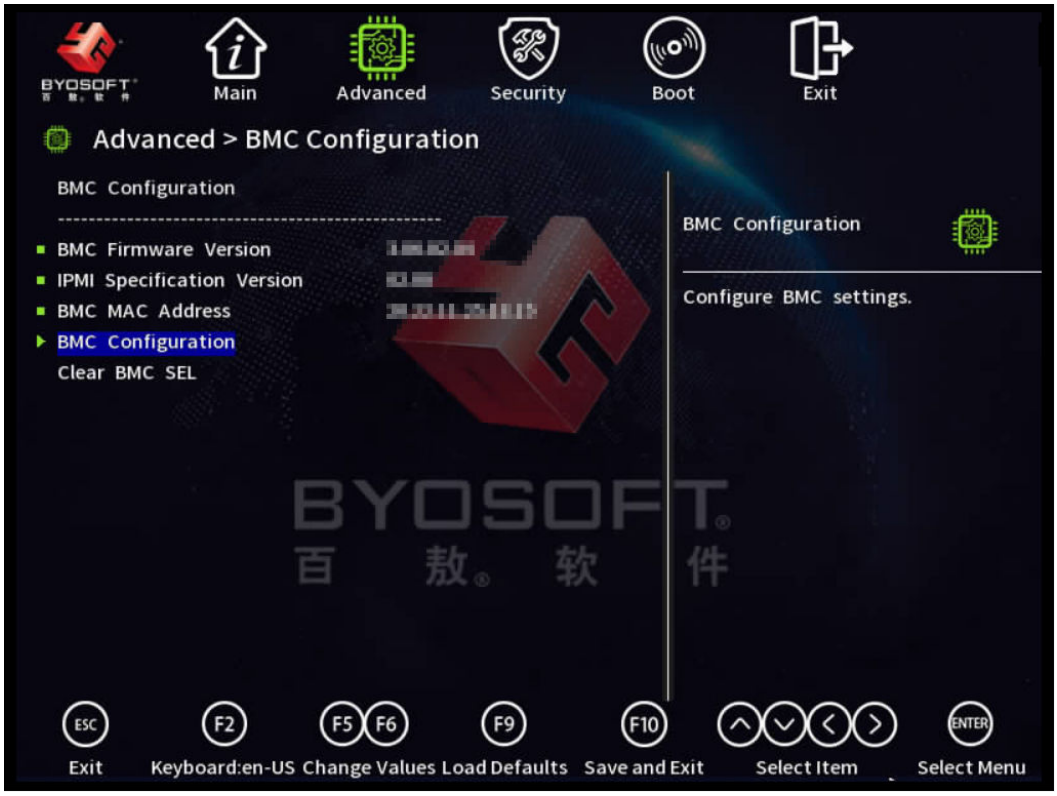


Step 3 Select **BMC Configuration** and press **Enter**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-134**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-134 BMC Configuration screen



Step 4 Select **BMC Configuration**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-135** and **Figure 3-136**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-135 BMC Configuration screen 1

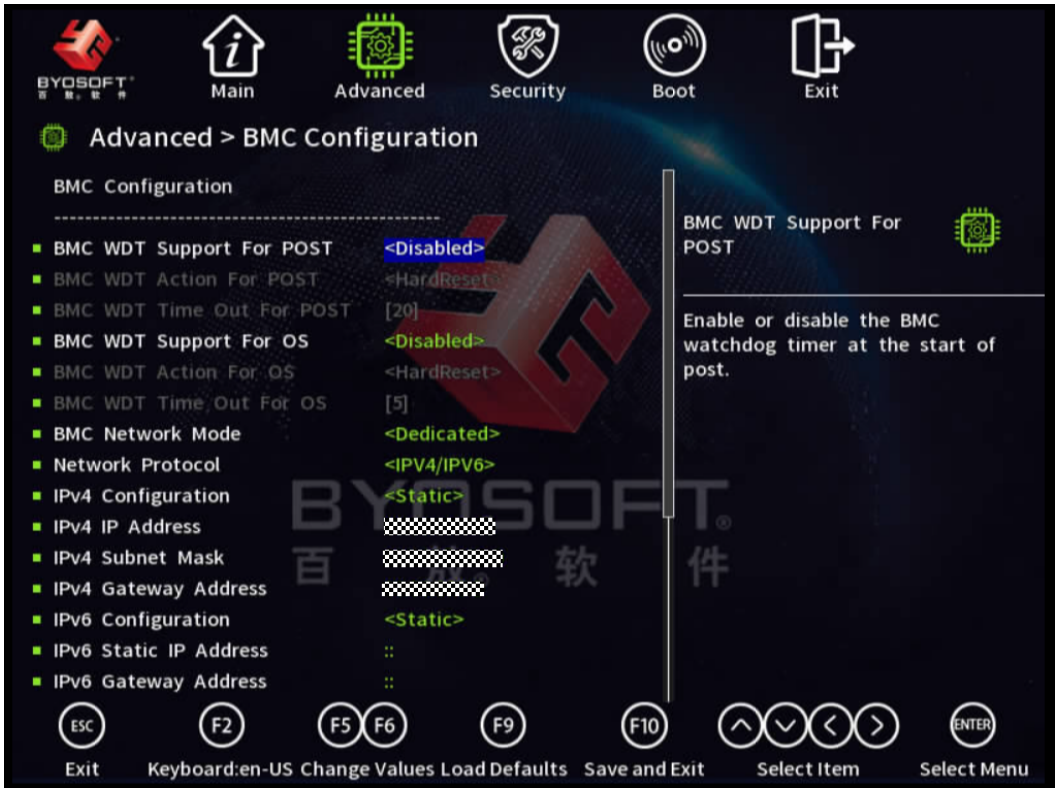
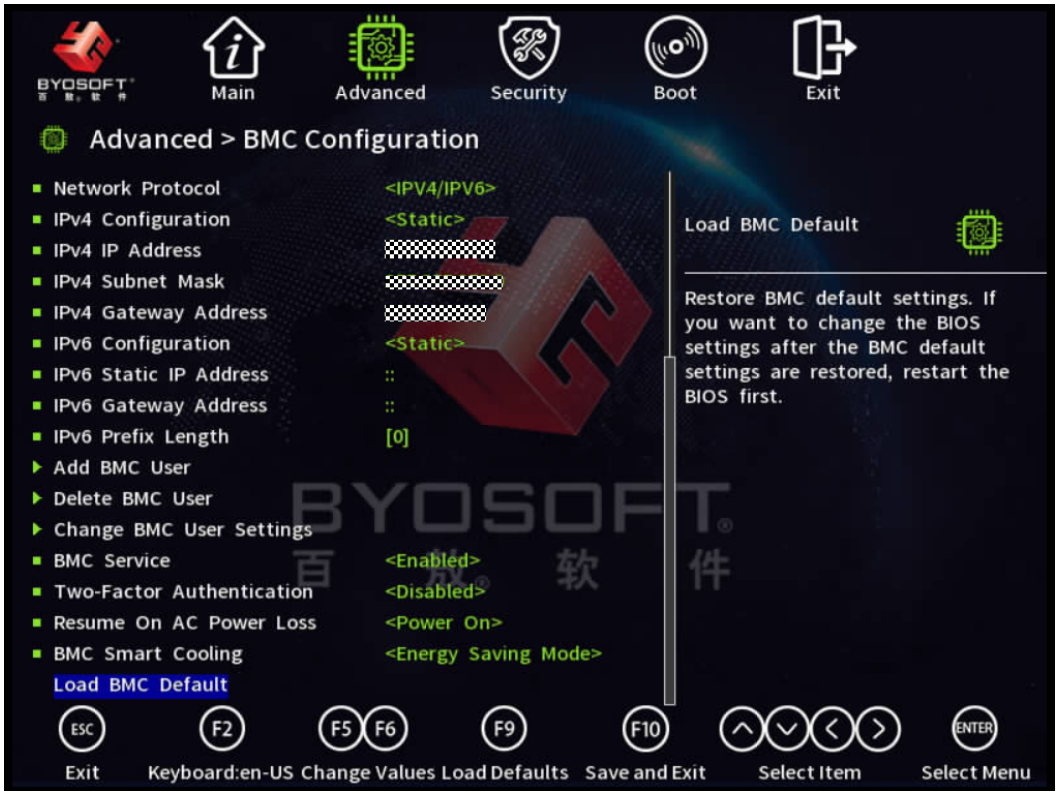


Figure 3-136 BMC Configuration screen 2

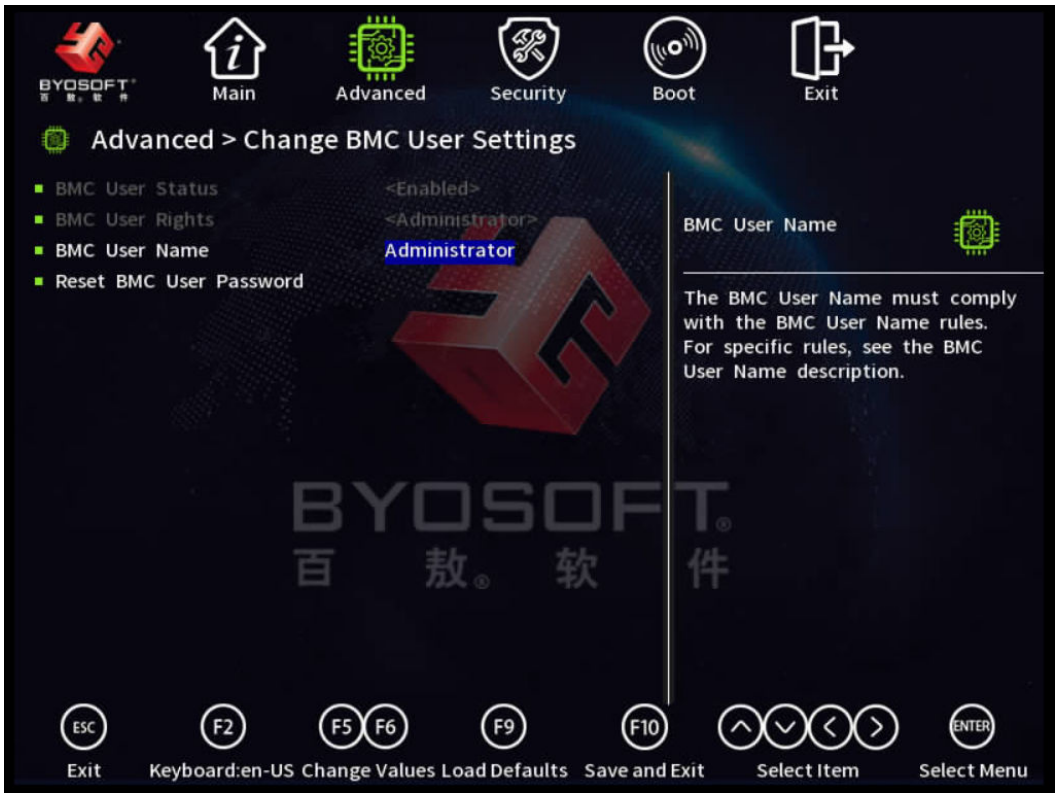


Step 5 Select **Change BMC User Settings** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The **Change BMC User Settings** screen is displayed, as shown in **Figure 3-137**.

Figure 3-137 Change BMC User Settings screen



Step 6 Select **Reset BMC User Password** and press **Enter**.

The **Please type in your new password** dialog box is displayed.

NOTE

- If an BMC user password already exists, the **Please type in your password** dialog box is displayed. In the displayed dialog box, enter the current BMC user password and press **Enter**. Then, the dialog box for entering a new password is displayed.
- This parameter is used to change the password of the BMC user whose user ID is **2**.

Step 7 Enter the new BMC user password and press **Enter**.

- If password complexity check is disabled, the password length cannot be zero or exceed 20 characters.
- If password complexity check is enabled, the password must meet the following requirements:
  - The password is a string of 8 to 20 characters.
  - The password must contain at least one space or one of the following special characters:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - The password must also contain at least two types of the following characters:
    - Uppercase letters A to Z

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

  - Lowercase letters a to z
  - Digits 0 to 9
- The password must be different from the user name or the user name in reverse order.

- If the weak password dictionary authentication is enabled, the password must be different from passwords contained in the weak password dictionary.

NOTE

- Run the **ipmcset -t user -d weakpwddic -v export** command to obtain the weak password dictionary.
- For details about how to set the password check function and query the weak password dictionary, see the corresponding *iBMC User Guide*.

Step 8 In the dialog box displayed, type the new password again and press **Enter**.

The password is set successfully.

----End

3.2.18 Setting the BMC Network Information

Scenarios

Set the BMC network information, including the mode for obtaining the BMC IP address, subnet mask, and gateway address.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-138**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-138 Advanced screen



Step 3 Select **BMC Configuration**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-139**.

Figure 3-139 BMC Configuration screen

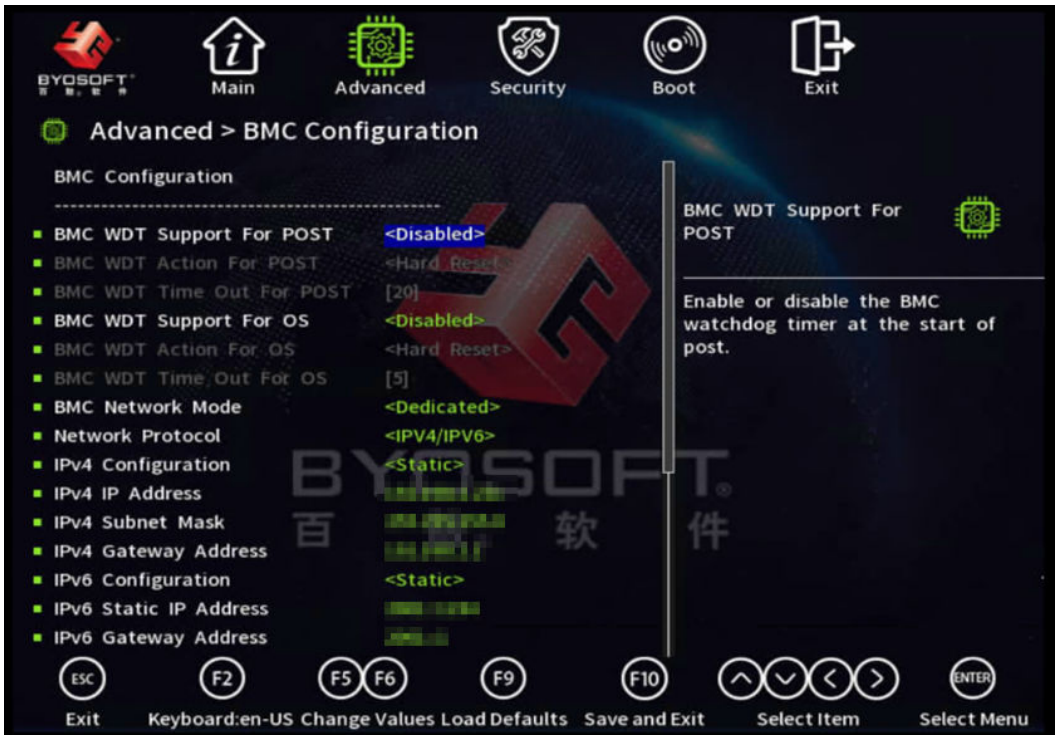


 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Select **BMC Configuration**.

The **BMC Configuration** screen is displayed, as shown in **Figure 3-140**.

Figure 3-140 BMC Configuration screen



Step 5 (Optional) Set the BMC network port mode.

1. Select **BMC Network Mode** and press **Enter**.
2. In the displayed dialog box, select **Auto**, **Dedicated**, **PCIe Shared**, or **Onboard OCP Shared**, and press **Enter**.
   - **Auto**: Auto-negotiation mode. You can access the BMC through the management network port or other network ports of the server.
   - **Dedicated**: Dedicated mode. You can access the BMC only through the management network port.
   - **PCIe Shared**: PCIe NIC sharing mode. You can access the BMC through the network port of the PCIe NIC.
   - **Onboard OCP Shared**: OCP NIC sharing mode. You can access the BMC through the OCP*X* NIC network port.

NOTE

- When this parameter is set to **Auto**, the **Vlan Id** option is displayed, which is used to set the BMC VLAN ID.
- When this parameter is set to **PCIe Shared**, the **Vlan Id** and **NCSI NIC Port Select** options are displayed, which are used to set the BMC VLAN ID and the service network port.
- When this parameter is set to **Onboard OCP Shared**, the **Vlan Id** and **NCSI OCP Port Select** options are displayed, which are used to set the BMC VLAN ID and the service network port.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

3. In the displayed dialog box, select **Auto**, **Dedicated**, **PCIe Shared**, **Onboard OCP1 Shared**, **Onboard OCP2 Shared**, or **Onboard OCP3 Shared**, and press **Enter**.
   - **Auto**: Auto-negotiation mode. You can access the BMC through the management network port or other network ports of the server.
   - **Dedicated**: Dedicated mode. You can access the BMC only through the management network port.
   - **PCIe Shared**: PCIe NIC sharing mode. You can access the BMC only through network ports of the PCIe NIC.
   - **Onboard OCP1 Shared**: OCP NIC sharing mode. You can access the BMC through the OCP1 NIC network port.
   - **Onboard OCP2 Shared**: OCP NIC sharing mode. You can access the BMC through the OCP2 NIC network port.
   - **Onboard OCP3 Shared**: OCP NIC sharing mode. You can access the BMC through the OCP3 NIC network port.

   NOTE

   - This operation applies only to the G5500 V7.
   - When both PCIe NICs and OCP NICs are installed, **PCIe Shared**, **Onboard OCP3 Shared**, **Onboard OCP1 Shared**, and **Onboard OCP2 Shared** are displayed in order. The remaining options are hidden.
   - When this parameter is set to **Auto**, the **Vlan Id** option is displayed, which is used to set the BMC VLAN ID.
   - When this parameter is set to **PCIe Shared**, the **Vlan Id** and **NCSI NIC Port Select** options are displayed, which are used to set the BMC VLAN ID and the service network port.
   - When this parameter is set to **Onboard OCP1 Shared**, **Onboard OCP2 Shared**, or **Onboard OCP3 Shared** the **Vlan Id** and **NCSI OCP Port Select** options are displayed, which are used to set the BMC VLAN ID and the service network port.

Step 6 (Optional) Set the BMC IPv4 network information.

- Manually configure the IP address as follows:
  a. Select **IPv4 Configuration** and press **Enter**.
  b. In the displayed dialog box, select **Static** and press **Enter**.
  c. Select **IPv4 IP Address** and press **Enter**.
     The **Please type in your data** dialog box is displayed.
  d. Enter the BMC IPv4 address and press **Esc** to exit the dialog box.
  e. Select **IPv4 Subnet Mask** and press **Enter**.
     The **Please type in your data** dialog box is displayed.
  f. Enter the BMC IPv4 subnet mask and press **Esc** to exit the dialog box.
  g. Select **IPv4 Gateway Address** and press **Enter**.
     The **Please type in your data** dialog box is displayed.
  h. Enter the BMC IPv4 gateway and press **Esc** to exit the dialog box.
     The BMC network is configured.
- Dynamically assign an IP address as follows:
  a. Select **IPv4 Configuration** and press **Enter**.

b. In the displayed dialog box, select **DHCP** and press **Enter**.

The configuration of dynamically obtaining the BMC network information through the DHCP protocol is completed.

Step 7 (Optional) Set the BMC IPv6 network information.

NOTE

You can set the BMC IPv6 network information in the same way of setting the BMC IPv4 network information.

Step 8 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 9 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.19 Setting a PCIe Port

Scenarios

Enable or disable a PCIe port using the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab  .

The **Advanced** screen is displayed, as shown in **Figure 3-141**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-141 Advanced screen



Step 3 Select **Socket Configuration** and press **Enter**.

The **Socket Configuration** screen is displayed, as shown in **Figure 3-142**.

Figure 3-142 Socket Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Select **IIO Configuration** and press **Enter**.

The **IIO Configuration** screen is displayed, as shown in **Figure 3-143**.

Figure 3-143 IIO Configuration screen



Step 5 Select a socket configuration screen, for example, **Socket 1 Configuration**, and press **Enter**.

The **Socket 1 Configuration** screen is displayed, as shown in **Figure 3-144**.

NOTE

The parameters on the displayed screen vary depending on the bandwidth configuration and used port of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-144 Socket 1 Configuration screen



Step 6 Select a port, for example, **Port 1A**, and press **Enter**.

The **Port 1A** screen is displayed, as shown in **Figure 3-145**.

Figure 3-145 Port 1A screen



Step 7 Select **PCIe Port** and press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 8 In the displayed dialog box, select **Enabled**, **Disabled**, or **Auto** as required, and press **Enter**.

- **Enabled/Auto**: Enable the PCIe port.
- **Disabled**: disables the PCIe port.

Step 9 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 10 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.20 Setting Serial Port Redirection

Scenarios

Enable or disable serial port redirection on the BIOS.

NOTE

If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.

Procedure

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Advanced** tab .

The **Advanced** screen is displayed, as shown in **Figure 3-146**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

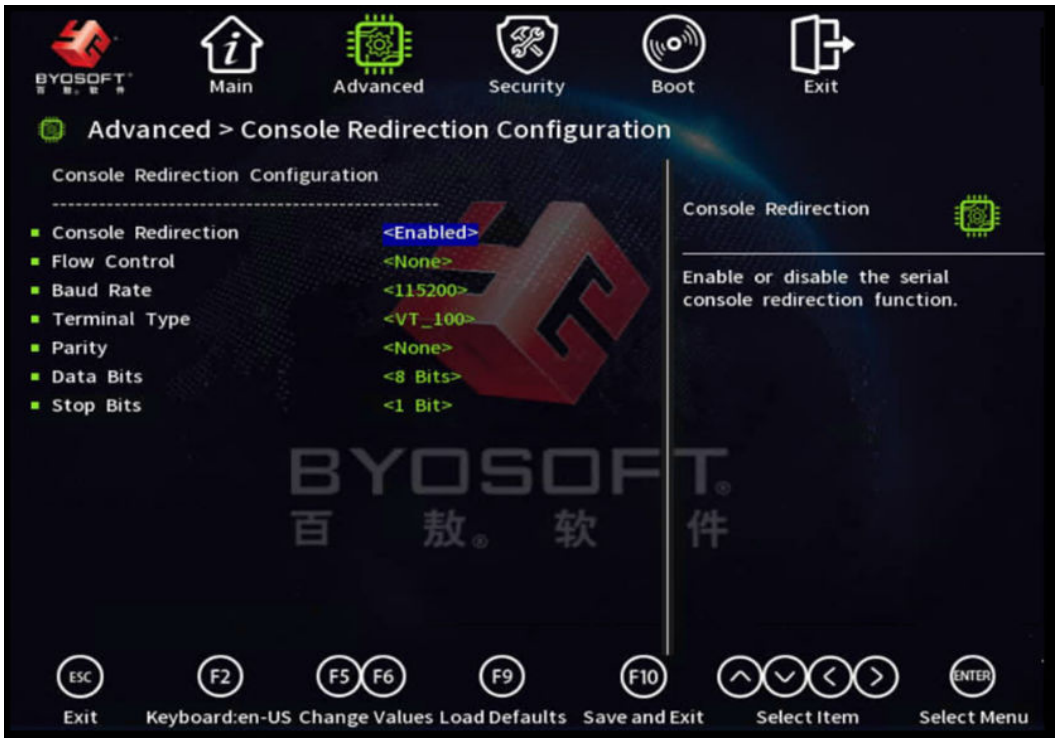
Figure 3-146 Advanced screen



Step 3 Select **Console Redirection Configuration** and press **Enter**.

The **Console Redirection Configuration** screen is displayed, as shown in **Figure 3-147**.

Figure 3-147 Console Redirection Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Step 4 Select **Console Redirection Configuration** and press **Enter**.

NOTE

For details about other parameters on the **Console Redirection Configuration** screen, see **6.2.9 Console Redirection Configuration**.

Step 5 In the displayed dialog box, select **Enabled** or **Disabled**, and press **Enter**.

- **Enabled**: enables serial port redirection.
- **Disabled**: disables serial port redirection.

Step 6 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 7 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

3.2.21 Restoring BIOS Factory Settings

Scenarios

Restore the BIOS factory settings of the server.

NOTE

- If the BIOS password is enabled, this task is supported only when you enter the Setup Utility screen as the BIOS administrator.
- Except for the following information that cannot be restored, the other BIOS parameters will be restored to default values of the current BIOS version. Modify related parameters again if the service requires special configurations on the BIOS parameters.
  - Date and time information on the **Main** screen
  - BIOS password and BIOS startup logo
  - All parameters (except watchdog-related parameters) on the **BMC Configuration** screen under the **Advanced** screen
  - All parameters on the **Device Manager** and **Administer Secure Boot** screens in UEFI mode
- For details about how to restore the default BIOS settings using the iBMC CLI, see the corresponding *iBMC User Guide*.

Method 1

Step 1 Access the Setup Utility screen.

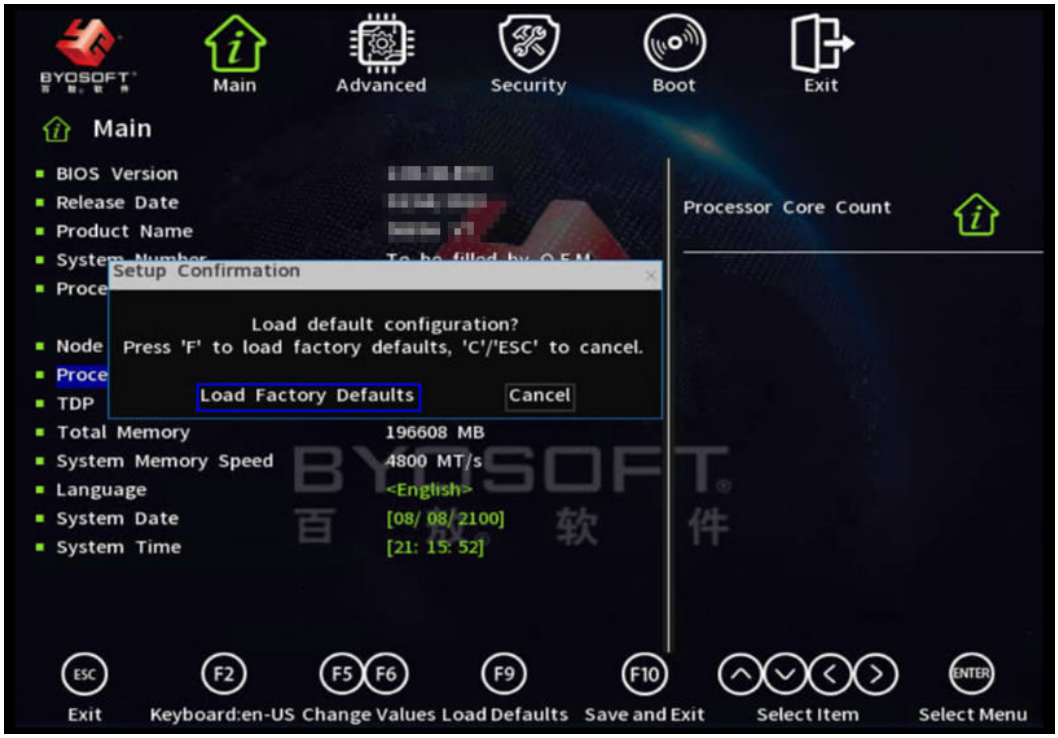
For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Press **F9**.

The **Load default configuration Press 'F' to confirm, 'C'/'ESC' to ignore.** dialog box is displayed, as shown in **Figure 3-148**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-148 Load default configuration dialog box



Step 3 Click **Load Factory Defaults** or press **F** to restore the default configuration.

NOTE

The BIOS parameters are restored to the default values of the current BIOS version. If the service requires special BIOS parameter configuration, you need to modify the parameters.

Step 4 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

NOTE

You can also select **Save Changes & Exit** and press **Enter** to save the settings and exit, or select **Save Changes Without Exiting** and press **Enter** to save the settings. For details, see **6.5 Exit**.

Step 5 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

Method 2

Step 1 Access the Setup Utility screen.

For details, see **3.2.2 Accessing the Setup Utility Screen**.

Step 2 Select the **Exit** tab .

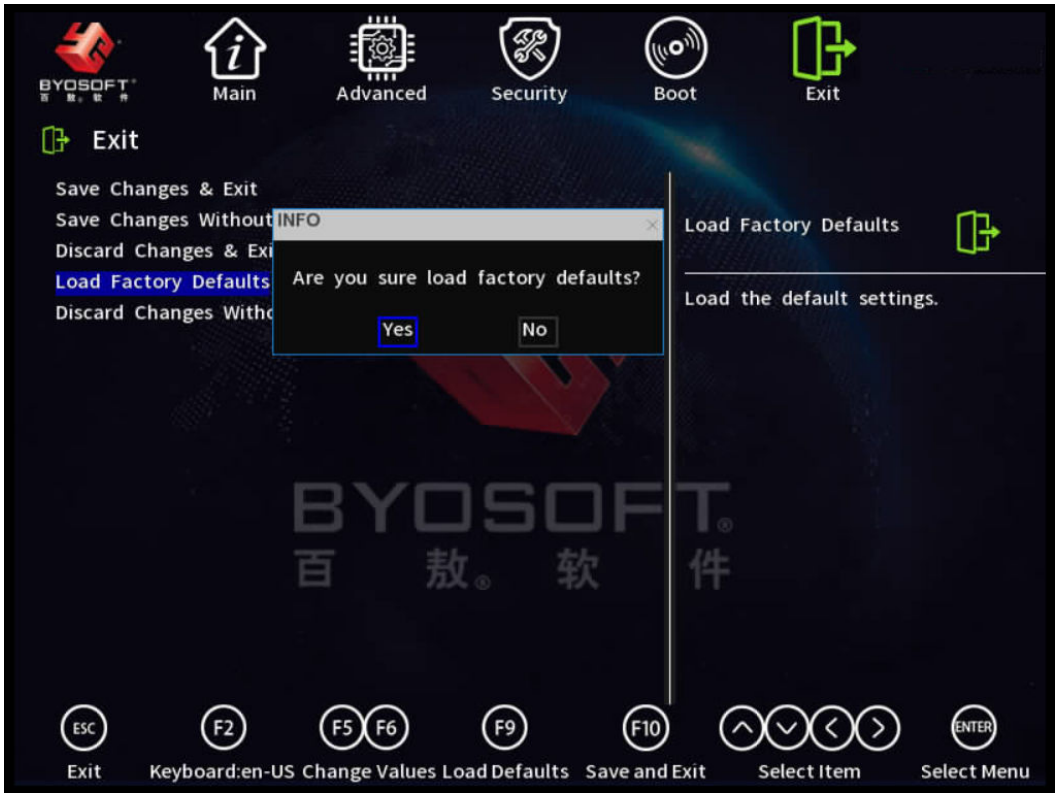
The **Exit** screen is displayed, as shown in **Figure 3-149**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 3-149 Exit screen



Step 3 Select **Load Factory Defaults** and press **Enter**.



Step 4 Select **Yes** or press **Enter**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

The BIOS parameters are restored to the default values of the current BIOS version. If the service requires special BIOS parameter configuration, you need to modify the parameters.

Step 5 Press **F10**.

The **Save configuration changes? Press'Y' to confirm,'N'/'ESC' to ignore.** dialog box is displayed.

Step 6 Select **Yes** or press **Y** to save the settings.

The server automatically restarts for the setting to take effect.

----End

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

4 Description of the Front Page

- For the description of the Front Page for 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7, see **4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**.
- For the description of the Front Page for 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see **4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**.

4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)

4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

4.1 of the Front Page (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)

NOTE

This section applies to the 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7. For description of the Front Page for the 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see **4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)**.

From the front page, you can access the **Boot Manager**, **Device Manager**, **Administer Secure Boot**, and **Setup Utility**. **Figure 4-1**, **Figure 4-2**, and **Figure 4-3** show the front pages. **Table 4-1** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- For details about how to access the front page, see **3.1.1 Accessing the Front Page**.
- **Figure 4-1** and **Figure 4-2** show the front pages displayed in different modes when you log in to the system as the administrator. In legacy mode, only the **Continue**, **Boot Manager**, **Device Manager**, and **Setup Utility** options are displayed on the front page. The administrator can set all parameters on the Setup Utility screen and use shortcut keys **F10** (save and exit) and **F9** (restore defaults).
- **Figure 4-3** shows the front page displayed when you log in to the system as a common user. In this case, only the **Continue** and **Setup Utility** menus are displayed. On the **Setup Utility** screen, common users can only view menu options, set or change their own passwords (that is, editing the **Set User Password** option on the **5.3 Security** screen), set parameters (except **Load Defaults**) on the **5.5 Exit** screen, and press **F10** to save the settings and exit. Other options are all grayed out and cannot be edited, and the **F9** shortcut function (restoring default settings) is unavailable.
- There is no logo on the front page background of BIOS V01.01.02.05 or later.

Figure 4-1 Front page (UEFI mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-2 Front page (legacy mode)



Figure 4-3 Front page (login as a common user)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 4-1 Parameters on the front page

Parameter	Description
Continue	Press **Enter** to continue the boot process.
Boot Manager	Enter the **Boot Manager** screen.
Device Manager	Enter the **Device Manager** screen.
Boot From File	Boot from the specific file or device.
Administer Secure Boot	Enter the secure boot configuration menu.
Setup Utility	Enter the BIOS configuration menu.

4.1.1 Boot Manager

On the **Boot Manager** screen, you can select a boot device. **Figure 4-4** shows the **Boot Manager** screen. **Table 4-2** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the configuration of the server.

Figure 4-4 Boot Manager screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

- The **Boot Manager** screen displays information about boot options and bootable devices.
- The **Boot Manager** screen varies according to the connected boot device.
- Press **F5** or **F6** to adjust the device boot sequence.

Table 4-2 Parameters on the Boot Manager screen

Parameter	Description
Hard Disk Drive	Specifies a drive as the boot device.
DVD-ROM Drive	Specifies a CD/DVD-ROM as the boot device.
PXE	Specifies a PXE as the boot device. **NOTE** The PXE boot option is a network device boot option.
Other Device	Specifies other boot devices. **NOTE** Other boot devices include floppy drives, SAN boot devices, and removable devices.
Manage Custom Boot Options	Adds permanent customized boot options in case that the BIOS does not recognize certain OS bootloader applications. This function is available only in UEFI mode.

4.1.2 Device Manager

On the **Device Manager** screen, you can query or perform operations on connected devices. **Figure 4-5** shows the **Device Manager** screen. **Table 4-3** describes parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-5 Device Manager screen



NOTE

The information displayed on the **Device Manager** screen varies depending on the hardware configuration of the server. Different options are displayed when different devices are connected.

Table 4-3 Parameters on the Device Manager screen

Parameter	Description
Driver Health Manager	Displays the health status of connected devices.
iSCSI Configuration	Provides access to iSCSI configurations.
BROADCOM MegaRAID SAS 9560-8i RAID	Manages RAID controller card configurations. **NOTE** • This parameter is displayed only when a RAID controller card is configured. • Parameter names vary depending on the RAID controller card. • Configuration screens vary depending on the RAID controller cards. For details, see the *V7 Server RAID Controller Card User Guide*.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Network Device List	Provides access to NIC configurations. **NOTE** • This parameter is displayed only when an NIC is configured. • The configuration screen varies according to the NIC. For details, see the user guide of the related NIC.

4.1.3 Boot From File

On the **Boot From File** screen, you can select a file or device to start. **Figure 4-6** shows the **Boot From File** screen.

NOTE

The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.

Figure 4-6 Boot From File screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

4.1.4 Administer Secure Boot

On the **Administer Secure Boot** screen, you can configure the Secure Boot function. Figure 4-7 shows the **Administer Secure Boot** screen. Table 4-4 describes parameters.

Secure Boot is defined as a security technology by the UEFI specification to ensure the security of the boot environment. The main purpose is to secure the firmware running in the BIOS, such as the third-party UEFI driver and OS boot loader.

Figure 4-7 Administer Secure Boot screen



Table 4-4 Parameters on the Administer Secure Boot screen

Parameter	Description	Default Value
Secure Boot Database	Displays the installation status of the current Secure Boot certificate database. PK, KEK, DB, and DBX certificates are included. The menu options are as follows: • **Installed and Locked**: The Secure Boot certificate database has been installed. • **Unlocked**: The Secure Boot certificate database has not been installed.	Unlocked

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Secure Boot Status	Displays the current Secure Boot status. The menu options are as follows: ● **Enabled**: Secure Boot is enabled. ● **Disabled**: Secure Boot is disabled.	Disabled
User Customized Security	Displays whether the current user has added or deleted certificates. The menu options are as follows: ● **Yes**: The current user has added or deleted certificates. ● **No**: The current user has not added or deleted certificates.	No
Select a UEFI file as trusted for execution	Sets the UEFI file as a trusted file and adds its hash to the database.	-
Enforce Secure Boot	Sets the Secure Boot function. The menu options are as follows: ● **Enabled**: Secure Boot is enabled. ● **Disabled**: Secure Boot is disabled. **NOTE** If Secure Boot is enabled for the first time, you need to restore factory settings, save the settings, and exit. That is, set **Restore Secure Boot to Factory Settings** to **Enabled** and press **F10** to save the settings and exit.	Disabled
Erase all Secure Boot Settings	Sets the function of clearing security configurations. The menu options are as follows: ● **Enabled**: All Secure Boot settings are cleared and the Secure Boot function is disabled. ● **Disabled**: The function of clearing security configurations is disabled.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Restore Secure Boot to Factory Settings	Restores the factory settings of Secure Boot. The menu options are as follows: ● **Enabled**: The factory settings of Secure Boot are restored and Secure Boot is enabled. ● **Disabled**: The factory settings of Secure Boot are not restored. **NOTE** When the status of **Secure Boot Database** is **Unlocked**, **Enforce Secure Boot** cannot be configured. To configure **Enforce Secure Boot**, set **Restore Secure Boot to Factory Settings** to **Enabled**, press **F10** to save and exit, and go to the secure boot screen again.	Disabled
PK Options	The entrance to the platform key (PK) certificate setting page. PK is vital to establish a trust relationship between the platform owner and the platform firmware.	-
KEK Options	The entrance to the key exchange key (KEK) certificate setting page. KEK is used to update the current signature database and sign binary files to ensure effective execution.	-
DB Options	The entrance to the DB certificate setting page to set the trust whitelist. The signature database is used to verify that the signed EFI binary file and the loaded ROM are valid.	-
DBX Options	The entrance to the DBX certificate setting page to set the untrusted blacklist. The prohibited signature database is used to invalidate EFI binary files and loadable ROM.	-
DBT Options	The entrance to the DBT certificate setting page. The DBT is a timestamp database. It authenticates the time when data is generated by using certain technical methods.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

The **PK Options** screen is similar to the **KEK Options** screen, and the **DB Options** screen is similar to the **DBX Options** screen. The following uses the **PK Options** and **DBX Options** screens as examples. For details, see **4.1.4.1 PK Options** and **4.1.4.2 DBX Options**.

4.1.4.1 PK Options

Figure 4-8 shows the **PK Options** screen. **Table 4-5** describes parameters.

Figure 4-8 PK Options screen

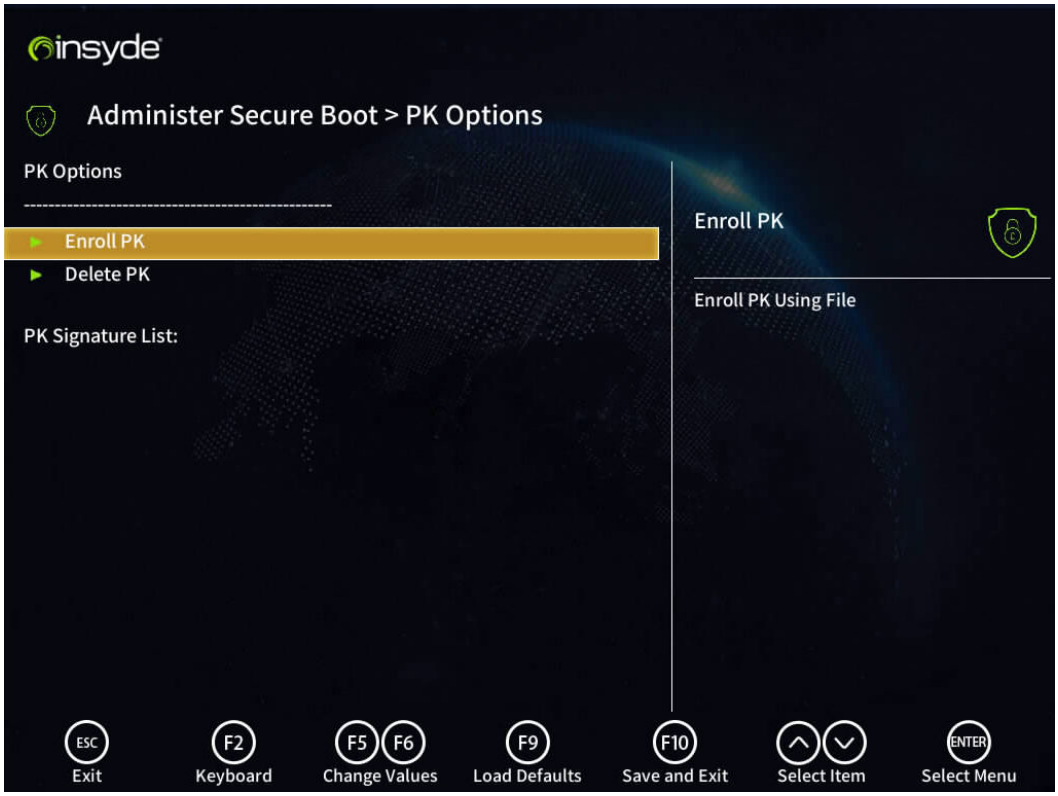


Table 4-5 Parameters on the PK Options screen

Parameter	Description
Enroll PK	Registers a PK certificate.
Delete PK	Deletes a PK certificate.
PK Signature List	Displays a list of PK signatures. **NOTE** The file list is automatically identified and displayed by the BIOS. The file list varies depending on the actual server configuration. If no related file exists, no content is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

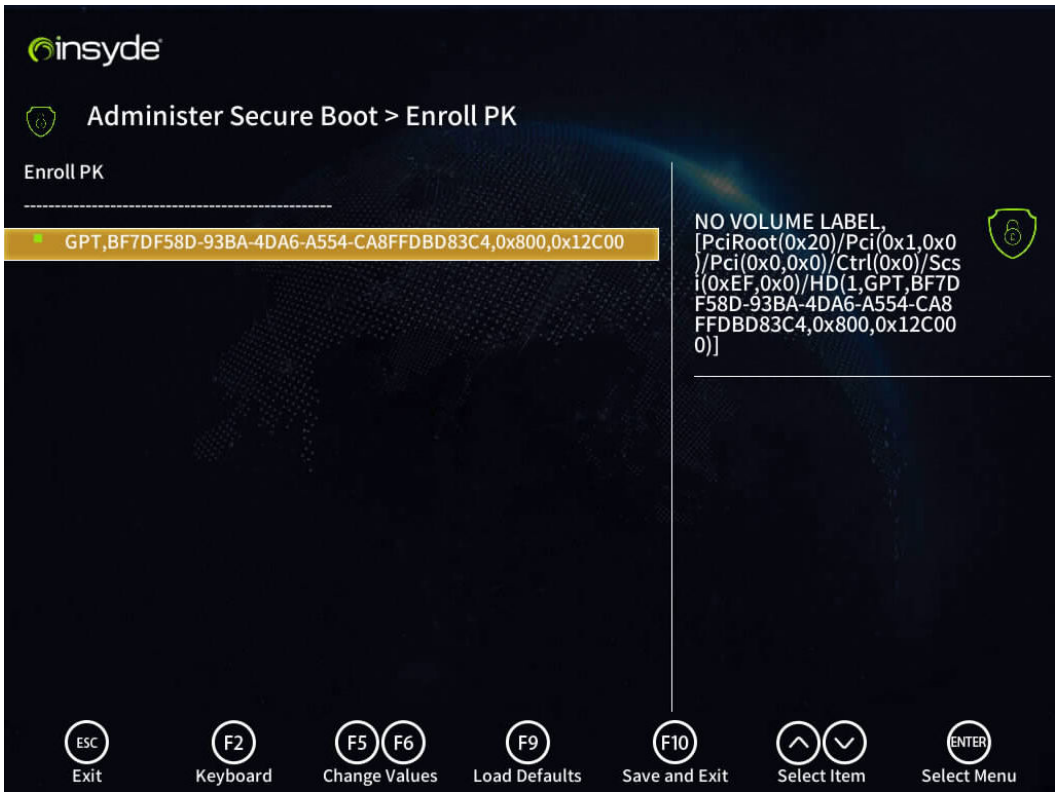
4.1.4.1.1 Enroll PK

On the **Enroll PK** screen, you can register PK certificates. **Figure 4-9** shows the **Enroll PK** screen.

NOTE

The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.

Figure 4-9 Enroll PK screen



4.1.4.1.2 Delete PK

On the **Delete PK** screen, you can delete existing PK certificates. **Figure 4-10** shows the **Delete PK** screen.

NOTE

The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-10 Delete PK screen



4.1.4.2 DBX Options

Figure 4-11 shows the **DBX Options** screen. Table 4-6 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-11 DBX Options screen

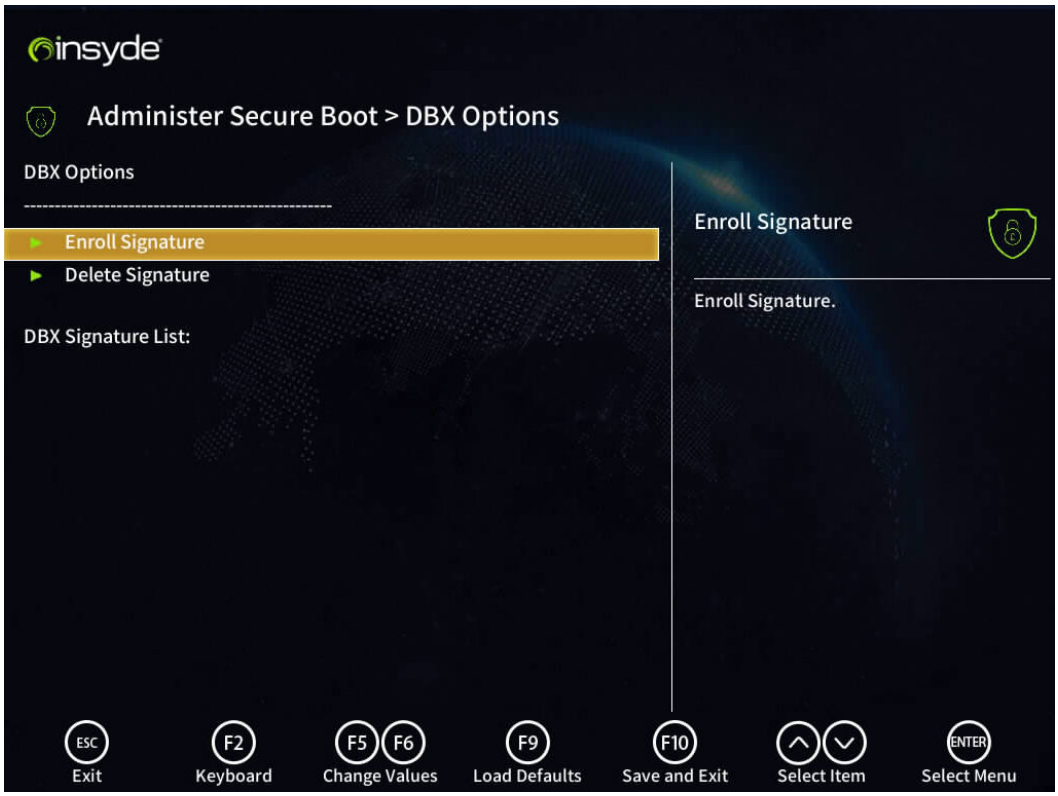


Table 4-6 Parameters on the DBX Options screen

Parameter	Description
Enroll Signature	Supports the selection of the signature format and path. The signature can be in the following formats: • PKCS7 • SHA256 • SHA512
Delete Signature	Displays the signature deletion screen. On this screen, you can delete loaded signatures. **NOTE** The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.
DBX Signature List	Displays the signature list. **NOTE** The file list is automatically identified and displayed by the BIOS. The file list varies depending on the actual server configuration. If no related file exists, no content is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

4.2 Description of the Front Page (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

From the front page, you can access the **Boot Manager**, **Device Manager**, **Administer Secure Boot**, and **Setup Utility**. Figure 4-12 and Figure 4-13 show the front pages. Table 4-7 describes the parameters.

NOTE

- For details about how to access the front page, see 3.2.1 Accessing the Front Page.
- Figure 4-12 shows the front page displayed when you log in to the system as the administrator.
- Figure 4-13 shows the front page displayed when you log in to the system as a common user. You can set only the **Continue** and **Setup Utility** menu options. Other options are grayed out and cannot be edited. On the Setup Utility screen, a common user can only view menu options, set or change their own password of (that is, editing the **Set User Password** option on the 6.3 Security screen and **Save Changes & Exit** option on the 6.5 Exit screen). Other options are grayed out and cannot be edited.

Figure 4-12 Front page 1 (login as the administrator in UEFI mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-13 Front page 2 (login as a common user in UEFI mode)



Figure 4-14 Front page 3 (login as the administrator in legacy mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-15 Front page 4 (login as a common user in legacy mode)



Table 4-7 Parameters on the front page

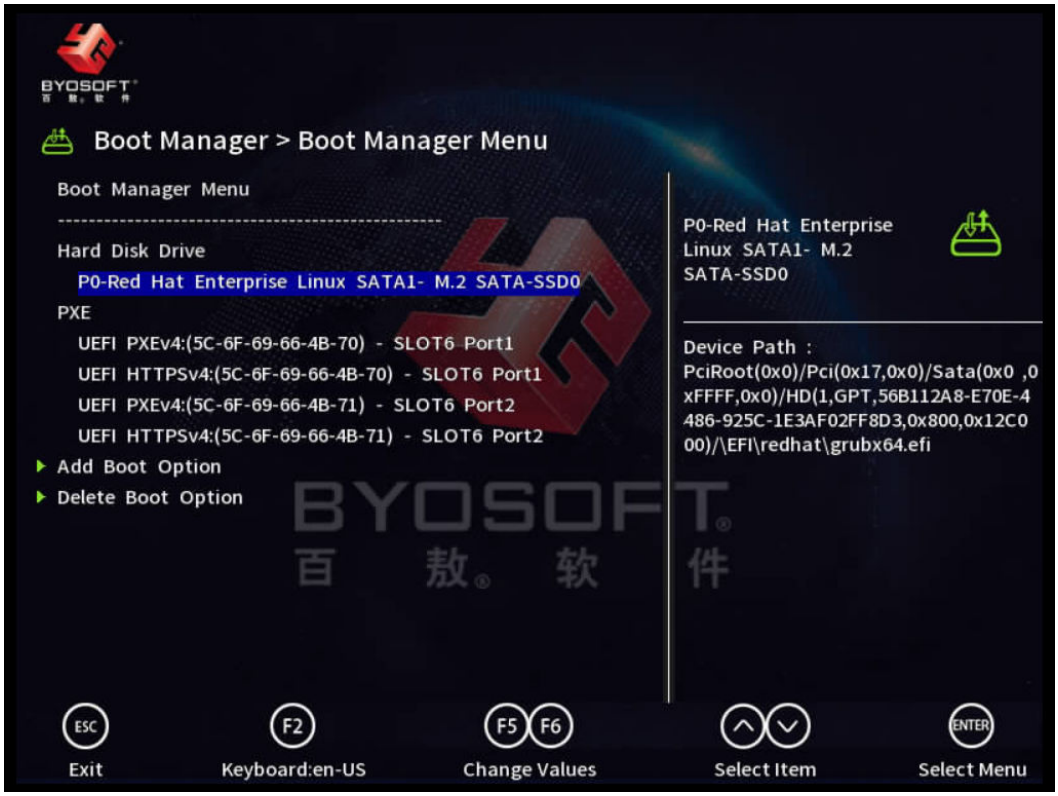
Parameter	Description
Continue	Continues the boot process by pressing **Enter**.
Boot Manager	Enters the **Boot Manager** screen.
Device Manager	Enter the **Device Manager** screen.
Boot From File	Boot from the specific file or device.
Administer Secure Boot	Enter the secure boot configuration menu.
Setup Utility	Enter the BIOS configuration menu.

4.2.1 Boot Manager

On the **Boot Manager** screen, you can select a boot device. **Figure 4-16** shows the **Boot Manager** screen. **Table 4-8** describes parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-16 Boot Manager screen



NOTE

The **Boot Manager** screen displays information about boot options and bootable devices. The **Boot Manager** screen varies according to the connected boot device.

Table 4-8 Parameters on the Boot Manager screen

Parameter	Description
Hard Disk Drive	Specifies a drive as the boot device.
DVD-ROM Drive	Specifies a CD/DVD-ROM as the boot device.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description

PXE	Specifies a PXE as the boot device.
	NOTE
	• The PXE boot option is a network device boot option and is automatically hidden when no PXE device is available.
	• If there are a large number of PXE boot items, the iPXE boot item may fail to be started. The threshold for the number of boot items depends on the specific NIC and the version of ipxe.efi, for example:
	  • The MCX623106AN-CDAT NIC with ipxe-gd3c89.efi supports a maximum of 90 PXE boot options.
	  • The MCX623106AN-CDAT NIC with ipxe-gc30b7.efi supports a maximum of 88 PXE boot options.
	  • The BCM957414N4140C NIC with ipxe-gd3c89.efi supports a maximum of 124 PXE boot options.
	  If the boot fails due to the large number of PXE boot items, you are advised to disable unused iPXE network ports to reduce the number of boot items.

Others	Specifies other boot devices. **NOTE** Other boot devices include floppy drives and removable devices.
Add Boot Option	Adds a boot device.
Delete Boot Option	Deletes a boot device.

NOTE

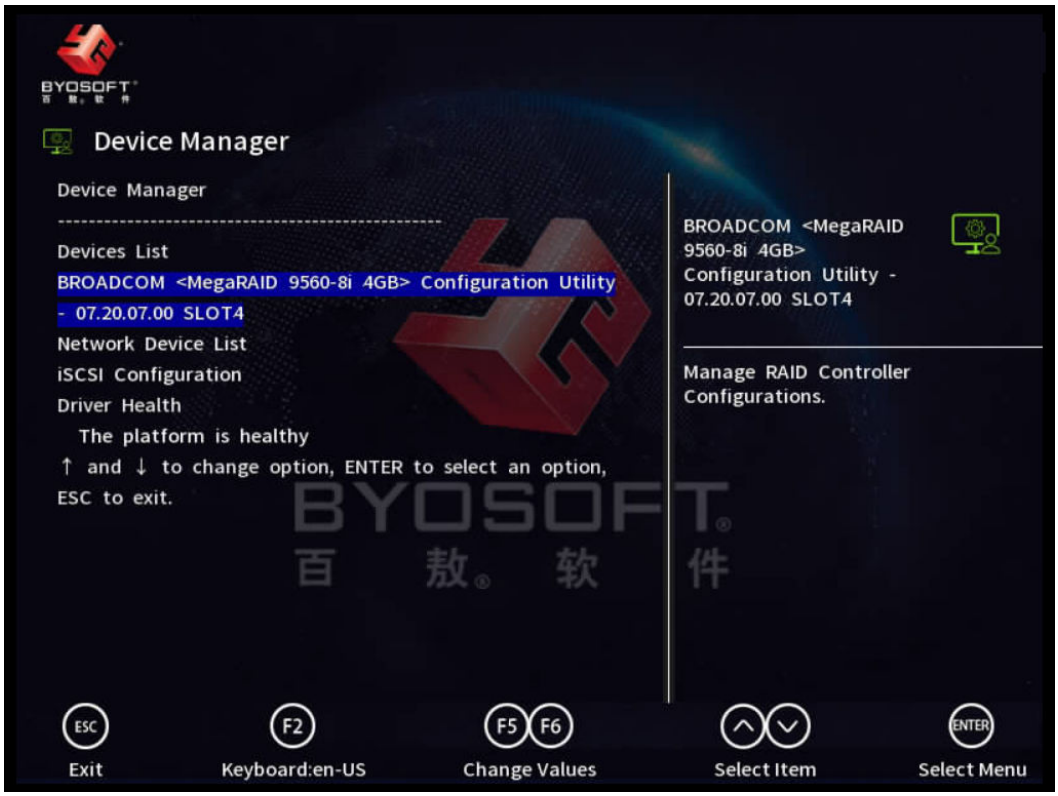
Press F5 or F6 to adjust the device boot sequence.

4.2.2 Device Manager

On the **Device Manager** screen, you can query or perform operations on connected devices. **Figure 4-17** shows the **Device Manager** screen. **Table 4-9** describes parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-17 Device Manager screen



NOTE

The information displayed on the **Device Manager** screen varies depending on the hardware configuration of the server. Different options are displayed when different devices are connected.

Table 4-9 Parameters on the Device Manager screen

Parameter	Description
BROADCOM <MegaRAID 9560-8i 4GB> Configuration Utility - 07.22.03.00 SLOT4	Manages RAID controller card configurations. **NOTE** • This parameter is displayed only when a RAID controller card is configured. • Configuration screens vary depending on the RAID controller card. For details, see the *V7 Server RAID Controller Card User Guide*.
Network Device List	Provides access to NIC configurations. **NOTE** • This parameter is displayed only when an NIC is configured. • The configuration screen varies depending on the NIC. For details, see the user guide of the related NIC.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
iSCSI Configuration	Provides access to **iSCSI** configurations.
Driver health	Displays the health status of connected devices. If the message "The platform is healthy" is displayed, the device status is normal.

4.2.3 Boot From File

On the **Boot From File** screen, you can select a file or device to start. **Figure 4-18** shows the **Boot From File** screen.

NOTE

The information displayed on the screen varies depending on the configuration of the server. If no related file or device exists, no content is displayed.

Figure 4-18 Boot From File screen



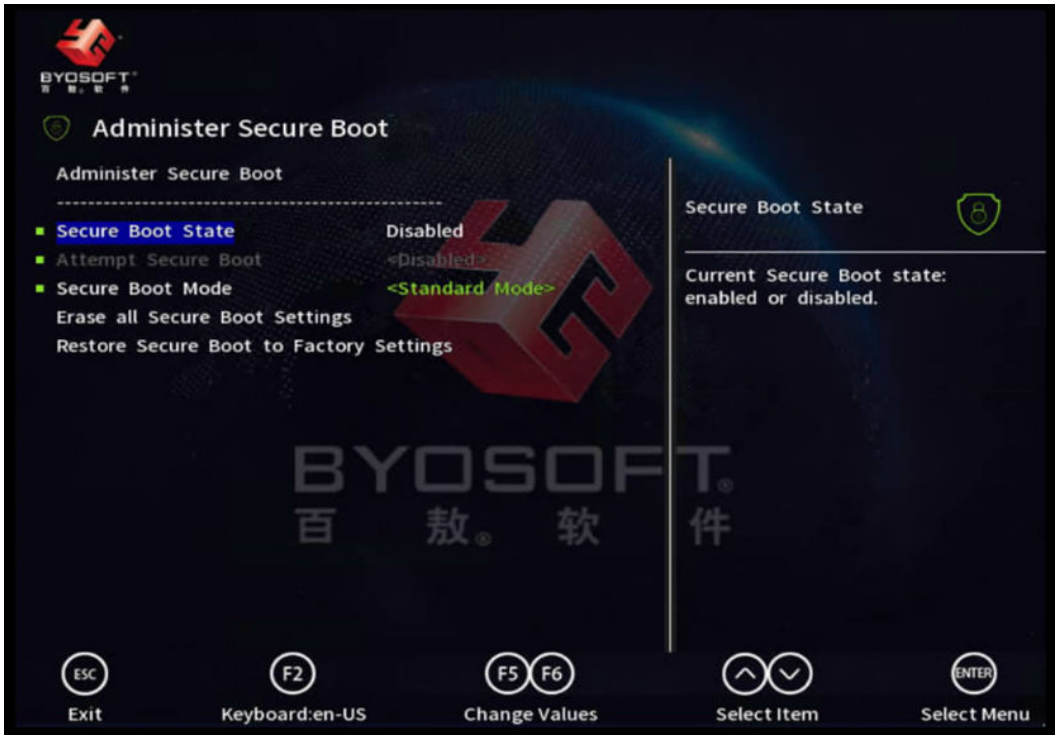
4.2.4 Administer Secure Boot

On the **Administer Secure Boot** screen, you can configure the Secure Boot function. **Figure 4-19** shows the **Administer Secure Boot** screen. **Table 4-10** describes parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Secure Boot is defined as a security technology by the UEFI specification to ensure the security of the boot environment. The main purpose is to secure the firmware running in the BIOS, such as the third-party UEFI driver and OS boot loader.

Figure 4-19 Administer Secure Boot screen 1



When **Secure Boot Mode** is set to **Custom Mode**, **Custom Secure Boot Options** is displayed, as shown in **Figure 4-20**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-20 Administer Secure Boot screen 2

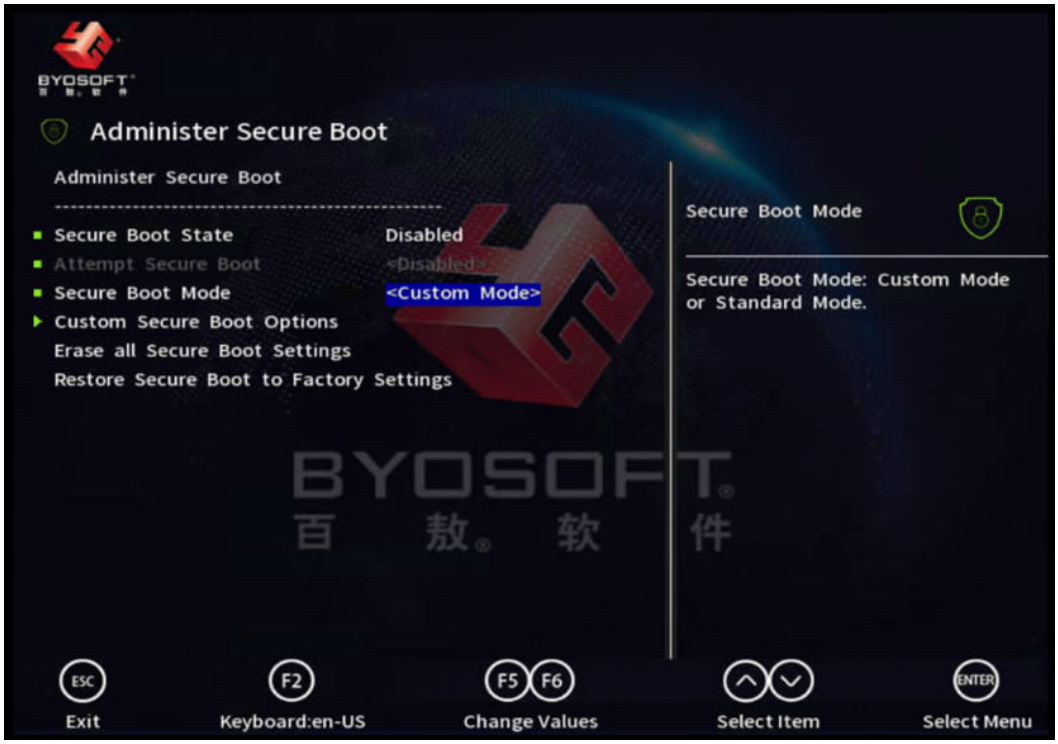


Table 4-10 Parameters on the Administer Secure Boot screen

Parameter	Description	Default Value
Secure Boot State	Displays the current Secure Boot status. The menu options are as follows: ● **Enabled**: Secure Boot is enabled. ● **Disabled**: Secure Boot is disabled.	Disabled
Attempt Secure Boot	Enables or disables secure boot in the user mode. ● **Enabled**: Secure Boot is enabled. ● **Disabled**: Secure Boot is disabled. **NOTE** This parameter is editable when **Secure Boot State** is set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Secure Boot Mode	Selects the secure boot mode. The menu options are as follows: • **Custom Mode**: sets the user mode. In this mode, you can access the **Custom Secure Boot Options** screen to set required information, such as the PK, KEK, DB, and DBX. • **Standard Mode**: sets the standard mode. In this mode, parameters on the **Custom Secure Boot Options** screen are unavailable and default parameter settings are retained.	Standard Mode
Custom Secure Boot Options	Accesses the **Custom Secure Boot Options** screen. **NOTE** This parameter is available when **Secure Boot Mode** is set to **Custom Mode**.	-
Erase all Secure Boot Settings	Clears all secure boot settings and disables secure boot.	-
Restore Secure Boot to Factory Settings	Restores the secure boot settings to the factory settings and enables secure boot.	-

4.2.4.1 Custom Secure Boot Options

Figure 4-21 shows the **Custom Secure Boot Options** screen. **Table 4-11** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-21 Custom Secure Boot Options screen

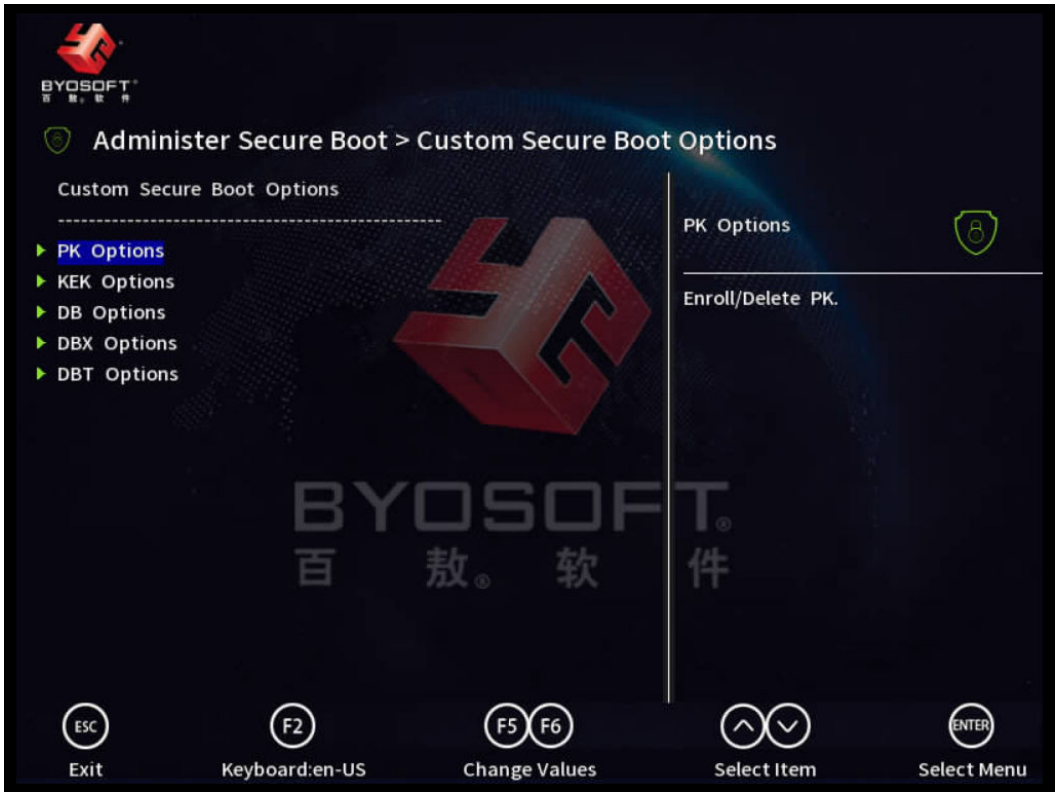


Table 4-11 Parameters on the Custom Secure Boot Options screen

Parameter	Description
PK Options	Provides access to the platform key (PK) certificate setting page. PK is vital to establish a trust relationship between the platform owner and the platform firmware.
KEK Options	Provides access to the key exchange key (KEK) certificate setting page. KEK is used to update the current signature database and sign binary files to ensure effective execution.
DB Options	Provides access to the DB certificate setting page for setting the trust allowlist. The signature database is used to verify that the signed EFI binary file and the loaded ROM are valid.
DBX Options	Provides access to the DBX certificate setting page for setting the untrusted blocklist. The prohibited signature database is used to invalidate EFI binary files and loadable ROM.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
DBT Options	Provides access to the DBT certificate setting page. The DBT is a timestamp database. It authenticates the time when data is generated by using certain technical methods.

NOTE

The **PK Options**, **KEK Options**, **DB Options**, **DBX Options**, and **DBT Options** screens are similar. The following uses the **DB Options** screen as an example. For details, see **4.2.4.1.1 DB Options**.

4.2.4.1.1 DB Options

Figure 4-22 shows the **DB Options** screen. **Table 4-12** describes the parameters.

Figure 4-22 DB Options screen

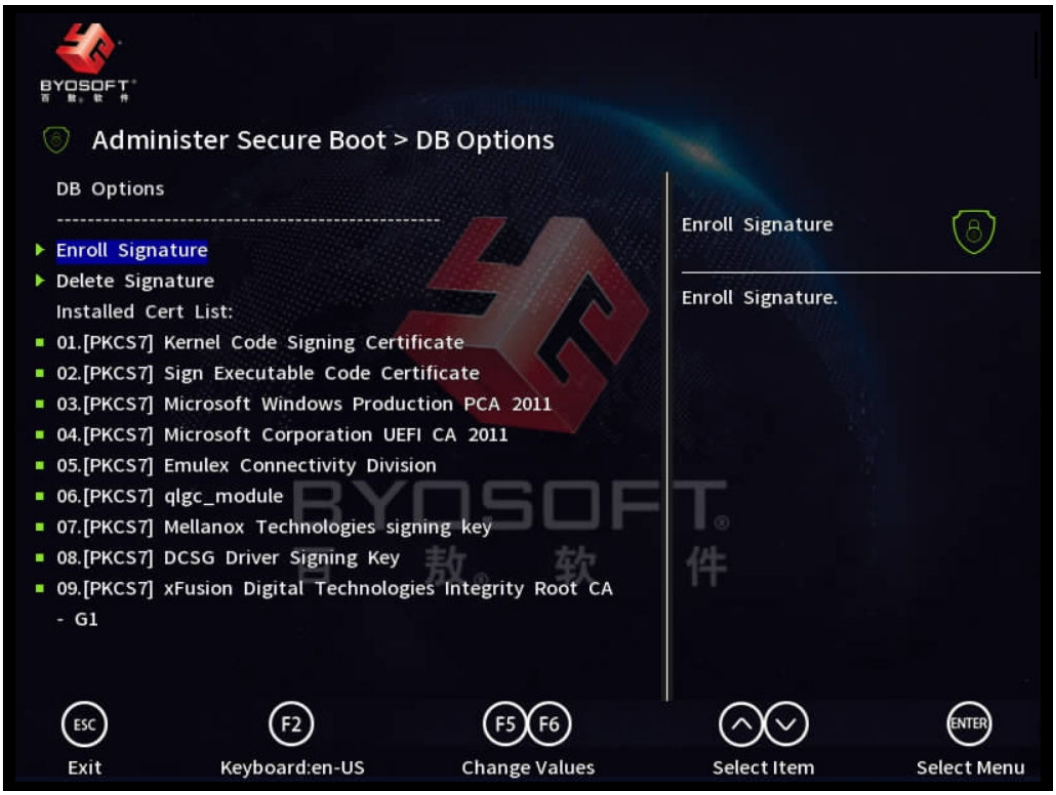


Table 4-12 Parameters on the DB Options screen

Parameter	Description
Enroll Signature	Registers a signature.
Delete Signature	Deletes a signature.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Installed Cert List	Displays the loaded signature list. **NOTE** When **Secure Boot State** is set to **Enabled**, the certificate list is displayed.

Enroll Signature

Figure 4-23 shows the **Enroll Signature** screen. **Table 4-13** describes the parameters.

Figure 4-23 Enroll Signature screen

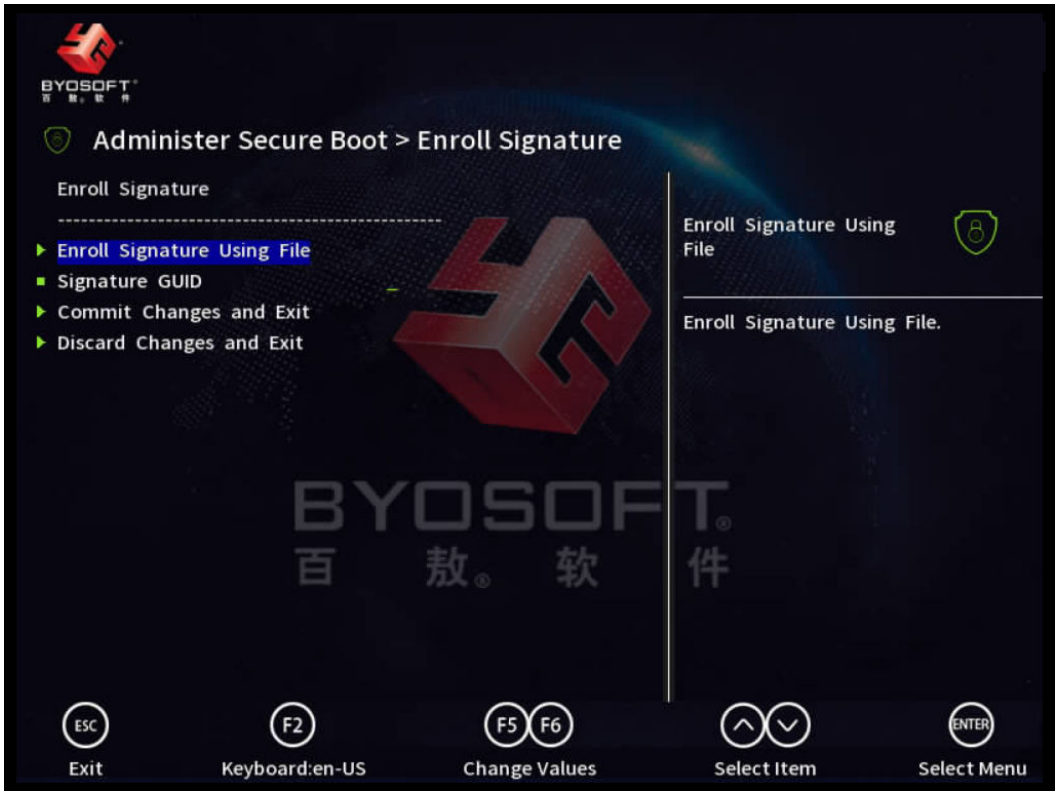


Table 4-13 Parameters on the Enroll Signature screen

Parameter	Description
Enroll Signature Using File	Registers a signature by using a file. Select the file and press **Enter**. Select a proper file to register the signature.
Signature GUID	Sets the signature GUID.
Commit Changes and Exit	Saves the changes and exits the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

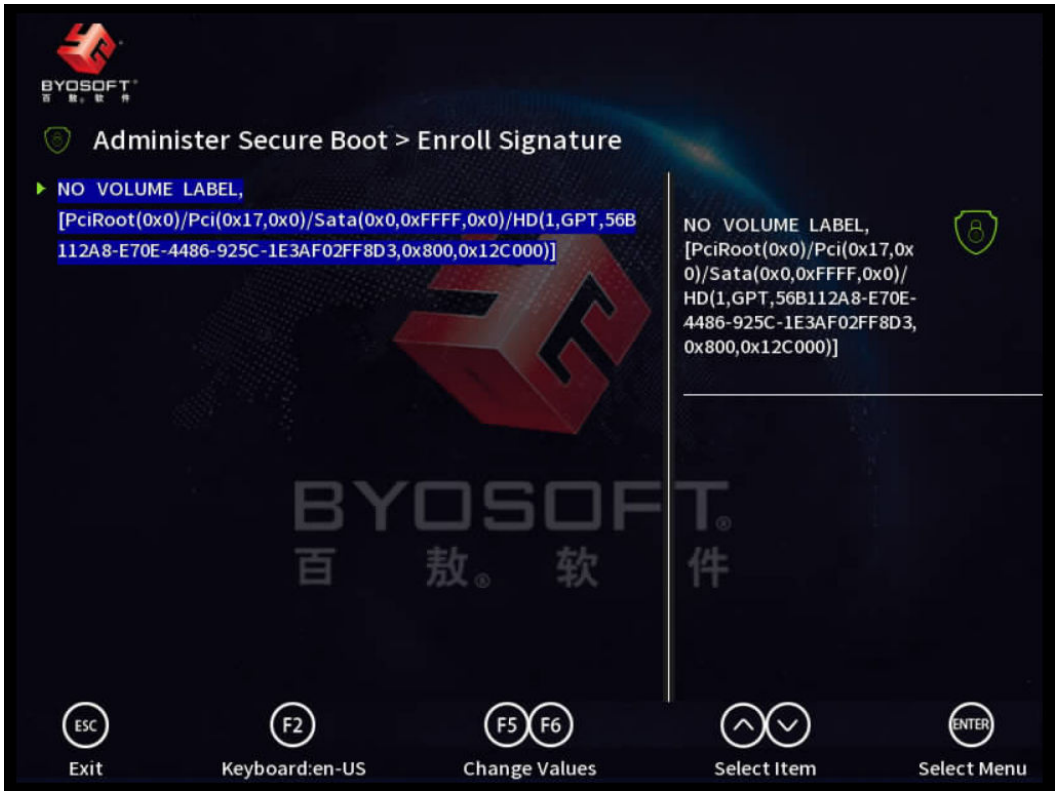
Parameter	Description
Discard Changes and Exit	Discards the changes and exits the screen.

Figure 4-24 shows the **Enroll Signature Using File** screen.

NOTE

The information displayed on the screen varies depending on the configuration of the server. If no related file exists, no content is displayed on the screen.

Figure 4-24 Enroll Signature Using File screen



Delete Signature

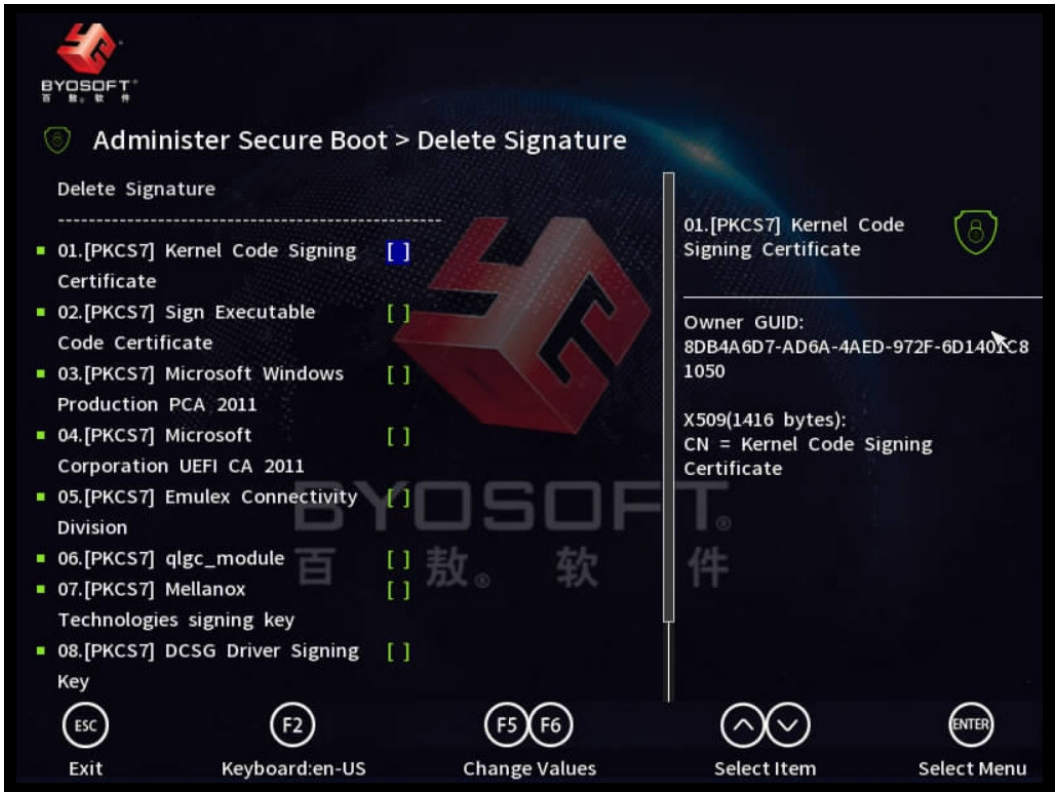
Figure 4-25 shows the Delete Signature screen. On this screen, you can delete loaded signatures.

NOTE

If files exist, the files are automatically identified and displayed by the BIOS. If no related file exists, no content is displayed on this screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 4-25 Delete Signature screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5 Description of Setup Utility (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7/2288 V8)

NOTE

- This section applies to the 1288H V7, 2288H V7, 5288 V7, 5298 V7, and G5200 V7. For the description of Setup Utility for 2288 V7, 2488H V7, 5885H V7, G5500 V7, and G8600 V7, see **6 Description of Setup Utility (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7/2288 V8)**.
- For details about how to access the Setup Utility screen, see **3.1.2 Accessing the Setup Utility Screen**.
- If you log in to the **Setup Utility** screen as the administrator, you can set all parameters on the Setup Utility screen and use shortcut keys **F10** (save and exit) and **F9** (restore defaults).
- If you log in to the **Setup Utility** screen as a common user, you can only view menu options and set or change the password of the common user (that is, only the **Set User Password** option on the **5.3 Security** screen can be set), set parameters (except **Load Defaults**) on the **5.5 Exit** screen, and press **F10** to save the settings and exit. Other options are all grayed out and cannot be edited, and the **F9** shortcut function is unavailable.
- There is no logo on the setup utility background of BIOS V01.01.02.05 or later.

5.1 Main

5.2 Advanced

5.3 Security

5.4 Boot

5.5 Exit

5.1 Main

The **Main** screen provides basic BIOS information, including the BIOS version, CPU model, memory capacity, system time, and system language. **Figure 5-1** shows the **Main** screen. **Table 5-1** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-1 Main screen 1



Figure 5-2 Main screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-1 Parameters on the Main screen

Parameter	Description	Default Value
BIOS Version	Indicates the BIOS version.	-
Release Date	Indicates the compiling date of the BIOS.	-
Product Name	Indicates the product name. **NOTE** The value is dynamically obtained from the BMC. If no information is obtained, the message **To be filled by O.E.M.** is displayed.	-
System Number	Indicates the product serial number. **NOTE** The value is dynamically obtained from the BMC. If no information is obtained, the message **To be filled by O.E.M.** is displayed.	-
Processor Type	Indicates the processor model.	-
Node Number	Indicates the number of processors that a server has been installed with.	-
Processor Core Count	Indicates the total number of physical processor cores, excluding hyper threads. **NOTE** The total number of physical processor cores varies depending on the processor model.	-
TDP	Thermal design power, which is the heat released when the processor reaches the maximum load.	-
System Bus Speed	Indicates the system bus speed.	-
System Memory Speed	Actual operating frequency of the memory.	-
Cache RAM	Second-level cache.	-
Total Memory	Total memory capacity of the server.	-
Language	Language in use. The menu options are as follows: ● English ● Chinese ● Japanese	English

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
System Time	Current BIOS time. The system time is in the format of *HH:MM:SS* in the 24-hour system. To switch among the hour, minute, and second, press **Enter**. To change the time, use the following methods: ● Press **+** to increase the value by 1. ● Press **-** to decrease the value by 1. ● Press a number to change the value directly.	-
System Date	Current BIOS date. The system date is in the format of *YYYY/MM/DD*. To switch among the year, month, and day, press **Enter**. To change the date, use the following methods: ● Press **+** to increase the value by 1. ● Press **-** to decrease the value by 1. ● Press a number to change the value directly.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Time Zone	Sets the time zone of system time. The menu options are as follows: ● UTC-12:00 ● UTC-11:00 ● UTC-10:00 ● UTC-09:30 ● UTC-09:00 ● UTC-08:00 ● UTC-07:00 ● UTC-06:00 ● UTC-05:00 ● UTC-04:00 ● UTC-03:30 ● UTC-03:00 ● UTC-02:30 ● UTC-02:00 ● UTC-01:00 ● UTC+00:00 ● UTC+01:00 ● UTC+02:00 ● UTC+03:00 ● UTC+03:30 ● UTC+04:00 ● UTC+04:30 ● UTC+05:00 ● UTC+05:30 ● UTC+05:45 ● UTC+06:00 ● UTC+06:30 ● UTC+07:00 ● UTC+08:00 ● UTC+08:45 ● UTC+09:00 ● UTC+09:30 ● UTC+10:00 ● UTC+10:30 ● UTC+11:00 ● UTC+12:00 ● UTC+12:45	UTC+00:00

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
	• UTC+13:00 • UTC+13:45 • UTC+14:00 **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	
Daylight Saving Time	Enables or disables the daylight saving time of system time. The menu options are as follows: • Disabled • Enabled **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	Disabled
Synchronize Time Zone With BMC	Enables or disables the synchronize the system time zone from BMC at boot time, and set the BMC time zone when the system time zone is changed by user. The menu options are as follows: • Disabled • Enabled **NOTE** Only BIOS 01.01.08.03 and later versions support this parameter.	Disabled

5.2 Advanced

The **Advanced** screen provides advanced BIOS configuration options. **Figure 5-3** shows the **Advanced** screen. **Table 5-2** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-3 Advanced screen



Table 5-2 Parameters on the Advanced screen

Parameter	Description
Platform Information	Displays the platform information.
Peripheral Configuration	Provides access to configuration of peripheral devices, including PCIe ASPM, SR-IOV, and serial port I/O.
Video Configuration	Provides access to the video card mode configurations.
ACPI Table or Features Control	Provides access to the ACPI table configurations.
Misc Configuration	Provides access to miscellaneous configurations.
System Event Log	Provides access to the system event log configurations, including MCA and PCIe AER.
Socket Configuration	Provides access to the CPU, UPI, memory, I/O, and power management configurations.
ME Configuration	Provides access to the ME configurations.
PCH-IO Configuration	Provides access to SATA and USB configurations.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
BMC Configuration	Provides access to the BMC configurations.
Console Redirection Configuration	Provides access to configuration of serial port redirection.
PXE Configuration	Provides access to the PXE configurations.
NVMe Information	Displays details about the NVMe drives.

5.2.1 Platform Information

On the **Platform Information** screen, you can query platform information. **Figure 5-4** shows the **Platform Information** screen. **Table 5-3** describes the parameters.

Figure 5-4 Platform Information screen

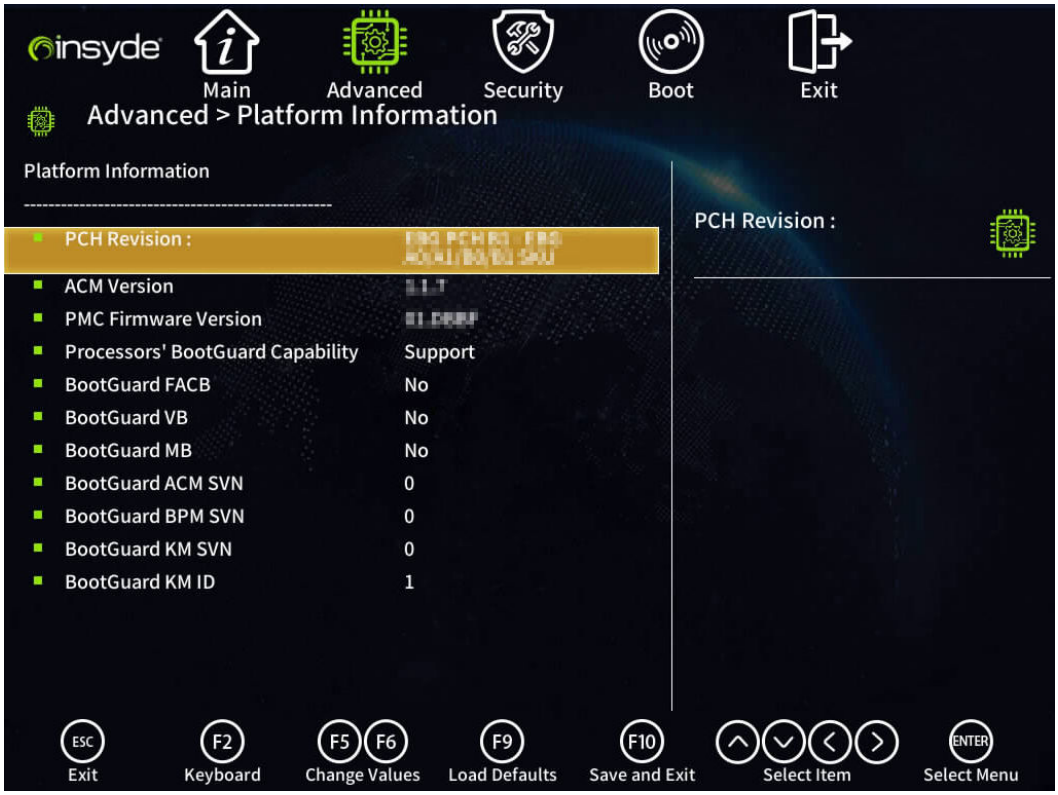


Table 5-3 Parameters on the Memory Information screen

Parameter	Description
PCH Revision	Displays the PCH version.
ACM Version	Displays the ACM version.
PMC Firmware Version	Displays the PMC version.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Processors' BootGuard Capability	Displays the information about Processors' BootGuard Capability.
BootGuard FACB	Displays the BootGuard FACB information.
BootGuard VB	Displays the BootGuard check startup status.
BootGuard MB	Displays the BootGuard measurement startup status.
BootGuard ACM SVN	Displays the BootGuard ACM SVN information.
BootGuard BPM SVN	Displays the BootGuard BPM SVN information.
BootGuard KM SVN	Displays the BootGuard KM SVN information.
BootGuard KM ID	Displays the BootGuard KM ID information.

5.2.2 Peripheral Configuration

On the **Peripheral Configuration** screen, you can configure peripheral devices of the server. Figure 5-5 shows the **Peripheral Configuration** screen. Table 5-4 describes the parameters.

Figure 5-5 Peripheral Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-4 Parameter on the Peripheral Configuration screen

Parameter	Description	Default Value
SR-IOV Setup Settings	Provides access to PCIe SR-IOV configurations.	-
PCIe ARI	Enables or disables ARI of the PCIe card. The menu options are as follows: ● Enabled ● Disabled	Disabled
PCIe ASPM Support (Global)	Sets the PCIe ASPM Support (Global) function. The menu options are as follows: ● **Disabled**: ASPM is disabled. ● **Per individual port**: The I/O of each port is controlled independently. ● L1 Only: Low-power standby mode.	Disabled
Degrade 64-bit PCI MMIO BARs	Provides access to the 64-bit PCI MMIO BARs degradation configurations. For legacy BIOS with Options ROMS, downgrades 64-bit PCI MMIO BARs. The menu options are as follows: ● Enabled ● Disabled	Disabled
SIO 1711	Provides access to the BMC serial port configuration.	-

5.2.2.1 SR-IOV Setup Settings

On the **SR-IOV Setup Settings** screen, you can configure the SR-IOV function. **Figure 5-6** and **Figure 5-7** show the **SR-IOV Setup Settings** screen. **Table 5-5** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-6 SR-IOV Setup Settings screen 1

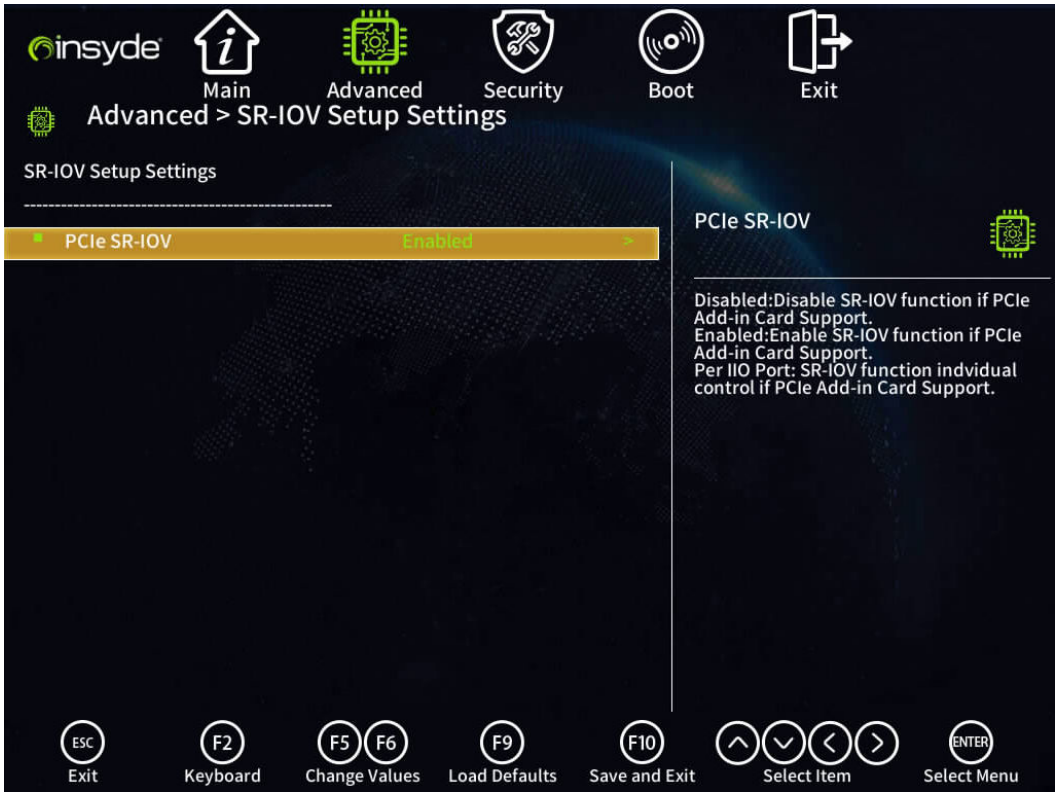
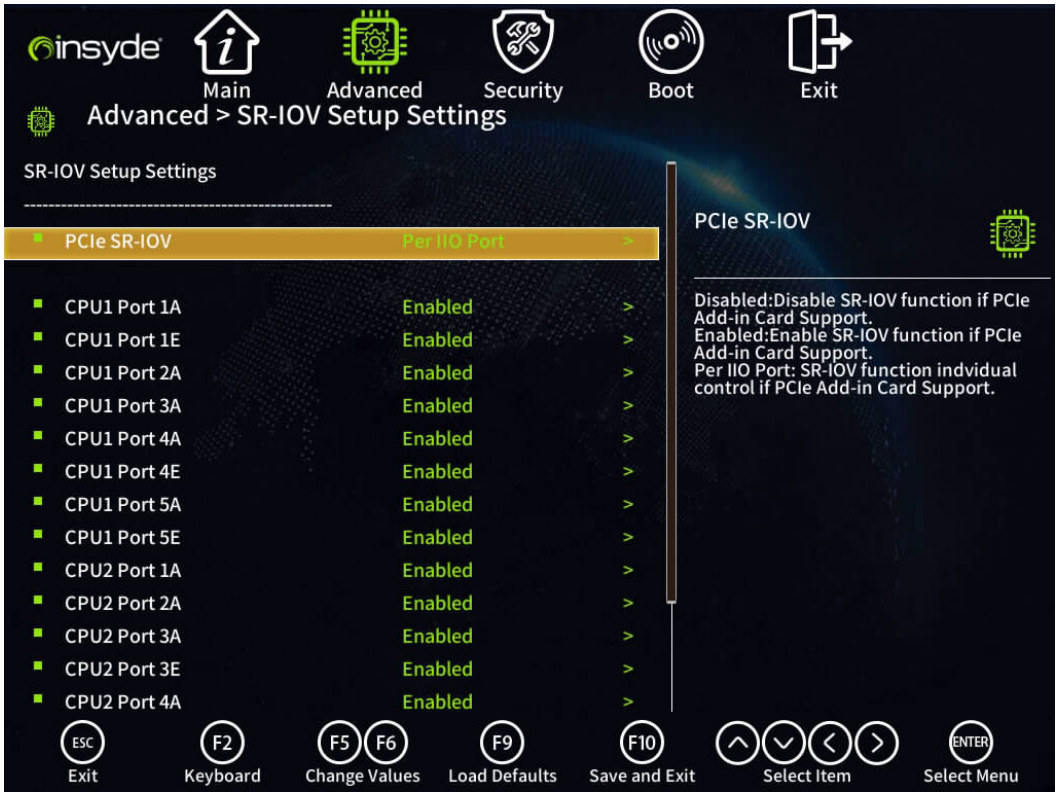


Figure 5-7 SR-IOV Setup Settings screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-5 Parameters on the SR-IOV Setup Settings screen

Parameter	Description	Default Value
PCIe SR-IOV	Provides access to PCIe SR-IOV configurations. The menu options are as follows: ● **Disabled**: If the PCIe card supports SR-IOV, the SR-IOV function is disabled. ● **Enabled**: If the PCIe card supports SR-IOV, the SR-IOV function is enabled. ● **Per IIO Port**: Individually controls the SR-IOV function depending on the I/O SR-IOV option of each I/O port.	Enabled
CPU*X* Port *Y*	Enables or disables the SR-IOV function for port Y of CPUX. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter varies depending on the riser card installed on the server. ● This parameter is available when **PCIe SR-IOV** is set to **Per IIO Port**. ● *X* indicates the physical slot number of the CPU. The value of *X* ranges from 1 to 2; *Y* indicates the port number.	Enabled

5.2.2.2 SIO 1711

On the **SIO 1711** screen, you can configure the BMC serial ports. **Figure 5-8** shows the **SIO 1711** screen. **Table 5-6** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-8 SIO 1711 screen



Table 5-6 Parameters on the SIO 1711 screen

Parameter	Description	Default Value
UART 1	Enables or disables the BMC serial port function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Base I/O Address	Sets the base address of the BMC serial port. The menu options are as follows: ● 2F8 ● 3F8 **NOTE** This parameter is unavailable when **UART 1** is set to **Disabled**.	3F8
Interrupt	Interrupts the BMC serial ports. The menu options are as follows: ● IRQ3 ● IRQ4 **NOTE** This parameter is unavailable when **UART 1** is set to **Disabled**.	IRQ3

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.3 Video Configuration

On the **Video Configuration** screen, you can configure video cards. **Figure 5-9** shows the **Video Configuration** screen. **Table 5-7** describes the parameters.

Figure 5-9 Video Configuration screen

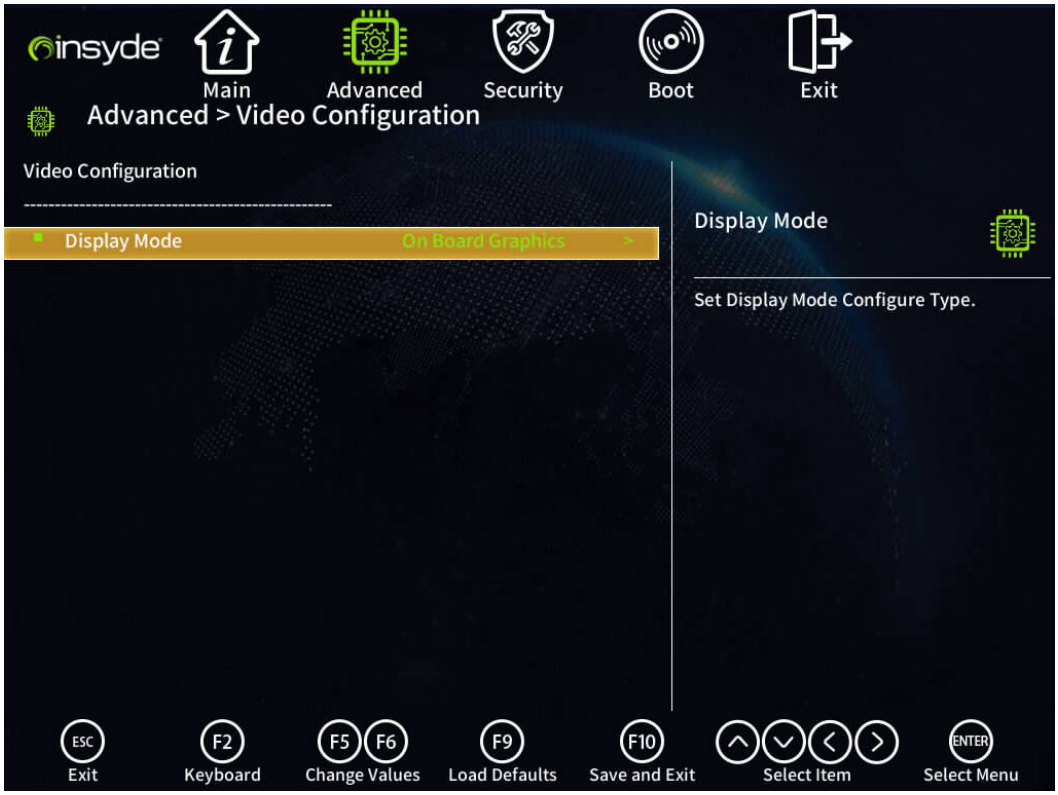


Table 5-7 Parameters on the Video Configuration screen

Parameter	Description	Default Value
Display Mode	Sets the video card mode. The menu options are as follows: • **Plug-in Graphics**: Use a plug-in video card. • **On Board Graphics**: Use an onboard video card.	On Board Graphics

5.2.4 ACPI Table or Features Control

On the **ACPI Table or Features Control** screen, you can configure ACPI tables and table features. **Figure 5-10** shows the **ACPI Table or Features Control** screen. **Table 5-8** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-10 ACPI Table or Features Control screen

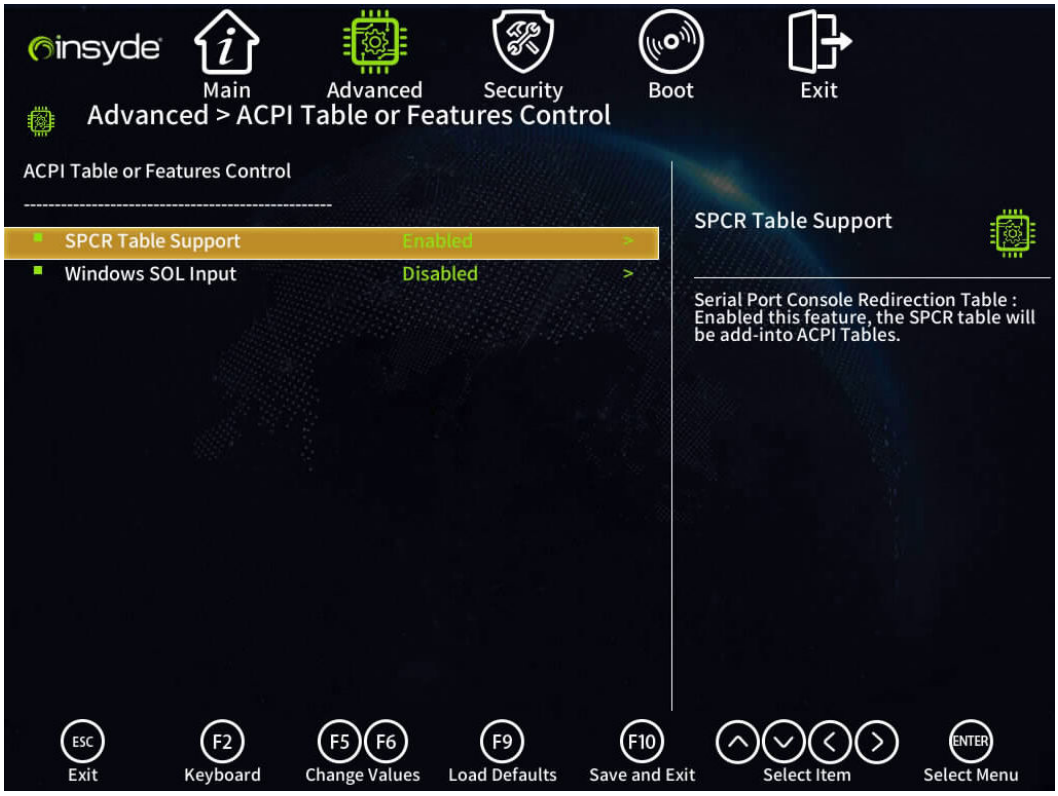


Table 5-8 Parameters on the ACPI Table or Features Control screen

Parameter	Description	Default Value
SPCR Table Support	Sets the SPCR table function. The menu options are as follows: ● **Enabled**: Adds SPCR tables to ACPI tables. ● **Disabled**: Disables this function.	Enabled
Windows SOL Input	Enables or disables redirection input of the serial port in the Windows OS. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **SPCR Table Support** is set to **Disabled**.	Disabled

5.2.5 Misc Configuration

On the **Misc Configuration** screen, you can configure other settings. **Figure 5-11** shows the **Misc Configuration** screen. **Table 5-9** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-11 Misc Configuration screen

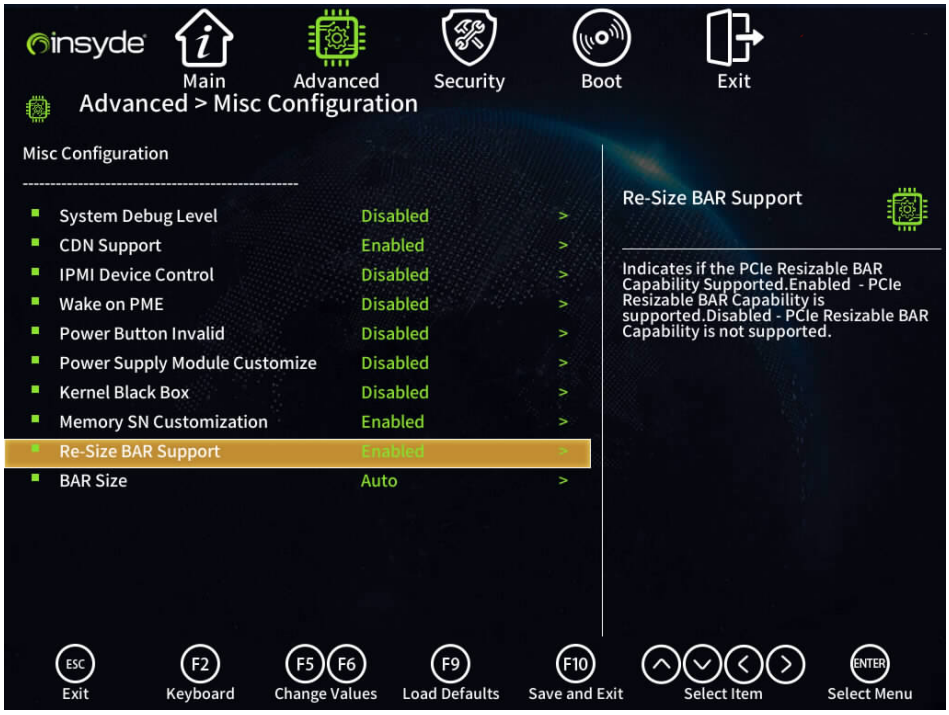


Table 5-9 Parameters on the Misc Configuration screen

Parameter	Description	Default Value
System Debug Level	Enables or disables the system debug level. If you enable the parameter, debug information is printed to serial ports, which increases the system startup time. The menu options are as follows: ● **Disabled**: Minimal debug information is sent in the POST phase, and the system startup time is decreased. ● **Enabled**: All debug information is sent to serial ports in the POST phase, and the system startup time is increased.	Disabled
CDN Support	Enables or disables the function of Consistent Network Device Naming (CDN). The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPMI Device Control	Enables or disables Advanced Configuration and Power Interface (ACPI) reporting on the IPMI device. The menu options are as follows: ● Enabled ● Disabled	Disabled
Wake on PME	Enables or disables the Wake on Power Management Event (PME) function. The menu options are as follows: ● Enabled ● Disabled	Disabled
Power Button Invalid	Enables or disables the function of powering off the server through the power button, which does not affect Forced Power Off (Power Button Override Function). The menu options are as follows: ● Enabled ● Disabled	Disabled
Power Supply Module Customize	Enables or disables the display of the power supply model in the power supply module part number. The menu options are as follows: ● Enabled ● Disabled	Disabled
Memory SN Customization	Enables or disables the memory serial number customization function. The menu options are as follows: ● Enabled ● Disabled **NOTE** Only BIOS 01.01.08.03 and later versions support this parameter.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Re-Size BAR Support	Enables or disables the PCIe resizable BAR capability supported. The options are as follows: ● Disabled ● Enabled **NOTE** Only BIOS 01.01.08.08 and later versions support this parameter.	Disabled
BAR Size	Choose the BAR size for the PCIe device. **Auto** means max of Re-size BAR supported each PCIe Device. This option will not take effect if the PCIe card does not support the Resizable BAR feature. The options are as follows: ● Auto ● 8G ● 16G ● 32G ● 64G **NOTE** ● This parameter is available when **Re-Size BAR Support** is set to **Enabled**. ● Only BIOS 01.01.08.08 and later versions support this parameter.	Auto

5.2.6 System Event Log

On the **System Event Log** screen, you can configure the event log function, including system error logging and system memory poisoning configuration. **Figure 5-12** shows the **System Event Log** screen. **Table 5-10** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-12 System Event Log screen



Table 5-10 Parameters on the System Event Log screen

Parameter	Description	Default Value
System Errors	Enables or disables the function of recording system errors. After enabling this function, both correctable and uncorrectable errors can be reported to BMC and OS. The menu options are as follows: ● Auto ● Enabled: Enable the System Errors function. ● Disabled: Disable the System Errors function.	Enabled
RAS Log Level	Sets the RAS log level. The menu options are as follows: ● None ● MIN (BASIC_FLOW) ● MID (BASIC_FLOW, FUNC_FLOW) ● MAX (BASIC_FLOW, FUNC_FLOW, REG)	MIN (BASIC_FLOW)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
System Memory Poisoning	Enables or disables the memory poisoning function. After this function is enabled, a detected error is tagged as poisoned and an interrupt will not be triggered until the error data is used. The options are as follows: ● Enabled ● Disabled	Enabled
FDM	Enables or disables the Fault Diagnosis Management (FDM) function. The FDM provides automatic troubleshooting capabilities covering the entire system, including fault data collection, fault data analysis, and fault diagnosis and location. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **System Errors** is set to **Disabled** or **Auto**.	Enabled
CE Record	Enables or disables the CE record. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **System Errors** is set to **Disabled** or **Auto**.	Disabled
Memory CE Record	Enables or disables the memory CE record. The options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is available when **CE Record** is set to **Enabled**. ● Only BIOS 01.01.06.13 and later versions support this parameter.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe CE Record	Enables or disables the PCIe CE record. The options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is available when **CE Record** is set to **Enabled**. ● Only BIOS 01.01.06.13 and later versions support this parameter.	Enabled
Error Data Revison	Compatible error data version. The menu options are as follows: ● 0x201 ● 0x300	0x201
Viral Status	Enables or disables the virus status. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **System Errors** and **System Memory Poisoning** are set to **Enabled**.	Disabled
Clear Viral Status	Enables or disables the function of clearing virus status. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **System Errors** and **Viral Status** are set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
System Cloaking	Enables or disables the system cloaking function. When enabled, Corrected and Uncorrected No Action Required (UCNA) errors are masked from OS/SW visibility. The menu options are as follows: ● Enabled: Corrected and Uncorrected No Action Required (UCNA) errors are masked from OS/SW visibility. ● Disabled: Disable the System Cloaking feature. **NOTE** ● This parameter is available when **System Errors** is set to **Enabled**. ● BIOS 01.01.03.06 and later versions support this parameter.	Disabled
eMCA Settings	Enhanced Machine Check Architecture (eMCA), a CPU MCBank setting menu where you can set the MCBank fault reporting and CMCI-SMI morphing functions. **NOTE** This parameter is available when **System Errors** is set to **Enabled** or **Auto**.	-
WHEA Settings	Windows Hardware Error Architecture (WHEA), a framework setting menu where you can send, process, and record hardware errors. **NOTE** This parameter is available when **System Errors** is set to **Enabled** or **Auto**.	-
Error Injection Settings	Provides access to the menu for setting the error injection function. **NOTE** This parameter is available when **System Errors** is set to **Enabled** or **Auto**.	-
Memory Error Enabling	Provides access to memory error configurations. **NOTE** This parameter is available when **System Errors** is set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IIO Error Enabling	Provides access to I/O error configurations. **NOTE** This parameter is available when **System Errors** is set to **Enabled**.	-
PCIe Error Enabling	Provides access to PCIe error configurations. **NOTE** This parameter is available when **System Errors** is set to **Enabled**.	-
Error Control Setting	Provides access to patrol scrub error type configurations. **NOTE** This parameter is available when **System Errors** is set to **Enabled**.	-
DWR Configuration	Provides access to the menu for setting the Dirty Warm Reset (DWR) function.	-

5.2.6.1 eMCA Setttings

On the **eMCA Settings** screen, you can configure eMCA. **Figure 5-13** shows the **eMCA Settings** screen. **Table 5-11** describes the parameters.

Figure 5-13 eMCA Settings screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-11 Parameters on the eMCA Settings screen

Parameter	Description	Default Value
eMCA Logging Support	Enables or disables the Enhanced Machine Check Architecture (eMCA) logging function. After this function is enabled, an area in the memory is allocated to store the MCBank register information and error DIMM information for the OS to access. However, after this function is enabled, uncorrectable errors can trigger SMIs. The options are as follows: ● Enabled ● Disabled	Enabled
LMCE Support	Enables or disables the Local Machine Check Exception (LMCE) firmware support. After the LMCE function is enabled, it supports delivering Software Recoverable Action Required (SRAR, which requires software to perform recovery operations) type UCR (uncorrectable recoverable) error reporting events only to the affected logical processor without global participation. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **System Memory Poisoning** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
eMCA CMCI-SMI Morphing	Enables or disables the eMCA CMCI-SMI mapping. After this function is enabled, the SMI is triggered each time a correctable error occurs. If the number of correctable errors on the MCBank exceeds the threshold, SMI is triggered, but CMCI is not triggered. The options are as follows: ● eMCA Gen 2 CSMI: Configure **EMCA CMCI-SMI Morphing** to **EMCA gen 2 CSMI** mode. ● Disabled: Disable EMCA CMCI-SMI Morphing. **NOTE** This parameter is unavailable when **eMCA Logging Support** is set to **Disabled**.	eMCA Gen 2 CSMI
Opportunistic Spare Core	Enables or disables the opportunity spare core. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **eMCA Logging Support** is set to **Disabled**.	Disabled

5.2.6.2 WHEA Setttings

On the **WHEA Settings** screen, you can configure WHEA. **Figure 5-14** shows the **WHEA Settings** screen. **Table 5-12** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-14 WHEA Settings screen

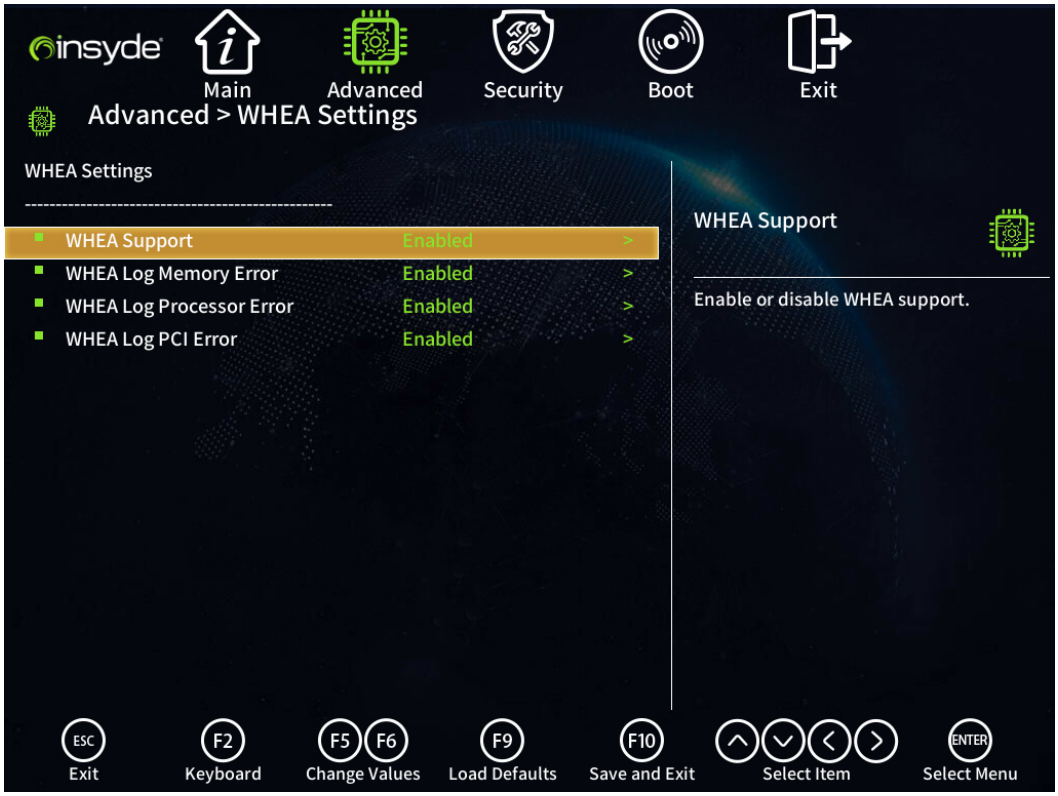


Table 5-12 Parameters on the WHEA Settings screen

Parameter	Description	Default Value
WHEA Support	Enables or disables the Windows Hardware Error Architecture (WHEA) function. WHEA provides rich hardware error reports for running servers, helping maintenance personnel locate hardware faults and shortening the average recovery time caused by hardware faults. The options are as follows: ● Enabled ● Disabled	Enabled
Whea Log Memory Error	Enables or disables the WHEA log memory error function. The options are as follows: ● Enabled ● Disabled **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	Enabled

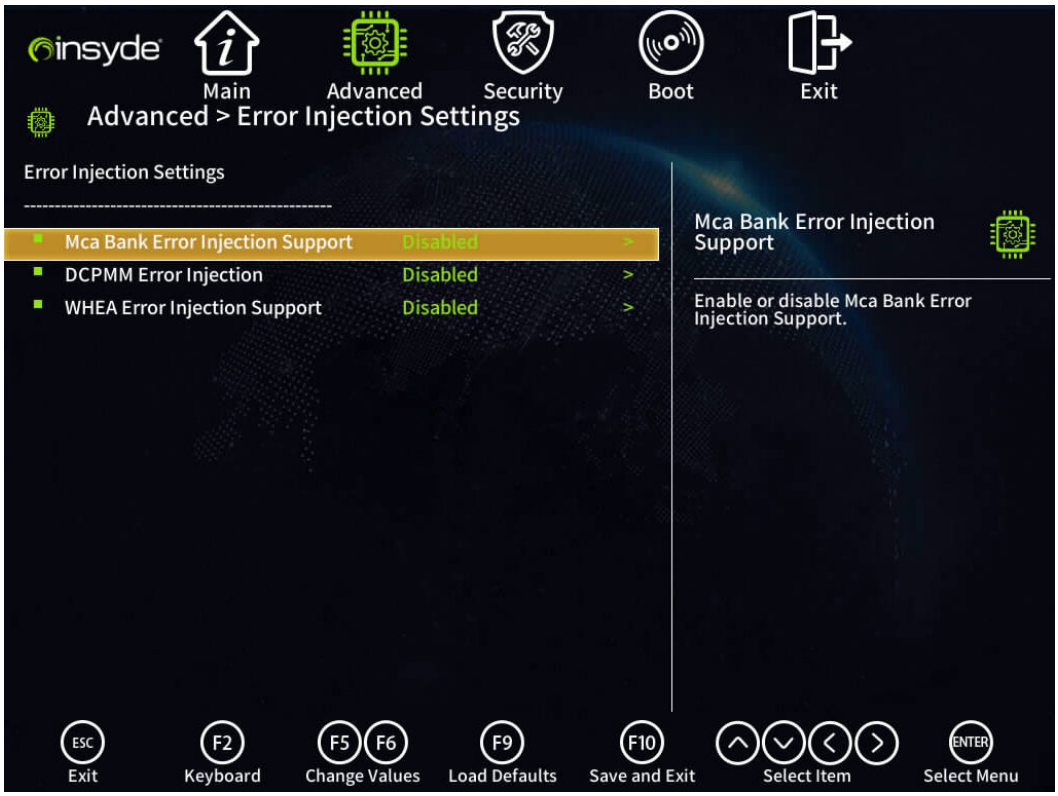
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Whea Log Processor Error	Enables or disables the WHEA log processor error function. The options are as follows: ● Enabled ● Disabled **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	Enabled
Whea Log PCI Error	Enables or disables the WHEA log PCI error function. The options are as follows: ● Enabled ● Disabled **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	Enabled

5.2.6.3 Error Injection Settings

On the **Error Injection Settings** screen, you can configure the error injection function. **Figure 5-15** shows the Error Injection Settings screen. **Table 5-13** describes the parameters.

Figure 5-15 Error Injection Settings screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-13 Parameters on the Error Injection Settings screen

Parameter	Description	Default Value
Mca Bank Error Injection Support	Enables or disables the Mca Bank error injection support function. The menu options are as follows: ● Enabled ● Disabled	Disabled
DCPMM Error Injection	Enables or disables the DCPMM error injection function. The menu options are as follows: ● Enabled ● Disabled	Disabled
WHEA Error Injection Support	Enables or disables the WHEA error injection support function. The menu options are as follows: ● Enabled ● Disabled	Disabled
WHEA Error Injection 5.0 Extension	Enables or disables the WHEA error injection 5.0 extension function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **WHEA Error Injection Support** is set to **Enabled**.	Enabled
WHEA PCIe Error Injection Support	Enables or disables the WHEA PCIe error injection support function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **WHEA Error Injection Support** is set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
WHEA PCIe Error Injection Action Table	Enables or disables the WHEA PCIe error injection operation table. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **WHEA Error Injection Support** is set to **Enabled**.	Disabled
ME Seg Error Injection Support	Enables or disables the ME Seg error injection support function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is available when **WHEA Error Injection Support** is set to **Enabled**. ● BIOS 01.01.03.06 and later versions support this parameter.	Disabled

5.2.6.4 Memory Error Enabling

On the **Memory Error Enabling** screen, you can configure the memory error function. **Figure 5-16** shows the **Memory Error Enabling** screen. **Table 5-14** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-16 Memory Error Enabling screen



Table 5-14 Parameters on the Memory Error Enabling screen

Parameter	Description	Default Value
PFD	Enables or disables the permanent fault detection (PFD) function. The PFD function identifies hard faults from faults. The value **Auto** indicates that PFD is dynamically enabled based on the system configuration. The menu options are as follows: ● Enabled ● Disabled ● Auto	Auto
PMem CTLR Errors	Enables or disables PMem CTLR error reporting and logging. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PMem CTLR Low Priority Error Signaling	Sets the signal selection function for PMem CTLR low-priority errors. The menu options are as follows: ● Disabled ● SMI ● ERR0# Pin	SMI
PMem CTLR High Priority Error Signaling	Sets the signal selection function for PMem CTLR high-priority errors. The menu options are as follows: ● Disabled ● SMI ● ERR0# Pin	SMI
Set PMem Address Range Scrub	Enables or disables the physical address range inspection for PMem DIMMs. The menu options are as follows: ● Enabled ● Disabled	Disabled

5.2.6.5 IIO Error Enabling

On the **IIO Error Enabling** screen, you can configure the I/O error function. **Figure 5-17** shows the **IIO Error Enabling** screen. **Table 5-15** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-17 IIO Error Enabling screen

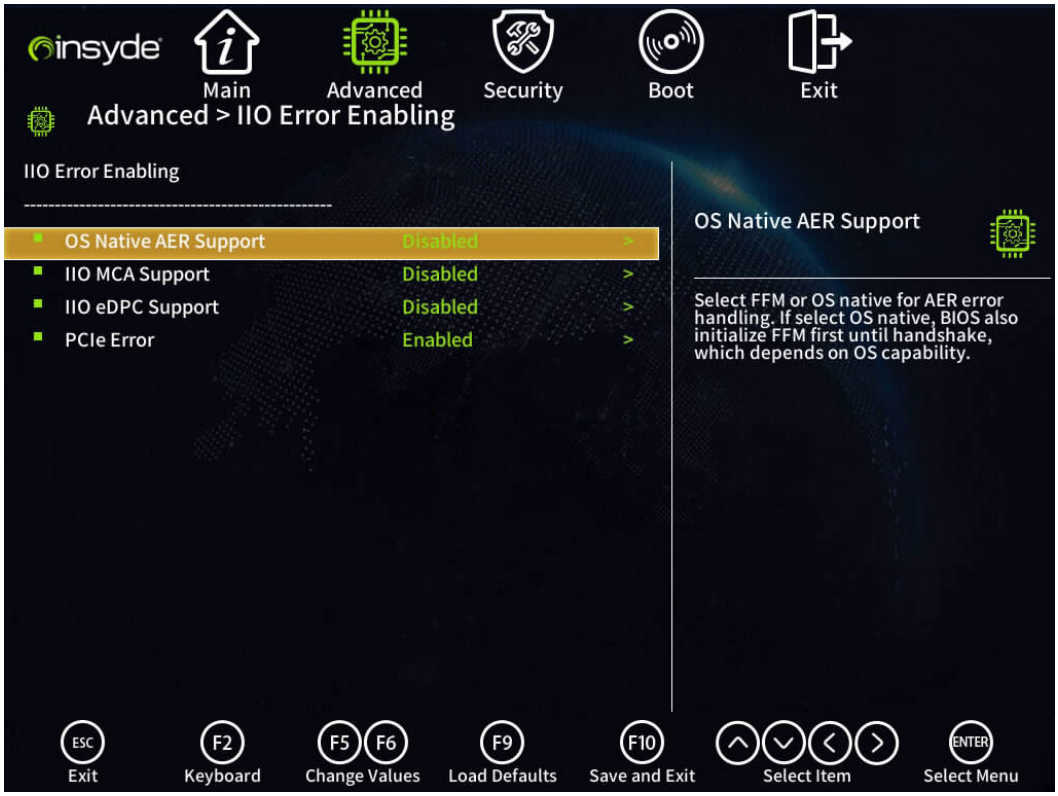


Table 5-15 Parameters on the IIO Error Enabling screen

Parameter	Description	Default Value
OS Native AER Support	Enables or disables the advanced error reporting (AER) function controlled by the OS. By default, the BIOS firmware preferentially controls AER errors. To enable the OS to control AER errors, set this parameter to **Enabled**. The options are as follows: ● **Enabled**: The OS can control AER error handling. ● **Disabled**: The firmware can control AER error handling.	Disabled
IIO MCA Support	Enables or disables the I/O MCA support function. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IIO eDPC Support	Sets the I/O eDPC support function. The menu options are as follows: ● **Enabled**: Enables this function. ● **Disabled**: Disables this function. ● **On Fatal and Non-Fatal Errors**: Enables this function when fatal errors and non-fatal errors occur.	Disabled
IIO eDPC Interrupt	Enables or disables the I/O eDPC interrupt function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Disabled **NOTE** For BIOS versions earlier than 01.01.06.03 it is **Enabled** by default.
IIO eDPC ERR_COR Message	Enables or disables the I/O eDPC ERR_COR function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Enabled
PCIe Poison TLP Egress Blocking	Enables or disables the PCIe Poison TLP egress blocking function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Enabled
PCIe Error	Enables or disables PCIe error detection. The menu options are as follows: ● Enabled ● Disabled	Enabled

5.2.6.6 PCIe Error Enabling

On the **PCIe Error Enabling** screen, you can configure the PCIe error function. **Figure 5-18** shows the **PCIe Error Enabling** screen. **Table 5-16** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-18 PCIe Error Enabling screen

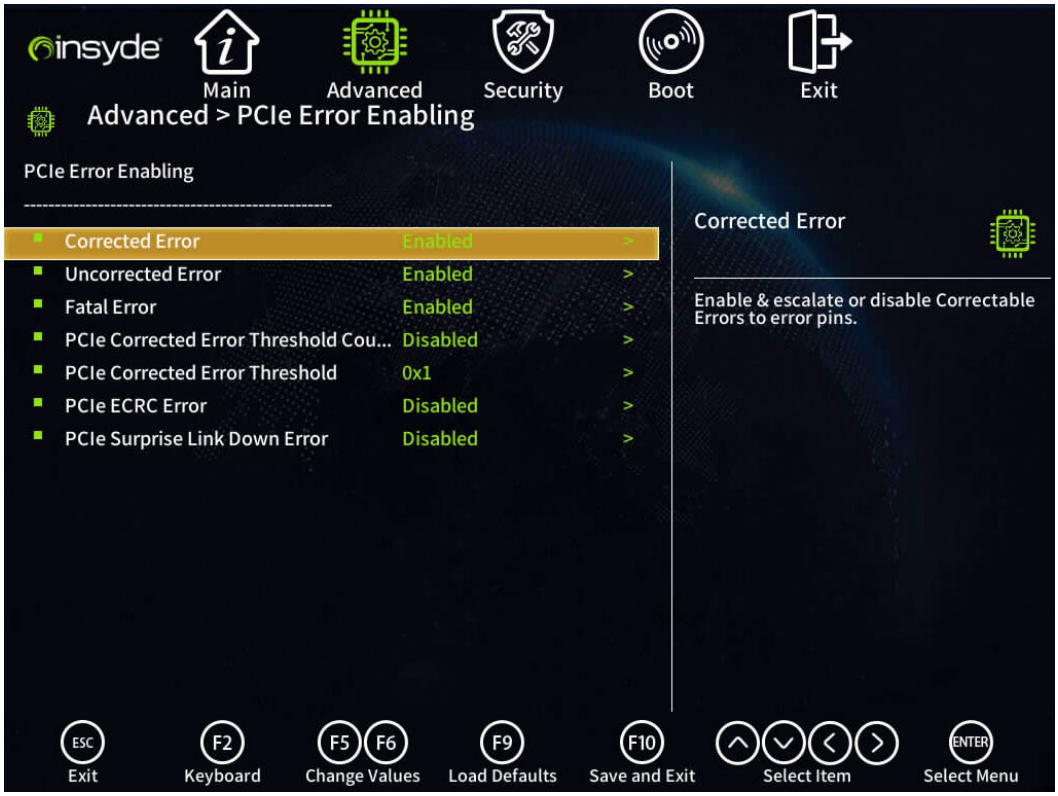


Table 5-16 Parameters on the PCIe Error Enabling screen

Parameter	Description	Default Value
Corrected Error	Enables or disables the PCIe correctable error detection. The menu options are as follows: ● Enabled ● Disabled	Enabled
Uncorrected Error	Enables or disables the PCIe uncorrectable error detection. The menu options are as follows: ● Enabled ● Disabled	Enabled
Fatal Error	Enables or disables the PCIe fatal error detection. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Corrected Error Threshold Counter	Enables or disables the PCIe correction error threshold counter. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **Corrected Error** is set to **Disabled**.	Disabled
PCIe Corrected Error Threshold	Sets the PCIe correction error threshold. The value ranges from 0 to 0xFFFFFFFF. **NOTE** This parameter is unavailable when **Corrected Error** is set to **Disabled**.	0x1
PCIe ECRC Error	Enables or disables the PCIe ECRC error function. The menu options are as follows: ● Enabled ● Disabled	Disabled
PCIe Surprise Link Down Error	Enables or disables unexpected PCIe link disconnection. The options are as follows: ● Enabled ● Disabled	Disabled

5.2.6.7 Error Control Setting

On the **Error Control Setting** screen, you can select the patrol scrub error type. **Figure 5-19** shows the **Error Control Setting** screen. **Table 5-17** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-19 Error Control Setting screen

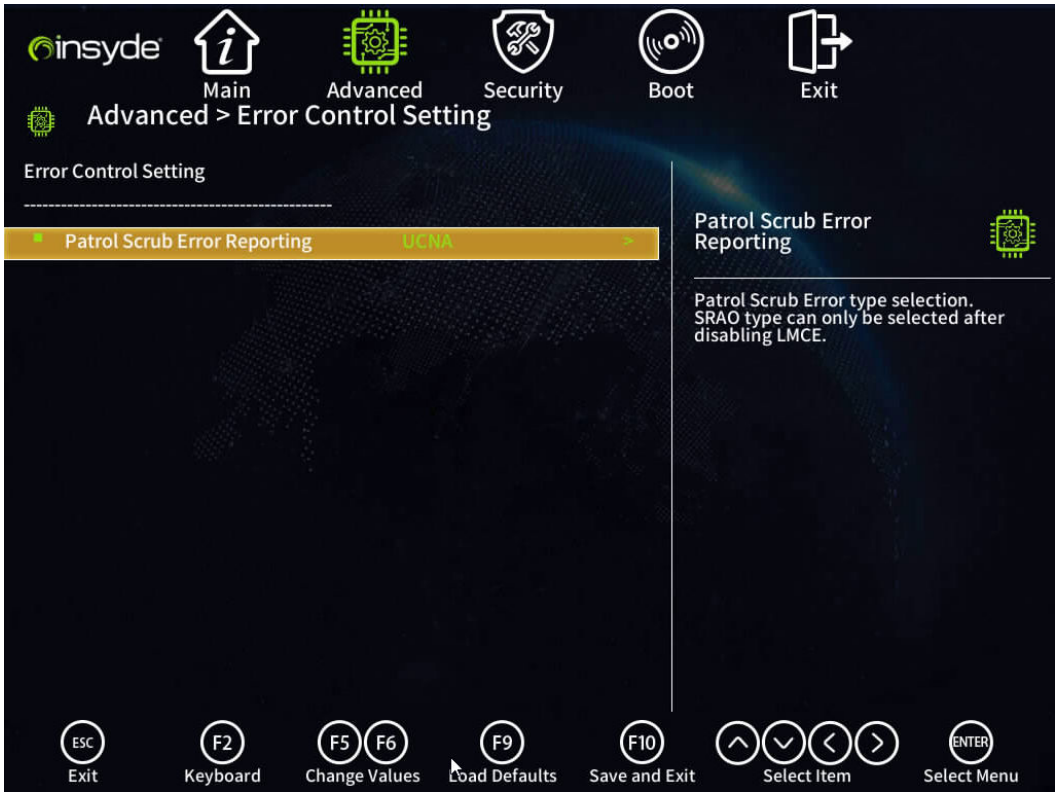


Table 5-17 Parameters on the Error Control Setting screen

Parameter	Description	Default Value
Patrol Scrub Error Reporting	Allows you to select the patrol scrub error type. The menu options are as follows: • UCNA • SRAO **NOTE** The **SRAO** option is available when **LCE Support** is set to **Disabled**.	UCNA

5.2.6.8 DWR Configuration

On the **DWR Configuration** screen, you can configure the dirty warm reset (DWR) function. Figure 5-20 shows the **DWR Configuration** screen. Table 5-18 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-20 DWR Configuration screen

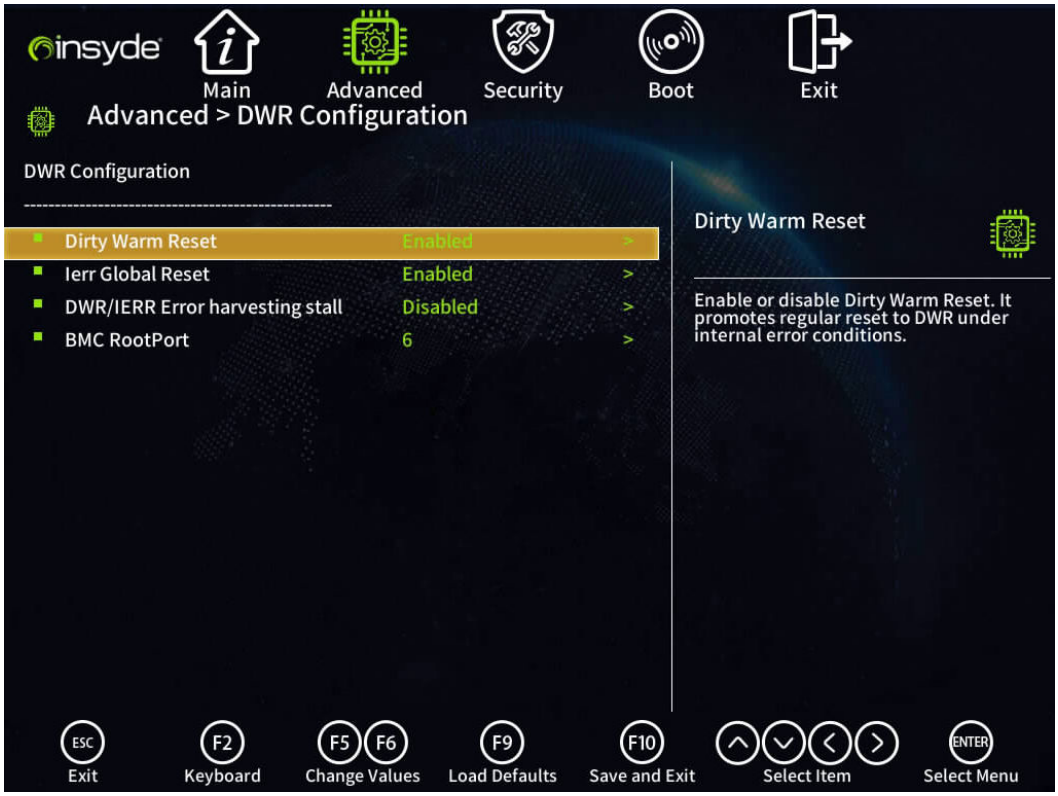


Table 5-18 Parameters on the DWR Configuration screen

Parameter	Description	Default Value
Dirty Warm Reset	Enables or disables the DWR function. The function promotes regular resets of DWR under internal error conditions. The menu options are as follows: ● Enabled ● Disabled	Enabled
Ierr Global Reset	Enables or disables the global IERR reset function. The menu options are as follows: ● Enabled ● Disabled	Enabled

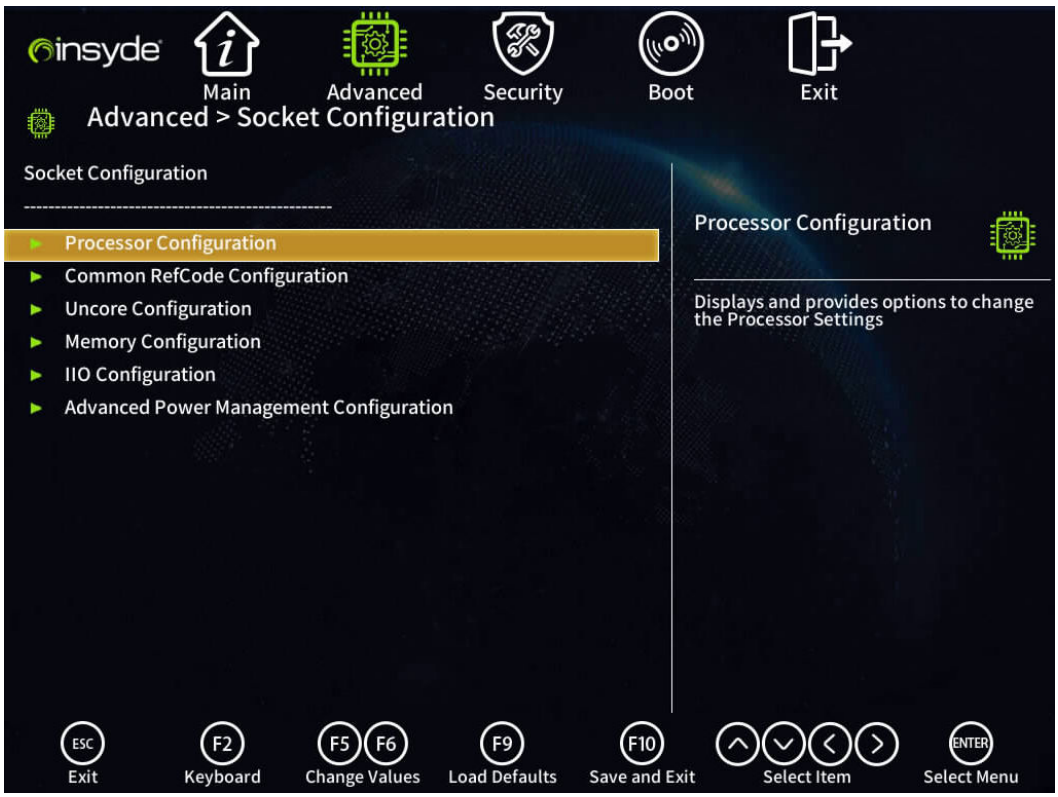
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DWR/IERR Error harvesting stall	Enables or disables the DWR/IERR Error harvesting stall function. When it is enabled, the system enters a spin loop during the DWR, allowing manual error collection. The menu options are as follows: ● Enabled ● Disabled	Disabled
BMC RootPort	Sets the BMC root port. The menu options are as follows: ● 6 ● 12	6

5.2.7 Socket Configuration

On the **Socket Configuration** screen, you can configure CPU-related features. Figure 5-21 shows the **Socket Configuration** screen. Table 5-19 describes the parameters.

Figure 5-21 Socket Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-19 Parameter on the Peripheral Configuration screen

Parameter	Description
Processor Configuration	Provides access to the processor CFR configurations.
Common RefCode Configuration	Provides access to Common RefCode configurations.
Uncore Configuration	Provides access to uncore configurations.
Memory Configuration	Provides access to memory configurations.
IIO Configuration	Provides access to I/O configurations.
Advanced Power Management Configuration	Provides access to advanced power management configurations.

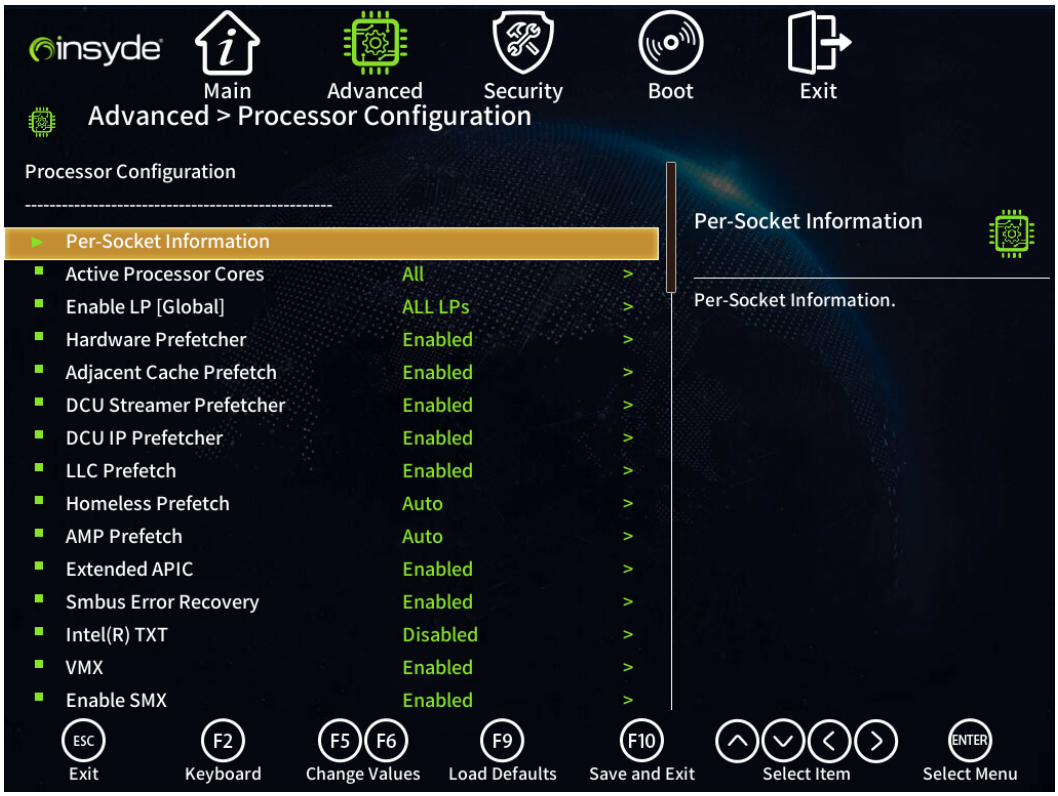
5.2.7.1 Processor Configuration

On the **Processor Configuration** screen, you can configure processors. **Figure 5-22** and **Figure 5-23** show the **Processor Configuration** screen. **Table 5-20** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

Figure 5-22 Processor Configuration screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-23 Processor Configuration screen 2

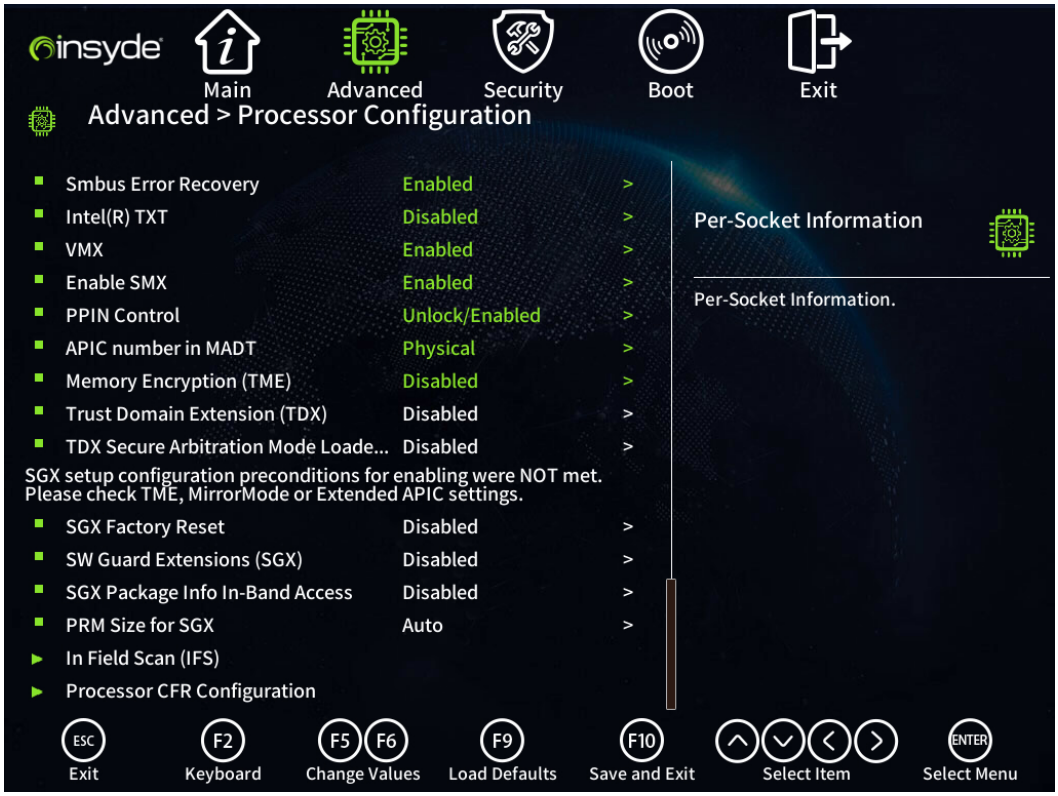


Table 5-20 Parameter on the Processor Configuration screen

Parameter	Description	Default Value
Per-Socket Information	Queries detailed CPU configurations in the current environment.	-
Active Processor Cores	Sets the number of physical cores for each CPU to be used. The value can be **All**, **1**, or **2** to *N*-1 (*N* indicates the maximum number of physical CPU cores supported by the CPU).	All

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Enable LP [Global]	Enables or disables the hyper-threading function of the Intel processor. If this function is enabled, each physical processor core functions as two logical processor cores. If this function is disabled, each physical processor core functions as only one logical processor core. Enabling this function can improve the overall application performance. The options are as follows: ● **ALL LPs**: When **All LPs** is enabled, each physical processor core is equivalent to two logical processor cores, thereby increasing the processor core count and improving overall application performance. ● **Single LP**: Enables only a single logical processor, making each physical processor core equivalent to only one logical processor core.	ALL LPs
Hardware Prefetcher	Enables or disables the hardware prefetcher function. This function enables the hardware prefetching function of CPU. If this function is enabled, the CPU prefetches instructions or data from the memory to the L2 cache before processing the instructions or data. This function helps reduce the memory access time and eliminate potential bottlenecks, therefore improving system efficiency. If this function is disabled, performance of some workloads can be improved. Decide whether to enable this function based on the results of benchmark tests. The options are as follows: ● **Enabled**: Enables the Hardware Prefetcher function. ● **Disabled**: Disables the Hardware Prefetcher function.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Adjacent Cache Prefetch	Enables or disables the adjacent cache prefetch function. If this function is enabled, the system intelligently reads the adjacent data in advance, thereby improving the read speed. Enabling this function can improve the performance if the application accesses memory in sequence. Disable this option when the application accesses memory randomly. The options are as follows: ● **Enabled**: Enables proximity cache prefetching. ● **Disabled**: Disables proximity cache prefetching.	Enabled
DCU Streamer Prefetcher	Enables or disables the data cache unit (DCU) streamer prefetching function. In most scenarios, enabling this function can achieve optimal performance. In some high-load scenarios, disabling this option may improve performance. Decide whether to enable this function based on the results of benchmark tests. The options are as follows: ● **Enabled**: Enables DCU Streamer Prefetcher, which prefetches streams and sends them to its L1 cache to improve data processing and system performance. ● **Disabled**: Disables DCU Streamer Prefetcher.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DCU IP Prefetcher	Enables or disables the data cache unit (DCU) IP prefetching function. In most scenarios, enabling this function can achieve optimal performance. In some high-load scenarios, disabling this option may improve performance. Decide whether to enable this function based on the results of benchmark tests. The options are as follows: ● **Enabled**: Enables DCU IP prefetching, which prefetches IP addresses to improve network connectivity and system performance. ● **Disabled**: Disables DCU IP prefetching.	Enabled
LLC Prefetch	Enables or disables the L3 cache prefetch feature. The menu options are as follows: ● **Enabled** ● **Disabled**	Enabled
Homeless Prefetch	Enables or disables Homeless Prefetch on all threads. Homeless cache prefetching, when there are insufficient resources to track requests in the L1 cache, Homeless Prefetch allows requests that miss to be pre-fetched into the mid-level cache. The menu options are as follows: ● **Enabled**: Enables Homeless cache prefetching. ● **Disabled**: Disables Homeless cache prefetching. ● **Auto**: Automatically configured based on hardware.	Auto
DCU Mode	Selects the data cache unit (DCU) mode, which can be used to enable the level-1 cache error correction function. The options are as follows: ● **Normal** ● **Mirror-Mode**	Normal

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
L1 Next Page Prefetcher	Enables or disables the next page prefetcher feature of the L1 cache. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when the CPU model is **SierraForest**.	Enabled
AMP Prefetch	Enables or disables the MLC AMP Prefetch feature. The menu options are as follows: ● **Enabled** ● **Disabled** ● Auto **NOTE** Only BIOS version 01.01.03.05 and later supports the Auto option.	Auto **NOTE** The default value for BIOS versions 01.01.02.08 and earlier is Disabled.
Extended APIC	Enables or disables the extended advanced programmable interrupt controller (APIC) feature. If the total number of CPU cores exceeds 256, enable this option to enable the OS to support the CPU multi-core feature more efficiently. The options are as follows: ● **Enabled**: Enables Extended APIC mode. ● **Disabled**: Disables Extended APIC mode. **NOTE** ● When the total number of active processor cores in the system is greater than 255, the BIOS will force enables x2APIC even if **Extended APIC** is set to **Disabled**.	Enabled
Smbus Error Recovery	Enables or disables the SMBus error recovery function. The menu options are as follows: ● **Enabled** ● **Disabled**	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Intel (R) TXT	Enables or disables the Intel TXT function. The menu options are as follows: ● **Enabled**: Enables support for Intel Trusted Execution Technology, fully protecting data security in virtualized computing environments. ● **Disabled**: Disables support for Intel Trusted Execution Technology.	Disabled
VMX	Enables or disables the CPU virtualization function. If this function is enabled, the virtualization layer or OS that supports this function can use the hardware capabilities of the Intel virtualization technology. For some virtualization layers that do not support this function directly, Intel virtualization technology needs to be enabled for them. If you do not use the virtualization layer or OS that supports this function, you can also enable this option. The options are as follows: ● **Enabled**: Enables the Hardware Prefetcher function. ● **Disabled**: Enables the Hardware Prefetcher function. **NOTE** When **Intel (R) TXT** is set to **Enabled**, **VMX** is **Enabled** and unavailable.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Enable SMX	Enables or disables the Safer Mode Extensions (SMX) function. SMX provides a programmable interface to the operating system to establish a measurable environment that provides a trusted environment for users. The options are as follows: ● Enabled: Enables Intel CPU virtualization technology to improve server hardware resource utilization. ● Disabled: Disables Intel CPU virtualization technology. **NOTE** ● This parameter is unavailable when **Intel(R) TXT** is set to **Enabled**. ● Only BIOS 01.01.03.13 and later versions support this parameter.	Enabled
PPIN Control	PPIN control function enabling switch. The menu options are as follows: ● Unlock/Enable: Enables the PPIN control function. ● Lock/Disable: Disables the PPIN control function.	Unlock/Enable
APIC number in MADT	Sets whether the values of local APICs or X2APICs that are physically enabled is reported or the maximum number of supported local APICs or X2APICs is reported in the MADT. The menu options are as follows: ● Physical ● Maximum	Physical
Memory Encryption (TME)	Enables or disables the Total Memory Encryption (TME) function. The options are as follows: ● **Enabled** ● **Disabled** **NOTE** When the parameter is set to **Disabled**, the BIOS disables both the TME and MK-TME technologies.	**Disabled**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Total Memory Encryption (TME) Bypass	Enables or disables the Total Memory Encryption (TME) Bypass function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **Memory Encryption (TME)** is set to **Enabled**.	**Disabled**
Total Memory Encryption Multi-Tenant (TME-MT)	Enables or disables the TME-MT function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** ● This parameter is available when **Memory Encryption (TME)** is set to **Enabled**. ● This parameter is configurable only when **Limit CPU PA to 46 bits** is set to **Disabled** in the **Socket Configuration > Uncore Configuration > Uncore General Configuration**.	**Disabled**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value

Memory integrity	Enables or disables the TME-MT integrity function. The menu options are as follows:
	● Enabled
	● Disabled
	NOTE
	● Only BIOS 01.01.03.16 and later versions support this parameter.
	● This parameter is available under the following conditions:
	  ● The CPU model is Emerald Rapids.
	  ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC.
	  ● **Memory Encryption (TME)** is set to **Enabled**.
	● This parameter is configurable under the following condition: **Limit CPU PA to 46 bits** is set to **Disabled** in the **Socket Configuration > Uncore Configuration > Uncore General Configuration**.
		Disabled

Key stock amount	Displays the amount of key stock. **NOTE** This parameter is available when **Memory Encryption (TME)** is set to **Enabled**.	-
TME-MT key ID bits	Displays the number of bits in the TME-MT key ID. **NOTE** This parameter is available when **Memory Encryption (TME)** is set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Trust Domain Extension (TDX)	Enables or disables the Trust Domain Extension (TDX) function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is configurable under the following conditions: ● The CPU model is Emerald Rapids. ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC. ● **Total Memory Encryption Multi-Tenant (TME-MT)** is set to **Enabled**. ● The BIOS version is 01.01.03.16 or later.	**Disabled**
TDX Secure Arbitration Mode Loader (SEAM Loader)	Enables or disables the TDX Secure Arbitration Mode Loader (SEAM Loader) function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable under the following conditions: ● The CPU model is Emerald Rapids. ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC. ● **Total Memory Encryption Multi-Tenant (TME-MT)** is set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Disable excluding Mem below 1MB in CMR	Enables or disables the function to include memory region below 1 MB in the Convertible Memory Range (CMR). The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable when **Trust Domain Extension (TDX)** is set to **Enabled**.	Auto
TME-MT/TDX key split	Sets the number of bits used by TDX in the TME-MT/TDX key split, and the rest of bits will be used by TME-MT. The value ranges from 1 to 0x7. **NOTE** This parameter is configurable when **Trust Domain Extension (TDX)** is set to **Enabled**.	1
TME-MT Keys	Displays the number of TME-MT keys. **NOTE** This parameter is available when **Memory Encryption (TME)** is set to **Enabled** and **Trust Domain Extension (TDX)** is set to **Enabled**.	0x0
TDX keys:	Displays the number of keys specified for TDX. **NOTE** This parameter is available when **Total Memory Encryption Multi-Tenant (TME-MT)** and **Trust Domain Extension (TDX)** are set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PRM Size	Sets the total PRM size. The menu options are as follows: ● **No valid PRMRR size** ● **128M** ● **256M** ● **512M** ● **1G** ● **2G** ● **4G** ● **8G** ● **16 G** ● **32G** ● **64G** ● **128G** ● **256G** ● **512G** **NOTE** This parameter is available when the CPU model is Sapphire Rapids.	**256M**
SGX Factory Reset	Enables or disables the function of restoring factory settings of the SGX function. The options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **Total Memory Encryption (TME)** is set to **Enabled**.	**Disabled**
SW Guard Extensions (SGX)	Enables or disables the SGX function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **Total Memory Encryption (TME)** is set to **Enabled**.	**Disabled**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SGX Package Info In-Band Access	Enables or disables the SGX Package Info In-Band Access function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **Total Memory Encryption (TME)** is set to **Enabled**.	**Disabled**
PRM Size for SGX	Sets the SGX PRM size. The menu options are as follows: ● **Auto** ● **No valid PRMRR size** ● **128M** ● **256M** ● **512M** ● **1G** ● **2G** ● **4G** ● **8G** ● **16 G** ● **32G** ● **64G** ● **128G** ● **256G** ● **512G**	**256M**
SGX QoS	Enables or disables the SGX quality of service (QoS). The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	**Enabled**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Select Owner EPOCH input type	Selects the owner EPOCH input type. The menu options are as follows: ● **SGX Owner EPOCH activated** ● **Change to New Random Owner EPOCHs** ● **Manual User Defined Owner EPOCHs** **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	Manual User Defined Owner EPOCHs
Software Guard Extensions Epoch 0	Sets the software guard extension Epoch 0. The value ranges from **0** to **0xFFFFFFFFFFFFFFFF**. **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	0
Software Guard Extensions Epoch 1	Sets the software guard extension Epoch 1. The value ranges from **0** to **0xFFFFFFFFFFFFFFFF**. **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	0
SGXLEPUBKEYHASHx Write Enable	Sets whether to allow OS/SW to write to the SGXLEPUBKEYHASH[0~3]. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	**Enabled**
SGXLEPUBKEYHASH0	Sets the bytes from 0 to 7 for SGX Launch Enclave Public Key Hash. The value ranges from 0 to 0xFFFFFFFFFFFFFFFF. **NOTE** This parameter is available when **SGXLEPUBKEYHASHx Write Enable** is set to **Enabled**.	0

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SGXLEPUBKEYHASH1	Sets the bytes from 8 to 15 for SGX Launch Enclave Public Key Hash. The value ranges from 0 to 0xFFFFFFFFFFFFFFFF. **NOTE** This parameter is available when **SGXLEPUBKEYHASHx Write Enable** is set to **Enabled**.	0
SGXLEPUBKEYHASH2	Sets the bytes from 16 to 23 for SGX Launch Enclave Public Key Hash. The value ranges from 0 to 0xFFFFFFFFFFFFFFFF. **NOTE** This parameter is available when **SGXLEPUBKEYHASHx Write Enable** is set to **Enabled**.	0
SGXLEPUBKEYHASH3	Sets the bytes from 24 to 31 for SGX Launch Enclave Public Key Hash. The value ranges from 0 to 0xFFFFFFFFFFFFFFFF. **NOTE** This parameter is available when **SGXLEPUBKEYHASHx Write Enable** is set to **Enabled**.	0
SGX Auto MP Registration	Enables or disables automatic registration in the OS MPA agent. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when **SW Guard Extensions (SGX)** is set to **Enabled**.	**Disabled**
In Field Scan (IFS)	Provides access to the In Field Scan (IFS) configurations.	-
Processor CFR Configuration	Provides access to the processor CFR configurations.	-

5.2.7.1.1 Per-Socket Information

Figure 5-24 shows the **Per-Socket Information** screen. Table 5-21 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-24 Per-Socket Information screen

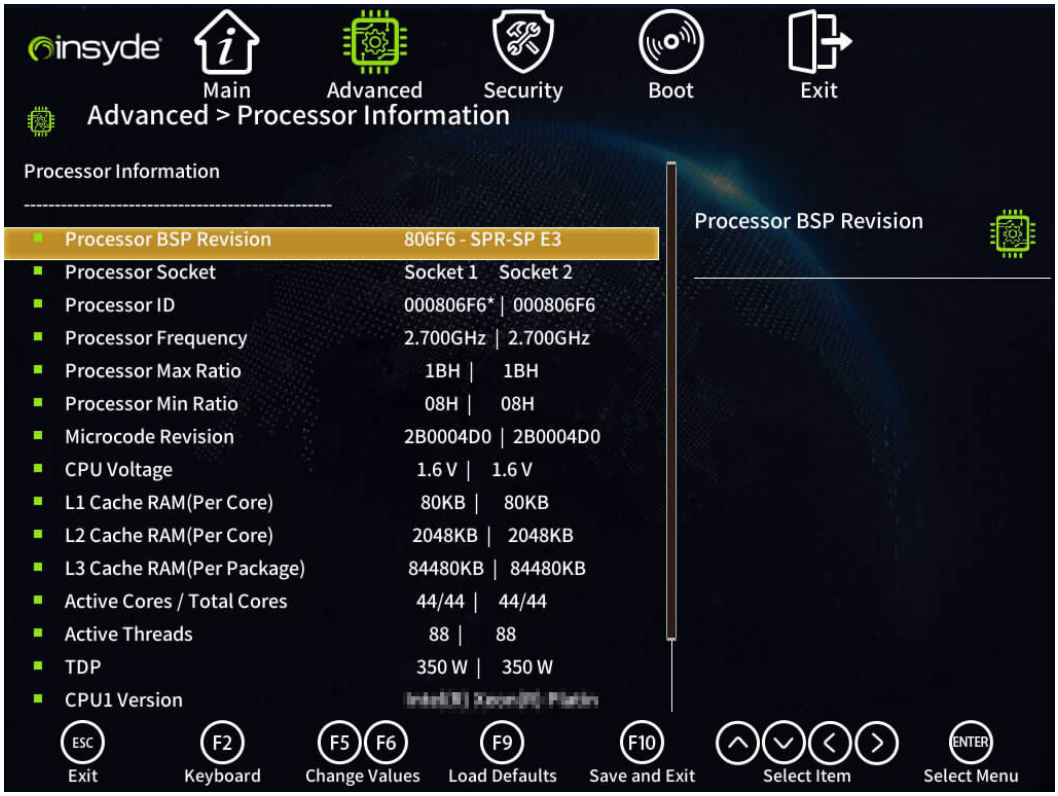


Table 5-21 Parameters on the Per-Socket Information screen

Parameter	Description
Processor BSP Revision	Displays the board support package version.
Processor Socket	Displays the CPU physical slot number.
Processor ID	Displays the CPU ID information.
Processor Frequency	Displays the CPU frequency.
Processor Max Ratio	Indicates the maximum frequency adjustment ratio allowed for the processors.
Processor Min Ratio	Indicates the minimum frequency adjustment ratio allowed for the processors.
Microcode Revision	Displays the uploading microcode version.
CPU Voltage	Displays the CPU voltage.
L1 Cache RAM(Per Core)	Displays the L1 cache capacity of each physical core.
L2 Cache RAM(Per Core)	Displays the L2 cache capacity of each physical core.
L3 Cache RAM(Per Package)	Displays the L3 cache capacity.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Active Cores / Total Cores	Displays the number of enabled physical cores/ total number of physical cores.
Active Threads	Displays the number of enabled threads.
TDP	Thermal design power, which is the heat released when the processor reaches the maximum load.
CPU*X* Version	Displays the model of the CPUX. **NOTE** X indicates the slot number of the CPU. The slot number starts from 1.

5.2.7.1.2 In Field Scan (IFS)

Figure 5-25 shows the **In Field Scan (IFS)** screen. **Table 5-22** describes the parameters.

Figure 5-25 In Field Scan (IFS) screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-22 Parameters on the In Field Scan (IFS) screen

Parameter	Description	Default Value
Enable SAF	Enables or disables the Scan At Field (SAF) function. The menu options are as follows: • **Enabled** • **Disabled** **NOTE** This parameter is unavailable when **Memory Encryption (TME)** or **Extended APIC** is set to **Disabled**.	Disabled
SAF size	Sets the size of the SAF in the PRM. **NOTE** This parameter is available when **Enable SAF** is set to **Enabled**.	**128M**

5.2.7.1.3 Processor CFR Configuration

Figure 5-26 shows the **Processor CFR Configuration** screen. Table 5-23 describes the parameters.

Figure 5-26 Processor CFR Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-23 Parameters on the Processor CFR Configuration screen

Parameter	Description	Default Value
Provision S3M CFR	Enables or disables the function of provisioning S3M CFR. The menu options are as follows: ● Enabled ● Disabled	Enabled
Manual Commit S3M FW CFR	Enables or disables the function of manually submitting S3M FW CFR. The menu options are as follows: ● Enabled ● Disabled ● Auto	Auto
Provision PUcode CFR	Enables or disables the function of provisioning PUcode CFR. The menu options are as follows: ● Enabled ● Disabled	Enabled
Manual Commit PUcode CFR	Enables or disables the function of manually submitting PUcode CFR. The menu options are as follows: ● Enabled ● Disabled ● Auto	Auto
Socket*X* CFR Revision Info	Displays Socket*X* CFR revision information.	-

Figure 5-27 shows the **Socket*X* CFR Revision Info** (for example, **Socket1 CFR Revision Info**) screen. **Table 5-24** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-27 Socket1 CFR Revision Info screen



Table 5-24 Parameters on the Socket1 CFR Revision Info screen

Parameter	Description
S3M CFR Committed SVN	Displays the SVN information that has been submitted by the S3M CFR.
S3M CFR Committed RevID	Displays the REVID information that has been submitted by the S3M CFR.
S3M CFR Uncommitted SVN	Displays the SVN information that has not been submitted by the S3M CFR.
S3M CFR Uncommitted RevID	Displays REVID information that has not been submitted by the S3M CFR.
PUcode CFR Committed SVN	Displays SVN information that has been submitted by the PUcode CFR.
PUcode CFR Committed RevID	Displays REVID information that has been submitted by the PUcode CFR.
PUcode CFR Uncommitted SVN	Displays SVN information that has not been submitted by the PUcode CFR.
PUcode CFR Uncommitted RevID	Displays REVID information that has not been submitted by the PUcode CFR.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

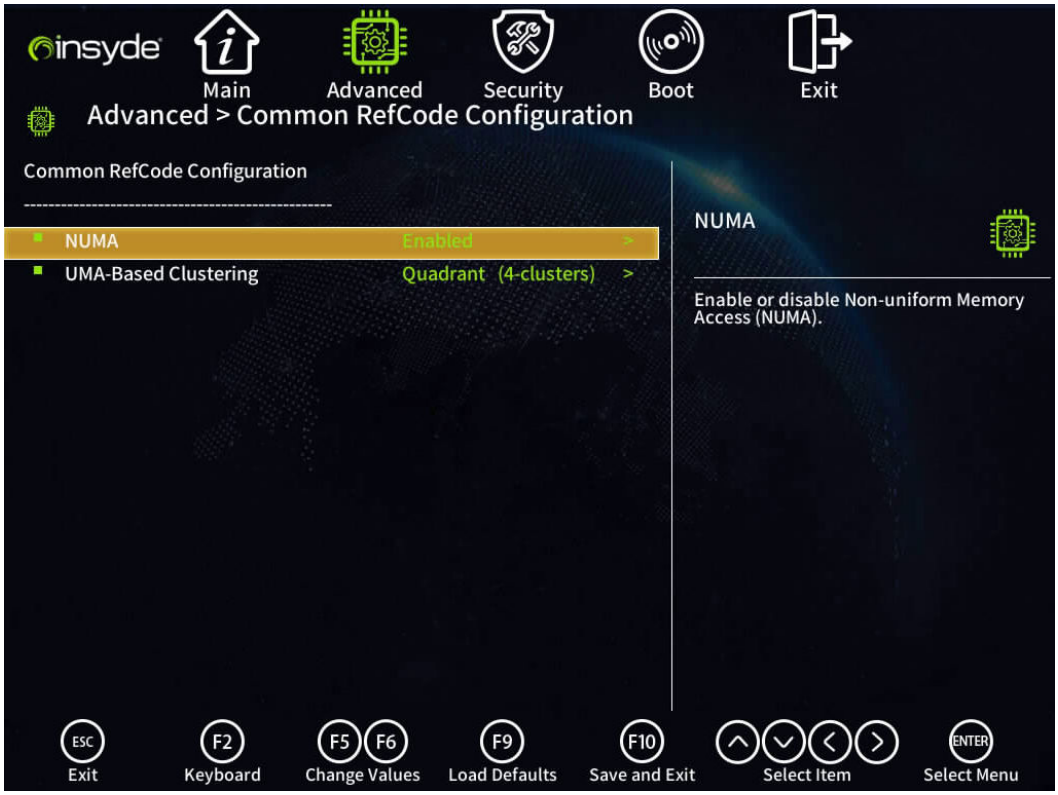
5.2.7.2 Common RefCode Configuration

On the **Common RefCode Configuration** screen, you can configure memory-related features. **Figure 5-28** shows the **Common RefCode Configuration** screen. **Table 5-25** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

Figure 5-28 Common RefCode Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-25 Parameters on the Common RefCode Configuration screen

Parameter	Description	Default Value
NUMA	Enables or disables the NUMA architecture of the system. All OSs support NUMA. In most cases, if this function is enabled, the performance of some high-workload applications will be improved. Ensuring the memory size used by each processor is the same before disabling NUMA. The options are as follows: ● Enabled: Enables NUMA. In most cases, enabling this option will improve performance for certain workloads. ● Disabled: Disables NUMA.	Enabled
UMA-Based Clustering	Sets the UMA-Based Clustering function. The setting of this function is valid only when SNC is disabled. If SNC is enabled, the BIOS automatically disables the UMA-based cluster. The menu options are as follows: ● Disabled (All2All): Disables UMA-Based Clustering mode. ● Hemisphere (2-clusters): Enables Hemisphere (HEMI) mode, also known as UMA-Based Clustering (UBC) mode. This mode provides affinity between memory addresses and the LLC, minimizing the distance between memory addresses and the LLC being cached. This setting can only be enabled when the memory configuration is completely symmetric and requires that SNC mode be disabled. The corresponding option for SNC mode is SNC (Sub-NUMA). ● Quadrant (4-clusters) **NOTE** This parameter is available when the CPU model is **Sapphire Rapids-HBM**.	Quadrant (4-clusters)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.7.3 Uncore Configuration

On the **Uncore Configuration** screen, you can configure UPI parameters. **Figure 5-29** shows the **Uncore Configuration** screen. **Table 5-26** describes the parameters.

Figure 5-29 Uncore Configuration screen

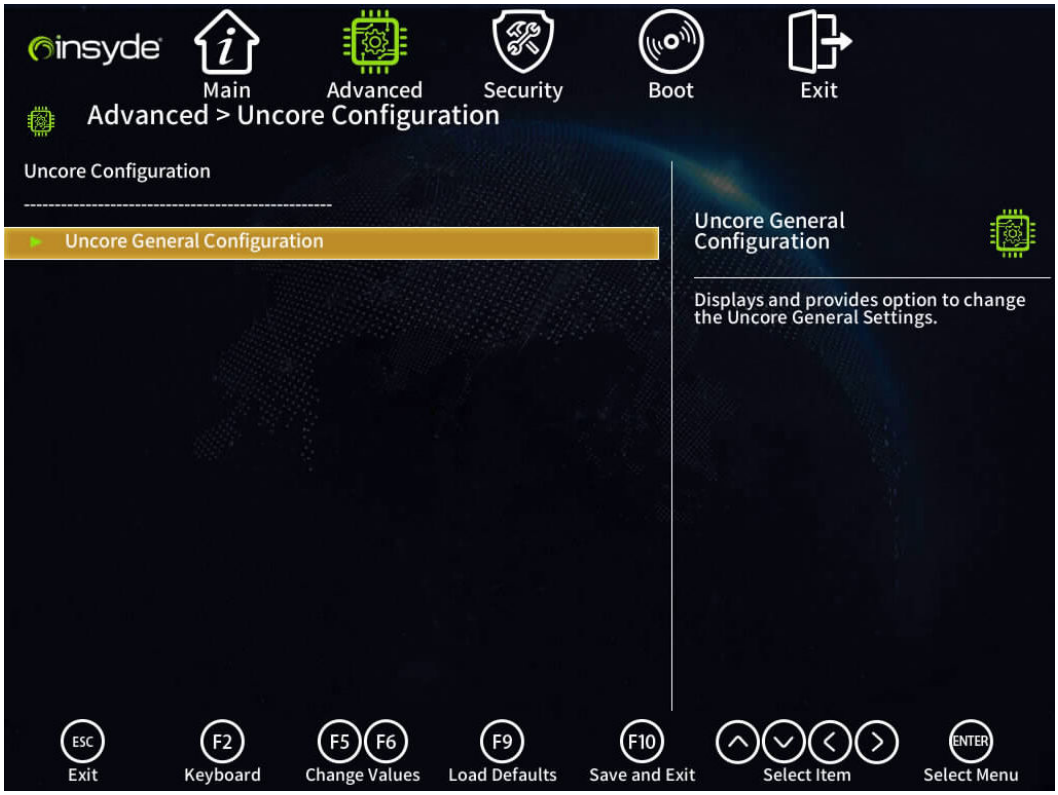


Table 5-26 Parameters on the Uncore Configuration screen

Parameter	Description
Uncore General Configuration	Provides access to uncore general configurations.

5.2.7.3.1 Uncore General Configuration

On the **Uncore General Configuration** screen, you can configure the general features of uncore. **Figure 5-30** and **Figure 5-31** show the **Uncore General Configuration** screen. **Table 5-27** describes the parameters.

NOTE

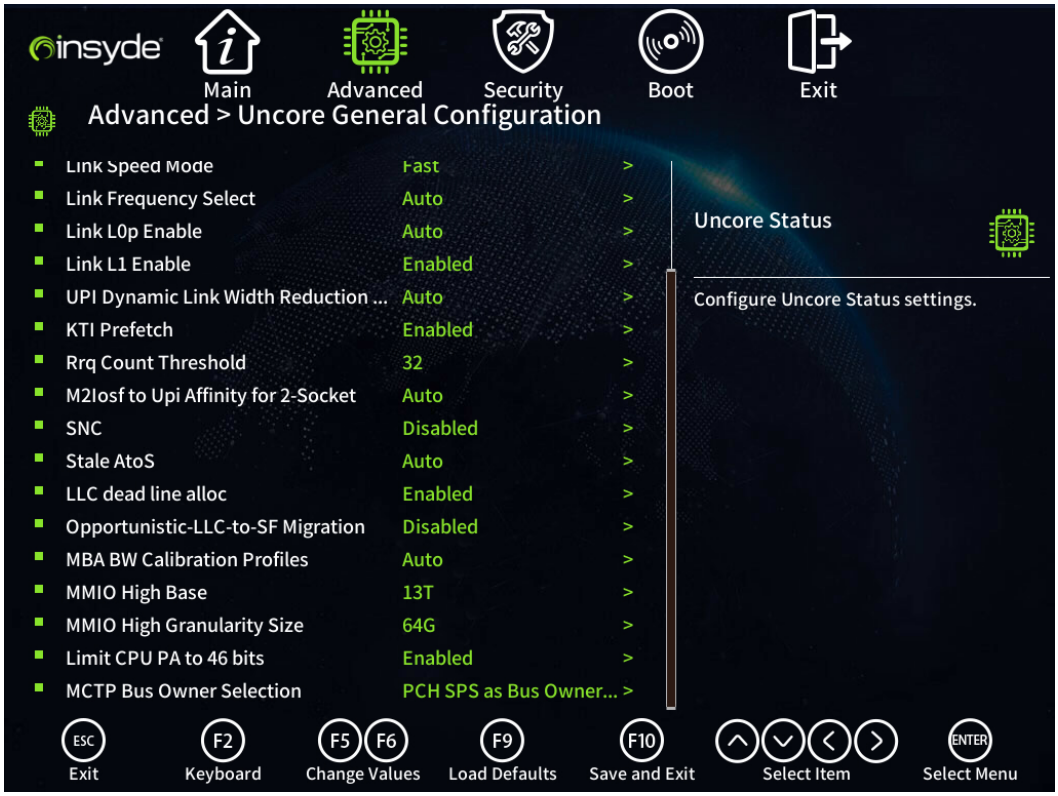
The parameters displayed on the screen vary depending on the CPU configuration of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-30 Uncore General Configuration screen 1



Figure 5-31 Uncore General Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-27 Parameters on the Uncore General Configuration screen

Parameter	Description	Default Value
Uncore Status	Displays the uncore status.	-
Link Speed Mode	Sets the UPI link speed mode. The menu options are as follows: ● Slow: Low speed mode, the link speed is slower. This can save energy and reduce heat dissipation. For scenarios where the data transfer requirements between processors are not high, and low power consumption and low heat dissipation are prioritized. ● Fast: High speed mode, the link speed is faster. It provides higher bandwidth and data transfer efficiency, with higher power consumption and heat dissipation requirements. For scenarios with high requirements for data transfer between processors, such as high-performance computing (HPC), big data analytics, and virtualization. **NOTE** Only BIOS 01.01.06.08 and later versions support this parameter.	Fast
Link Frequency Select	Selects the UPI link frequency. If the UPI link frequency is set to a low value, the power consumption is reduced but the system performance is affected. The menu options are as follows: ● 12.8GT/s ● 14.4GT/s ● 16GT/s ● 20GT/s ● Auto: Automatically selects the UPI link frequency. ● Use Per Link Setting: Uses the per-link setting. **NOTE** When the CPU type is **Emerald Rapids-SP**, the option **20GT/s** is available.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Link L0p Enable	UPI energy saving option. If the L0p option is enabled, the bandwidth of the eight UPI physical channels with low usage will be reduced to x8. When the UPI is not connected and the UPI is set to automatic mode, this function is disabled. In other cases, this function is enabled automatically. The menu options are as follows: ● Auto ● Enabled ● Disabled	Auto
Link L1 Enable	UPI energy saving option. If the L1 option is enabled, UPI is allowed to enter the L1 state when it is idle. In this case, UPI does not generate transmission. The access and exit of L1 are controlled by the PCU. When the UPI is not connected, this function is disabled automatically. In other cases, this function is enabled automatically. The menu options are as follows: ● Auto ● Enabled ● Disabled	Enabled
UPI Dynamic Link Width Reduction Support	Sets the function of recovery from a hard fault on one or more UPI data channels by dynamically adjusting the UPI link to a width of 1/2. When the parameter is set to **Auto**, the function is automatically set based on Si compatibility. The menu options are as follows: ● Auto ● Enabled ● Disabled	Auto
KTI Prefetch	Sets the KTI prefetch function. The KTI prefetch function enables memory read operations on the DDR bus to be performed earlier. The options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Rrq Count Threshold	Sets the RRQ count threshold. The value ranges from 1 to 0x7. **32** indicates that the parameter is automatically set.	32
M2Iosf to Upi Affinity for 2-Socket	Sets whether to select the optimal UPI for different M2IOSF traffic to enhance performance (enabled by default). If disabled, all available UPI links are selected. The menu options are as follows: ● Auto ● Enabled ● Disabled	Auto
SNC	Sets the Sub-NUMA Clustering (SNC) function, which is a mode that reduces the latency of the last level cache (LLC) to local memory. Assume that one CPU can access one memory cluster of its own. In a case of two CPUs, when the SNC is enabled, each CPU can access two memory clusters, but the speed of accessing the memory cluster of its own is fast, and the speed of accessing the external memory cluster is slow. If the SNC is disabled, each CPU can access only one memory cluster of its own. The menu options are as follows: ● Auto: CPU automatically sets. ● **Disabled**: Supports one-cluster SNC. ● **Enable SNC (2-clusters)**: Supports interleaving of 2-cluster SNC and 2-channel IMC. ● **Enable SNC (4-clusters)**: Supports interleaving of 4-cluster SNC and 1-channel IMC.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
XPT Prefetch	Sets the pre-fetching function of the processor extension pre-processing table (XPT). The XPT prefetcher is located above other prefetchers which prefetch data in the core DCU, the MLC, and the LLC. The XPT prefetcher sends a speculative DRAM read request while the LLC lookup is in progress. This prefetch bypasses the LLC, reducing latency. The options are as follows: ● Auto ● Enabled ● Disabled **NOTE** **Auto** functions the same as **Enabled**.	Auto
Stale AtoS	Enables or disables the switching between the SnoopAll (A) state and the Shared (S) state of the memory. If this function is enabled, the delay of cross-CPU memory access is shortened. The options are as follows: ● **Auto**: The SnoopAll (A) state is used by default. During uncore post MRC, the state is reconfigured based on the setup knob, number of sockets, and BPS memory. ● **Enabled**: The SnoopAll (A) state is changed to the Shared (S) state. ● **Disabled**: The SnoopAll (A) state is used.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
LLC dead line alloc	LLC dead line allocation. The processor marks the row replaced by the MLC as **dead**, indicating that the row will not be read again. This function is used to set the allocation policy for the data marked as **dead** in the LLC. The menu options are as follows: ● **Auto** ● **Enabled**: Allows the LLC to fill dead lines into the LLC if there is free space. ● **Disabled**: The dead lines are dropped and are never filled into the LLC, saving the LLC space.	Enabled
UPI Adaptation Enable	Enables or disables the UPI adaptation flow. The menu options are as follows: ● Auto ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Auto
Opportunistic-LLC-to-SF Migration	Enables or disables the function of controlling opportunistic LLC-to-SF migration. The menu options are as follows: ● Auto ● Enabled ● Disabled	Disabled
MBA BW Calibration Profiles	Sets the MBA BW throttling curve. The menu options are as follows: ● Low core BW shaping (for BIOS versions earlier than 01.01.06.03 it is **Linear BW shaping**) ● Mid core BW shaping (for BIOS versions earlier than 01.01.06.03 it is **Biased BW shaping**) ● High core BW shaping (for BIOS versions earlier than 01.01.06.03 it is **Legacy BW shaping**) ● Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PMM MBA BW downscale	Sets the ratio of the PMM BW downscale to the baseline total memory BW configuration file. For example, **1/2x** indicates the downscale ratio of PMM BW throttling and DDR throttling is 2:1. The menu options are as follows: ● 1x ● 1/2x ● 1/4x ● 1/8x **NOTE** This parameter is available when the CPU model is **Granite Rapids** or **Sierra Forest**.	1x
CXL (Type3) MBA BW downscale	Sets the ratio of the CXL (Type3) BW downscaling to the baseline total memory BW profile. For example, **1/2x** indicates the scaling ratio of CXL (Type3) BW throttling and DDR throttling is 2:1. The menu options are as follows: ● 1x ● 1/2x ● 1/4x ● 1/8x **NOTE** This parameter is available when the CPU model is **Granite Rapids** or **Sierra Forest**.	1x
Remote Target MBA BW downscale	Sets the ratio of the remote target BW downscaling to the baseline total memory BW profile. For example, **1/2x** indicates that the scaling ratio of remote target BW throttling and DDR throttling is 2:1 and the ratio of throttling is 2:1. The menu options are as follows: ● 1x ● 1/2x ● 1/4x ● 1/8x **NOTE** This parameter is available when the CPU model is **Granite Rapids** or **Sierra Forest**.	1x

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
UPI Adaptation Speed	Sets the UPI adaptation speed. The menu options are as follows: ● 12.8GT/s ● 14.4GT/s ● 16.0GT/x ● 20.0GT/s ● Auto **NOTE** This parameter is available when **UPI Adaptation Enable** is set to **Enabled**.	Auto
MMIO High Base	Configures the high base address of the memory mapped I/O (MMIO). Adjust this parameter based on requirements of the connected PCIe device for the MMIO high base resources above 4 GB. Improper configuration may cause the system startup failure or abnormal device resource allocation. Do not modify this parameter. The menu options are as follows: ● 56T ● 40T ● 32T ● 24T ● 16T ● 13T ● 3.5T ● 4T ● 2T ● 1T ● 512T **NOTE** The value of this parameter varies depending on the value of **MMIO High Granularity Size**.	13T

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MMIO High Granularity Size	Specifies the I/O high base granularity size. By default, the size of MMIO resources allocated to each stack is equal to the I/O high base granularity. Adjust this parameter based on requirements of the connected PCIe device for the MMIO high base resources above 4 GB. So, exercise caution when modifying the parameter. When a large number of PCIe devices (especially GPU devices) are connected, you may need to increase the value to enlarge the MMIO high base space to ensure that the MMIO high base resources of PCIe devices are properly allocated. The menu options are as follows: ● 1G ● 4G ● 16G ● 64G ● 256G ● 1024G	64G
Limit CPU PA to 46 bits	Enables or disables the limit on the CPU physical address to 46 bits to support earlier versions of Hyper-V. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is unavailable when the CPU model is **SierraForest**. ● Enabling this parameter automatically disables the T**otal Memory Encryption Multi-Tenant (TME-MT)** in **Socket Configuration** > **Processor Configuration**.	Enabled
MCTP Bus Owner Selection	Allows you to select the MCTP bus owner. The menu options are as follows: ● PCH SPS as Bus Owner (Proxy) ● CPU as Bus Owner	PCH SPS as Bus Owner (Proxy)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-32 shows the **Uncore Status** screen. **Table 5-28** describes the parameters.

Figure 5-32 Uncore Status screen

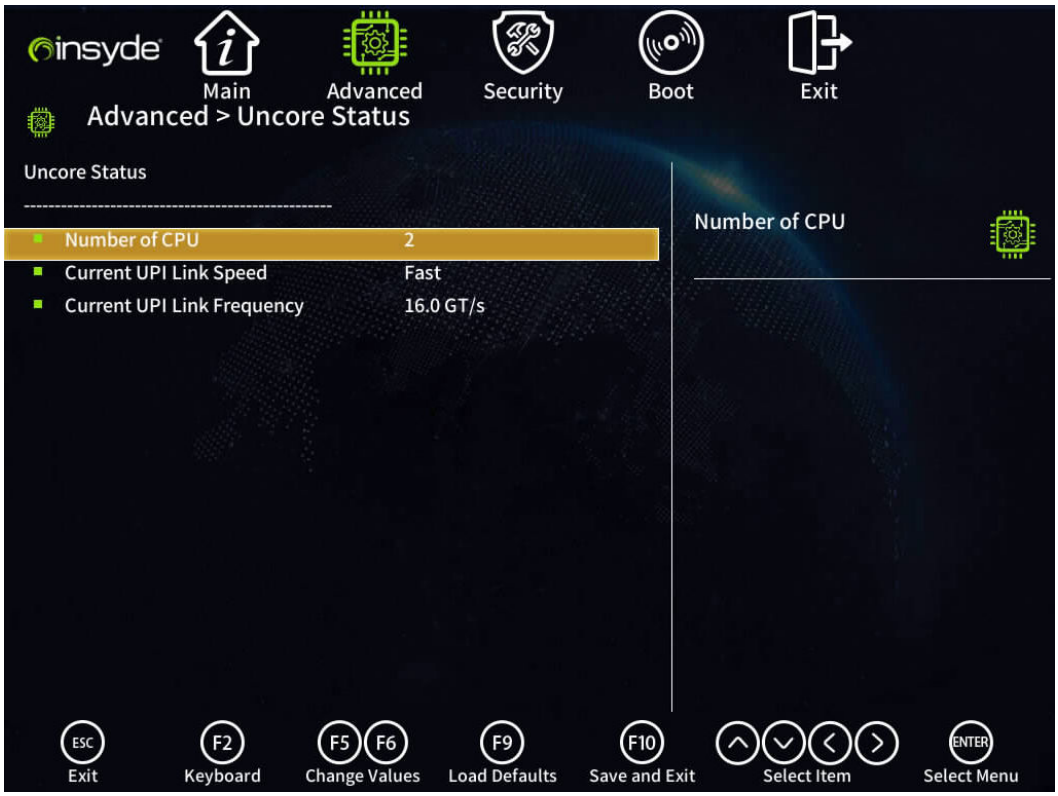


Table 5-28 Parameters on the Uncore Status screen

Parameter	Description
Number of CPU	Displays the current CPU number.
Current UPI Link Speed	Indicates the current UPI link speed.
Current UPI Link Frequency	Displays the current UPI link frequency.

5.2.7.4 Memory Configuration

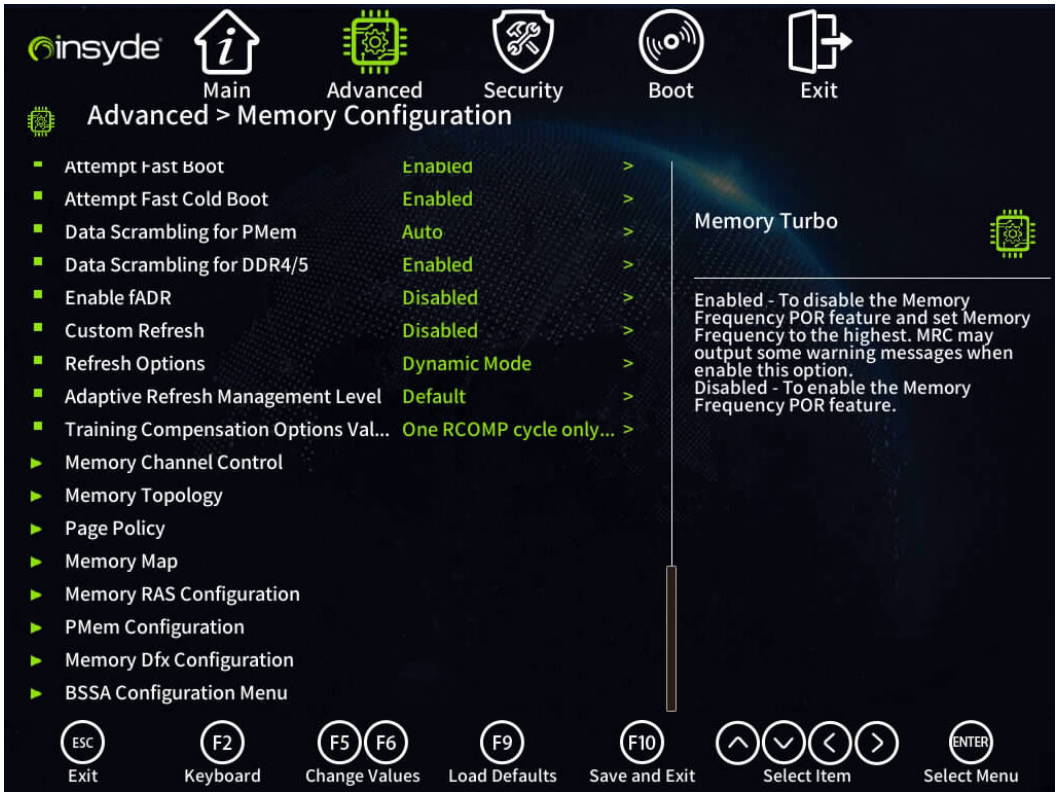
On the **Memory Configuration** screen, you can configure memory. **Figure 5-33** and **Figure 5-34** show the **Memory Configuration** screen. **Table 5-29** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-33 Memory Configuration screen 1



Figure 5-34 Memory Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-29 Parameters on the Memory Configuration screen

Parameter	Description	Default Value
Memory Turbo	Enables or disables memory overclocking. The menu options are as follows: ● **Enabled**: Disables the memory frequency POR feature and sets the memory frequency to the highest. When this parameter is enabled, MRC may output some warning messages. ● **Disabled**: Enables the memory frequency POR feature.	Disabled
Enforce Population POR	Enables or disables the memory population Plan of Record (POR) enforcement function. If this function is enabled, Memory Reference Code (MRC) forcibly requires the memory module insertion to meet the POR requirements. (verified and officially supported by Intel). The memory module insertion configuration not meeting the requirements will be degraded to the supported configuration. The menu options are as follows: ● Enabled ● Disabled	Enabled
DDR PPR Type	Selects the DDR PPR type. The menu options are as follows: ● PPR Disabled: Disables PPR. ● Hard PPR: A permanent fix. ● Soft PPR: A temporary fix.	Soft PPR
HBM Memory Test Type	Selects the HBM memory test type. The menu options are as follows: ● Advanced Memory Test ● mBIST Memory Test **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Advanced Memory Test

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
HBM PPR Type	Selects the HBM post package repair type. The menu options are as follows: ● PPR Disabled ● Hard PPR ● Soft PPR **NOTE** This parameter is available when the CPU model is **HBM SKU**.	PPR Disabled
PTRR DDR Enable	Enables or disables the support for PTRR in the DDR. The menu options are as follows: ● Enabled ● Disabled	Enabled
PTRR HBM Enable	Enables or disables the support for PTRR in the HBM. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **HBM SKU** and the value of **Volatile Memory Mode** is **1LM**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory Frequency	Sets the DDR frequency in MT/s. When the CPU type is SPR, the menu options are as follows: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 When the CPU type is EMR, the menu options are as follows: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 ● 5200 ● 5600 **NOTE** ● When **Memory Turbo** is set to **Enabled**, this parameter is grayed out. ● Only BIOS version 01.01.03.05 and later supports EMR CPUs.	Auto
Refresh Watermarks	Automatically selects low WM (Hi/Panic = 1/2) for 16 Gbit/s DIMMs and high WM (Hi/Panic = 8/9) for other DIMM configurations. Low WM alleviates power supply issues for 128 GB and larger DIMMs, and also mitigates failures due to row hammer traffic patterns. High WM can provide better performance when power delivery and row hammer satisfy requirements. The menu options are as follows: ● Auto ● High WM ● Low WM **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MRC Promote Warnings	Sets whether to raise MRC warnings to the system level. The menu options are as follows: ● Enabled ● Disabled	Disabled
Promote Warnings	Sets whether to raise warnings to the system level. The menu options are as follows: ● Enabled ● Disabled	Disabled
PMem MediaStatus Exception	Enables or disables the PMem media status exception. The menu options are as follows: ● Enabled ● Disabled	Enabled
Sockets in parallel	Sets the sockets in parallel. The menu options are as follows: ● **ALL**: All sockets are operating in parallel. ● **1**: Only one socket is operating at any time. ● **2**: Only two sockets are operating at any time. ● **4**: Only four sockets are operating at any time.	ALL
SPD CRC Check	Enables, disables, or automatically sets the SPD CRC function. An SPD is an erasable EEPROM on a memory module. The menu options are as follows: ● Enabled ● Disabled	Enabled
Attempt Fast Boot	Enables or disables the fast boot function. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Attempt Fast Cold Boot	Enables or disables the fast cold boot function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Data Scrambling for PMem	Enables or disables the function of data scrambling for PMem. The menu options are as follows: ● **Enabled**: Enables data scrambling for PMem. ● **Disabled**: Disables this function. ● **Auto**: Sets this parameter based on stepping.	Auto
Data Scrambling for DDR4/5	Enables or disables the function of data scrambling for DDR4 and DDR5. The menu options are as follows: ● Enabled ● Disabled	Enabled
Data Scrambling for HBM	Enables or disables the function of data scrambling for HBM. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Enabled
Enable fADR	Enables or disables the fADR function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **SPR CPU**.	Disabled
fADR Configuration	Provides access to fADR configurations. **NOTE** This parameter is available when **Enable fADR** is set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Custom Refresh	Enables or disables the custom refresh function. The menu options are as follows: ● Enabled ● Disabled	Disabled
Custom Refresh Rate	Sets the custom memory refresh rate. The value ranges from 20 to 80. **NOTE** This parameter is available when **Custom Refresh** is set to **Enabled**. **20** indicates 2x refresh.	20
Refresh Options	Sets the memory self-refresh frequency mode. The menu options are as follows: ● Dynamic Mode: dynamic self-refresh mode. ● Static 2x Mode: forcible double self-refresh mode. **NOTE** This parameter is unavailable when **Custom Refresh** is set to **Enabled**.	Dynamic Mode
Adaptive Refresh Management Level	Selects the adaptive refresh management (ARFM) level when refresh management (RFM) is required. The menu options are as follows: ● **Default**: Default (RAAIMT, RAAMMT, RAADEC). ● **Level A**: Level A (RAAIMT-A, RAAMMT-A, RAADEC-A). ● **Level B**: Level B (RAAIMT-B, RAAMMT-B, RAADEC-B). ● **Level C**: Level C (RAAIMT-C, RAAMMT-C, RAADEC-C).	Default

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
HBM Refresh Mode	Selects the HBM memory self-refresh mode. The menu options are as follows: ● Refresh mode disabled ● All refresh mode supported - x1, x2, x4 ● refresh mode supported - x1 ● refresh mode supported – x2 ● refresh mode supported – x4 **NOTE** This parameter is available when the CPU model is **HBM SKU**.	All refresh mode supported - x1, x2, x4
HBM Refresh Postponement	Enables or disables optimistic refresh. The menu options are as follows: ● Disabled ● Enabled **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Disabled
Training Compensation Options Values	Provides options for issuing the recompletion (RCOMP) at specific points in training. The menu options are as follows: ● One RCOMP cycle only on PHY Init (MMRC Init) ● One RCOMP cycle after every JEDEC Init ● One RCOMP cycle right before every training step	One RCOMP cycle only on PHY Init (MMRC Init)
Memory Channel Control	Provides access to memory channel control configurations.	-
Memory Topology	Displays memory topology information.	-
Page Policy	Provides access to the page management policy configurations.	-
Memory Map	Provides access to the menu for setting the memory mapping function.	-
Memory RAS Configuration	Provides access to the menu for setting RAS parameters.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
NGN Configuration	Provides access to NGN configurations.	-
Memory Dfx Configuration	Provides access to memory Dfx configurations.	-
BSSA Configuration Menu	Provides access to the menu for setting BSSA.	-

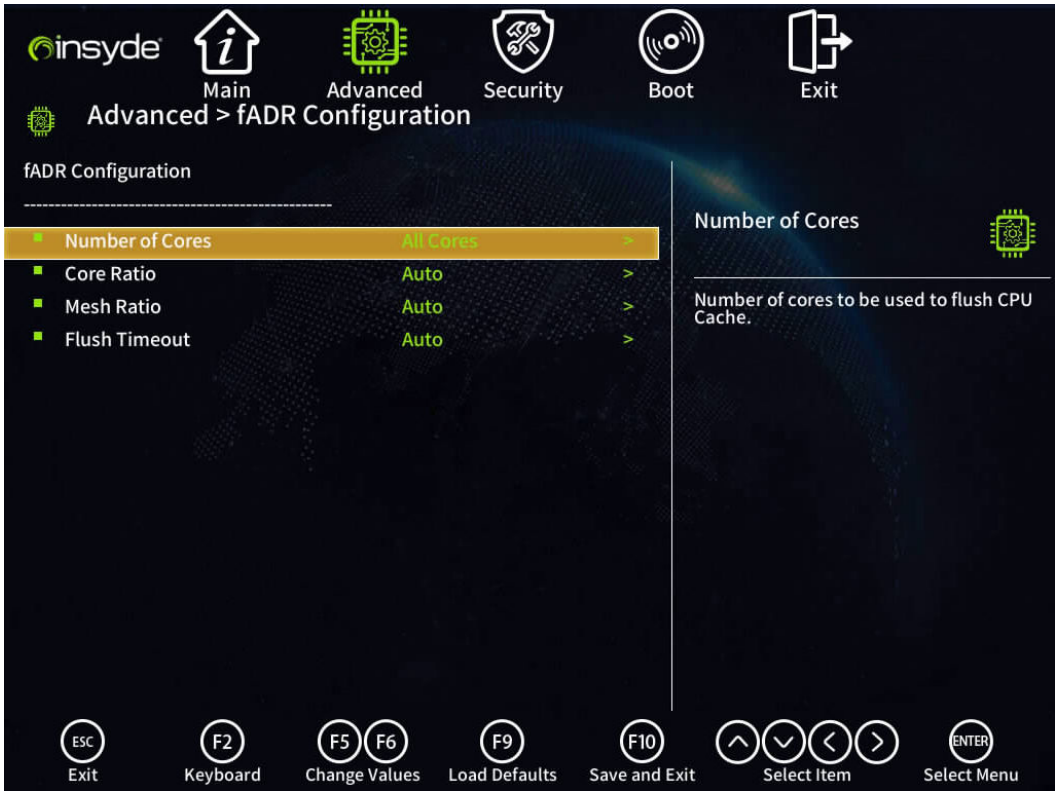
5.2.7.4.1 fADR Configuration

On the **fADR Configuration** screen, you can configure the fADR. **Figure 5-35** shows the **fADR Configuration** screen. **Table 5-30** describes the parameters.

NOTE

This parameter is available when **Enable fADR** is set to **Enabled**.

Figure 5-35 fADR Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-30 Parameters on the fADR Configuration screen

Parameter	Description	Default Value
Number of Cores	Sets the number of cores used to flush the CPU cache. The menu options are as follows: ● 1 Core ● 4 Cores ● All Cores	All Cores
Core Ratio	Sets the core ratio used during the ADR event. The menu options are as follows: ● **Auto**: The core ratio is automatically set to the core/IA P1 ratio. ● **Manual**: The core ratio is manually set to the value requested by the user.	Auto
Core Ratio Value	Sets the core ratio used during the ADR event. The value ranges from 0 to 0xFF. **NOTE** This parameter is available when **Core Ratio** is set to **Manual**.	0xFF
Mesh Ratio	Sets the mesh ratio used during the ADR event. The menu options are as follows: ● **Auto**: The mesh ratio is automatically set to the mesh/CLM P1 ratio. ● **Manual**: The mesh ratio is manually set to the value requested by the user.	Auto
Mesh Ratio Value	Sets the mesh ratio used during the ADR event. The value ranges from 0 to 0xFF. **NOTE** This parameter is available when **Mesh Ratio** is set to **Manual**.	0xFF

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Flush Timeout	Sets the flush timeout value used during the ADR event. The menu options are as follows: • **Auto**: The flush timeout value is automatically set and increases linearly with each enabled socket. • **Manual**: The flush timeout value is manually set to the value requested by the user.	Auto
Flush Timeout Value	Specifies the flush timeout value (the value must be a multiple of 4 ms). **0** indicates timeout. The value ranges from 0 to 0xFFF. **NOTE** This parameter is available when **Flush Timeout** is set to **Manual**.	0xFFF

5.2.7.4.2 Memory Channel Control

On the **Memory Channel Control** screen, you can enable or disable the CPU channel. Figure 5-36 shows the **Memory Channel Control** screen. Table 5-31 describes the parameters.

Figure 5-36 Memory Channel Control screen

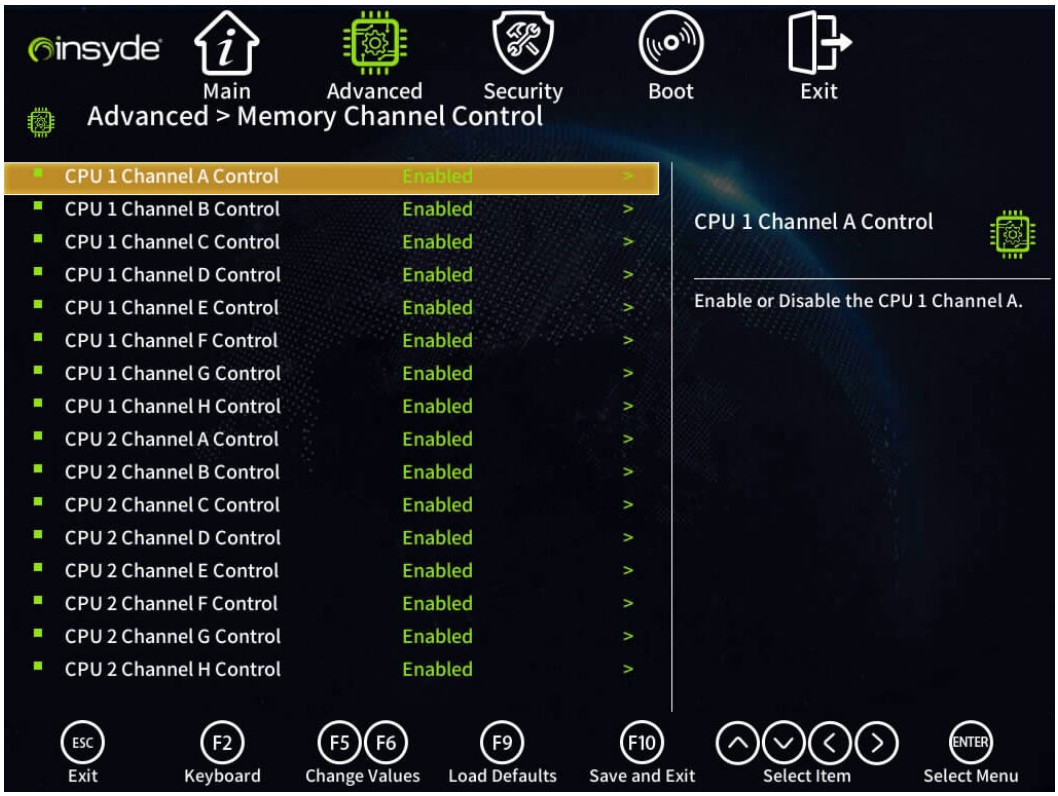


Table 5-31 Parameters on the Memory Channel Control screen

Parameter	Description	Default Value
CPU n Channel m Control	Enables or disables memory *m* channel of CPU *n*. The menu options are as follows: • Enabled • Disabled **NOTE** • *n* indicates the physical CPU slot number and its value is 1 or 2. *m* indicates the channel number and its value ranges from 0 to 7. • At least one channel inserted with DIMM must be enabled for CPU1. Otherwise, the system cannot be powered on.	Enabled

5.2.7.4.3 Memory Topology

On the **Memory Topology** screen, you can query memory information. **Figure 5-37** shows the **Memory Topology** screen. **Table 5-32** describes the parameters.

Figure 5-37 Memory Topology screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

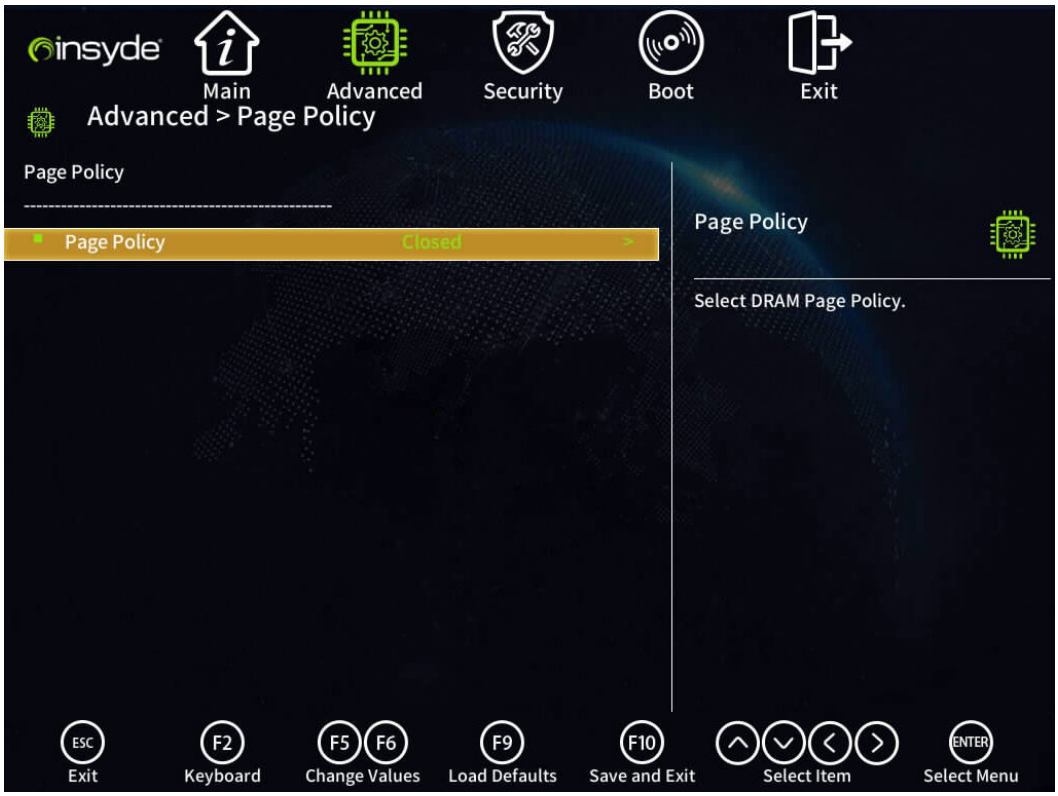
Table 5-32 Parameters on the **Memory Topology** screen

Parameter	Description
DIMMxyz	Displays memory information. • *x* indicates the slot number of the CPU, which is the actual CPU slot number minus 1. • *y* indicates the memory channel. The value ranges from 0 to 7. • *z* indicates the slot number of the memory. **NOTE** For example, the displayed memory information and description of DIMM000: 4800 MT/s Samsung DRx4 64 GB RDIMM are as follows: • **4800MT/s**: The dominant frequency of the memory is 4800 MT/s. • **Samsung**: The memory vendor is Samsung. • **DRx4**: The memory bit width is DRx4. • **64GB**: The memory capacity is 64 GB. • **RDIMM**: The memory type is RDIMM.

5.2.7.4.4 Page Policy

On the **Page Policy** screen, you can set page management policies. **Figure 5-38** shows the **Page Policy** screen. **Table 5-33** describes the parameters.

Figure 5-38 Page Policy screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-33 Parameters on the Page Policy screen

Parameter	Description	Default Value
Page Policy	Sets the page management policy. The menu options are as follows: • **Closed**: Disables the page management policy. • **Adaptive**: Indicates the adaptive mode.	Closed

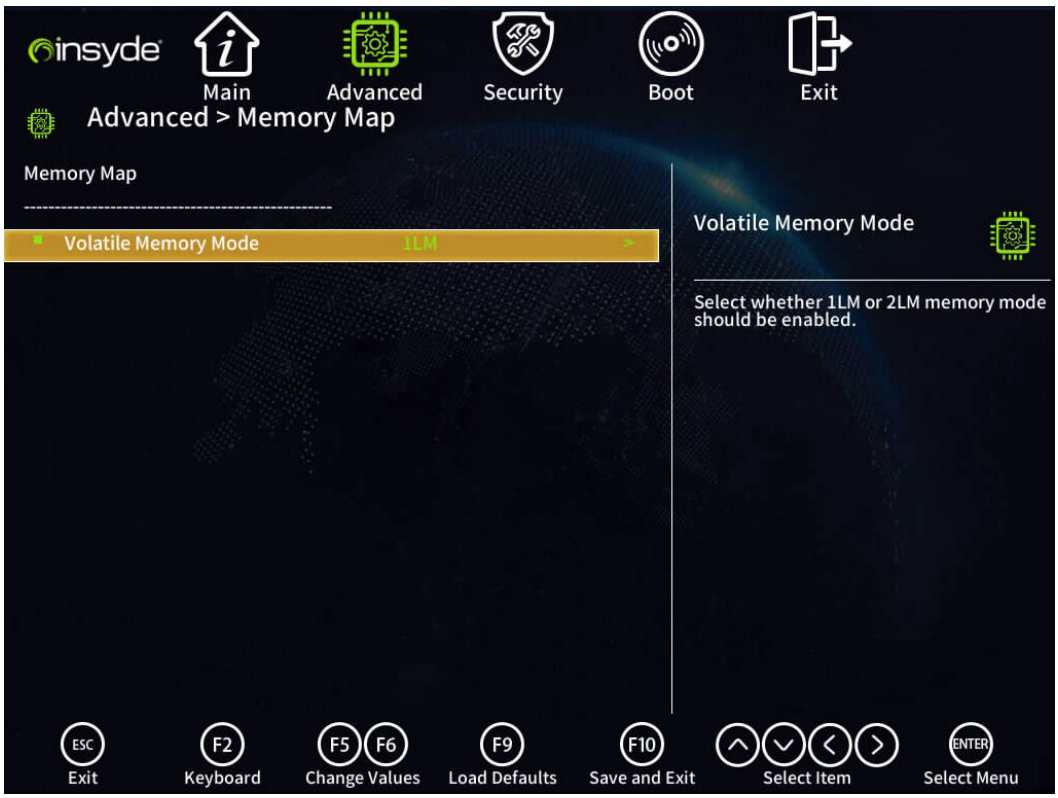
5.2.7.4.5 Memory Map

On the **Memory Map** screen, you can set the volatile memory mode and eADR function. **Figure 5-39** shows the **Memory Map** screen. **Table 5-34** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the configuration of the server.

Figure 5-39 Memory Map screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-34 Parameters on the Memory Map screen

Parameter	Description	Default Value
Volatile Memory Mode	Enables the 1LM or 2LM memory mode. The menu options are as follows: ● 1LM ● 2LM **NOTE** ● This parameter is unavailable when **Common RefCode Configuration>NUMA** is set to **Disabled**. ● This parameter is unavailable when the CPU model is **Emerald Rapids**. ● This parameter is unavailable when the CPU model is not **HBM SKU** and the CPU does not support DCPMMs. ● The 2LM memory mode is available when the CPU model is **HBM SKU**.	1LM
2LM Memory Type	Selects the type of volatile memory to be used as the cache. The menu options are as follows: ● DDR caching PMem ● HBM caching DDR **NOTE** This parameter is available when the CPU model is **HBM SKU** and the value of **Volatile Memory Mode** is **2LM**.	DDR caching PMem

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DDR Cache Size	Sets the DDR cache size for each populated channel used for 2LM configurations. Any remaining DDR will be mapped as 1LM. The menu options are as follows: ● All ● 8G ● 16G ● 32G ● 64G ● 128G ● 256G ● 512G **NOTE** This parameter is available when the following conditions are met: ● The CPU model is not **Grand Ridge**, **Sapphire Rapids-SP**, or **Emerald Rapids-SP**. ● DCPMM is supported. ● **2LM Memory Type** is set to **DDR caching PMem**. ● **Volatile Memory Mode** is set to **2LM**.	All
Flat 2LM Support	Enables or disables Flat 2LM support. The menu options are as follows: ● Disabled ● Enabled **NOTE** This parameter is available when the following conditions are met: ● The CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**. ● **2LM Memory Type** is set to **DDR caching PMem**. ● **Volatile Memory Mode** is set to **2LM**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
eADR Support	Enables/disables or automatically sets the extended Asynchronous DRAM Refresh (eADR) function. The ADR ensures that all pending writes on the write pending queues of the storage controller are written to the PMem during a power failure. The options are as follows: ● Auto ● Enabled ● Disabled	Disabled
CPU Cache Flush Mode	Sets the execution mode of CPU cache refresh. The menu options are as follows: ● **Serial**: sequential execution mode ● **Parallel**: parallel execution mode **NOTE** This parameter is available when **eADR Support** is set to **Enabled** or **Auto**.	Parallel
DDR CXL Heterogeneous Interleave support	Enables or disables DDR CXL heterogeneous interleaving support. The menu options are as follows: ● Disabled ● Enabled **NOTE** This parameter is available when the CPU model is **Emerald Rapids-SP**.	Disabled

5.2.7.4.6 Memory RAS Configuration

On the **Memory RAS Configuration** screen, you can configure memory RAS functions. **Figure 5-40** and **Figure 5-41** show the **Memory RAS Configuration** screen. **Table 5-35** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the memory configuration of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-40 Memory RAS Configuration screen 1

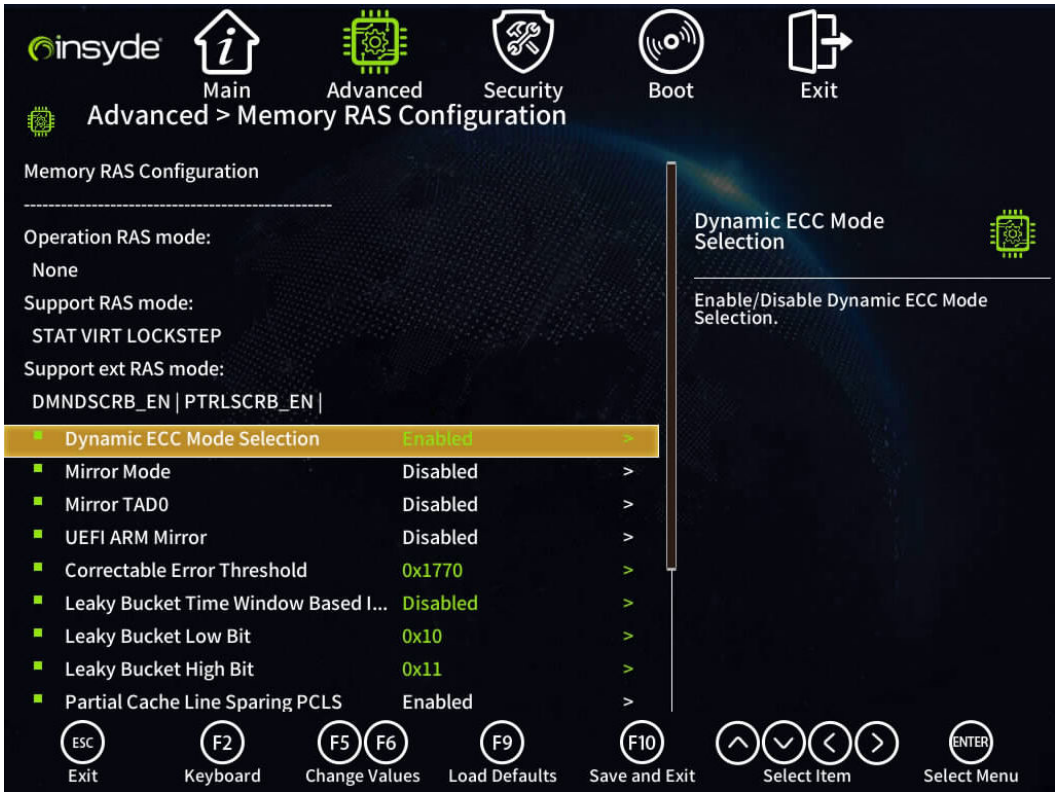
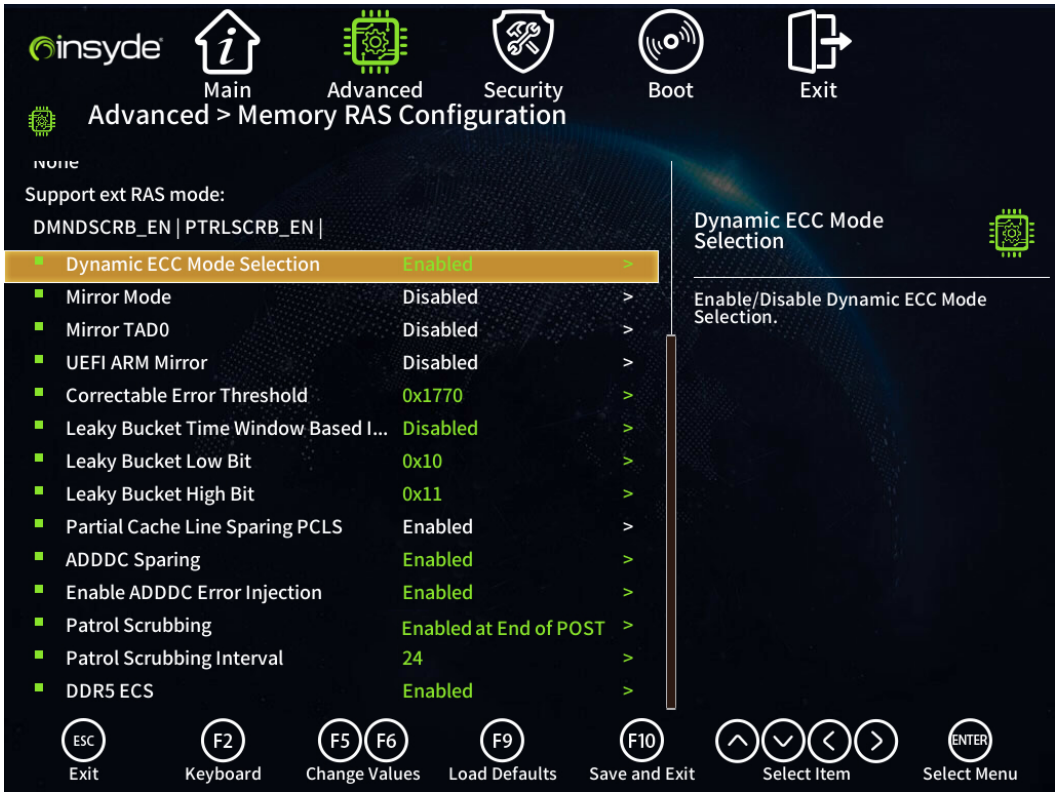


Figure 5-41 Memory RAS Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-35 Parameters on the Memory RAS Configuration screen

Parameter	Description	Default Value
Operation RAS mode	Displays the current RAS mode.	-
Support RAS mode	Displays the supported RAS mode.	-
Support ext RAS mode	Displays the additional supported RAS mode.	-
Enhanced SDDC	Enables or disables the enhanced SDDC. The menu options are as follows: ● **Enabled** ● **Disabled**	Enabled
Mirror Mode	Sets the memory mirroring mode. The menu options are as follows: ● **Disabled**: Disables the memory mirroring mode. ● **Full Mirror Mode**: Indicates the full mirroring mode. Enabling this mode will set all 1LM memory in the system to mirror mode, reducing the available memory capacity by half. ● **Partial Mirror Mode**: Indicates the partial mirroring mode. Allows you to set the mirrored memory size. **NOTE** ● This parameter is unavailable when DIMMs are not installed in the mirror mode. ● This parameter is unavailable when **UEFI ARM Mirror** is set to **Enabled** or **ADDDC Sparing** is set to **Enabled**. ● The full mirror mode will set the entire 1LM in system to be mirrored, consequently reducing the memory capacity by half. Enabling the partial mirroring mode indicates setting part of the memory to be mirrored.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Mirror TAD0	Enables mirroring on the entire memory of TAD0. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is unavailable when DIMMs are not installed in the mirror mode.	Disabled
Partial Mirror 1 Size (GB)	Sets the size of the partial mirror 1. Select the capacity of the SAD to be created (the value must be a multiple of 1 GB). Note that the image size must be less than half of the total memory capacity. **NOTE** This parameter is available when **Mirror Mode** is set to **Partial Mirror Mode**.	0
Partial Mirror 2 Size (GB)	Sets the size of the partial mirror 2. Select the capacity of the SAD to be created (the value must be a multiple of 1 GB). Note that the image size must be less than half of the total memory capacity. **NOTE** This parameter is available when **Mirror Mode** is set to **Partial Mirror Mode**.	0
Partial Mirror 3 Size (GB)	Sets the size of partial mirror 3. Select the capacity of the SAD to be created (the value must be a multiple of 1 GB). Note that the image size must be less than half of the total memory capacity. **NOTE** This parameter is available when **Mirror Mode** is set to **Partial Mirror Mode**.	0

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Partial Mirror 4 Size (GB)	Set the size of partial mirror 4. Select the capacity of the SAD to be created (the value must be a multiple of 1 GB). Note that the image size must be less than half of the total memory capacity. **NOTE** This parameter is available when **Mirror Mode** is set to **Partial Mirror Mode**.	0
UEFI ARM Mirror	Enables or disables the UEFI ARM mirroring mode. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** ● This parameter is unavailable when DIMMs are not installed in the mirror mode. ● This parameter is unavailable when **Mirror Mode** is set to **Full Mirror Mode** or **Partial Mirror Mode**.	Disabled
ARM Mirror percentage	Sets the ARM image percentage. **NOTE** This parameter is available when **UEFI ARM Mirror** is set to **Enabled**.	0
Memory Bank Sparing	Enables or disables memory bank sparing. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when the CPU model is **HBM SKU**.	**Disabled**
Runtime PPR/Row Sparing	Enables or disables runtime PPR/row sparing. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Disabled
Correctable Error Threshold	Sets the correctable error threshold. The value ranges from **1** to **0x7FFF**.	0x1770

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Leaky Bucket Time Window Based Interface	Enables or disables the interface based on the leaky bucket time window. The menu options are as follows: ● **Enabled** ● **Disabled**	Disabled
Leaky Bucket Time Window Based Interface Hour	Sets the value of Leaky Bucket Time Window Based Interface Hour. The value ranges from **0** to **24**. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	24
Leaky Bucket Time Window Based Interface Minute	Sets the value of Leaky Bucket Time Window Based Interface Minute. The value ranges from **0** to **60**. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	0
Leaky Bucket Low Bit	Sets the low bit of the leaky bucket. The value ranges from **0x1** to **0x29**. **NOTE** This parameter is unavailable when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	0x10
Leaky Bucket High Bit	Sets the high bit of the leaky bucket. The value ranges from **0x1** to **0x29**. **NOTE** This parameter is unavailable when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	0x11
Partial Cache Line Sparing PCLS	Enables or disables PCLS. The menu options are as follows: ● **Enabled** ● **Disabled**	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
ADDDC Sparing	Enables or disables the Adaptive Double Device Data Correction Sparing (ADDDC) reservation function. If this parameter is enabled, the BIOS supports a maximum of two failed area replacements and one backup in a memory channel for memory errors detected during the running phase. If the performance is preferred, it is recommended that the ADDDC reservation function be disabled. If reliability is preferred, it is recommended that X4 memory be used and the ADDDC reservation function be enabled. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** The ADDDC function is not supported and this parameter is unavailable when the X8 memory is configured.	Enabled
Enable ADDDC Error Injection	Enables or disables the ADDDC error injection function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	Enabled
Patrol Scrubbing	Enables or disables the patrol scrubbing function. The CPU actively performs periodic inspections on memory data and corrects correctable memory errors. The menu options are as follows: ● **Disabled** ● **Enabled at End of POST** (for BIOS versions earlier than 01.01.06.03 it is **Enable at End of POST**)	Enabled at End of POST
Patrol Scrubbing Interval	Sets the time interval (in hours) at which patrol scrubbing is performed. The value ranges from **0** to **24**. 0 means automatic inspection.	24

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DDR5 ECS	Enables or disables the DDR5 error check and scrubbing (ECS) function. The menu options are as follows: • **Enabled** • **Disabled**	Disabled

5.2.7.4.7 PMem Configuration

On the **PMem Configuration** screen, you can set PMem-related functions. **Figure 5-42** and **Figure 5-43** show the **PMem Configuration** screen. **Table 5-36** describes the parameters.

Figure 5-42 PMem Configuration screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-43 PMem Configuration screen 2



Table 5-36 Parameters on the PMem Configuration screen

Parameter	Description	Default Value
PMem Secure Erase Unit	Provides access to the menu for setting PMem secure erasure.	-
PMem Factory Reset/ Clear	Enables or disables the PMem Factory Reset/Clear function. The menu options are as follows: ● Enabled ● Disabled	Disabled
Always-ON 12v Support	Enables or disables BIOS and PMem module **Always-ON 12v** support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available only when the PMem module supports this function.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
300 Series PMem Average Power Limit (in mW)	Specifies the limit on average power in mW. The valid range of the power limit starts from 10,000 mW and must be a multiple of 250 mW. The value ranges from 0x0 to 0xFFFF.	15000
300 Series PMem Turbo/Memory Bandwidth Boost(MBB) Feature	Enables or disables the Turbo/ Memory Bandwidth Boost (MBB) feature on the module. The menu options are as follows: ● Enabled ● Disabled	Enabled
300 Series PMem Memory Bandwidth Boost(MBB) Average Power Time Constant (in mSec)	Sets the value used as the base time window for power consumption measurements. The valid value ranges from 1000 milliseconds to 120,000 milliseconds (which must be in an increment of 1000 milliseconds). The value ranges from 0x0 to 0xFFFFFFFF.	15000
300 Series PMem Turbo/Memory Bandwidth Boost Feature(MBB) Power Limit (in mW)	Sets the power limit (in mW) used to limit the power consumption of Turbo/Memory Bandwidth Boost (MBB). The valid range of the Turbo power limit starts from 15,000 mW. The value ranges from 0x0 to 0xFFFF.	18000
Publish ARS capability	Enables or disables the address range inspection capability open to the OS. The menu options are as follows: ● Enabled ● Disabled	Enabled
PMem CMD Time	Sets the NGN command time. The unit is nanosecond. Different values indicate different delays. A smaller value indicates a smaller delay. The menu options are as follows: ● Auto ● 1N ● 2N **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PMem ECC Read Check	Enables or disables the PMem ECC read check function. The menu options are as follows: ● Enabled ● Disabled	Enabled
PMem FastGo Configuration	Selects the PMem QoS configuration file. The menu options are as follows: ● Auto ● Enable FastGo optimization ● Disable FastGo optimization **NOTE** This parameter is available when the PMem module is installed on the server.	Auto
PMem QoS	Sets the PMem QoS tuning recipe. The menu options are as follows: ● Disabled ● Profile 1 **NOTE** This parameter is available when the PMem module is installed on the server.	Disabled
PMem Latch System Shutdown State	Enables or disables the PMem latch shutdown function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Snoopy mode for 2LM	Enables or disables the snoopy mode for 2LM. The menu options are as follows: ● Enabled ● Disabled	Disabled
PMem Performance Setting	Sets the baseline performance for the PMem workload behavior. The menu options are as follows: ● BW Optimized ● Balanced Profile **NOTE** This parameter is available when the PMem module is installed on the server.	BW Optimized

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Enable power cycle policy	Enables or disables the power restart mechanism. The menu options are as follows: ● Enabled ● Disabled	Enabled
Snoopy mode for AD	Enables or disables the APP Direct (AD) mode. If it is enabled, directory updates from non-NUMA optimized workloads to DDRT memory can be avoided. The DDRT memory is a memory that supports the DDRT protocol. DDR-T is a transaction protocol that allows an unordered transaction and a variable latency. The options are as follows: ● Enabled ● Disabled	Disabled
LSx implementation	Selects the ACPI method implementation mode. The menu options are as follows: ● SWSMI ● ASL	ASL
Extended Type 17 Structure	Enables or disables the extended type 17 structure. The menu options are as follows: ● Enabled ● Disabled	Enabled
SMBus Max Access Time	Sets the maximum SMBus access time.	350
SMBus Release Delay	Sets the SMBus release delay.	150
NVDIMM Mailbox in NFIT	Enables or disables the NVDIMM mailbox in NFIT. The menu options are as follows: ● Enabled ● Disabled	Disabled
Seamless: Opt-in DIMMs	Enables or disables opt-in DIMMs (if supported by the firmware). The menu options are as follows: ● Keep ● Disabled ● Enabled	Keep

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-44 shows the **PMem Secure Erase Unit** screen. Table 5-37 describes the parameters.

Figure 5-44 PMem Secure Erase Unit screen

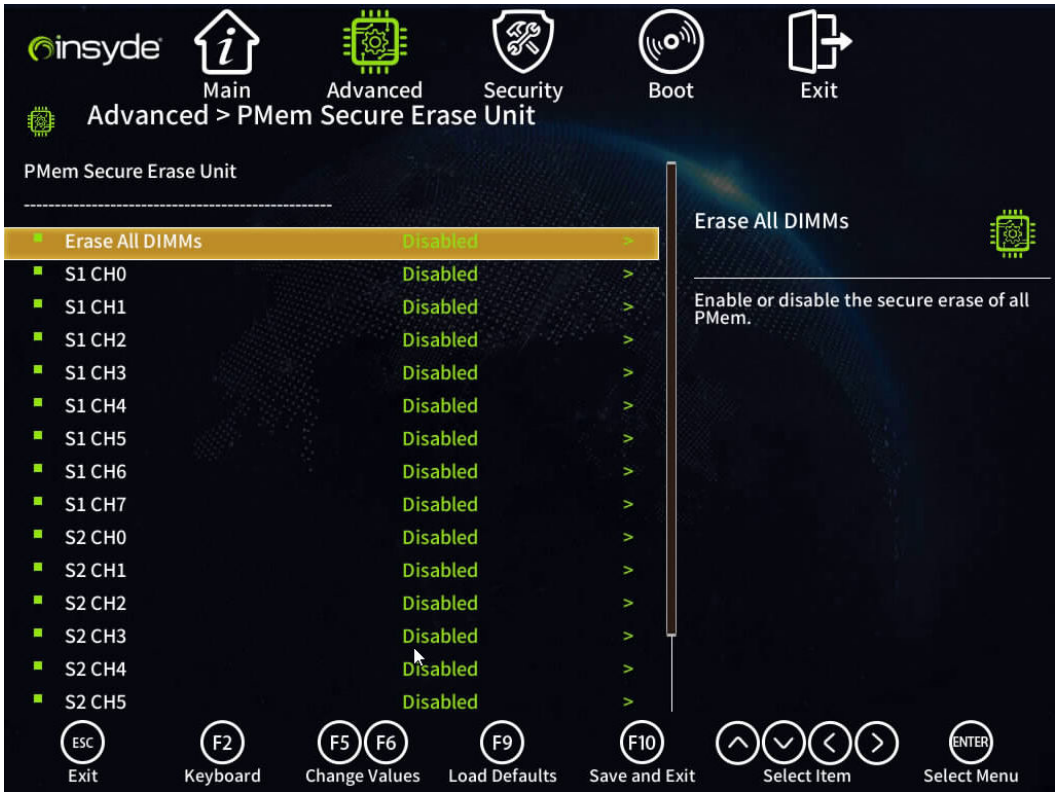


Table 5-37 Parameters on the PMem Secure Erase Unit screen

Parameter	Description	Default Value
Erase All DIMMs	Enables or disables the function of securely erasing all DIMM data. The menu options are as follows: • Enabled • Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
S*x* CH*y*	Enables or disables the function of erasing the persistent storage area of the PMem in slot *x* channel *y*. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● *x* indicates the CPU slot number, which is equal to the actual CPU slot number minus 1. *y* indicates the channel number, ranging from 0 to 7. ● This parameter is unavailable when **Erase All DIMMs** is set to **Enabled**.	Disabled

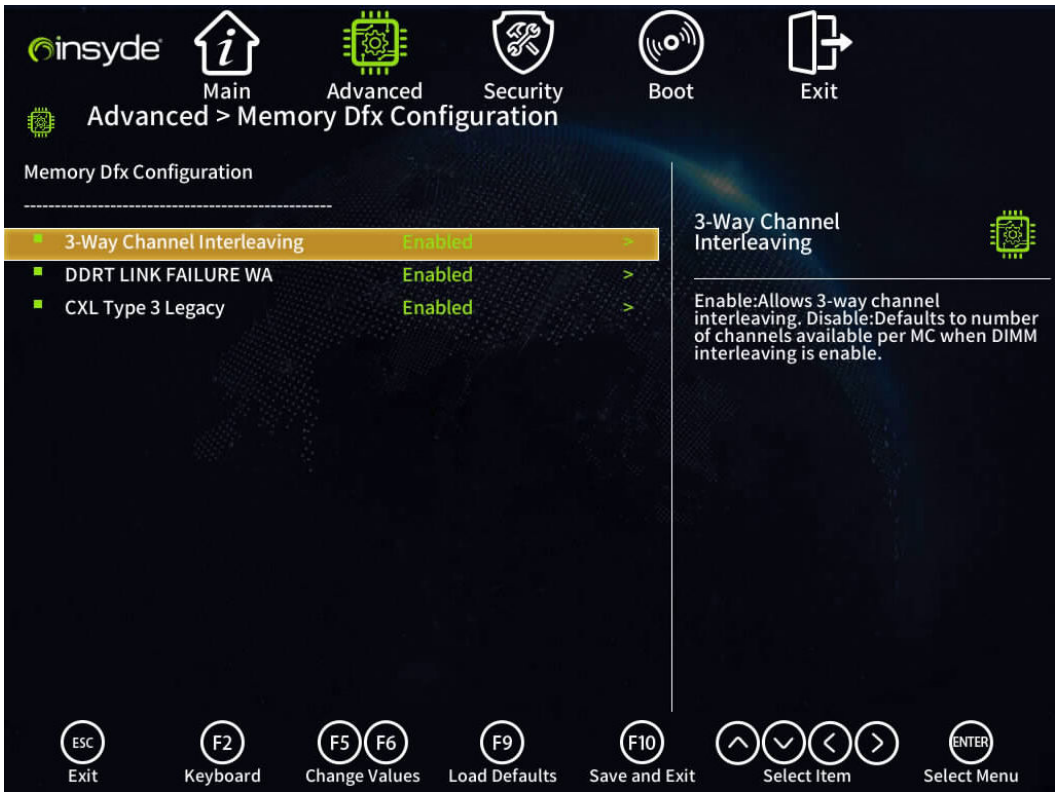
5.2.7.4.8 Memory Dfx Configuration

On the **Memory Dfx Configuration** screen, you can configure memory. **Figure 5-45** shows the **Memory Dfx Configuration** screen. **Table 5-38** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

Figure 5-45 Memory Dfx Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-38 Parameters on the Memory Dfx Configuration screen

Parameter	Description	Default Value
HBM Bank Group Interleaving Mode	Sets the HBM Bank group interleaving mode to fine-grained or coarse-grained. The menu options are as follows: ● Coarse Grained Mode ● Fine Grained Mode BANK_INT_7_10_11_13 (HBM) ● Fine Grained Mode BANK_INT_8_10_11_13 (HBM) ● Fine Grained Mode BANK_INT_6_11_12_13 (HBM) **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Fine Grained Mode BANK_INT_8_10_11_13 (HBM)
3-Way Channel Interleaving	Enables or disables 3-channel interleaving. When enabled, 3-way channel interleaving is allowed. When disabled, the value displayed by default is the number of channels available for per MC. The menu options are as follows: ● Enabled ● Disabled	Enabled
DDRT LINK FAILURE WA	Sets whether to apply the DDRT link failure workround. The menu options are as follows: ● Enabled ● Disabled	Enabled
DDR EarlyCmp	Enables or disables early completion for all DDR memory controllers. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
HBM EarlyCmp	Enables or disables early completion for all HBM memory controllers. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Enabled
CXL Type 3 Legacy	Enables or disables CXL Type 3 Legacy. The menu options are as follows: ● Enabled ● Disabled	Enabled
CXL Hot Plug Support	Enables or disables CXL hot swap support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Enabled

5.2.7.4.9 BSSA Configuration Menu

On the **BSSA Configuration Menu** screen, you can configure BSSA-related parameters. **Figure 5-46** shows the **BSSA Configuration Menu** screen. **Table 5-39** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-46 BSSA Configuration Menu screen

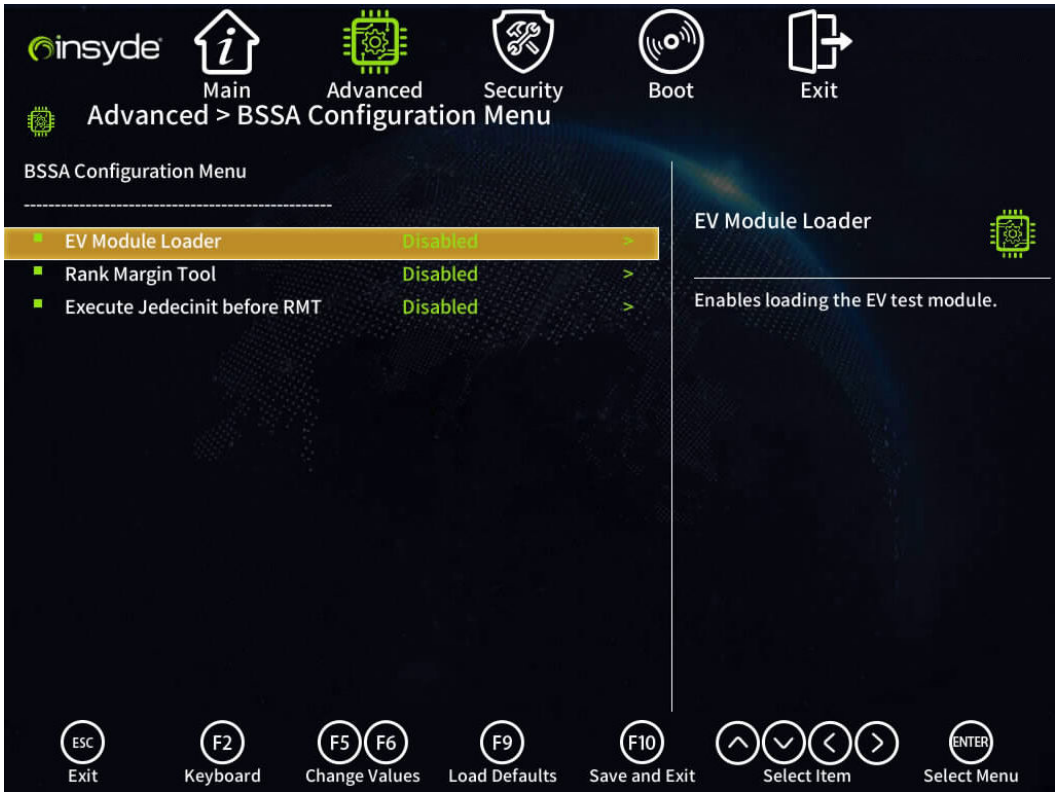


Table 5-39 Parameters on the BSSA Configuration Menu screen

Parameter	Description	Default Value
EV Module Loader	Enables or disables the EV test module loading. The menu options are as follows: ● Enabled ● Disabled	Enabled
Rank Margin Tool	Enables or disables Rank Margin Tool (RMT), which is used to test the memory rank margin. The menu options are as follows: ● Enabled ● Disabled	Disabled
Execute Jedecinit before RMT	Enables or disables the function of executing Jedecinit before the Rank Margin Tool. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Per CA Lane Margining	Enables or disables each CA lane margin. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **Rank Margin Tool** is set to **Enabled**.	Enabled
Scrambler	Enables or disables the scrambler during the RMT test. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **Rank Margin Tool** is set to **Enabled**.	Enabled
RMT Supress Serial Message Log	Enables or disables suppression for the output of only error messages in serial messages when the RMT is running. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **Rank Margin Tool** is set to **Enabled**.	Enabled

5.2.7.5 IIO Configuration

On the **IIO Configuration** screen, you can configure PCIe slots, including the link speed and maximum load of PCIe ports. **Figure 5-47** shows the **IIO Configuration** screen. **Table 5-40** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-47 IIO Configuration screen



Table 5-40 Parameters on the IIO Configuration screen

Parameter	Description	Default Value
Socket*X* Configuration	Provides access to Socket *X* configurations, which is used to set the link speed, Max Payload Size, and ASPM settings of the PCIe device on CPU *X*, and to display the link status, maximum link, and current link speed of the current PCIe port. **NOTE** X indicates the physical slot number of the CPU. The value can be **1** or **2**.	-
IOAT Configuration	Provides access to IOAT configurations.	-
IIO Stack IO Resource Configuration	Provides access to IIO stack I/O resource configurations.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Intel Virtualization for Directed I/O (VT-d)	Provides access to VT-d configurations. Intel VT-d technology switch settings are used to improve system security and reliability and improve the performance of I/O devices in virtual environments. **NOTE** To disable **VT-d**, **Extended APIC** must be set to **Disabled** first for the VT-d setting to take effect.	-
Intel(R) VMD Technology	Provides access to VMD configurations. **NOTE** This parameter is available only in UEFI mode.	-
IIO DFX Configuration	Provides access to IIO DFX configurations.	-
IIO Global Performance Tuning	Provides access to I/O global performance tuning configurations.	-
PCI 64-Bit Resource Allocation	Enables or disables PCI 64-bit resource allocation. After this option is disabled, it will be automatically enabled when the server is restarted if the PCIe device requires more than 4 GB memory resources. The options are as follows: ● Enabled ● Disabled	Enabled
Skip Halt On DMI Degradation	Prevents the system halt due to DMI width/link degradation. The menu options are as follows: ● No ● Yes	No
Rx Clock WA	Sets whether to receive the clock WA. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Completion Timeout	Sets the PCIe transfer completion timeout function. The menu options are as follows: ● Per-Port ● Global	Per-Port
PCIe Completion Timeout Value	Sets the timeout period of PCIe transfer completion. The menu options are as follows: ● 50us to 50ms ● 50us to 100us ● 1ms to 10ms ● 16ms to 55ms ● 65ms to 210ms ● 260ms to 900ms ● 1s to 3.5s ● Disabled	260ms to 900ms
PCIe ENQCMD/ ENQCMDS	Provides access to PCIe ENQCMD/ ENQCMDS configurations. The menu options are as follows: ● No ● Yes	No

5.2.7.5.1 Socket*X* Configuration

On the **SocketX Configuration** screen, you can configure CPU*X*-related features. The following uses **Socket1 Configuration** as an example. **Figure 5-48** shows the **Socket1 Configuration** screen. **Table 5-41** describes the parameters.

NOTE

The parameters on the displayed screen vary depending on the bandwidth configuration and used port of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-48 Socket1 Configuration screen



Table 5-41 Parameters on the Socket1 Configuration screen

Parameter	Description	Default Value
IOUx (IIO PCIe Port y)	Indicates the PCIe port bandwidth information. The value is dynamically obtained and cannot be edited.	-
Port *X*	Provides access to Port *X* configurations. **NOTE** The displayed port configuration menu list varies depending on server configurations.	-

The parameters displayed on the Port *X* setting screens are the same. Port 1A is used as an example here.

Figure 5-49 shows the **Port 1A** screen. **Table 5-42** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-49 Port 1A screen



Table 5-42 Parameters on the Port 1A screen

Parameter	Description	Default Value
PCIe Port	Enables, disables, or automatically sets the PCIe port parameters. The menu options are as follows: • **Auto**: Enables the PCIe device and its related parameter settings when a device is installed in the PCIe slot corresponding to the PCIe port. Disables the PCIe device and its related parameter settings when no device is installed in the PCIe slot corresponding to the PCIe port. • **Enabled**: Enables the PCIe port. • **Disabled**: Disables the PCIe port. • **Only Disable Boot Driver**: Disables only the boot driver.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Link Speed	Sets the link speed of a PCIe port. The menu options are as follows: ● **Auto** ● **Gen 1 (2.5 GT/s)** ● **Gen 2 (5 GT/s)** ● **Gen 3 (8 GT/s)** ● **Gen 4 (16 GT/s)** ● **Gen 5 (32 GT/s)** **NOTE** This parameter is unavailable when **PCIe Port** is set to **Disabled**.	Auto
PCIe Port DeEmphasis Level	Sets de-emphasis for a PCIe port. The menu options are as follows: ● **-6.0 dB** ● **-3.5 dB** **NOTE** ● This parameter is unavailable when **Link Speed** is set to **Gen 1 (2.5 GT/s)**. ● This parameter is unavailable when **PCIe Port** is set to **Disabled**.	**-6.0 dB**
PCIe Port Link Status	Displays the PCIe port link status.	-
PCIe Port Link Max Width	Displays the maximum link bandwidth of a PCIe port.	-
PCIe Port Link Speed	Displays the link speed of a PCIe port. **NOTE** This parameter is unavailable when **PCIe Port** is set to **Disabled**.	-
Data Link Feature Exchange	Enables or disables the data link function negotiation in the data link feature capabilities register (DLFCAP). The menu options are as follows: ● **Auto** ● **Enabled** ● **Disabled**	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Port Max Payload Size	Sets the maximum payload size for a PCIe port. The menu options are as follows: ● **128B** ● **256B** ● **512B** ● **Auto**	Auto
PCIe Completion Timeout Value	Sets the timeout period of PCIe transfer completion. The menu options are as follows: ● **50us to 50ms** ● **50us to 100us** ● **1ms to 10ms** ● **16ms to 55ms** ● **65ms to 210ms** ● **260ms to 900ms** ● **1s to 3.5s** ● **Disabled**	**260ms to 900ms**
PCIe ASPM Support	Set the PCIe Active-state power management (ASPM) function for the PCIe device on the corresponding port. The ASPM function can save power in the PCIe subsystem and reduce the power state of the PCIe link when the PCIe device is not in use. ASPM controls the power state of both ends of the link. The menu options are as follows: ● **L1 Only**: Enters L1 mode only. ● **Disabled**: Disables this function. **NOTE** This parameter is available when **PCIe ASPM Support (Global)** is set to **Per Individual port** on the **Miscellaneous Configuration** screen.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Port L1 Exit Latency	Sets the time required by this port to complete the transition from L1 to L0. The menu options are as follows: ● **<1uS** ● **1uS - 2uS** ● **2uS - 4uS** ● **4uS - 8uS** ● **8uS - 16uS** ● **16uS - 32uS** ● **32uS - 64uS** ● **>64uS** **NOTE** This parameter is available when **PCIe ASPM Support** is set to **L1 Only**.	**8uS - 16uS**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe 10-bit Tag Support	Sets the PCIe 10-bit Tag Support function. When this parameter is set to **Disabled**, PCIe 10-bit Tag Requester support can be disabled in the PCIe root port hierarchy. When this parameter is set to **Auto**, the hardware defaults are retained. Advanced users can set this parameter to **Force Enable** to forcibly enable the 10-bit Tag Requester in a hierarchy where the root port supports the 10-bit Tag Completer, but not all nodes support the 10-bit Tag Completer. The user guarantees that there will be no point-to-point traffic tag completer function from a node with 10-bit Tag Requester capability to a node without 10-bit Tag Requester capability. In this hierarchy, the 10-bit Tag Requester is not enabled in the root port, regardless of root port capabilities. The menu options are as follows: ● **Disabled**: Disables PCIe 10-bit support for this device. ● **Auto**: Retains the hardware device's default value. ● **Force Enabled**: Forces PCIe 10-bit support for this device (**Force Enable** for BIOS versions earlier than 01.01.06.03).	Auto
MCTP	Enables or disables the Management Component Transport Protocol (MCTP) menu. The menu options are as follows: ● **Disabled** ● **Enabled**	Enabled
Equalization Bypass To Highest Rate	Enables or disables the function of Equalization Bypass To Highest Rate. The menu options are as follows: ● **Disabled** ● **Enabled**	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CXL Drift Buffer	Enables or disables the CXL drift buffer if there is a common reference clock. The menu options are as follows: • **Disabled** • **Enabled**	Disabled

5.2.7.5.2 IOAT Configuration

On the **IOAT Configuration** screen, you can configure IOAT. **Figure 5-50** shows the **IOAT Configuration** screen. **Table 5-43** describes the parameters.

Figure 5-50 IOAT Configuration screen

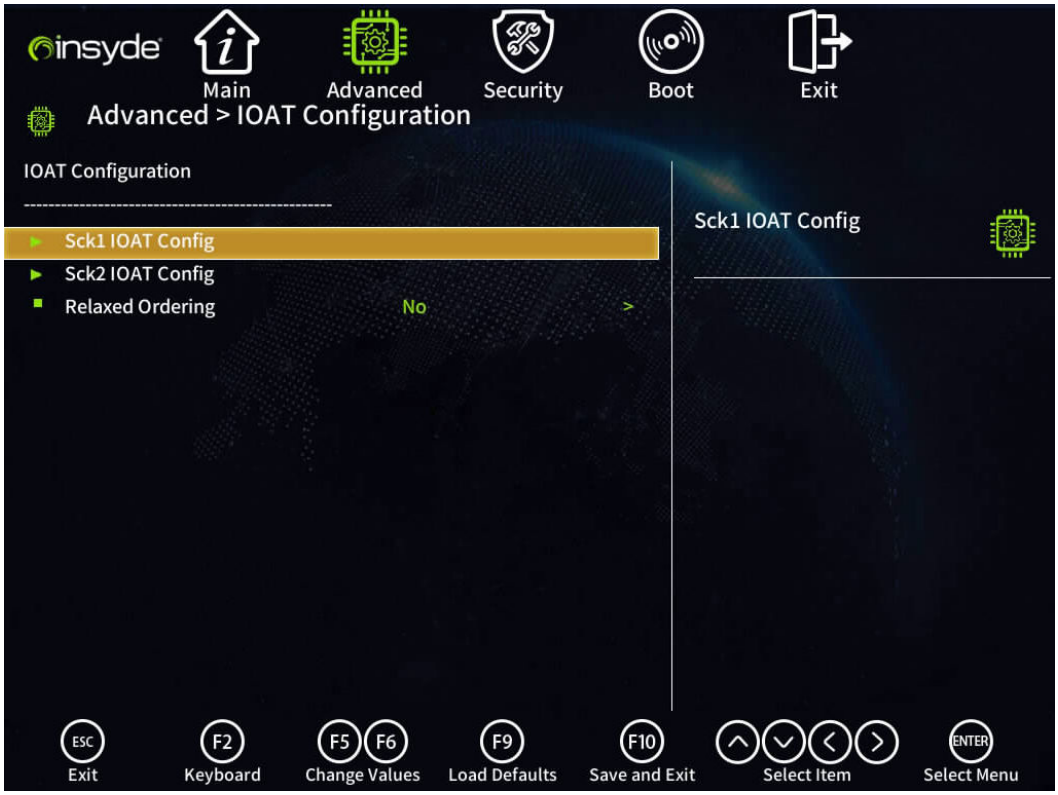


Table 5-43 Parameters on the IOAT Configuration screen

Parameter	Description	Default Value
Sck*X* IOAT Config	Displays Sck*X* IOAT configuration information.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Relaxed Ordering	Enables or disables the Relaxed Ordering function. The menu options are as follows: • **No** • **Yes**	No

Sck*X* IOAT Config

This screen provides access to IOAT configurations of SckX. **Figure 5-51** shows the **SckXX IOAT Config** screen. **Table 5-44** describes the parameters.

Figure 5-51 SckX IOAT Config screen

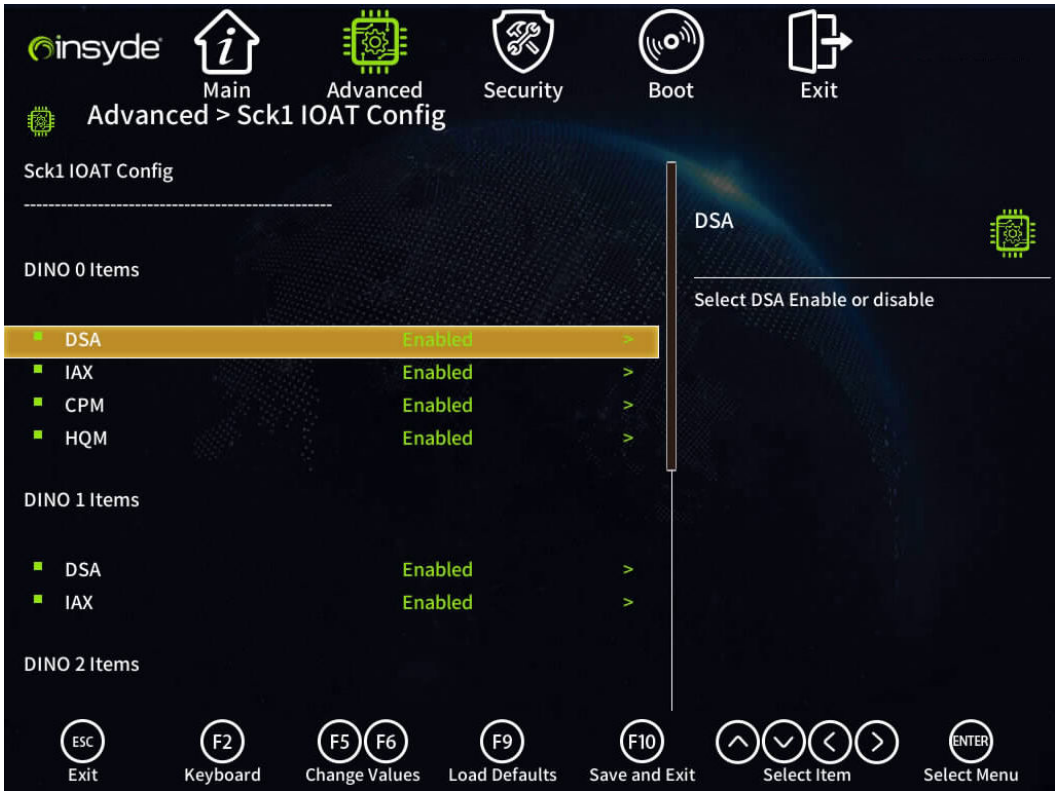


Table 5-44 Parameters on the SckX IOAT Config screen

Parameter	Description	Default Value
DSA	Enables or disables DSA. The menu options are as follows: • **Disabled** • **Enabled**	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IAX	Enables or disables IAX. The menu options are as follows: ● **Disabled** ● **Enabled**	Enabled
CPM	Enables or disables CPM to check whether the driver used to enable QAT is available. The menu options are as follows: ● **Disabled** ● **Enabled** **NOTE** Whether this parameter is supported and its options depend on the CPU configuration of the server. When the CPU type supports QAT, the parameter is available.	Enabled
HQM	Enables or disables HQM. The menu options are as follows: ● **Disabled** ● **Enabled** **NOTE** Whether this parameter is supported and its options depend on the CPU configuration of the server. When the CPU type supports QAT, the parameter is available.	Enabled

5.2.7.5.3 IIO Stack IO Resource Configuration

On the **IIO Stack IO Resource Configuration** screen, you can configure IIO Stack. **Figure 5-52** shows the **IIO Stack IO Resource Configuration** screen. **Table 5-45** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-52 IIO Stack IO Resource Configuration screen



Table 5-45 Parameters on the IIO Stack IO Resource Configuration screen

Parameter	Description	Default Value
Socket*X* Configuration	Displays the CPU*X* configuration information.	-
IIO Stack *X*	Enables or disables the default I/O resources of the request stack. The menu options are as follows: • Enabled • Disabled	Enabled

5.2.7.5.4 Intel Virtualization for Directed I/O(VT-d)

On the **Intel Virtualization for Directed I/O(VT-d)** screen, you can configure VT-d. **Figure 5-53** shows the **Intel Virtualization for Directed I/O (VT-d)** screen. **Table 5-46** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-53 Intel Virtualization for Directed I/O (VT-d) screen



Table 5-46 Parameters on the Intel Virtualization for Directed I/O (VT-d) screen

Parameter	Description	Default Value
Intel VT for Directed I/O (VT-d)	Enables or disables the Intel Virtualization Technology for Directed I/O (Intel VT-d feature). The VT-d feature enables the virtual machine manager (VMM) to manage multiple VMs by using one physical I/O device. The menu options are as follows: • Enabled • Disabled **NOTE** • This parameter can be set but will not take effect when **Extended APIC** is set to **Enabled**. • To disable the **VT-d**, need to set **Extended APIC** to **Disabled** first.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Cache Allocation	Enables or disables cache allocation. The menu options are as follows: ● Enabled ● Disabled	Enabled
Opt-Out Illegal MSI Mitigation	Enables or disables exiting illegal MSI mitigation. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **Intel VT for Directed I/O (VT-d)** is set to **Disabled**.	Disabled
DMA Control Opt-In Flag	Enables or disables DMA_CTRL_PLATFORM_OPT_IN_FLAG in the ACPI's DMAR table. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **Intel VT for Directed I/O (VT-d)** is set to **Disabled**.	Disabled
Interrupt Remapping	Enables or disables the VT-d interrupt remapping function. After this function is enabled, the interrupt remapping function can be provided for directed I/O. Even if the management programs and OSs are not used, you can also enable this option. The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** This parameter is unavailable when **Intel(R) VT for Directed I/O (VT-d)** is set to **Disabled**.	Auto
SATC Support	Enables or disables SATC support. The menu options are as follows: ● Enabled ● Disabled	Enabled

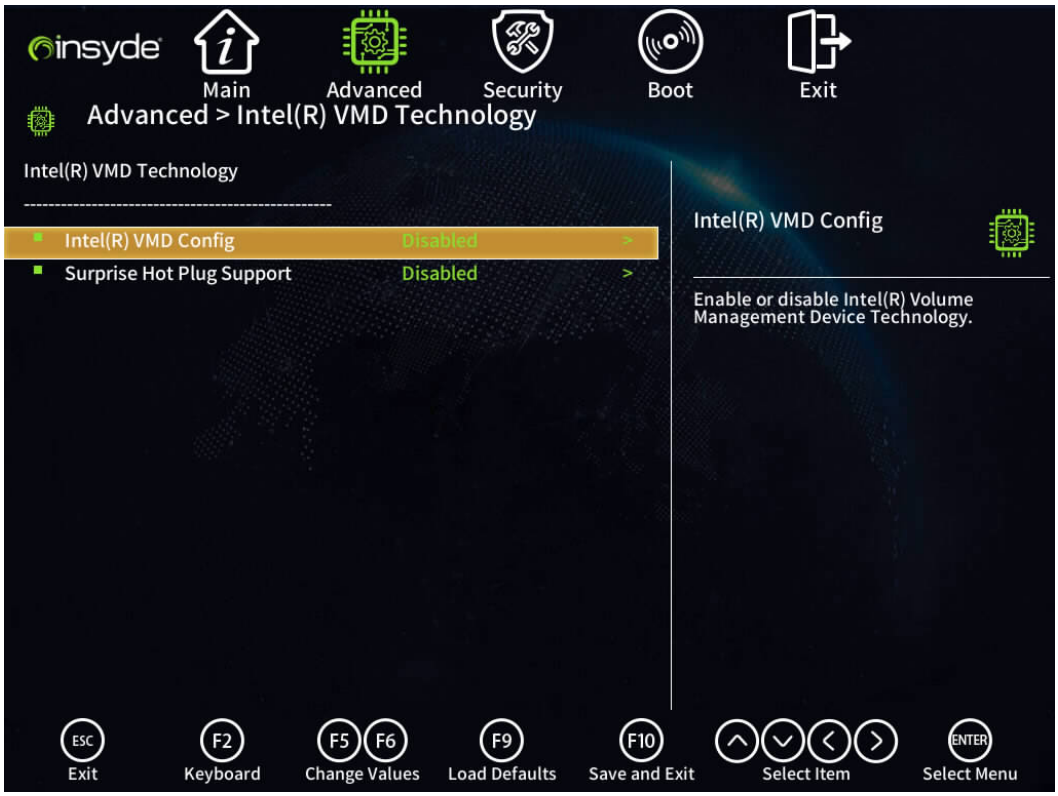
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
RHSA Support	Enables or disables RHSA support. The menu options are as follows: ● Enabled ● Disabled	Enabled

5.2.7.5.5 Intel(R) VMD Technology

On this screen, you can configure PCIe VMD. **Figure 5-54** shows the **Intel(R) VMD Technology** screen. **Table 5-47** describes the parameter.

Figure 5-54 Intel(R) VMD Technology screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-47 Parameter on the Intel(R) VMD Technology screen

Parameter	Description	Default Value
Intel(R) VMD Config	Enables or disables the volume management device (VMD) function for PCIe devices. If it is enabled, hot upgrade and replacement of NVMe SSDs through the PCIe bus is supported. In addition, LED management can be standardized to help quickly identify the SSD status. The options are as follows: ● Enabled ● Disabled	Disabled
Surprise Hot Plug Support	Enables or disables the surprise hot plug function of NVMe drives. The options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is unavailable when **Intel(R) VMD Config** is set to **Enabled**. ● This function can be configured only when the BC15NHBC drive backplane is installed on the 5288 V7 server. ● This parameter is supported only in BIOS 01.01.03.13 and later. ● iBMC version matching requirements: The iBMC version is 3.07.03.17 or later. ● CPLD version matching requirements: The drive backplane (BC15NHBC) CPLD version is 1.06 or later.	Disabled

5.2.7.5.6 IIO DFX Configuration

On the **IIO DFX Configuration** screen, you can configure IIO DFX. **Figure 5-55** shows the **IIO DFX Configuration** screen. **Table 5-48** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-55 IIO DFX Configuration screen



Table 5-48 Parameters on the IIO DFX Configuration screen

Parameter	Description	Default Value
Socket*X* Configuration	Provides access to CPU*X* configurations.	-
EV DFX Features	Enables or disables the EV DFX function. The menu options are as follows: ● Enabled ● Disabled	Disabled
CXL Header Bypass	Enables or disables the CXL header bypass. The menu options are as follows: ● Enabled ● Disabled	Disabled
DINO Native PCIe	Enables or disables native PCIe for DINO devices. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Trace Hub Allocation Flow	Enables or disables allocation writes. The menu options are as follows: • Enabled • Disabled	Enabled

Figure 5-56 shows the **Socket*X* Configuration** screen (**Socket1 Configuration** is used as an example). Table 5-49 describes the parameters.

Figure 5-56 Socket1 Configuration screen

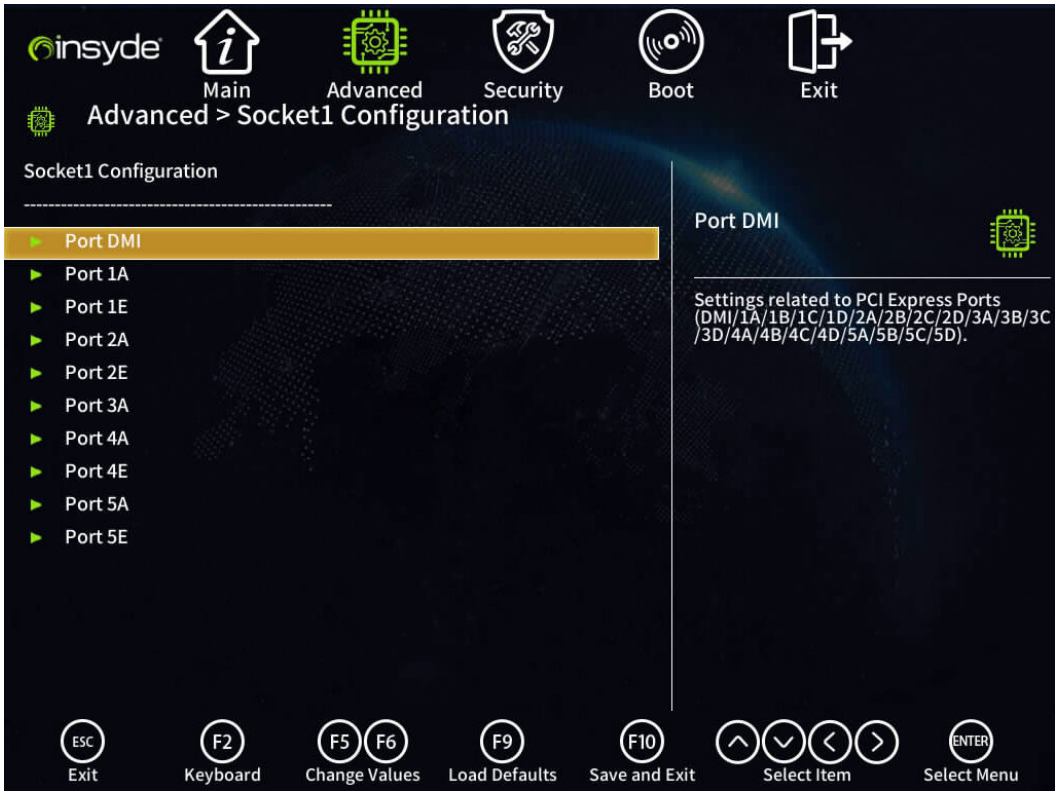


Table 5-49 Parameters on the Socket1 Configuration screen

Parameter	Description
Port *X*	Provides access to PCIe port configurations. **NOTE** The displayed port configuration menu list varies according to server configurations.

Figure 5-57 shows the **Port** *X* screen (the **Port 1A** screen is used as an example). Table 5-50 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-57 Port 1A screen

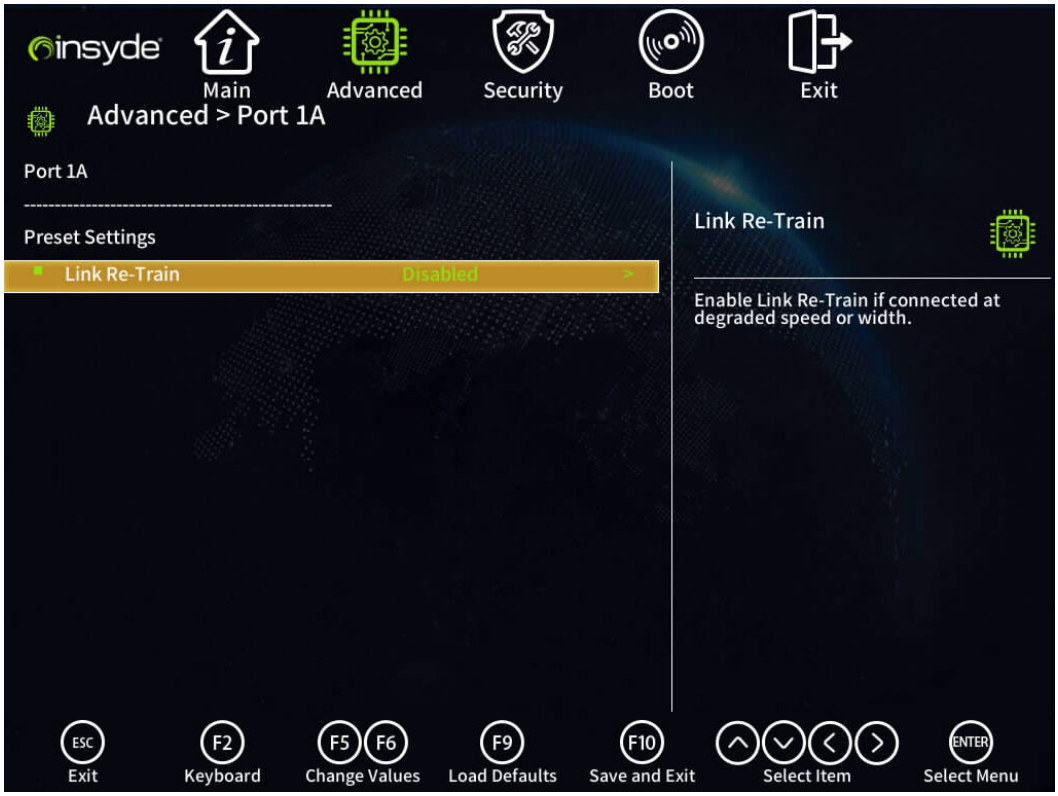


Table 5-50 Parameters on the Port 1A screen

Parameter	Description	Default Value
Link Re-Train	Enables the link retraining function when the link speed or bandwidth decreases. ● Enabled ● Disabled	Disabled

5.2.7.5.7 IIO Global Performance Tuning

On the **IIO Global Performance Tuning** screen, you can configure the I/O global performance parameters. Table 5-51 shows the **IIO Global Performance Tuning** screen. Table 5-51 describes the parameters.

Figure 5-58 IIO Global Performance Tuning screen

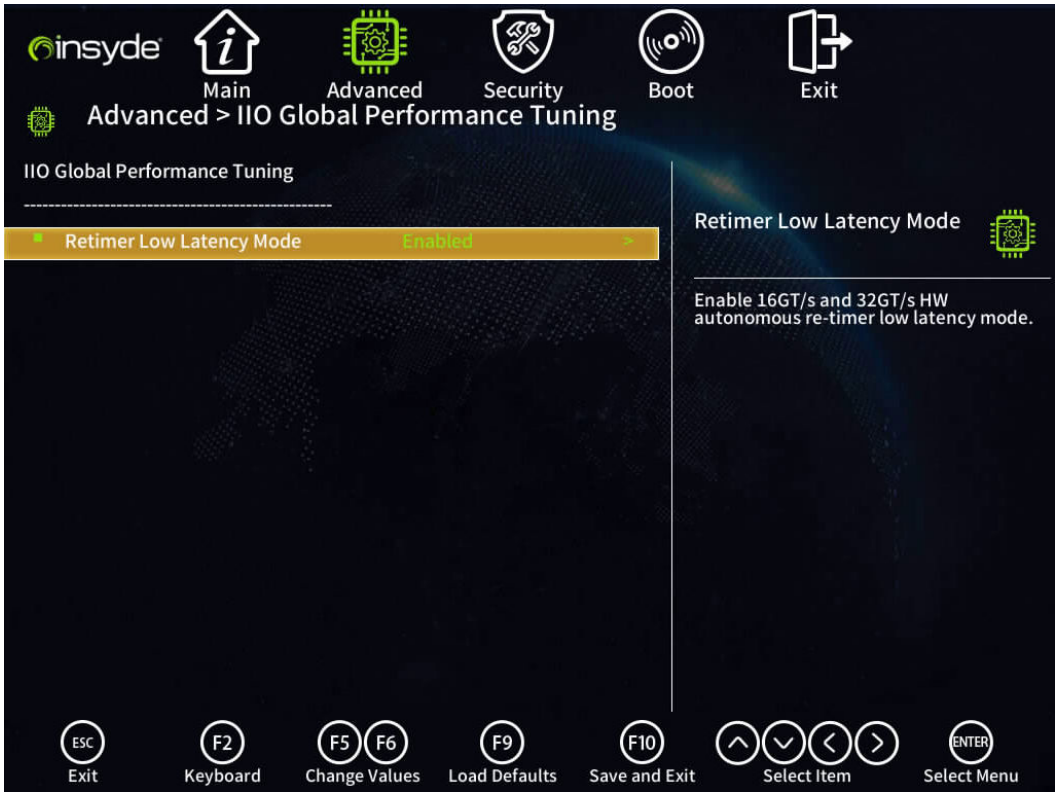


Table 5-51 Parameters on the IIO Global Performance Tuning screen

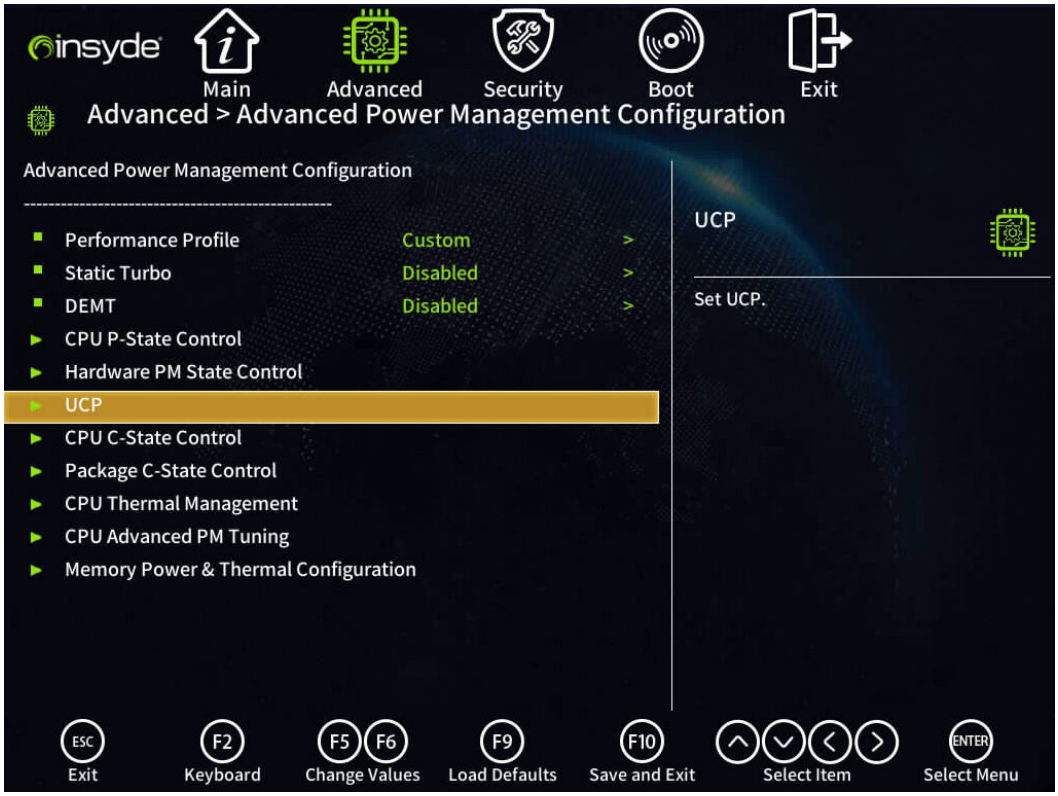
Parameter	Description	Default Value
Retimer Low Latency Mode	Enables or disables 16 GT/s or 32 GT/s hardware autonomous re-timer low latency mode. The menu options are as follows: ● Disabled ● Enabled ● 16GT/s Only ● 32GT/s Only	Enabled

5.2.7.6 Advanced Power Management Configuration

On the **Advanced Power Management Configuration** screen, you can configure advanced power management functions for processors. **Figure 5-59** shows the **Advanced Power Management Configuration** screen. **Table 5-52** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-59 Advanced Power Management Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-52 Parameters on the Advanced Power Management Configuration screen

Parameter	Description	Default Value
Performance Profile	Select an energy efficiency test scenario. The menu options are as follows: ● **Custom**: Specifies the user-defined mode. ● **Efficiency**: Recommended for the high energy efficiency ratio. ● **Performance**: performance prioritized ● **Load Balance**: Power load balance. ● **High RAS**: Recommended for the high reliability mode. ● **HPC**: Recommended for high-performance computing (HPC). ● **General Computing**: Recommended for CPU general computing. ● **Low Latency**: Recommended for real-time transaction and low latency. ● **Server Side Java**: Recommended for high-performance Java on the server side. ● **Memory Throughput**: Recommended for high-performance memory. ● **I/O Throughput**: Recommended for high-performance storage. ● **Energy Saving**: Recommended for low power consumption. ● **NFV**: Recommended configuration for network function virtualization (NFV). **NOTE** For details about the default values for the linkage Options in energy efficiency test scenarios, see **D Linkage Options in Energy Efficiency Test Scenarios (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)**.	Custom

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Static Turbo	Selects a static frequency policy to fix the CPU frequency to a turbo frequency. The menu options are as follows: ● **Disabled**: Disables the static turbo frequency function. ● **Manual**: The frequency is the selected frequency. ● **Auto**: Enables the Static Turbo frequency function and fixes the frequency at the maximum turbo frequency on all cores.	Disabled
CPU Frequency Select	Selects the frequency value between the fundamental frequency and the turbo frequency for input. The unit is 100 MHz. When the input value is less than the fundamental frequency, the fundamental frequency is used. If the input value is greater than the supported maximum Turbo frequency, the maximum Turbo frequency is used. **NOTE** This parameter is available when **Static Turbo** is set to **Manual** or **Auto**.	50
DEMT	Enables or disables the Dynamic Energy Management Technology (DEMT) mode. This mode controls the processor performance and the power state based on processor workload. Enabling this option may have a negative impact on performance, depending on the workload. The menu options are as follows: ● **Enabled** ● **Disabled**	Disabled
SYS_USAGE Threshold	Sets the **SYS_USAGE** threshold. **NOTE** This parameter is available when **DEMT** is set to **Enabled**.	95
SMI Interval	Sets the SMI interval. **NOTE** This parameter is available when **DEMT** is set to **Enabled**.	6

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Low Occupy Control	Enables or disables the low usage control function. The menu options are as follows: ● **Disabled** ● **Enabled** **NOTE** This parameter is available when **DEMT** is set to **Enabled**.	Disabled
CPU P-State Control	Provides access to the **CPU P-state control** menu, where you can set the P-state of the CPU.	-
Hardware **PM State Control**	Provides access to the hardware power management (PM) status control menu, where you can set HWP.	-
Frequency Prioritization	Provides access to the frequency priority function configurations. **NOTE** This parameter is available only when **Hardware P-State** is set to **Native Mode** or **Native Mode with No Legacy Support**.	-
UCP	Provides access to **UCP** function settings.	-
CPU C-State Control	Provides access to the **CPU C-state** configurations, which allows you to control power consumption when the CPU is idle.	-
Package C-State Control	Provides access to the CPU hibernation depth control menu, where you can set the CPU Package C state.	-
CPU Thermal Management	Provides access to the CPU temperature control menu, where you can set the software T-state and CPU duty cycle.	-
CPU Advanced PM Tuning	Provides access to the CPU advanced PM settings menu, where you can adjust the power performance.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory Power & Thermal Configuration	Provides access to the memory power and thermal configuration menu, where you can set the memory power consumption and thermal features.	-

5.2.7.6.1 CPU P-State Control

On the **CPU P-State Control** screen, you can configure the CPU P-state. **Figure 5-60** shows the **CPU P-State Control** screen. **Table 5-53** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the CPU configuration of the server.

Figure 5-60 CPU P-State Control screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-61 CPU P-State Control screen 2



Table 5-53 Parameters on the CPU P-State Control screen

Parameter	Description	Default Value
AVX License Pre-Grant Override	Enables or disables AVX ICCP pre-grant level override. The menu options are as follows: ● Enabled ● Disabled	Disabled
AVX ICCP pre-grant Level	Specifies the pre-grant AVX levels. The menu options are as follows: ● 128 Heavy ● 256 Light ● 256 Heavy ● 512 Light ● 512 Heavy **NOTE** This parameter is available when **AVX License Pre-Grant Override** is set to **Enabled**.	128 Heavy

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
AVX P1	Sets the AVX P1 level. The menu options are as follows: ● Nomimal ● Level 1 ● Level 2 **NOTE** This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	Nomimal
Intel SST-PP	Sets Intel SST-PP (Speed Select Technology-Performance Profile). The menu options are as follows: ● Auto ● Level 0 ● Level 1 ● Level 2 ● Level 3 ● Level 4 **NOTE** ● Whether or not this parameter is supported and the value of this parameter depend on the CPU configuration of the server. If the CPU does not support this function, this parameter is unavailable. ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**. ● This parameter is unavailable when **Dynamic SST-PP** is set to **Enabled** and **AVX P1** is set to **Nominal**.	Auto
Dynamic SST-PP	Enables or disables dynamic SST-PP (Speed Select Technology-Performance Profile). The menu options are as follows: ● **Enabled**: dynamic SST-PP ● **Disabled**: static SST-PP **NOTE** ● Whether this parameter is supported depends on the CPU configuration of the server. ● This parameter is unavailable when **AVX P1** is set to **Nominal**. ● This parameter is unavailable when **Hardware P-State** is set to **Disable** or **Out of Band Mode**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SpeedStep (Pstates)	Enables or disables the EIST (P state). The Enhanced Intel SpeedStep Technology (EIST) can automatically adjust the voltage and frequency of the processor based on the system workload to reduce power consumption and heat. The options are as follows: ● Enabled ● Disabled	Enabled
EIST PSD Function	Specifies whether the P-state among CPUs are coordinated by the HW or SW. The options are as follows: ● **HW_ALL**: The processor hardware is responsible for coordinating the P-state among logical processors with dependencies. The OS is responsible for keeping the P-state request up to date on all logical processors. ● **SW_ALL**: The OS Power Manager is responsible for coordinating the P-state among logical processors with dependencies and must initiate the transition on all of those logical processors. **NOTE** This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	HW_ALL

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Boot Performance Mode	Selects the boot performance mode. The menu options are as follows: ● **Max Performance**: The boot performance is set to the maximum performance mode. ● **Max Efficiency**: The boot performance is set to the most efficient mode. ● **Set by Intel Node Manager**: The startup performance is controlled by ME. **NOTE** This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	Max Performance
Energy Efficient Turbo	Enables or disables the energy-efficient turbo mode. Controls whether the processor uses power-saving Turbo mode. The menu options are as follows: ● Enabled ● Disabled	Enabled
Turbo Mode	Enables or disables the dynamic acceleration (turbo) mode. The menu options are as follows: ● Enabled: Enables Turbo mode. When enabled, it intelligently increases the CPU speed based on workload, until the maximum Turbo frequency is reached. ● Disabled: Disables Turbo mode. **NOTE** ● If the CPU does not support the **Turbo Mode** feature, the value of **Turbo Mode** is displayed as **Disabled** and cannot be changed. ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PSS Table Turbo Frequency	Select the ACPI _PSS table turbo frequency. The default is the maximum non-turbo frequency plus 1MHz. ● Max Non-Turbo Frequency Plus One ● Max Turbo Frequency **NOTE** Only BIOS version 01.01.03.05 and later supports this parameter.	Max Non-Turbo Frequency Plus One
CPU Flex Ratio Override	Enables or disables the CPU frequency reset function in non-turbo mode. The options are as follows: ● Enabled: Allows modification of the CPU core frequency. When this option is selected, the CPU core frequency can be modified. ● Disabled: Disables modification of the CPU core frequency.	Disabled
CPU Core Flex Ratio	Sets the core frequency of the processor in non-Turbo mode. The value must be a ratio supported by the CPU. **NOTE** This parameter is available when **CPU Flex Ratio Override** is set to **Enabled**.	23

5.2.7.6.2 Hardware PM State Control

On the **Hardware PM State Control** screen, you can configure the hardware P-state. **Figure 5-62** shows the **Hardware PM State Control** screen. **Table 5-54** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-62 Hardware PM State Control screen

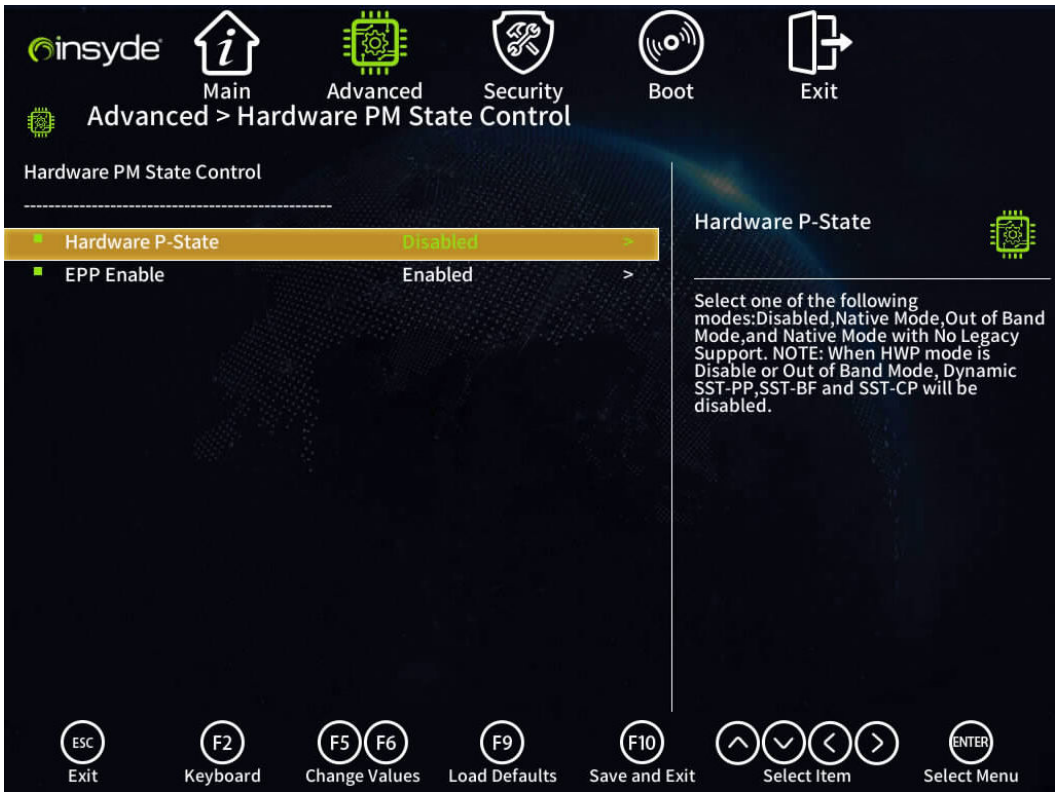


Table 5-54 Parameters on the Hardware PM State Control screen

Parameter	Description	Default Value
Hardware P-State	Sets the hardware P-state. The menu options are as follows: ● **Disabled**: Disables HWP. ● **Native Mode**: The OS directly accesses the HWPM register to configure the CPU. This mode supports the traditional ACPI table (_pct_pss\ppc) and the new ACPI specifications (_CPC v2). ● **Out of Band Mode**: The OS cannot access the HWPM register. The CPU can be configured only through the BMC in out-of-band mode. ● **Native Mode with No Legacy Support**: The native mode that is not traditionally supported. This mode is same as **Native Mode** except that it supports only the new ACPI specifications (_CPC V2).	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
EPP Enable	Enables or disables the energy performance preference (EPP). The menu options are as follows: ● Enabled: Enables EPP. ● Disabled: When disabled, uses EPB (ENEGY_PERF_BIAS) as EPP. **NOTE** This parameter is unavailable when **Hardware P-State** is set to **Disabled**.	Enabled
EPP profile	Sets the EPP policy. The menu options are as follows: ● **Performance**: performance prioritized ● **Balanced Performance**: performance balanced ● **Balanced Power**: power balanced ● **Power**: energy saving prioritized **NOTE** ● This parameter is available when **Hardware P-State** is set to **Out of Band Mode**. ● This parameter is unavailable when **EPP Enable** is set to **Disabled**.	Balanced Performance
Intel(R) Turbo Boost Max Technology 3.0	Enables or disables the Intel turbo boost max technology 3.0 support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the system supports the Intel turbo boost max technology 3.0.	Enabled

5.2.7.6.3 Frequency Prioritization

On the **Frequency Prioritization** screen, you can configure the CPU frequency priority function. **Figure 5-63** shows the **Frequency Prioritization** screen. **Table 5-55** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-63 Frequency Prioritization screen



Table 5-55 Parameters on the Frequency Prioritization screen

Parameter	Description	Default Value
SST-CP	Enables or disables the AVX ICCP pre-authorization level override function. The menu options are as follows: ● Enabled ● Disabled	Disabled

5.2.7.6.4 UCP

On this screen, you can configure the UCP function. **Figure 5-64** shows the Set UCP screen. **Table 5-56** describes the parameters.

Figure 5-64 UCP screen



Table 5-56 Parameters on the UCP screen

Parameter	Description	Default Value
UFMT	Enables or disables the Uncore Frequency Management Technology (UFMT) mode. When UFMT is enabled, UFS settings are overwritten. The menu options are as follows: • **Enabled** • **Disabled**	Disabled
URx	Specifies the maximum uncore ratio limit when the workload reaches *x* %. **NOTE** This parameter is available when **UFMT** is set to **Enabled**.	-

5.2.7.6.5 CPU C-State Control

On the **CPU C-State Control** screen, you can configure the CPU C-state. **Figure 5-65** shows the **CPU C-State Control** screen. **Table 5-57** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-65 CPU C-State Control screen



Table 5-57 Parameters on the CPU C-State Control screen

Parameter	Description	Default Value
Enable Monitor MWAIT	Enables or disables the MONITOR MWAIT instruction. Executing this command can monitor the CPU status to optimize the CPU instruction running. If this option is enabled, some OSs may obtain the capability of automatically adjusting energy saving options. Therefore, disable this parameter if you want to disable energy saving. The options are as follows: ● Auto ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CPU C6 Report	Sets the feature of reporting CPU C6 (ACPI C3) information to the OS. If this parameter is set to **Auto**, this feature is disabled when the CPU does not support it. The options are as follows: ● Auto: Reporting the C6 status to the operating system is enabled by default. ● Enabled: Reporting the C6 status to the operating system is enabled. ● Disabled: Reporting the C6 status to the operating system is disabled.	Disabled
Enhanced Halt State (C1E)	Enables or disables the enhanced halt state (C1E) function. The options are as follows: ● Enabled: When this feature is enabled, the operating system automatically adjusts the CPU to its lowest performance state when the processor is idle. ● Disabled: Disables the Enhanced Halt State feature.	Disabled
C1E OS Indicator	Enables or disables the CPU global C1E-state indicator of the OS. ● Enabled ● Disabled **NOTE** This parameter is available only when **Enable Monitor MWAIT** is set to **Enabled**.	Disabled
C6 OS Indicator	Enables or disables the CPU C6 status indicator of the OS. ● Enabled ● Disabled **NOTE** This parameter is available only when **Enable Monitor MWAIT** is set to **Enabled** and **CPU C6 Report** is set to **Auto** or **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.7.6.6 Package C-State Control

On the **Package C-State Control** screen, you can configure the CPU Package C-state. **Figure 5-66** shows the **Package C-State Control** screen. **Table 5-58** describes the parameters.

Figure 5-66 Package C-State Control screen

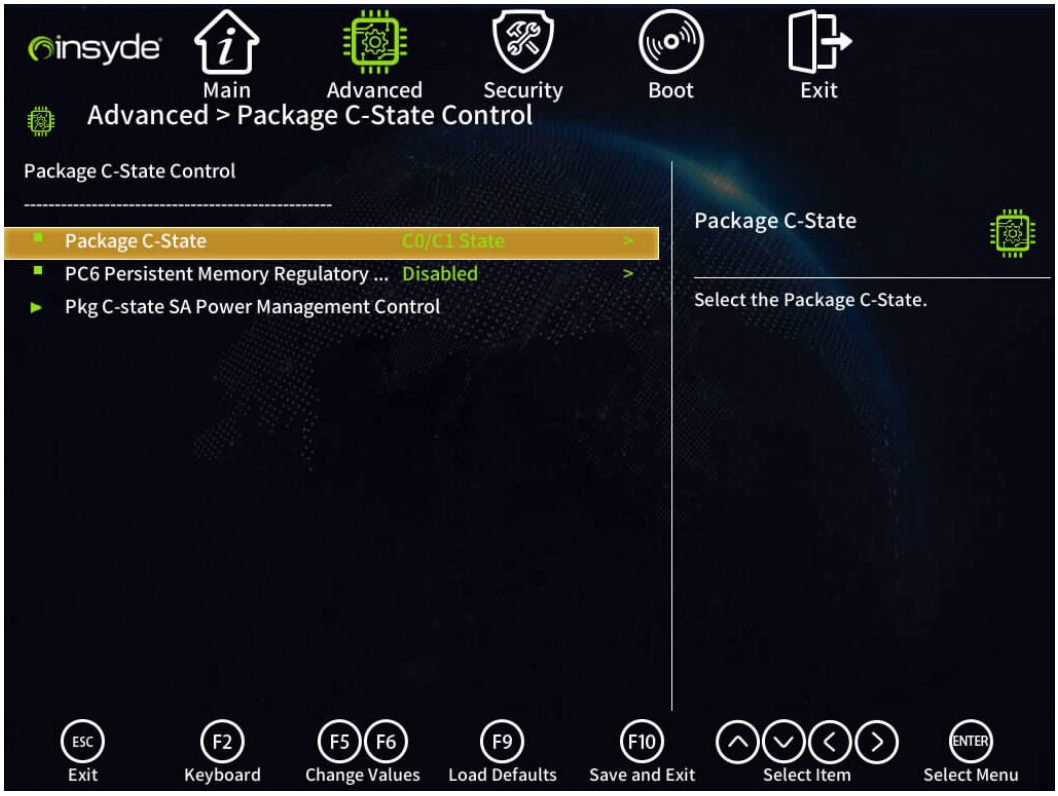


Table 5-58 Parameters on the Package C-State Control screen

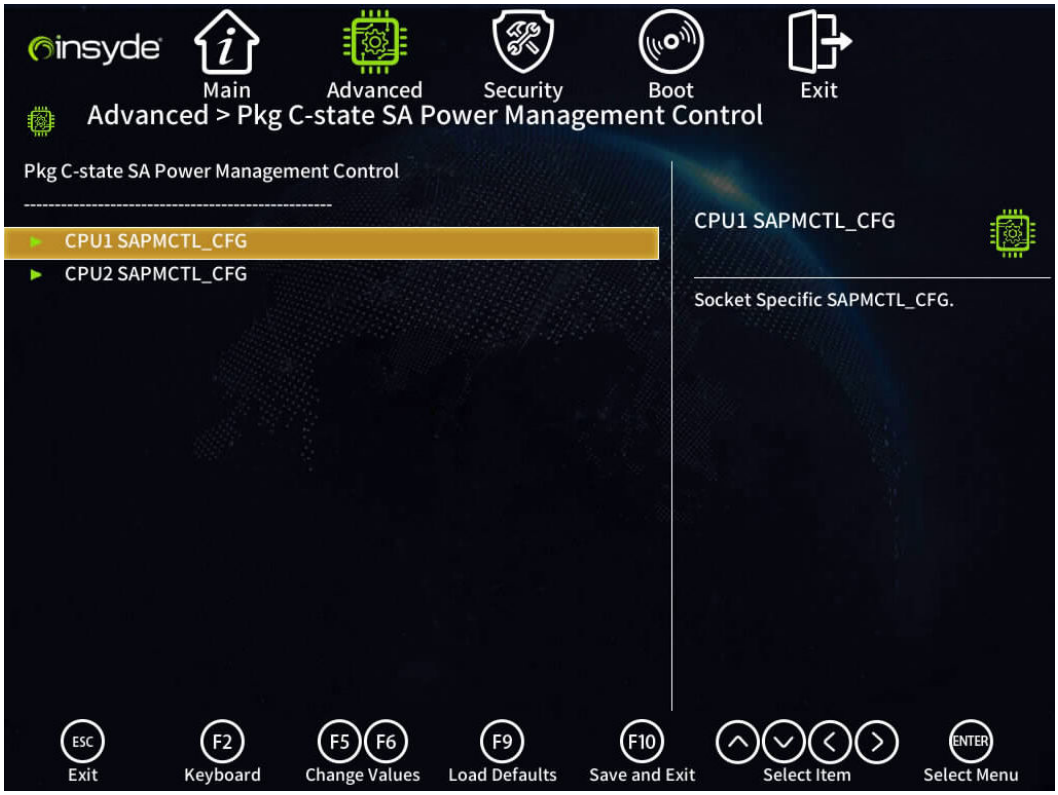
Parameter	Description	Default Value
Package C-State	Sets the deep energy saving. The menu options are as follows: ● C0/C1 State ● C2 State ● C6 (Non-Retention State) ● C6 (Retention State) ● No Limit ● Auto	C0/C1 State

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PC6 Persistent Memory Regulatory Test Mode	Enables or disables the PC6 persistent memory regulatory test mode. The menu options are as follows: ● Disabled ● Enabled **NOTE** This parameter is available when **Package C-State** is not set to **C0/C1 State** or **C2 State** and the CPU model is **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Disabled
Pkg C-state SA Power Management Control	Provides access to package C-state SA power management control configurations.	-

Figure 5-67 shows the **Pkg C-state SA Power Management Control** screen. **Table 5-59** describes the parameters.

Figure 5-67 Pkg C-state SA Power Management Control screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-59 Parameters on the Pkg C-state SA Power Management Control screen

Parameter	Description	Default Value
CPU*X* SAPMCTL_CFG	Provides access to CPU*X* package C-state SA power management control configurations.	-

Figure 5-68 shows the **CPU*X* SAPMCTL_CFG** screen (**CPU1 SAPMCTL_CFG** is used as an example). **Table 5-60** describes the parameters.

Figure 5-68 CPU1 SAPMCTL_CFG screen

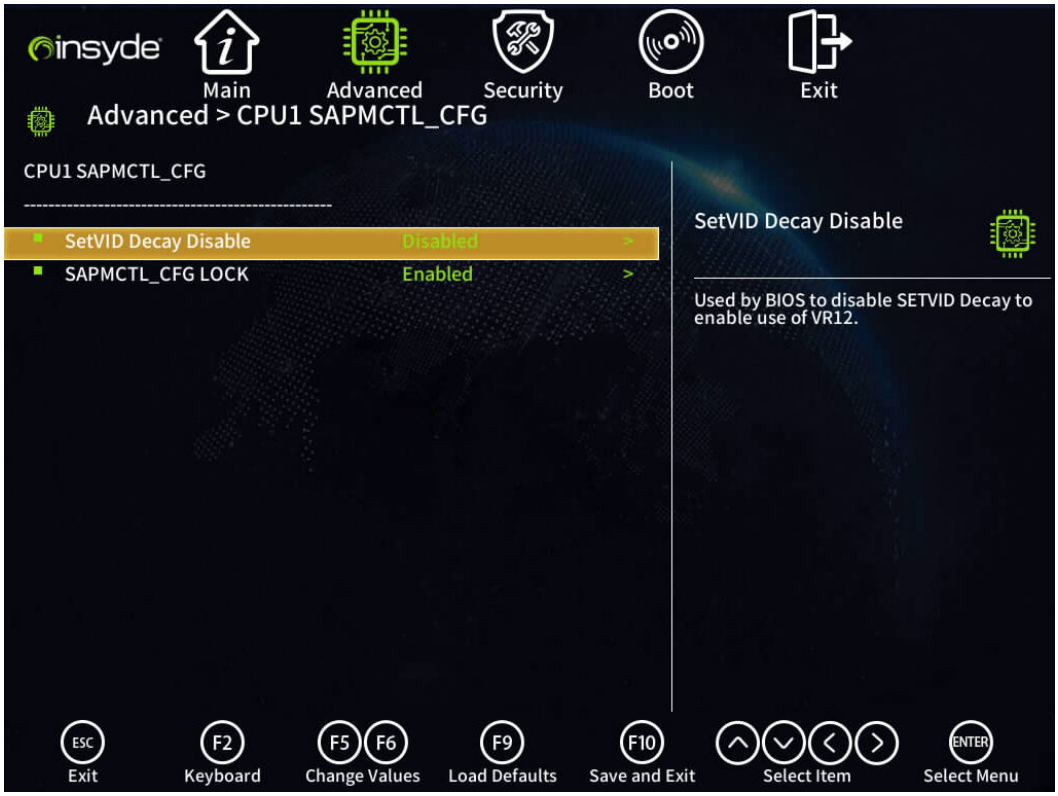


Table 5-60 Parameters on the CPU1 SAPMCTL_CFG screen

Parameter	Description	Default Value
SetVID Decay Disable	Enables or disables SetVID Decay. The menu options are as follows: • Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SAPMCTL_CFG LOCK	Enables or disables the SA power management control lock. The menu options are as follows: ● Disabled ● Enabled	Enabled

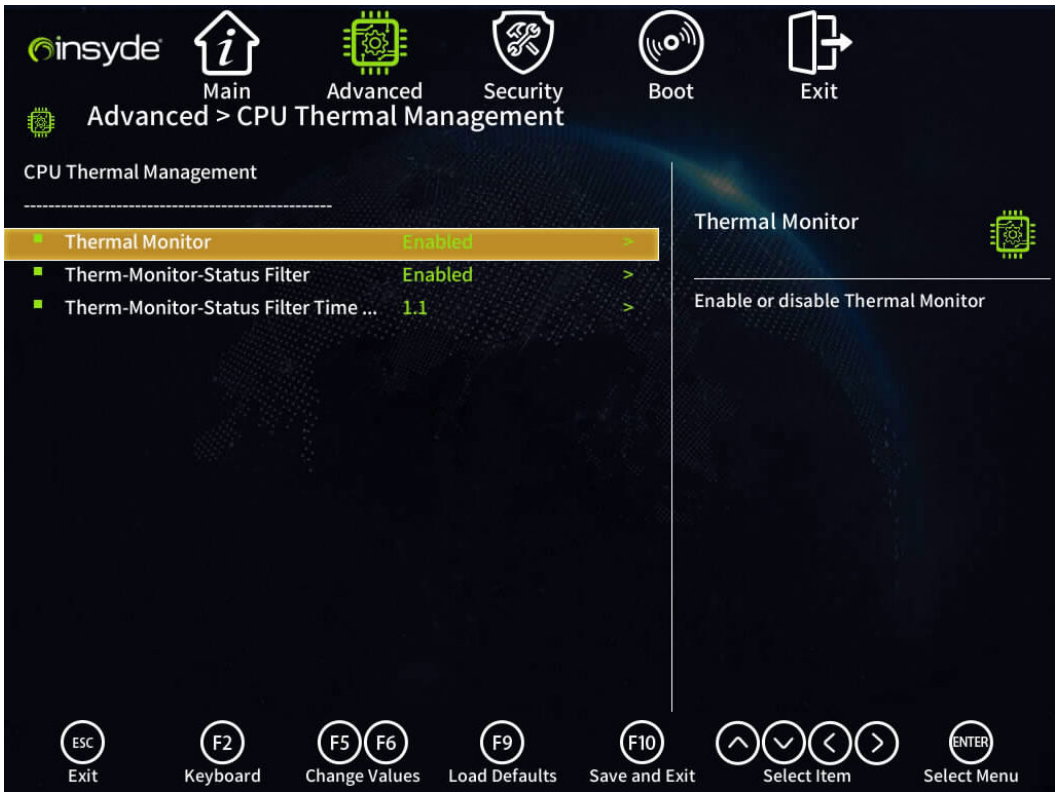
5.2.7.6.7 CPU Thermal Management

On the **CPU Thermal Management** screen, you can configure the CPU temperature. Figure 5-69 shows the **CPU Thermal Management** screen. Table 5-61 describes the parameters.

NOTE

The parameters on this screen are displayed based on the actual server configuration.

Figure 5-69 CPU Thermal Management screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-61 Parameters on the CPU Thermal Management screen

Parameter	Description	Default Value
Thermal Monitor	Enables or disables the thermal monitor. The menu options are as follows: ● Enabled ● Disabled	Enabled
Therm-Monitor-Status Filter	Enables the therm_monitor_status(IA32_THERM_STATUS[0]) based report of the filter. The menu options are as follows: ● Enabled ● Disabled	Enabled
Therm-Monitor-Status Filter Time Window	Sets the time window (in seconds) for the filter. The menu options are as follows: ● 0.07 ● 0.1 ● 0.24 ● 0.4 ● 1.1 ● 2.2 ● 4.64 ● 9.29 ● 18.8 ● 37.7 ● 75.5 ● 151 ● 302 **NOTE** This parameter is available when the CPU model is **Sapphire Rapids-SP** or **Emerald Rapids-SP** and **Thermal Monitor** and **Therm-Monitor-Status Filter** are set to **Enabled**.	1.1

5.2.7.6.8 CPU Advanced PM Tuning

On the **CPU Advanced PM Tuning** screen, you can adjust advanced PM settings for CPUs. **Figure 5-70**, **Figure 5-71**, or **Figure 5-72** shows the **CPU Advanced PM Tuning** screen. **Table 5-62** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-70 CPU Advanced PM Tuning screen 1

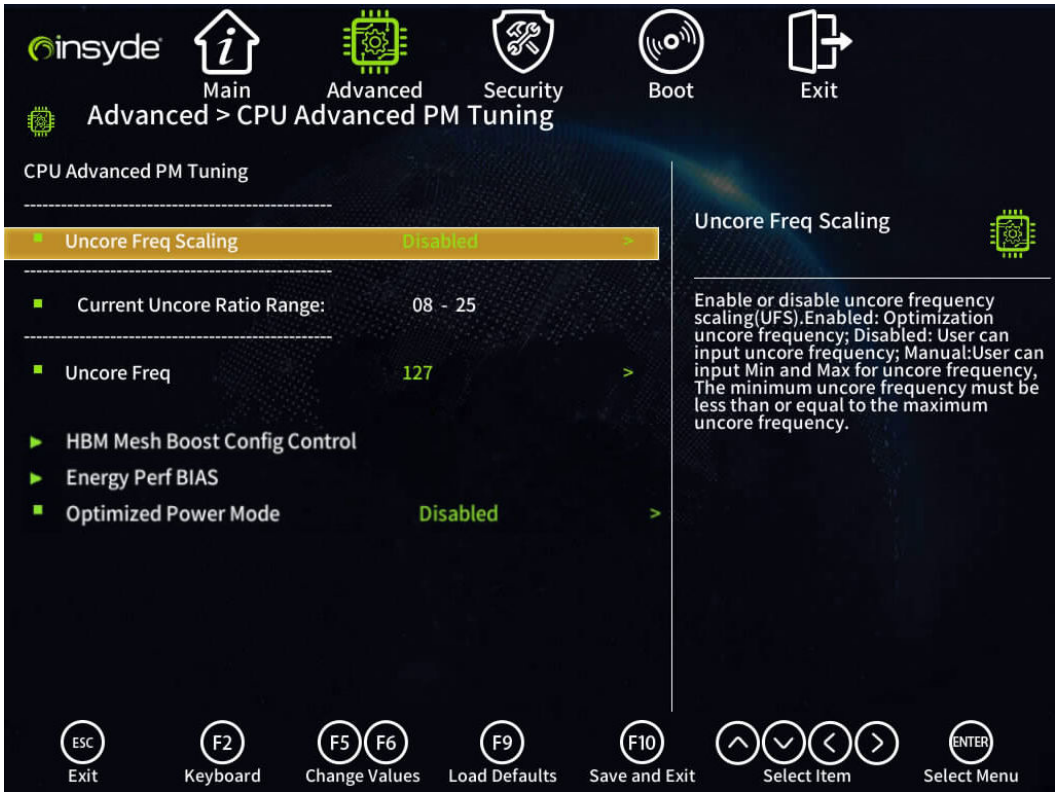
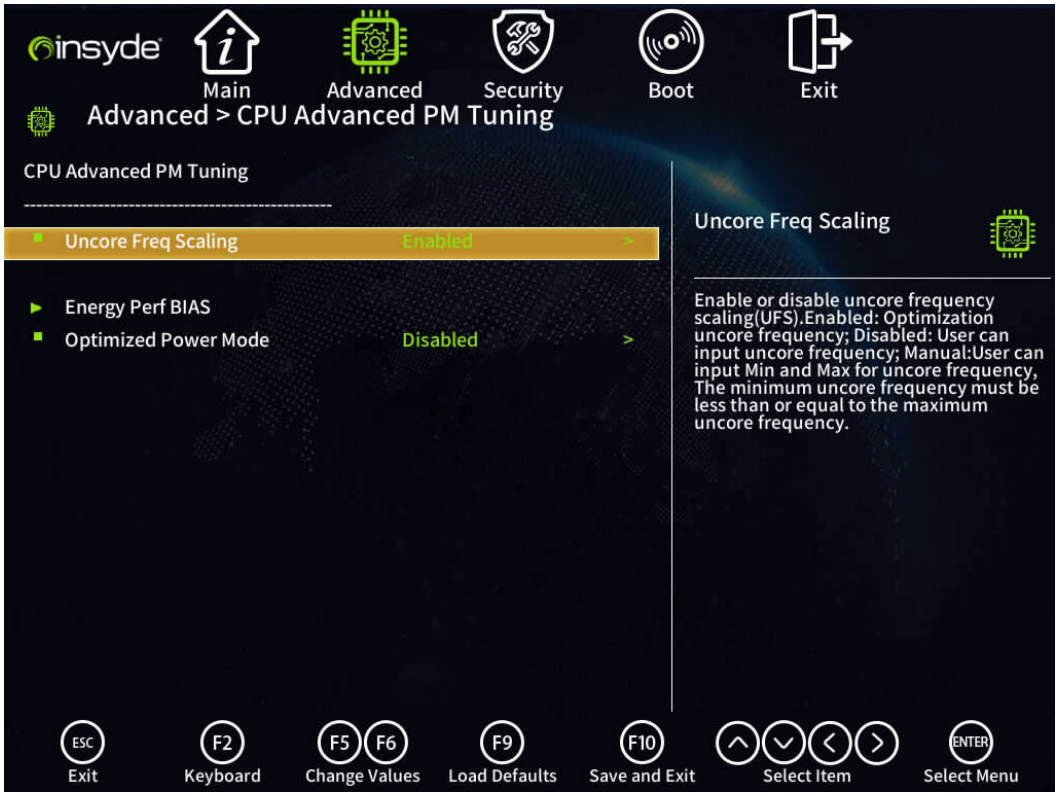


Figure 5-71 CPU Advanced PM Tuning screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-72 CPU Advanced PM Tuning screen 3

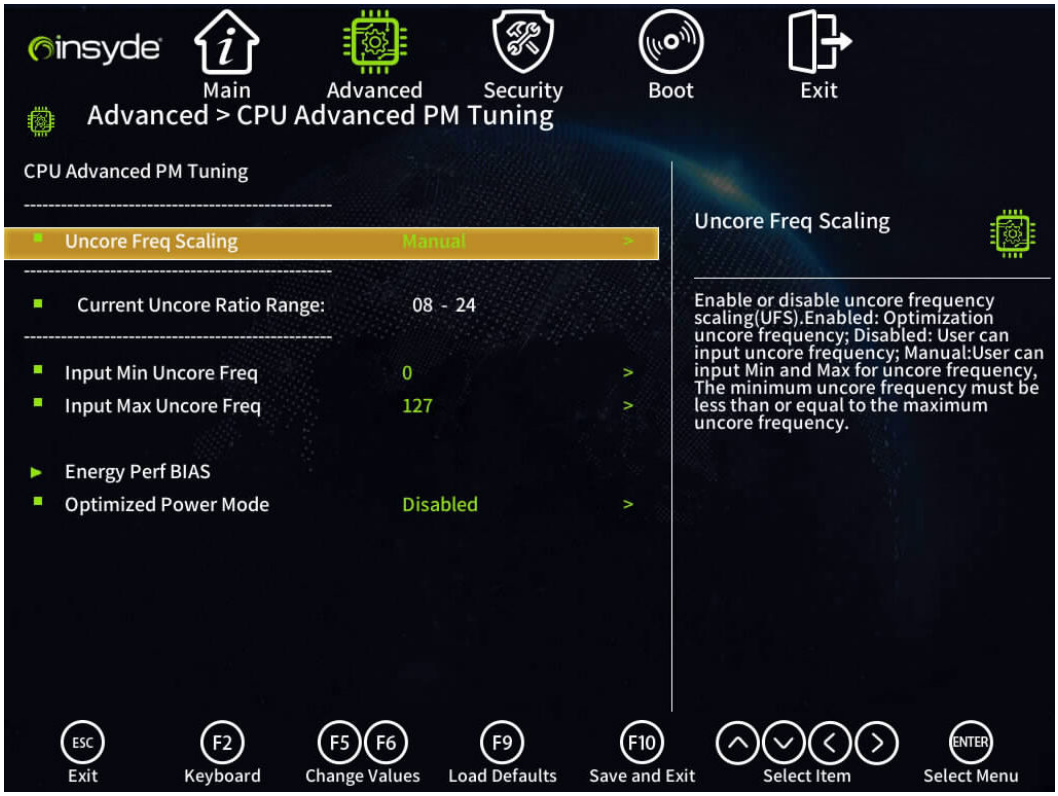


Table 5-62 Parameters on the CPU Advanced PM Tuning screen

Parameter	Description	Default Value
Uncore Freq Scaling	Enables or disables the non-core frequency scaling function. After this function is disabled, you can set non-core frequencies. The menu options are as follows: • **Enabled**: Enables uncore frequency scaling, which better distributes power across the core and uncore, maximizing performance without wasting power. • **Disabled**: Disables uncore frequency scaling. When disabled, users can customize uncore frequencies. • **Manual**	Enabled
Current Uncore Ratio Range	Current non-core frequency range. **NOTE** This parameter is available when **Uncore Freq Scaling** is set to **Disabled** or **Manual**.	08 - 24

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Uncore Freq	Uncore frequency input by the user.	127
Input Min Uncore Freq	Minimum input uncore frequency. The value ranges from 0 to 127. **NOTE** This parameter is available when **Uncore Freq Scaling** is set to **Manual**.	0
Input Max Uncore Freq	Maximum input uncore frequency. The value ranges from 0 to 127. **NOTE** This parameter is available when **Uncore Freq Scaling** is set to **Manual**.	127
HBM Mesh Boost Config Control	Provides access to HBM Mesh Boost configurations. **NOTE** This parameter is available when the CPU type is **HBM CPU**.	-
Energy Perf BIAS	Provides access to performance bias configurations.	-
Optimized Power Mode	Enables or disables the optimized power mode. The menu options are as follows: ● **Enabled** ● **Disabled**	Disabled

Figure 5-73 and **Figure 5-74** show the **HBM Mesh Boost Config Control** screen. **Table 5-63** describes the parameters on the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-73 HBM Mesh Boost Config Control screen 1

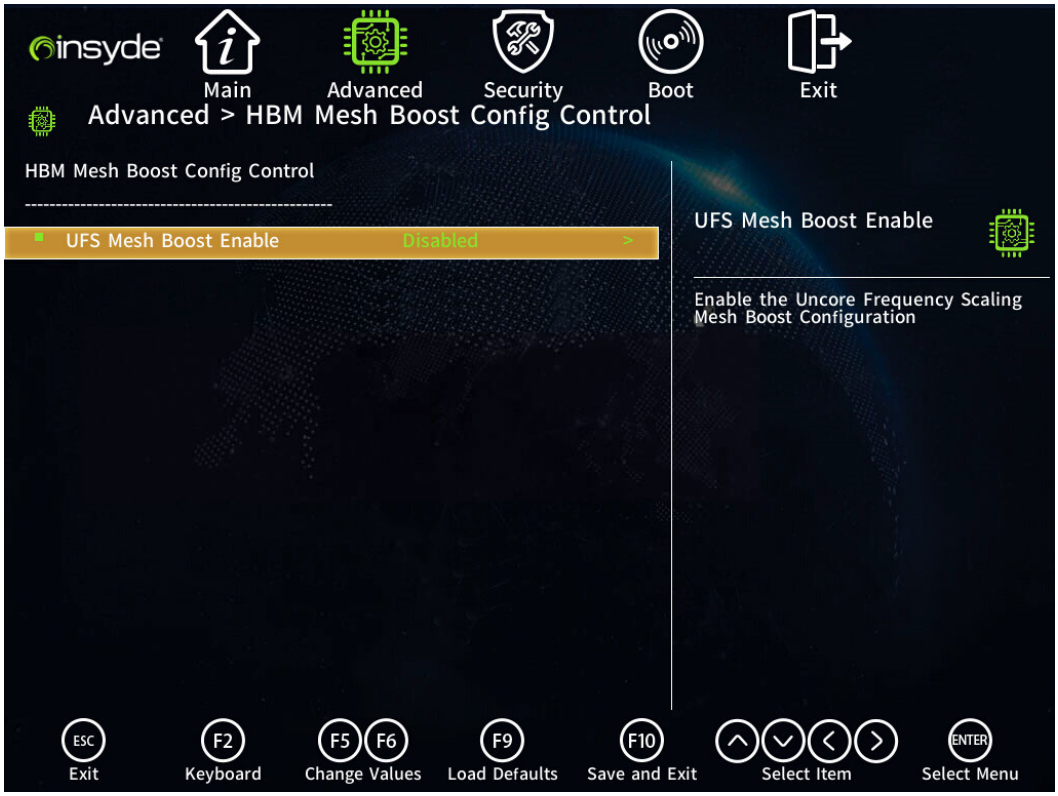
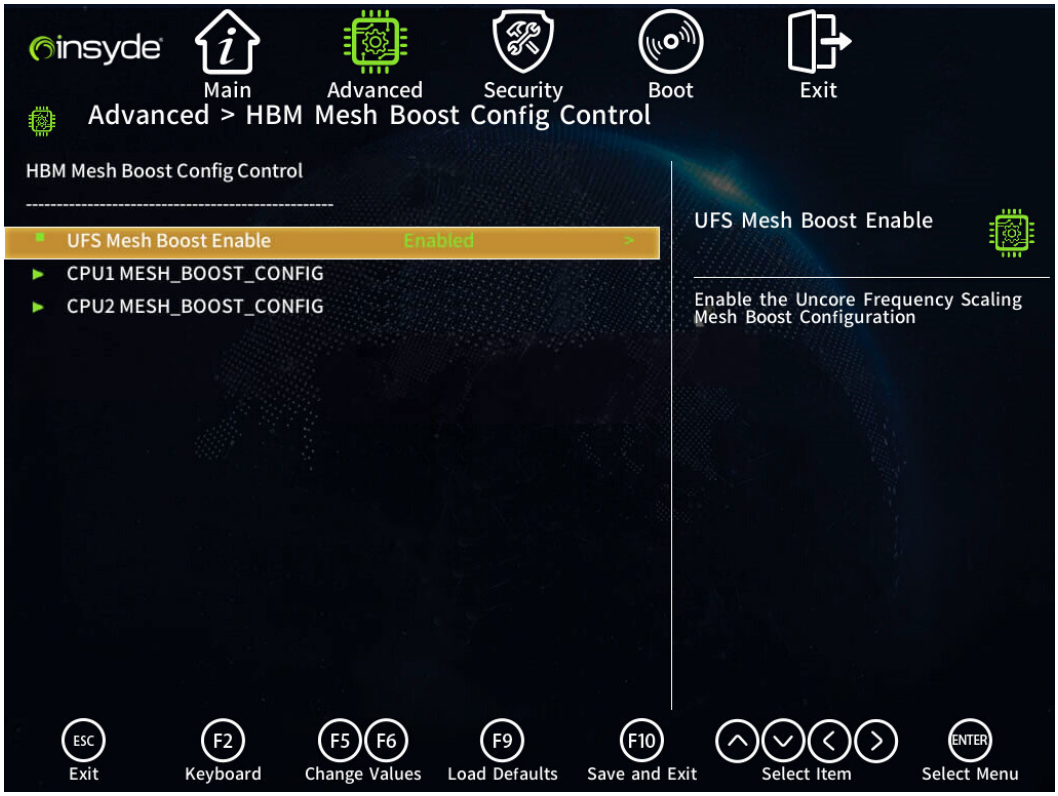


Figure 5-74 HBM Mesh Boost Config Control screen 2



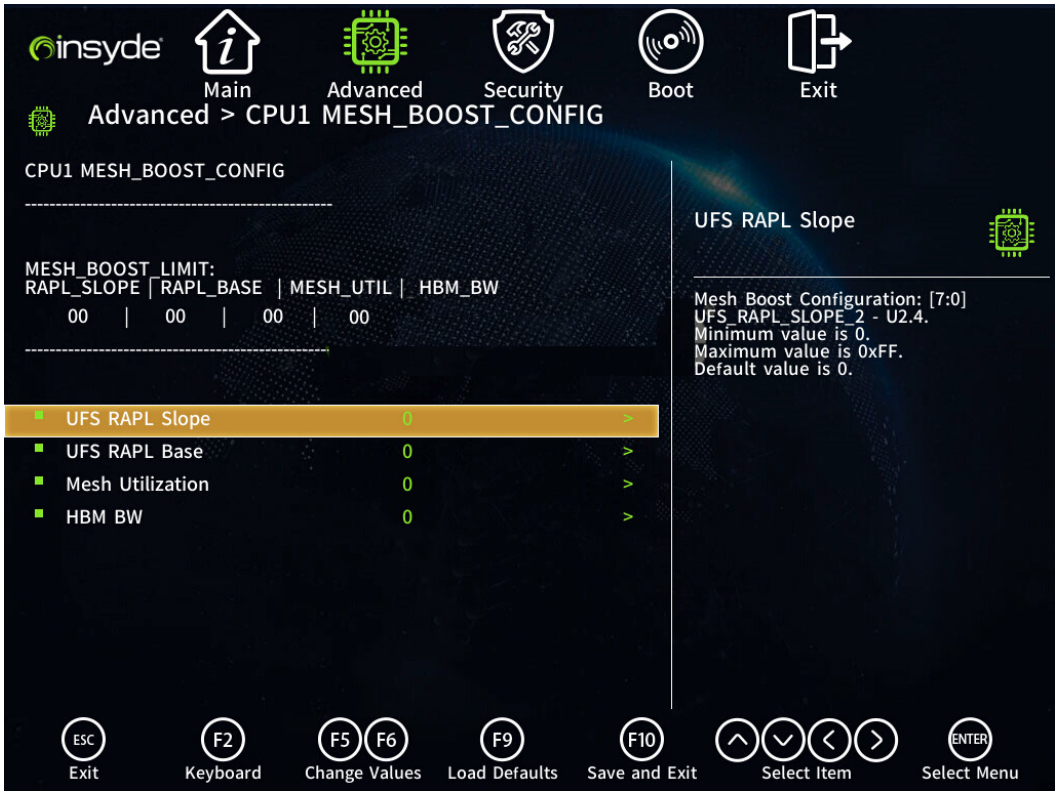
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-63 Parameters on the HBM Mesh Boost Config Control screen

Parameter	Description	Default Value
UFS Mesh Boost Enable	Enables or disables UFS Mesh Boost. The menu options are as follows: • **Disabled** • **Enabled** **NOTE** This parameter is available when the system supports HBM SKU.	Disabled
CPU*X* MESH_BOOST_CONFIG	Provides access to CPU*X* UFS Mesh Boost configurations. **NOTE** This parameter is available when **UFS Mesh Boost Enable** is set to **Enabled**.	-

Figure 5-75 shows the **CPU*X* MESH_BOOST_CONFIG** screen. **Table 5-64** describes the parameters on the screen.

Figure 5-75 CPUX MESH_BOOST_CONFIG screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-64 Parameters on the CPUX MESH_BOOST_CONFIG GUI screen

Parameter	Description	Default Value
UFS RAPL Slope	Sets the UFS RAPL slope. The value ranges from 0x0 to 0xFF.	0
UFS RAPL Base	Sets the UFS RAPL baseline (the value must be a multiple of 100 MHz). The value ranges from 0x0 to 0xFF.	0
Mesh Utilization	Sets the Mesh MAX frequency usage. The value ranges from 0x0 to 0xFF, and the corresponding usage ranges from 0% to 100%.	0
HBM BW	Sets the HBM bandwidth (the value must be a multiple of 8 Gbit/s). The value ranges from 0x0 to 0xFF.	0

Figure 5-76 shows the **Energy Perf BIAS** screen. Table 5-65 describes the parameters.

Figure 5-76 Energy Perf BIAS screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-65 Parameters on the Energy Perf BIAS screen

Parameter	Description	Default Value
Power Performance Tuning	Sets the power performance tuning function. The menu options are as follows: ● **OS Controls EPB**: Use IA32_ENERGY_PERF_BIAS in OS mode. ● **BIOS Controls EPB**: Uses ENERGY_PERF_BIAS_CONFIG in BIOS mode. ● **PECI Controls EPB**: Use the PCS53 in PECI mode. **NOTE** This parameter is unavailable when **Optimized Power Mode** is set to **Enabled**.	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Sets the **ENERGY_PERF_BIAS_CFG** mode. The CPU adjusts the internal operation of the processor according to the setting to meet the requirements of high performance or energy saving. This setting is available only when the energy efficiency adjustment is set to BIOS control energy efficiency policy. Selecting any one of them will overwrite the CPU performance adjustment configuration in the OS. The menu options are as follows: ● **Balanced Performance**: performance balanced ● **Performance**: performance prioritized ● **Balanced Power**: power balanced ● **Power**: energy saving prioritized **NOTE** This parameter is available when **Power Performance Tuning** is set to **BIOS Controls EPB**.	Balanced Performance

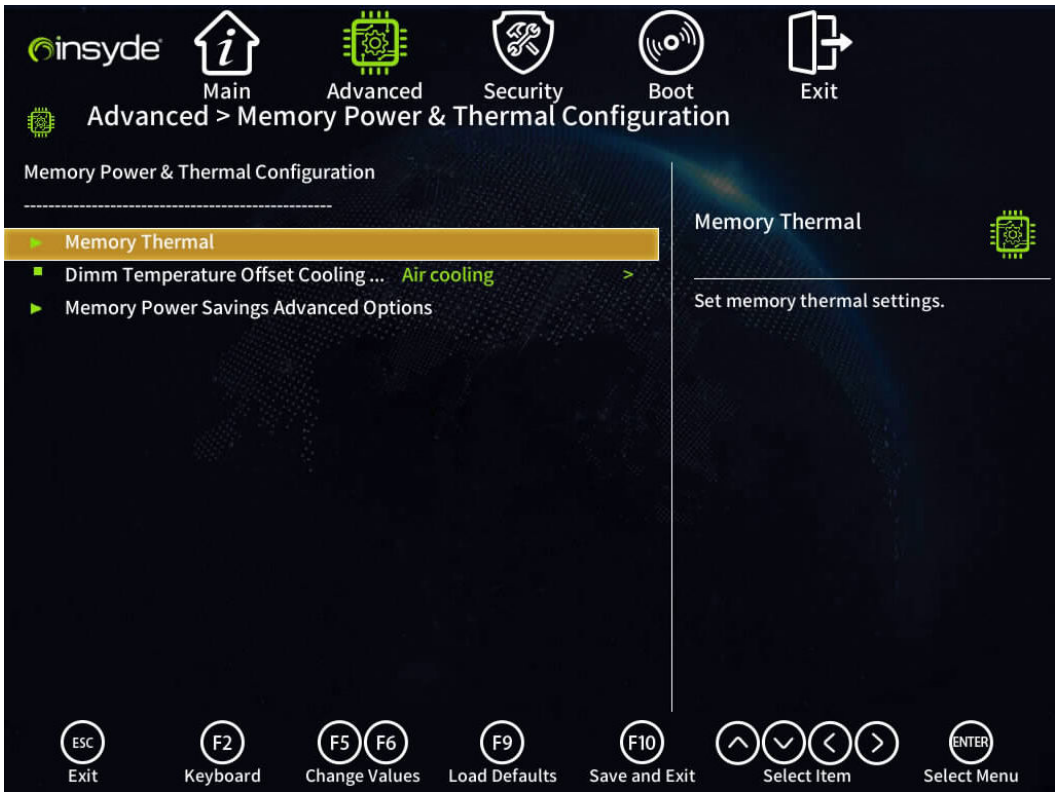
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Core High Voltage Mode	Enables or disables the core high voltage mode. The menu options are as follows: • **Disabled** • **Enabled** **NOTE** This parameter is available only when the system supports HEDT SKU.	Disabled
Non Core High Voltage Mode	Enables or disables the non-core high voltage mode. The menu options are as follows: • **Disabled** • **Enabled** **NOTE** This parameter is available only when the system supports HEDT SKU.	Disabled

5.2.7.6.9 Memory Power & Thermal Configuration

On the **Memory Power & Thermal Configuration** screen, you can configure the memory power and thermal feature of DIMMs. **Figure 5-77** shows the **Memory Power & Thermal Configuration** screen. **Table 5-66** describes the parameters.

Figure 5-77 Memory Power & Thermal Configuration screen



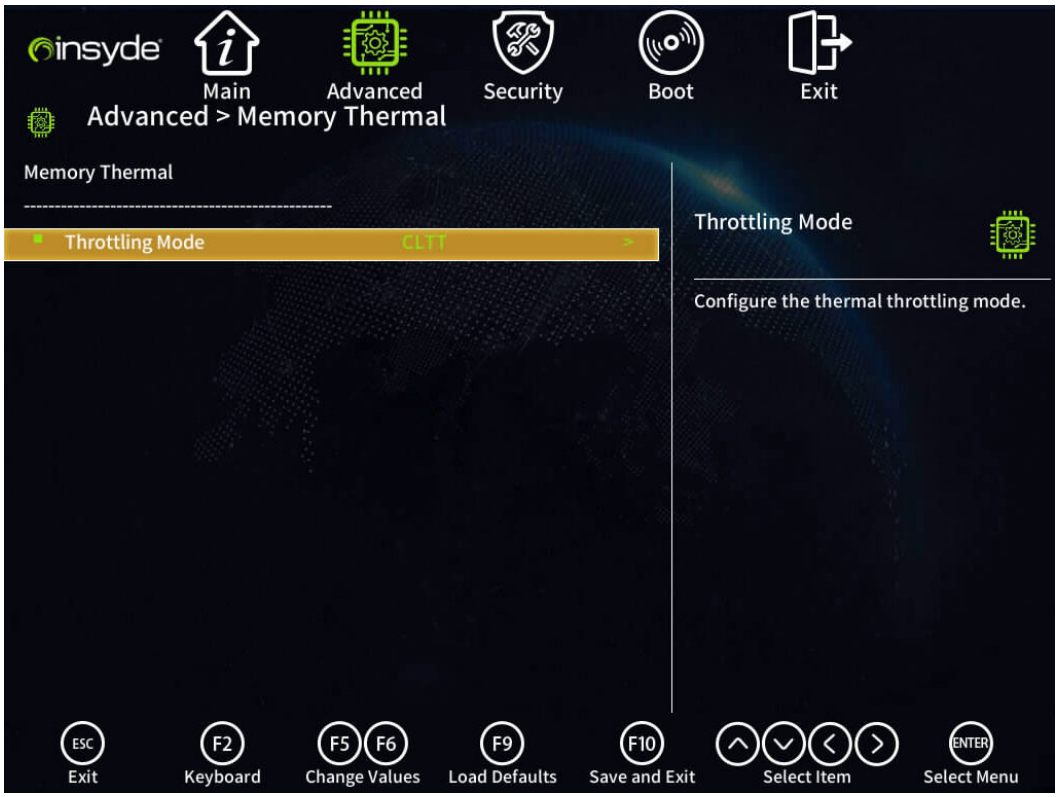
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-66 Parameters on the Memory Power & Thermal Configuration screen

Parameter	Description	Default Value
Memory Thermal	Sets memory thermal configuration.	-
Dimm Temperature Offset Cooling Type	Memory temperature compensation for different cooling types. The menu options are as follows: ● Air cooling ● Liquid cooling (tube) ● Immersion cooling	Air cooling
Memory Power Savings Advanced Options	Sets memory energy saving.	-

Figure 5-78 shows the **Memory Thermal** screen. Table 5-67 describes the parameters.

Figure 5-78 Memory Thermal screen



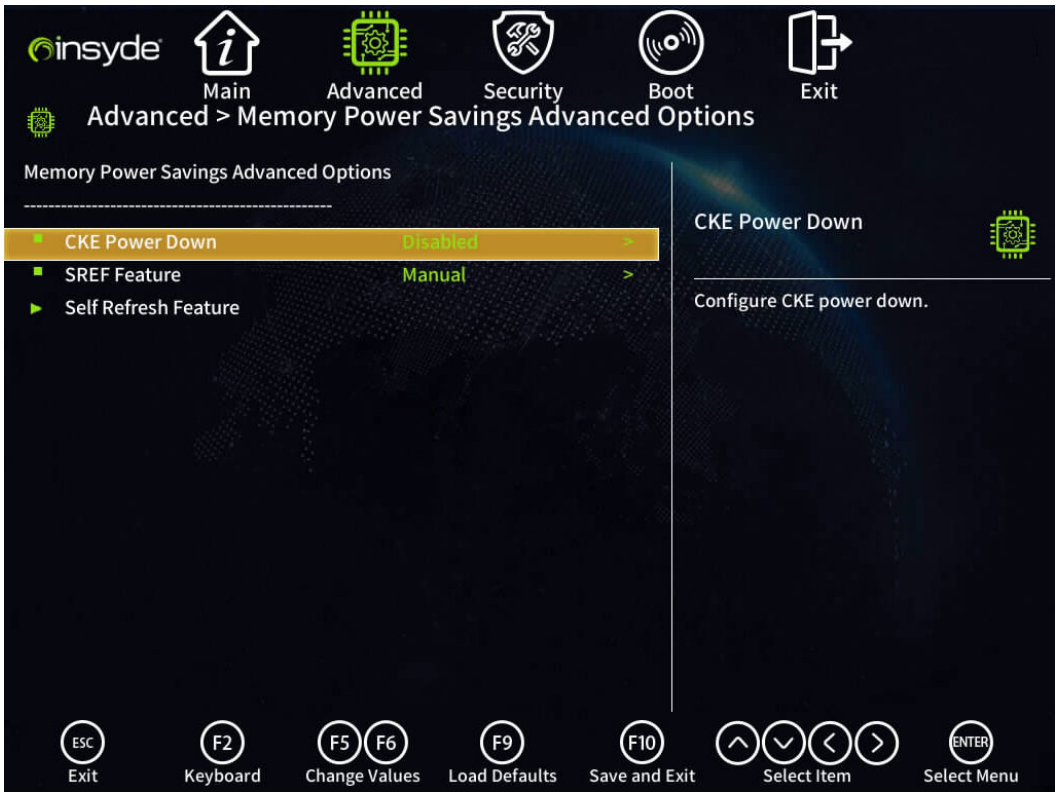
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-67 Parameters on the Memory Thermal screen

Parameter	Description	Default Value
Throttling Mode	Sets the throttling mode. The menu options are as follows: ● **Disabled**: Disables the throttling mode. ● **CLTT**: Sets the CLTT mode.	CLTT

Figure 5-79 shows the **Memory Power Savings Advanced Options** screen. **Table 5-68** describes the parameters.

Figure 5-79 Memory Power Savings Advanced Options screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-68 Parameters on the Memory Power Savings Advanced Options screen

Parameter	Description	Default Value
CKE Power Down	Enables or disables the CKE power down function. CKE power down is a basic power-saving function of the DRAM. The CKE pin is the input of the DRAM and is used to enter and exit the power down mode. If the CKE is disabled, the internal clock is disabled, which significantly reduces the DDR power consumption. The options are as follows: ● Enabled ● Disabled	Disabled
CKE Feature	Provides access to CKE (Clock Enable) feature configurations. **NOTE** This parameter is available when **CKE Power Down** is set to **Enabled**.	-
SREF Feature	Selects the self-refresh mode, which is used to retain data in sleep mode in low-power mode. The options are as follows: ● Auto ● Manual	Manual
Self Refresh Feature	Provides access to self-refresh function settings. **NOTE** This parameter is unavailable when **SREF Feature** is set to **Auto**.	-

Figure 5-80 shows the **CKE Feature** screen. **Table 5-69** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-80 CKE Feature screen



Table 5-69 Parameters on the CKE Feature screen

Parameter	Description	Default Value
CKE Idle Timer	Sets the CKE idle timer. The value ranges from 0 ns to 255 ns. **NOTE** This parameter is available when the CPU type is SPR or EMR.	CPU type is SPR: 20 CPU type is EMR: 160
PPD	Enables or disables the Pre-charge Power Down (PPD) function. In the PPD state, CKE is powered off, all bank pages on the rank are closed, and the CKE pin of the rank keeps talking. The options are as follows: ● Enabled ● Disabled **NOTE** For BIOS 01.01.06.03 and later versions, this parameter is available when **CKE Power Down** is set to **Enabled** and the CPU type is not SPR or EMR.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PMem CKE	Enables or disables PMem CKE. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the PMem memory exists.	Enabled

Figure 5-81 shows the **Self Refresh Feature** screen. **Table 5-70** describes the parameters.

Figure 5-81 Self Refresh Feature screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-70 Parameters on the Self Refresh Feature screen

Parameter	Description	Default Value
PMem SELF REFRESH	Enables or disables the PMem self-refresh function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **Opportunistic SR** is set to **Enabled**.	Disabled
CK in SR	Selects the clock behavior during self-refresh. The menu options are as follows: ● Driven ● Pulled Low	Pulled Low

5.2.8 ME Configuration

On the **ME Configuration** screen, you can configure ME. **Figure 5-82** shows the **ME Configuration** screen. **Table 5-71** describes the parameters.

Figure 5-82 ME Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-71 Parameters on the ME Configuration screen

Parameter	Description
Server ME Configuration	Provides access to the ME configurations.

5.2.8.1 Server ME Configuration

Figure 5-83 shows the **Server ME Configuration** screen. **Table 5-72** describes the parameters.

Figure 5-83 Server ME Configuration screen

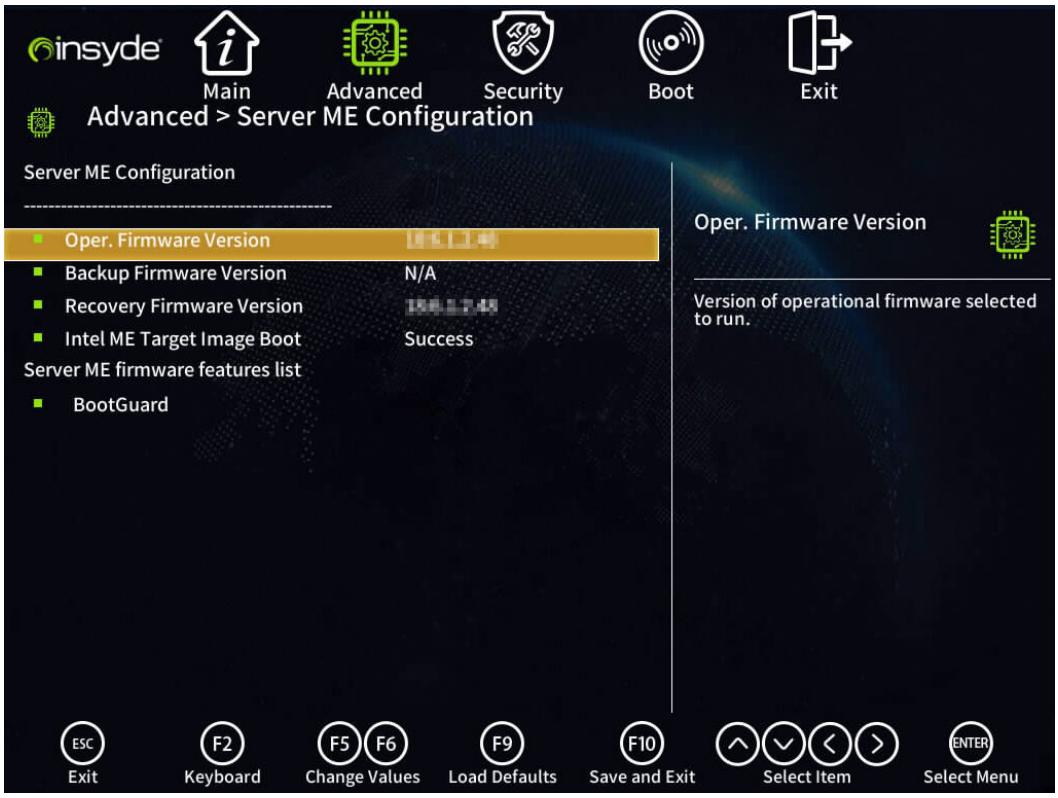


Table 5-72 Parameters on the Server ME Configuration screen

Parameter	Description
Oper. Firmware Version	Displays the version of the operating ME firmware.
Backup Firmware Version	Displays the version of the current backup ME firmware.
Recovery Firmware Version	Displays the version of the restored ME firmware.
Intel ME Target Image Boot	Displays information about the Intel ME target image boot failure.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Server ME firmware features list	Displays the ME firmware features. • BootGuard

5.2.9 PCH-IO Configuration

On the **PCH-IO Configuration** screen, you can configure PCH-related features. Figure 5-84 shows the **PCH-IO Configuration** screen. Table 5-73 describes the parameters.

Figure 5-84 PCH-IO Configuration screen



Table 5-73 Parameters on the PCH-IO Configuration screen

Parameter	Description
SATA And RST Configuration	Provides access to SATA and RST configurations.
USB Configuration	Provides access to USB configurations.

5.2.9.1 SATA And RST Configuration

On the **SATA And RST Configuration** screen, you can perform the SATA and RST configurations (including SATA controllers and drive ports) and disable a specified

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

port. There are three controllers, each of which can be configured with four or more SATA ports. If the server supports the Intel VROC (SATA RAID) function, you need to configure the SATA controller to work in RAID mode before configuring Intel VROC (SATA RAID). **Figure 5-85** shows the **SATA And RST Configuration** screen. **Table 5-74** describes the parameters.

Figure 5-85 SATA And RST Configuration screen



Table 5-74 Parameters on the SATA And RST Configuration screen

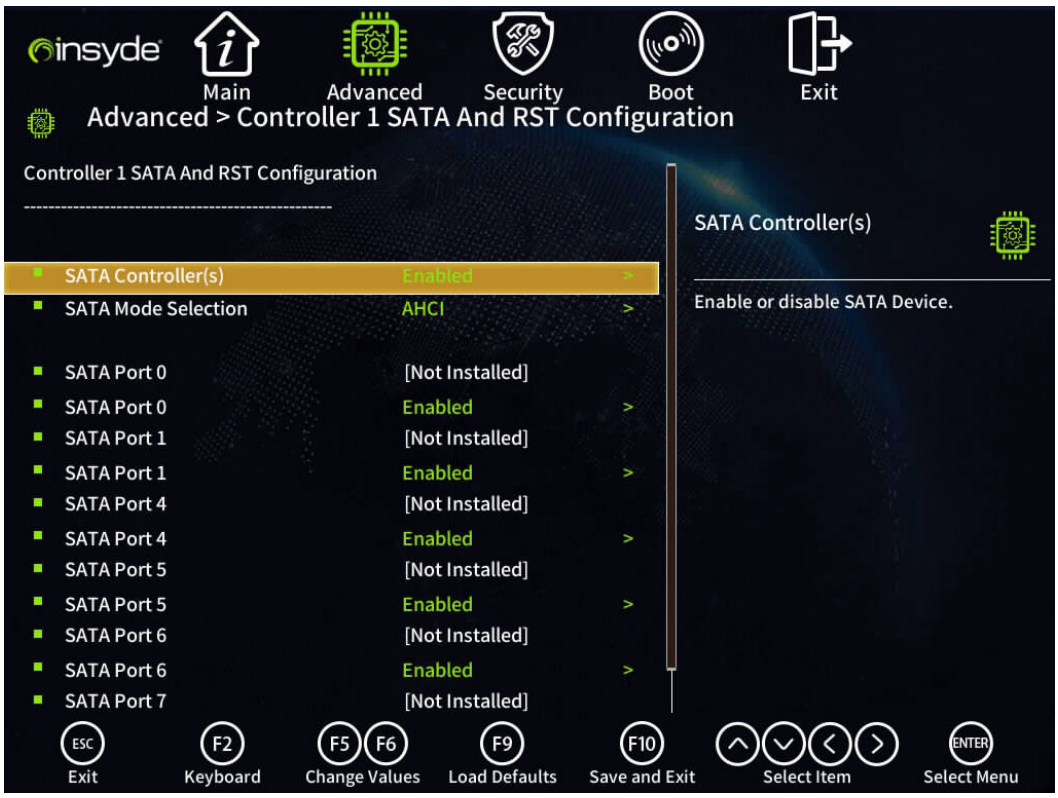
Parameter	Description
Controller 1 SATA And RST Configuration	Provides access to controller 1 SATA and RST configurations.
Controller 2 SATA And RST Configuration	Provides access to controller 2 SATA and RST configurations.
Controller 3 SATA And RST Configuration	Provides access to controller 3 SATA and RST configurations.
Controller 1 SATA Information	Displays controller 1 SATA information.
Controller 2 SATA Information	Displays controller 2 SATA information.
Controller 3 SATA Information	Displays controller 3 SATA information.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.9.1.1 Controller *X* SATA And RST Configuration

Figure 5-86, **Figure 5-87**, and **Figure 5-88** show the **Controller *X* SATA And RST Configuration** screen. **Table 5-75** describes the parameters.

Figure 5-86 Controller 1 SATA And RST Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-87 Controller 2 SATA And RST Configuration screen

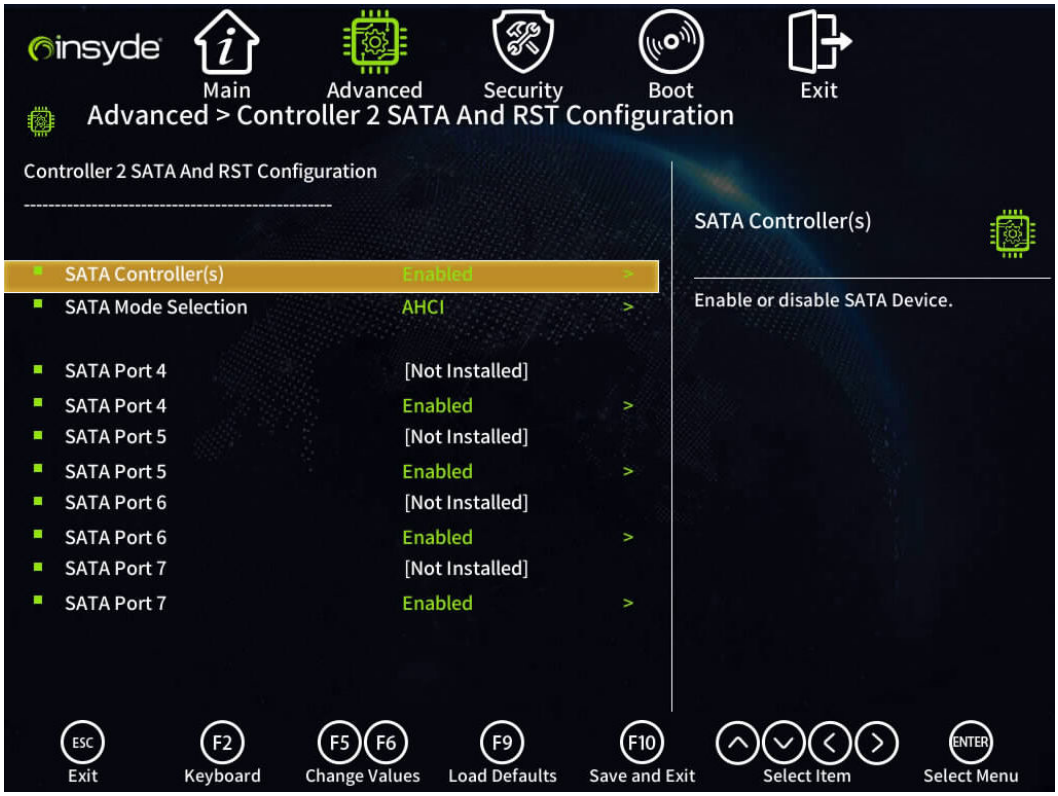
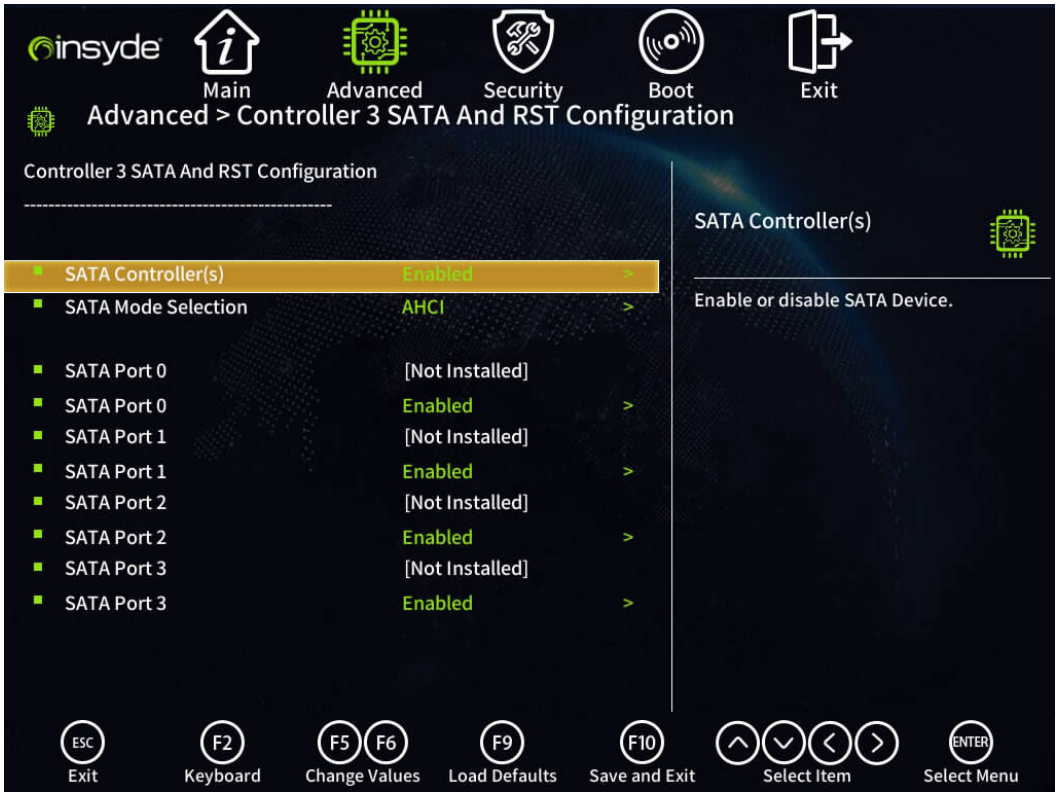


Figure 5-88 Controller 3 SATA And RST Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-75 Parameters on the Controller *X* SATA And RST Configuration screens

Parameter	Description	Default Value
SATA Configuration	Enables or disables the SATA controller. The menu options are as follows: ● Enabled ● Disabled	Enabled
SATA Mode Selection	Sets the working mode of the SATA controller. The menu options are as follows: ● AHCI ● RAID **NOTE** ● This parameter is unavailable when **SATA Configuration** is set to **Disabled**. ● To configure Intel VROC (SATA RAID), you must set this parameter to **RAID**.	AHCI
RAID Device ID	Sets the device ID in RAID mode. The menu options are as follows: The menu options are as follows: ● Client ● Alternate ● Server **NOTE** This parameter is available when **SATA Configuration** is set to **Enabled** and **SATA Mode Selection** is set to **RAID**.	Server
SATA Port *X*	Displays information about the connected SATA drives. The value is dynamically obtained based on the drive presence status. If the drive is not detected, **Not Installed** is displayed. **NOTE** X indicates the port number of the drive.	-
SATA Port *X*	Enables or disables the SATA port. The menu options are as follows: ● Enabled ● Disabled **NOTE** *X* indicates the port number of the drive.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

5.2.9.2 USB Configuration

On the **USB Configuration** screen, you can view the current USB devices and enable or disable a specified USB port. **Figure 5-89** shows the **USB Configuration** screen. **Table 5-76** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the server models.

Figure 5-89 USB Configuration screen



Table 5-76 Parameters on the USB Configuration screen

Parameter	Description	Default Value
x USB Mouse	Displays the number of currently valid mouses. *x* indicates the number of devices. The value **0** indicates that no valid device is identified.	The value is displayed as the number that is actually read. Example: **1 USB Mouse**
x USB Keyboard	Displays the number of currently valid keyboards. *x* indicates the number of devices. The value **0** indicates that no valid device is identified.	The value is displayed as the number that is actually read. Example: **1 USB Keyboard**

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
x USB MassStorage	Displays the number of currently valid USB storage devices. *x* indicates the number of devices. The value **0** indicates that no valid device is identified.	The value is displayed as the number that is actually read. Example: **0 USB MassStorage**
Front USB Control ● USB Physical Port 1 ● USB Physical Port 2	Specifies the USB ports on the front panel. Enables or disables the USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the front panel of the server.	Enabled
Rear USB Control ● USB Physical Port 1 ● USB Physical Port 2	Specifies the USB ports on the rear panel. Enables or disables the USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the rear panel of the server.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Built-in USB Control • USB Physical Port 1	Specifies the built-in USB port. Enables or disables the USB physical port. The menu options are as follows: • Enabled • Disabled **NOTE** • USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. • Mapping between ports and physical ports: Port 1 correspond to the built-in USB 3.0 ports of the server.	Enabled

5.2.10 BMC Configuration

On the **BMC Configuration** screen, you can view the BMC/IPMI version information and the BMC MAC address, and perform BMC configurations. **Figure 5-90** shows the **BMC Configuration** screen. **Table 5-77** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-90 BMC Configuration screen

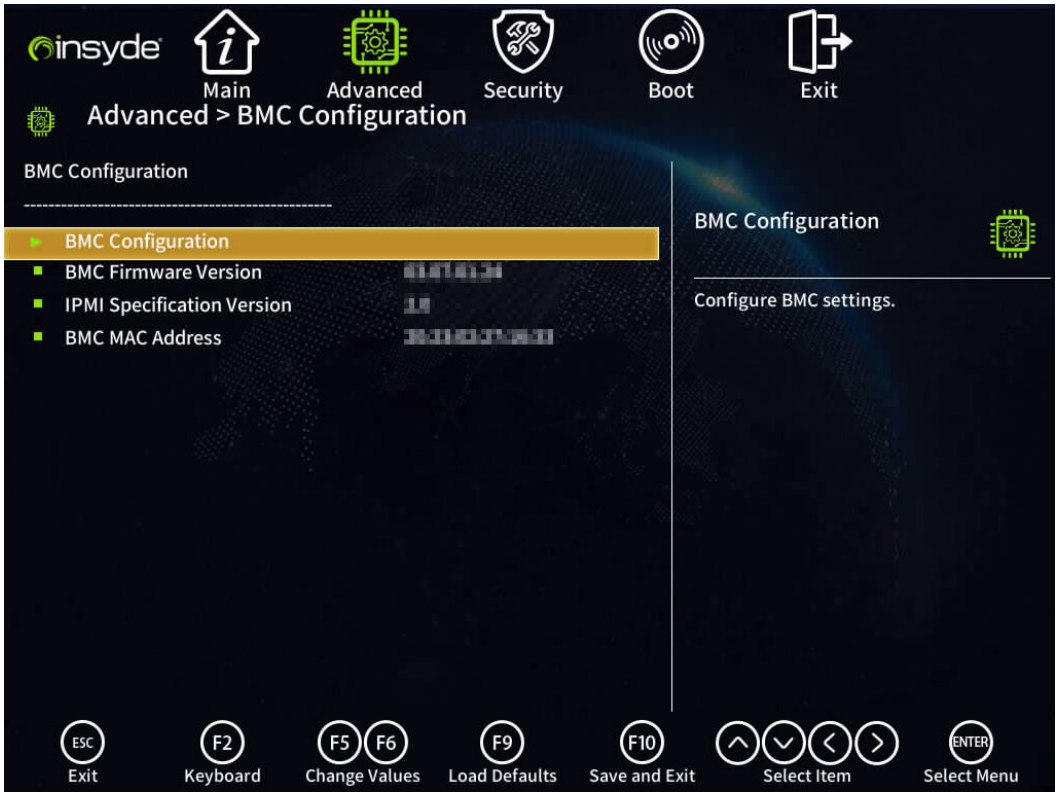


Table 5-77 Parameters on the BMC Configuration screen

Parameter	Description	Default Value
BMC Configuration	Provides access to the BMC configurations.	-
BMC Firmware Version	Displays the BMC version.	-
IPMI Specification Version	Displays the IPMI version information.	-
BMC MAC Address	Displays the BMC MAC address.	-

5.2.10.1 BMC Configuration

On the **BMC Configuration** screen, you can configure the BMC watchdog timer and the BMC IPv4/IPv6 information. **Figure 5-91** and **Figure 5-92** show the **BMC Configuration** screen. **Table 5-78** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-91 BMC Configuration screen 1



Figure 5-92 BMC Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-78 Parameters on the BMC Configuration screen

Parameter	Description	Default Value
BMC WDT Support For POST	Enables or disables the BMC watchdog timer at the start of POST. The menu options are as follows: ● Enabled ● Disabled	Disabled
BMC WDT Time Out For POST	Specifies the maximum time allowed for the system to start the BIOS. If timeout occurs, the watchdog is triggered. The valid time ranges from 18 to 25 minutes. **NOTE** This parameter can be configured when **BMC WDT Support For POST** is set to **Enabled**.	20
BMC WDT Action For POST	Sets the action to be taken after the watchdog timer times out. The menu options are as follows: ● **No Action**: No action is required. ● **Hard Reset**: Hard reset. ● **Power Down**: Powers off the system. ● **Power Cycle**: Powers off and restarts the system. **NOTE** This parameter can be configured when **BMC WDT Support For POST** is set to **Enabled**.	Hard Reset
BMC WDT Support For OS	Enables or disables the watchdog timer on the OS. The menu options are as follows: ● Enabled ● Disabled	Disabled
BMC WDT Time Out For OS	Sets the maximum time allowed for loading the OS completely, in minutes. The value ranges from 2 to 8. If timeout occurs, the watchdog is triggered. **NOTE** This parameter can be configured when **BMC WDT Support For OS** is set to **Enabled**.	5

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC WDT Action For OS	Sets the action to be taken after the watchdog timer times out. The menu options are as follows: ● **No Action**: No action is required. ● **Hard Reset**: Hard reset. ● **Power Down**: Powers off the system. ● **Power Cycle**: Powers off and restarts the system. **NOTE** This parameter can be configured when **BMC WDT Support For OS** is set to **Enabled**.	Hard Reset
Network protocol	Sets the network protocol. The menu options are as follows: ● IPv4 ● IPv6 ● IPv4/IPv6 **NOTE** If this parameter is set to **IPv4**, IPv6-related parameters are unavailable. If this parameter is set to **IPv6**, IPv4 parameters are unavailable.	IPv4/IPv6
IPv4 Configuration	Sets the IPv4 configuration mode. The menu options are as follows: ● Static ● DHCP **NOTE** **IPv4 IP Address**, **IPv4 Subnet Mask**, and **IPv4 Gateway Address** cannot be configured if this parameter is set to **DHCP**.	- **NOTE** The value is automatically obtained from the BMC. If the value cannot be obtained, the default value is **Static**.
IPv4 IP Address	If **IPv4 Configuration** is set to **Static**, you can specify an IPv4 address. If **IPv4 Configuration** is set to **Dynamic**, the automatically allocated IPv4 address is displayed. **NOTE** The IP address cannot be set to all **0** or empty.	-
IPv4 Subnet Mask	If **IPv4 Configuration** is set to **Static**, you can specify an IPv4 subnet mask. If **IPv4 Configuration** is set to **Dynamic**, the current IPv4 subnet mask is displayed.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPv4 Gateway Address	If **IPv4 Configuration** is set to **Static**, you can specify an IPv4 gateway address. If **IPv4 Configuration** is set to **Dynamic**, the default IPv4 gateway address is displayed. **NOTE** The gateway cannot be set to all **0** or empty.	-
IPv6 Configuration	Sets the IPv6 configuration mode. The menu options are as follows: ● Static ● DHCP **NOTE** **IPv6 Prefix Length**, **IPv6 Static IP Address**, and **IPv6 Gateway Address** cannot be configured if this parameter is set to **DHCP**.	- **NOTE** The value is automatically obtained from the BMC. If the value cannot be obtained, the default value is **Static**.
IPv6 Prefix Length	If **IPv6 Configuration** is set to **Static**, you can specify an IPv6 prefix length. If **IPv6 Configuration** is set to **Dynamic**, the current IPv6 prefix length is displayed.	-
IPv6 Static IP Address	If **IPv6 Configuration** is set to **Static**, you can specify an IPv6 address. If **IPv6 Configuration** is set to **Dynamic**, the automatically allocated IPv6 address is displayed.	-
IPv6 Gateway Address	If **IPv6 Configuration** is set to **Static**, you can specify an IPv6 gateway address. If **IPv6 Configuration** is set to **Dynamic**, the default IPv6 gateway address is displayed.	-
Two-Factor Authentication	Enables or disables the two-factor authentication function. After this function is enabled, all CLI interfaces of the BMC cannot be used. You can only log in to the BMC WebUI. A menu under the BIOS is added to enable and disable the function in emergency situations. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC Smart Cooling	Sets the BMC smart cooling mode. The menu options are as follows: ● **Energy saving mode**: Evaluates the current load and heat dissipation of the system, controls the fan speed at a balanced point, and keeps the system power consumption at the lowest level. ● **Low noise mode**: Minimizes the fan speed and reduces noise while meeting heat dissipation requirements. ● **High performance mode**: Increases the fan speed and ensures the heat dissipation for key components to maintain low temperature for highest performance. ● **Custom Mode**: Provides a custom interface. You can set the target CPU temperature and the fan speed corresponding to each temperature area of the air intake vent.	- **NOTE** The displayed value of this parameter depends on the BMC policy.
CPU Temp. Threshold	Specifies the target CPU temperature. **NOTE** This parameter is available when **BMC Smart Cooling** is set to **Custom Mode**.	-
Fan Speed Rate *x*	Controls the fan speed. **NOTE** This parameter is available when **BMC Smart Cooling** is set to **Custom Mode**.	-
BMC Service	Enables or disables the BMC SSH service. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Restore On AC Power Loss	Sets system power-off strategy. The menu options are as follows: ● **Power On**: The OS automatically starts after the PSU of the server is powered on. ● **Power Off**: The OS is not powered on after the PSU of the server is powered on. ● **Last State**: After being powered on, the PSU of the server keeps the state entered before the power-off. If the server OS is started before the power-off, it automatically powers on after the power supply is connected. If the server OS is shut down before the power-off, it will not be started after the power supply is connected.	- **NOTE** The displayed value of this parameter depends on the BMC policy.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC Network Mode	Sets the BMC management network port mode. The menu options are as follows: ● **Dedicated**: Dedicated mode. You can access the BMC only through the management network port. ● **Auto**: Auto-negotiation mode. You can access the BMC through the management network port or the NCSI service network port of the server. ● **PCIe Shared**: PCIe NIC sharing mode. You can access the BMC only through the NCSI network port of the PCIe NIC. ● **OCP1 Shared**: OCP1 NIC sharing mode. You can access the BMC only through the network port of the OCP1 NIC. ● **OCP2 Shared**: OCP2 NIC sharing mode. You can access the BMC only through the network port of the OCP2 NIC. **NOTE** The value options of this parameter vary depending on the server model and server configuration.	Dedicated **NOTE** The displayed value of this parameter depends on the BMC policy.
Vlan ID	Set the BMC VLAN ID. The value can be **0** (disabling the VLAN) or from 1 to 4094 (enabling the VLAN). **NOTE** This parameter is available when **BMC Network Mode** is set to **Auto** or **PCIe Shared**.	0

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
NCSI PCIe Port Select	Selects the NCSI PCIe port to be used. The menu options are as follows: ● Port1 ● Port2 ● Port3 ● Port4 **NOTE** ● This parameter is available when **BMC Network Mode** is set to **PCIe Shared**. ● The value of this parameter varies depending on the NIC configuration.	Port1
NCSI OCP Port Select	Selects the NCSI OCP port to be used. The menu options are as follows: ● Port1 ● Port2 **NOTE** ● This parameter is available when **BMC Network Mode** is set to **OCPx Shared**. ● The value of this parameter varies depending on the NIC configuration.	Port1
Add BMC User	Adds the BMC user.	-
Delete BMC User	Deletes the BMC user.	-
Change BMC User Settings	Changes the BMC user settings.	-
Load BMC Default	Restores the default BMC IP address, user name, and password.	-
Clear BMC SEL	Sets whether to clear the BMC system event logs.	-

5.2.10.1.1 Add BMC User

On the **Add BMC User** screen, you can add a BMC user. **Figure 5-93** shows the **Add BMC User** screen. **Table 5-79** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-93 Add BMC User screen

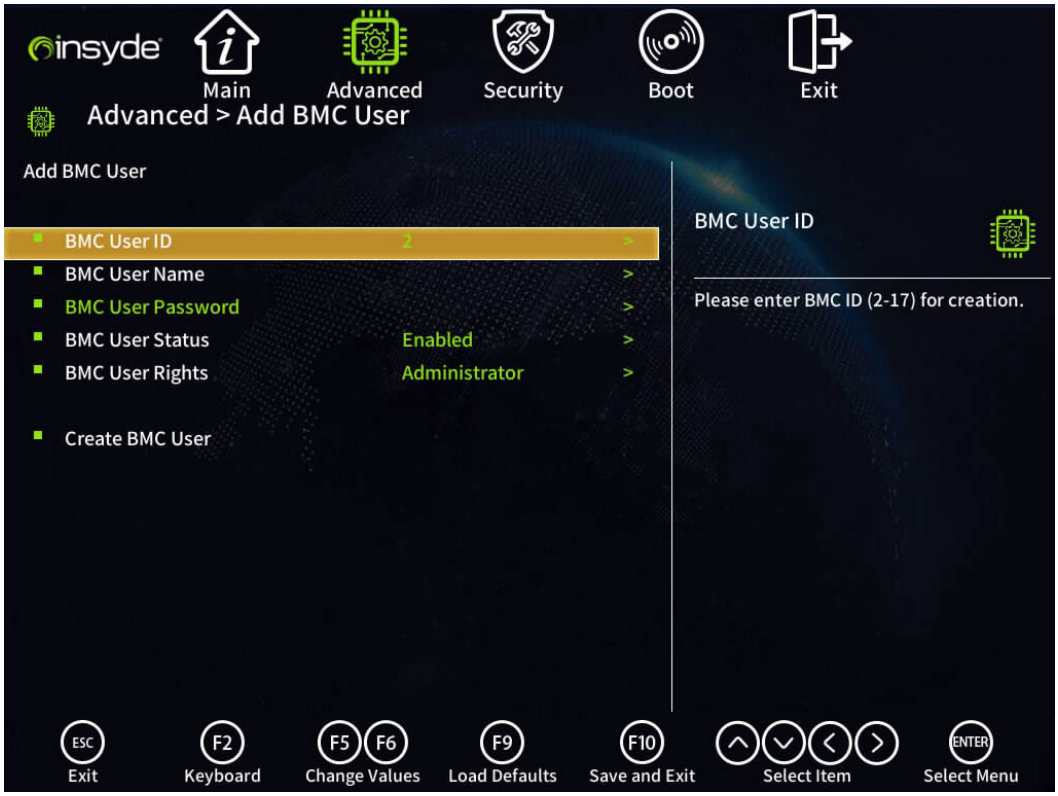


Table 5-79 Parameters on the Add BMC User screen

Parameter	Description	Default Value
BMC User ID	Sets the BMC user ID. The value ranges from 2 to 17.	-
BMC User Name	Sets the BMC user name. **NOTE** • The username contains 1 to 16 characters. • The value can contain letters, digits, and special characters. • The value cannot start with a number sign (#), plus sign (+), or hyphen (-). • The value cannot contain spaces or the following special characters: :<>&, '"/\%	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value

BMC User Password	Sets the BMC user password.
	NOTE
	The password complexity requirements are as follows:
	• Contain 8 to 20 characters.
	• Contain at least two types of the following characters:
	  • Uppercase letters A to Z
	  • Lowercase letters a to z
	  • Digits 0 to 9
	• Contain at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/?
	• Cannot be the same as the username or the username in reverse order.
		-

BMC User Status	Sets the BMC user state.	Enabled
BMC User Rights	Sets the BMC user rights. The menu options are as follows: • **Administrator**: Specifies the administrator. • **Operator**: Specifies the operator. • **Common User**: Specifies the common user. • **No Access**: Specifies that the BMC is not accessible.	Administrator
Create BMC User	Saves the user settings.	-

5.2.10.1.2 Delete BMC User

On the **Delete BMC User** screen, you can delete a BMC user. **Figure 5-94** shows the **Delete BMC User** screen. **Table 5-80** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-94 Delete BMC User screen

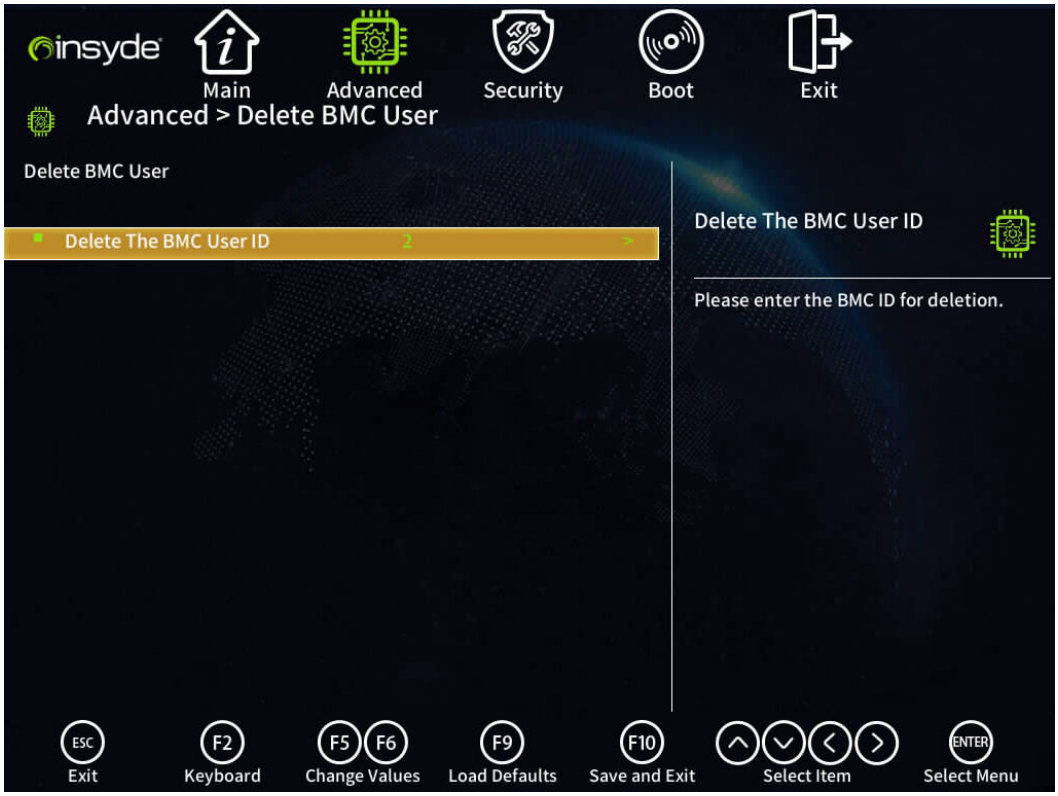


Table 5-80 Parameters on the Delete BMC User screen

Parameter	Description	Default Value
Delete The BMC User ID	Enters the BMC user ID to be deleted.	-

5.2.10.1.3 Change BMC User Settings

On the **Change BMC User Settings** screen, you can modify the BMC user settings. **Figure 5-95** shows the **Change BMC User Settings** screen. **Table 5-81** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-95 Change BMC User Settings screen



Table 5-81 Parameters on the Change BMC User Settings screen

Parameter	Description	Default Value
BMC User Status	Sets the BMC user state when **UserID** is set to **2**. **NOTE** This parameter cannot be configured when there is only one user.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC User Rights	Sets the BMC user rights when **UserID** is set to **2**. The menu options are as follows: ● **Administrator**: Specifies the administrator. ● **Operator**: Specifies the operator. ● **Common User**: Specifies the common user. ● **No Access**: Specifies that the BMC is not accessible. **NOTE** This parameter cannot be configured when there is only one user.	Administrator
BMC User Name	Displays or modifies the BMC user name when **UserID** is set to **2**. **NOTE** ● The username contains 1 to 16 characters. ● The value can contain letters, digits, and special characters. ● The value cannot start with a number sign (#), plus sign (+), or hyphen (-). ● The value cannot contain spaces or the following special characters: :<>&, '"/\%	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Reset BMC User Password	Modifies the BMC user password when **UserID** is set to **2**. **NOTE** The password complexity requirements are as follows: ● Contain 8 to 20 characters. ● Contain at least two types of the following characters: ● Uppercase letters A to Z ● Lowercase letters a to z ● Digits 0 to 9 ● Contain at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? ● Cannot be the same as the username or the username in reverse order.	-

5.2.11 Console Redirection Configuration

On the **Console Redirection Configuration** screen, you can set parameters related to the serial port, for example, enable the redirection function of the serial port. **Figure 5-96** shows the **Console Redirection Configuration** screen. **Table 5-82** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-96 Console Redirection Configuration screen



Table 5-82 Parameters on the Console Redirection Configuration screen

Parameter	Description	Default Value
Console Serial Redirect	Enables or disables the serial port redirection which maps the data of a specified physical serial port or virtual serial port to a specified system serial port. The options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Terminal Type	Selects the simulation type. The BIOS simulation type must match the mode selected in the terminal program. The options are as follows: ● VT_100 ● VT_100+ ● VT_UTF8 ● PC_ANSI ● LOG_TERM **NOTE** This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**.	VT_100
Baud Rate	Sets the baud rate for serial port redirection. The menu options are as follows: ● 115200 ● 57600 ● 38400 ● 19200 ● 9600 ● 4800 ● 2400 ● 1200 **NOTE** This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**.	115200
Data Bits	Sets the data length of serial port redirection. The menu options are as follows: ● 7 Bits ● 8 Bits **NOTE** This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**.	8 Bits

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Parity	Sets serial port redirection verification. The parity bit can be transmitted together with the data bit to detect certain transmission errors. The options are as follows: ● **None**: The verification function is disabled. ● **Even**: Sends even bits with data bits to detect data transmission errors. ● **Odd**: Sends odd bits with data bits to detect data transmission errors. **NOTE** This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**.	None
Stop Bits	Sets the stop bit of the serial port redirection function. The stop bit indicates the end of the serial data packet. The standard value is set to 1 stop bit. The communication with a slow device may require more than 1 stop bit. The options are as follows: ● 1 Bit ● 2 Bits **NOTE** This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**.	1 Bit

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Flow Control	Sets the control flow of the serial port redirection. The menu options are as follows: ● **None**: disables the serial port redirection control flow. ● **RTS/CTS**: Sends request/Clears request sending. ● **XON/XOFF**: The XON character or XOFF character is sent to the data transmit end according to the data amount in the input buffer of the receive end. **NOTE** ● This parameter is unavailable when **Console Serial Redirect** is set to **Disabled**. ● 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7 does not support the **RTS/CTS** option only in BIOS 01.01.08.07 and later versions.	None

5.2.12 PXE Configuration

On the **PXE Configuration** screen, you can enable or disable the PXE function of the slot. **Figure 5-97** shows the **PXE Configuration** screen. **Table 5-83** describes the parameters.

NOTE

The parameters displayed on this screen vary according to actual server NIC configuration.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-97 PXE Configuration screen



Table 5-83 Parameters on the PXE Configuration screen

Parameter	Description	Default Value
Slot PXE Control	Enables or disables the PXE function of all external PCIe NICs. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is displayed only when a PCIe NIC is installed in the corresponding slot. In legacy mode, if the NIC OptionRom resources are insufficient, this parameter is invalid and is disabled by default, for example, two RAID controller cards are configured.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CPU*X* First Slot Port *Y*	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU *X*. The menu options are as follows: ● Enabled ● Disabled **NOTE** In legacy mode, if the NIC OptionRom resources are insufficient, this parameter is invalid and is disabled by default, for example, two RAID controller cards are configured.	Enabled
FLEX IO *X* Port *Y*	Enables or disables the PXE function of port Y of OCP NIC X. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is displayed only when an OCP NIC is installed in the corresponding slot.	Enabled **NOTE** ● For details about the OCP NICs supported by each server, see the user guide of the corresponding server. ● All default values of network ports are set to **Enabled** in UEFI mode. ● In legacy mode, only the first network port of each NIC can be enabled. That is, the default value of PXE port 1 is **Enabled**, and the default value of PXE port 2 is **Disabled**.

5.2.13 NVMe Information

On the **NVMe Information** screen, you can view the NVMe drive information. **Figure 5-98** shows the **NVMe Information** screen. **Table 5-84** describes the parameters.

NOTE

The NVMe drive information is not displayed on this screen when **Intel VMD Config** is set to **Enabled**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-98 NVMe Information screen

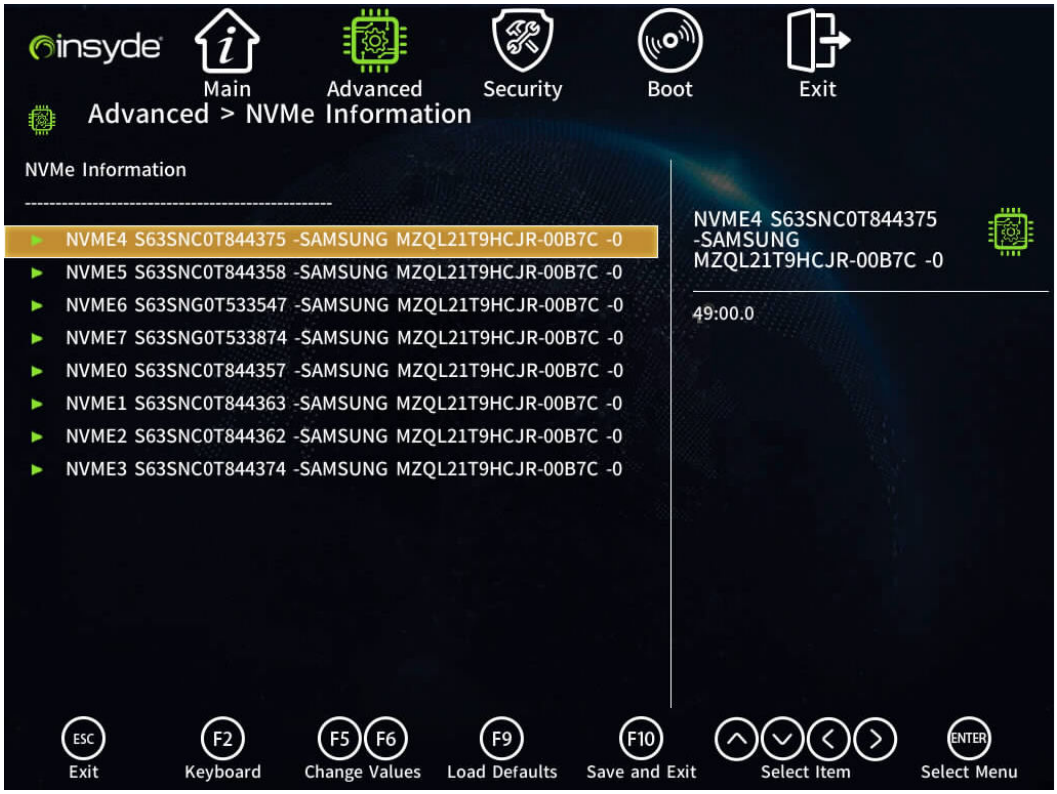


Table 5-84 Parameters on the NVMe Information screen

Parameter	Description
NVME*x*	Displays the NVMe drive information. **NOTE** The name displayed varies depending on the NVMe drives. If no NVMe drive is connected, **No NVMe Device** is displayed.

5.2.13.1 NVMe Device Information

On the **NVMe Device Information** screen, you can view NVMe drive specifications. **Figure 5-99** shows the **NVMe Device Information** screen. **Table 5-85** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-99 NVMe Device Information screen

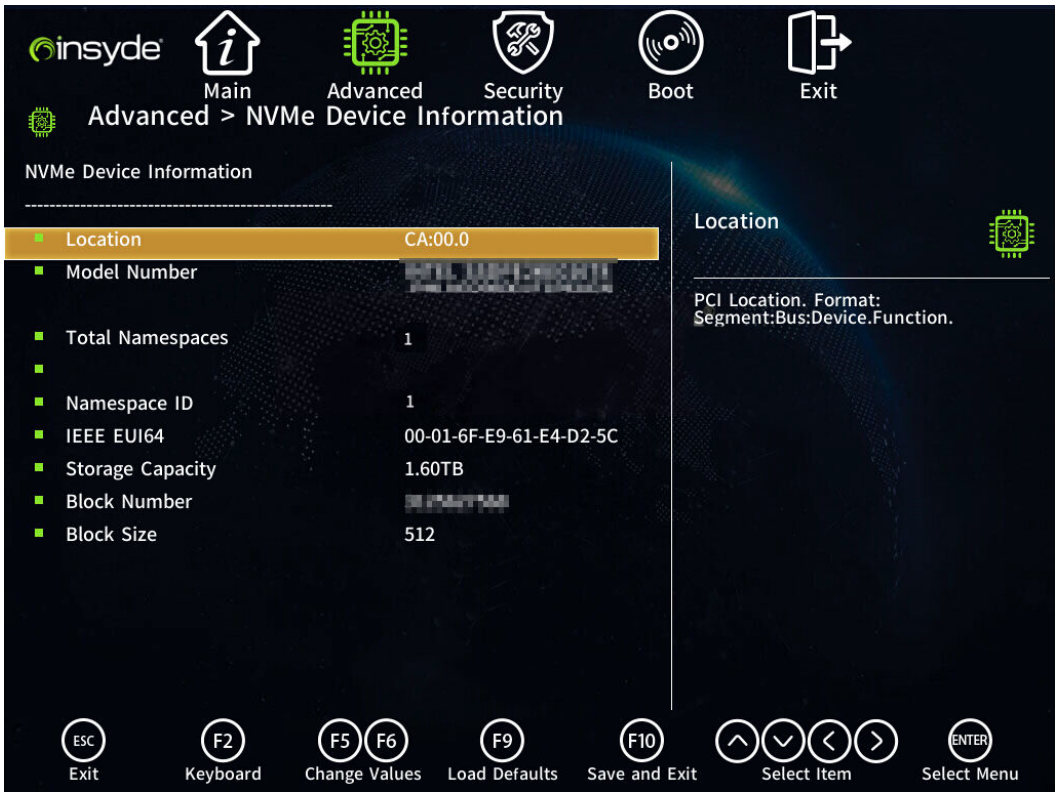


Table 5-85 Parameters on the NVMe Device Information screen

Parameter	Description
Location	Displays the location.
Model Number	Displays the model.
Total Namespaces	Displays the total number of namespaces.
Namespace ID	Displays the namespace information.
IEEE EUI64	Displays the IEEE EUI64 information.
Storage Capacity	Displays the storage capacity.
Block Number	Displays the block number.
Block Size	Displays the block size.

5.3 Security

On the **Security** screen, you can set the trusted platform module (TPM)/trusted cryptography module (TCM) function, the administrator, or the common user password.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

- **Figure 5-100** shows the **Security** screen if no TPM or TCM is installed on the server.
- **Figure 5-101** shows the **Security** screen if a TPM 2.0 is installed on the server.
- **Figure 5-102** shows the **Security** screen if a TCM is installed on the server.

Table 5-86 describes the parameters on the screen.

TPM is a security chip that complies with the TPM specification. It can effectively protect the PC and prevent unauthorized users from accessing the server. The TPM specification is formulated by the Trusted Computing Group (TCG).

TCM uses the cryptographic algorithm and engine developed by China to build a security chip.

Figure 5-100 Security screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-101 Security screen 2



Figure 5-102 Security screen 3



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-103 Security screen 4



Table 5-86 Parameters on the Security screen

Parameter	Description	Default Value

TPM Device	Dynamically displays the detected TPM device type. If no TPM device is installed on the server, **Not Detected** is displayed.
	NOTE
	• When installing a TPM type device, the following parameters are displayed:
	  • **TPM**
	  • **TPM Availability**
	  • **TPM Operation**
	  • **Clear TPM**
	• When installing a TCM type device, the following parameters are displayed:
	  • **TCM State**
	  • **TCM Availability**
	  • **TCM Operation**
	  • **TCM Force Clear**
		-

TPM	Displays the status of the TPM.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TPM Availability	Sets the usage status of the TPM. The menu options are as follows: ● **Available** ● **Hidden**	Available
TPM Operation	Sets the TPM operation. The menu options are as follows: ● **No Operation** ● **Enabled (**for BIOS versions earlier than 01.01.06.03 it is **Enable)** ● **SetPCRBanks(Algorithm)** ● **LogAllDigests** ● **SetPPRequiredForClear_True** ● **SetPPRequiredForClear_False** ● **SetPPRequiredForTurnOn_False** ● **SetPPRequiredForTurnOn_True** ● **SetPPRequiredForTurnOff_False** ● **SetPPRequiredForTurnOff_True** ● **SetPPRequiredForChangePCRs_False** ● **SetPPRequiredForChangePCRs_True** ● **SetPPRequiredForChangeEPS_False** ● **SetPPRequiredForChangeEPS_True** ● **ChangeEPS**	No Operation
Clear TPM	Specifies whether to forcibly clear the TPM key.	Disabled
TCM State	Displays the status of the TCM.	-
TCM Availability	Sets the usage status of the TCM. The menu options are as follows: ● **Available** ● **Hidden**	Available

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TCM Operation	Sets the TCM operation. The menu options are as follows: ● **No Operation** ● **Disable and Deactivate** ● **Enable and Activate**	No Operation
TCM Force Clear	Specifies whether to forcibly clear the TCM key.	Disabled
Supervisor Password	Displays the status of the BIOS administrator password. ● **Not Installed**: The administrator password is not set. You do not need to enter the password when accessing the BIOS. ● **Installed**: The administrator password has been set. You need to enter the password when accessing the BIOS.	-
User Password	Displays the status of the common BIOS user password. ● **Not Installed**: The password of a common BIOS user is not set. ● **Installed**: The password of a common BIOS user has been set.	-
Delete Password Support	Enables or disables the function of deleting passwords. This parameter can be configured when the BIOS login password is set. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** Clearing the BIOS password reduces system security. Exercise caution when performing this operation.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Set Supervisor Password	Sets the BIOS administrator password. **NOTE** ● The password complexity requirements are as follows: ● The password must contain 8 to 16 characters. ● The password must contain at least two types of the following characters: uppercase letters, lowercase letters, and digits. ● The password must contain at least one space or one of the following special characters: `~!@#$^&*%()-_=+|[{}];:'",<.>/? ● A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10. ● The new password must contain at least two different characters from the old password. ● The administrator password cannot be the same as a common user. ● Before changing the BIOS administrator password, you need to enter the current BIOS administrator password. If you enter incorrect passwords for three consecutive times, the server will be locked. You can restart the server to unlock it. ● The default BIOS password is **Admin@9000** (administrator password). If you use the default password to log in, the system prompts you to change the administrator password.	Admin@9000
Delete Supervisor Password	Deletes the administrator password. **NOTE** ● This parameter is available when **Delete Password Support** is set to **Enabled**. ● Exercise caution when you perform this operation deleting the administrator password will bring security risks.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value

Set User Password	Sets the common BIOS user password.
	NOTE
	● Only when the administrator password is set, a common user password can be set.
	● The password complexity requirements are as follows:
	  ● The password must contain 8 to 16 characters.
	  ● The password must contain at least two types of the following characters: uppercase letters, lowercase letters, and digits.
	  ● The password must contain at least one space or one of the following special characters: `~!@#$^&*%()-_=+|[{}];:'",<.>/?
	  ● A new password cannot be one of the last five passwords used or a weak password. The number of last passwords to be verified can be set to a value ranging from 5 to 10.
	  ● The new password must contain at least two different characters from the old password.
	  ● The administrator password cannot be the same as a common user.
	● If you log in using the administrator password, you can directly set a new common user password without verification of the original common user password. If you log in using a common user password, you need to verify the original common user password before setting a new common user password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it.
		-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Delete User Password	Clears the common BIOS user password that has been set. This parameter is available after a common user password is set. **NOTICE** ● After the common user password is deleted, you cannot use the common user password to log in to the BIOS. Exercise caution when performing this operation. ● If you log in to the BIOS using a common user password, you need to enter the current common user password first to clear the common user password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it.	-
Simple Password	Enables or disables the simple password function. The menu options are as follows: ● **Enabled** ● **Disabled** **NOTE** ● After the simple password function is enabled, the password complexity is not verified, but the password must contain 8 to 16 characters. ● Enabling the simple password function reduces system security. Exercise caution when you use this parameter.	Disabled
Power-On Password	Controls whether a password is required for POST. The options are as follows: ● **Enabled**: The system prompts you to enter the password during POST. ● **Disabled**: The system prompts you to enter the password when you access **Setup Utility**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Password Expiration Date	Sets the validity period of the password. The menu options are as follows: ● **0 day** ● **30 days** ● **60 days** ● **90 days** ● **180 days** ● **360 days** **NOTE** ● **0 day** means that the password never expires. ● This parameter is valid for administrators and common users. ● If the password expires, you can continue to log in to the BIOS using the password.	180 days
Saved password record numbers	Sets the number of historical password groups. The menu options are as follows: ● **5** ● **6** ● **7** ● **8** ● **9** ● **10**	5
Weak Password Dictionary	Displays the list of weak passwords. You can add or delete password strings on this screen. There are 25 weak passwords by default. **NOTE** This parameter is valid for administrators and common users.	-
MOR State	Enables or disables the MOR (Memory Overwrite Request) feature. The menu options are as follows: ● **Disabled** ● **Enabled** **NOTE** 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7 supports this parameter only in BIOS 01.01.08.07 and later versions.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TLS Certificate Manager	Refers to the TLS certificate management screen.	-

5.3.1 Weak Password Dictionary

On the **Weak Password Dictionary** screen, you can add or delete password strings. **Figure 5-104** shows the **Weak Password Dictionary** screen. **Table 5-87** describes the parameters.

Figure 5-104 Weak Password Dictionary screen

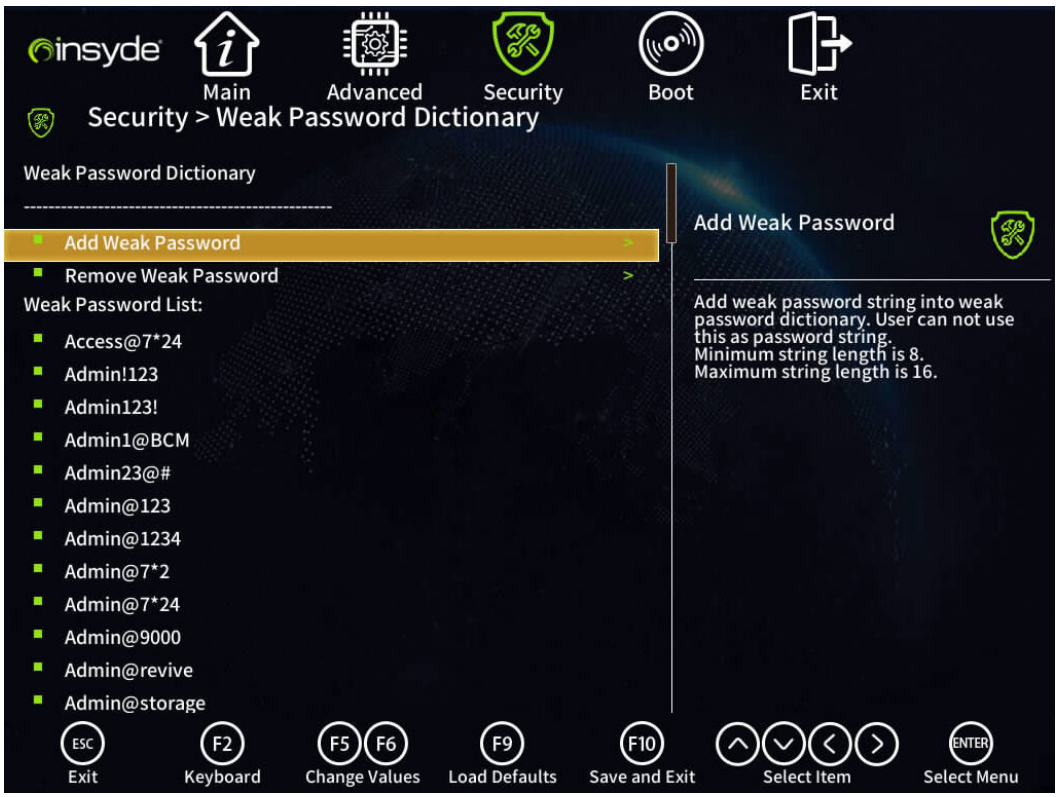


Table 5-87 Parameters on the Weak Password Dictionary screen

Parameter	Description
Add Weak Password	Enters the password string to be added to the weak password dictionary. **NOTE** • Strings in the weak password dictionary cannot be used as passwords. • A maximum of 75 password strings can be set.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Remove Weak Password	Enters the password string to be removed from the weak password dictionary. After the password string is removed, you can use this string as a password.
Weak Password List	Displays weak passwords that have been added. By default, there are 25 weak password strings.

5.3.2 TLS Certificate Manager

On the **TLS Certificate Manager** screen, you can manage TLS certificates. **Figure 5-105** shows the **TLS Certificate Manager** screen. **Table 5-88** describes the parameters.

Figure 5-105 TLS Certificate Manager screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-88 Parameters on the TLS Certificate Manager screen

Parameter	Description
Import Certificate	Registers the certificate. Import a certificate (example): 1. Use the storage medium to place the certificate in the root directory of the server. 2. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **Import Certificate**. 3. Select **xFusion.cer**, press **Enter**, and select **Yes**. 4. Select **Delete Certificate** to enter the certificate deletion screen. If the certificate information is displayed, the certificate is imported successfully. **NOTE** • Certificates can be imported only in UEFI mode. • Only certificates with the DER code in FAT16/ FAT32 format are supported.
Delete Certificate	Deletes the certificate. Delete a certificate (example): 1. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **Delete Certificate**. 2. Select **xFusion.cer**, **press Enter**, and select **Yes**. 3. If no certificate information is displayed on the certificate deletion screen, the certificate is deleted successfully.

5.3.2.1 Import Certificate

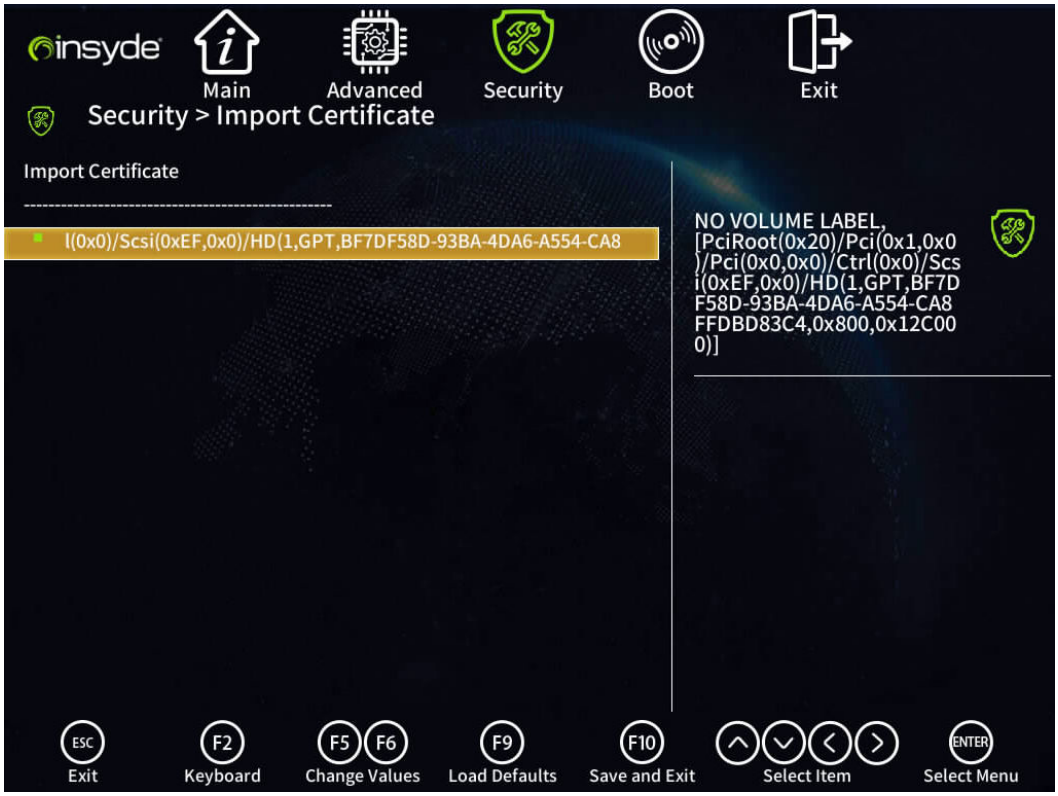
On the **Import Certificate** screen, you can register TLS certificates. **Figure 5-106** shows the **Import Certificate** screen.

NOTE

The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-106 Import Certificate screen



5.3.2.2 Delete Certificate

On this screen, you can delete TLS certificates. **Figure 5-107** shows the **Delete Certificate** screen.

NOTE

The file list on this screen is automatically identified and displayed by the BIOS. The information displayed on this screen varies according to the actual server configuration. If no related file exists, no content is displayed on the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-107 Delete Certificate screen



5.4 Boot

On the **Boot** screen, you can set the boot mode, boot method, and boot device of the server. **Figure 5-108** and **Figure 5-109** show the **Boot** screen. **Table 5-89** describes the parameters.

NOTE

The information displayed on this screen varies according to the actual server configuration.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-108 Boot screen (UEFI mode)



Figure 5-109 Boot screen (legacy mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 5-89 Parameters on the Boot screen

Parameter	Description	Default Value
Boot Type	Sets the system boot type. The menu options are as follows: ● Legacy Boot Type ● UEFI Boot Type	UEFI Boot Type

Parameter	Description	Default Value
	NOTE • After the Secure Boot function is enabled in UEFI mode, this parameter is grayed out and cannot be set (that is, it cannot be set to **Legacy Boot Type**). • If an OS has been installed in Legacy or UEFI mode, the OS cannot be accessed after the boot mode is changed. You need to change the boot mode to that used during OS installation. Only the ESXi OS is not affected. If the OS needs to be reinstalled, select UEFI or Legacy mode based on site requirements. • If the capacity of the target drive or RAID group is greater than 2 TB, set **Boot Type** to **UEFI Boot**. For details, see the release notes of the OS. • If the OS is to be installed on an NVMe drive, you can set **Boot Type** to only **UEFI Boot**. • In legacy mode, the Option ROM uses a fixed 128 KB memory address space. When a large number of devices are configured on the server, some devices in legacy mode may not have sufficient Option ROM space. As a result, the device functions are abnormal. For example, the OS cannot be booted on the RAID, the NIC fails to be started in PXE mode, or the GPU cannot be properly displayed. Based on this limitation, it is highly recommended that the UEFI mode be used. If you need to use legacy mode, you are advised to disable the serial port redirection function or NIC PXE function based on the actual service scenario to ensure that the OS can be started properly. For details, see **3.1.12 Setting PXE for an NIC** and **3.1.21 Setting Serial Port Redirection**. • Restrictions on boot options in legacy mode: The total number of boot options cannot exceed 32. The number of boot options of the same type cannot exceed 16. The number of RAID arrays configured by the RAID controller card cannot exceed 14. For details about the reasons for the restrictions, see **A.1 Restrictions on Boot Devices in Legacy Mode**.	

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Network Stack	Enables or disables the PXE boot function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is supported only in UEFI mode.	Enabled
PXE Boot Capability	Sets the PXE boot network. The menu options are as follows: ● Disabled ● UEFI:IPv4 ● UEFI:IPv6 ● UEFI:IPv4/IPv6 **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled**.	UEFI:IPv4
IPv4 PXE	Enables or disables the IPv4 PXE function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled** and **PXE Boot Capability** is set to **UEFI:IPv4** or **UEFI:IPv4/IPv6**.	Enabled
IPv6 PXE	Enables or disables the IPv6 PXE function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled** and **PXE Boot Capability** is set to **UEFI:IPv6** or **UEFI:IPv4/IPv6**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
HTTP(s) Boot Capability	Sets the HTTPS boot network. The menu options are as follows: ● Disabled ● HTTP(s): IPv4 ● HTTP(s): IPv6 ● HTTP(s): IPv4/IPv6 **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled**.	HTTP(s):IPv4
HTTP Support	Specifies whether to allow the HTTP connection. The menu options are as follows: ● **Enabled**: Allows the HTTP connection (insecure). Both URI schemes (*https://* and *http://*) are allowed. ● **Disabled**: Rejects the HTTP connection. Only the URI scheme (*https://*) is allowed. **NOTE** This parameter is supported only in UEFI mode.	Disabled
PXE Boot to LAN	Enables or disables the PXE boot function of the LAN. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is supported only in legacy boot mode.	Enabled
Boot Fail Policy	Selects the operation to be performed after the boot fails. The menu options are as follows: ● **None**: No operation is performed. ● **Cold Boot**: Cold boot. ● **Boot Retry**: Retries the boot.	Boot Retry

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PXE Retry Count	Sets the times of repeated boots from the PXE. The value ranges from 1 to 99. ● The value **99** indicates unlimited retries. ● The value from **1** to **98** indicates the number of PXE retries. When the number reaches the set value, the BIOS automatically attempts to boot from another device. **NOTE** This parameter is unavailable when **Boot Fail Policy** is set to **Cold Boot** or **None**.	1
PXE Timeout Control	Sets the number of DHCP connection retries due to timeout occurring when each enabled port is booted from the PXE. The menu options are as follows: ● **Disabled**: Disables this function. ● 1 ● 2 ● 3 ● 4 **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is unavailable when **Network Stack** is set to **Disabled**. ● When this parameter is set to **1**, **2**, **3**, or **4**, the maximum duration is 4s, 12s, 28s, or 60s respectively. If this parameter is set as **Disabled**, the maximum duration is 60s by default.	Disabled
SP Boot	Enables or disables the boot function of Smart Provisioning (SP). The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **USB Boot** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
USB Boot	Enables or disables the boot function of the external USB device. The menu options are as follows: ● **Enabled**: allows booting from external USB devices (such as virtual a CD-ROM drive, a floppy drive, and a physical USB CD-ROM drive). ● **Disabled**: It is forbidden to boot from external USB devices (such as a virtual CD-ROM drive, a floppy drive, and a physical USB CD-ROM drive).	Enabled
OEM Fast Boot	Enables or disables the BIOS fast boot function. The menu options are as follows: ● Enabled ● Disabled	Disabled
Sync Order	Enables or disables the synchronization sequence function. The menu options are as follows: ● **Disabled**: invalid. ● **Sync Boot Order**: Adjusts the order of boot options based on the priority of the boot device type. ● **Sync Boot Device Type Order**: Adjusts the priority of boot device types in the order of boot options.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Boot Override	Sets the first priority boot device. The menu options are as follows: ● **PCIE SSD First**: PCIe SSD as priority. ● **iSCSI First**: iSCSI as priority. ● **FC First**: Fiber Channel as priority. ● **FCOE First**: Fibre Channel over Ethernet as priority. ● **Direct First**: PCH pass-through device as priority. ● **RAID First**: RAID as priority. ● **USB First**: USB device as priority. ● **Local Disk Boot Only**: Local drive as priority. ● **Disabled**: Disables this function. **NOTE** After this option is set, the system starts from the boot device set in **Boot Override**. If the boot fails, the system starts according to the boot sequence set in **Boot Sequence**.	Disabled
Boot Sequence	Sets the boot sequence.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
UEFI	Sets the boot device when the boot type is UEFI. ● **Hard Disk Drive**: displays the drive boot device. ● **DVD-ROM Drive**: displays the CD boot device. ● **PXE**: displays the PXE boot device. ● **Other Device**: displays other boot devices. **NOTE** ● If no boot device is configured or boot devices do not support UEFI boot, the boot type is not displayed in the UEFI area. For example, if no drive is configured on the server, the **Hard Disk Drive** boot type to which represents boot from a drive is not displayed under the UEFI area. ● Press the ↑ and ↓ keys to select the boot device. ● Press **F5** (move down)/**F6** (move up) to change the boot sequence. ● You can enable or disable a boot device by dragging the button on the right of the boot device.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

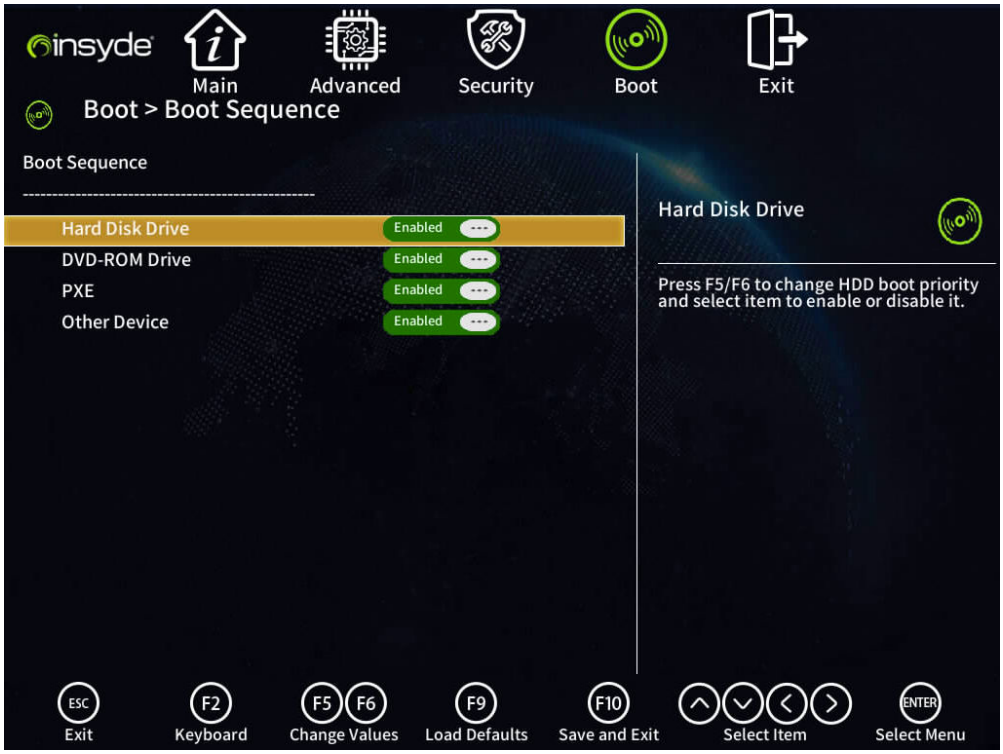
Parameter	Description	Default Value
Legacy	Sets the boot device when the boot type is legacy. ● **Hard Disk Drive**: displays the drive boot device. ● **DVD-ROM Drive**: displays the CD boot device. ● **PXE**: displays the PXE boot device. ● **Other Device**: displays other boot devices. **NOTE** ● If no boot device is configured or boot devices do not support legacy boot, the boot type is not displayed in the legacy area. For example, if no drive device is configured for the server, the **Hard Disk Drive** boot type to which the drive device belongs is not displayed under the legacy area. ● Press the ↑ and ↓ keys to select the boot device. ● Press **F5** (move down)/**F6** (move up) to change the boot sequence. ● You can enable or disable a boot device by dragging the button on the right of the boot device.	-

5.4.1 Boot Sequence

On the **Boot Sequence** screen, you can set the boot sequence of the system boot options. **Figure 5-110** shows the **Boot Sequence**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-110 Boot Sequence screen



NOTE

- The server boots in the sequence specified on this screen.
- The default boot sequence is **Hard Disk Drive**, **DVD-ROM Drive**, **PXE**, and then **Other Device**.
- Press the ↑ and ↓ keys to select the boot device.
- Press **F5** (move down)/**F6** (move up) to change the boot sequence.
- You can enable or disable a boot device by dragging the button on the right of the boot option.

5.5 Exit

On the **Exit** screen, you can control the function of keeping BIOS parameters or saving and exiting after BIOS parameters modification. **Figure 5-111** shows the **Exit** screen. **Table 5-90** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 5-111 Exit screen



Table 5-90 Parameters on the Exit screen

Parameter	Description
Save Changes & Exit	Saves all the modifications and exits the BIOS. **NOTE** You can also press **F10** to save the changes and exit the BIOS.
Save Changes Without Exiting	Saves all the modifications without exiting the BIOS.
Discard Changes & Exit	Discards all the modifications and exits the BIOS.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Load Defaults	Restores the BIOS factory settings. **NOTE** ● Except for the following information that cannot be restored, the other BIOS parameters will be restored to default values of the current BIOS version. Modify related parameters again if the service requires special configurations on the BIOS parameters. ● Date and time information on the **Main** screen ● BIOS password and BIOS startup logo ● All parameters (except watchdog-related parameters) on the **BMC Configuration** screen under the **Advanced** screen ● All parameters on the **Device Manager** and **Administer Secure Boot** screens in UEFI mode ● Press **F9** to load default values of BIOS parameters.
Load Custom Defaults	Restores the BIOS customized default settings. **NOTE** ● This parameter is displayed only when the BIOS of the server is customized before delivery. ● After the BIOS is upgraded, the factory-customized options are restored to the default values and this parameter will not be displayed.
Discard Changes Without Exiting	Discards the modification.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6 Description of Setup Utility (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

NOTE

On the **Setup Utility** screen, a common user can only view menu options, set or change their own password (that is, editing the **Set User Password** option on the **6.3 Security** screen and **Save Changes & Exit** option on the **6.5 Exit** screen). Other options cannot be edited.

6.1 Main

6.2 Advanced

6.3 Security

6.4 Boot

6.5 Exit

6.1 Main

The **Main** screen provides basic BIOS information, including the BIOS version, CPU model, memory capacity, and system time. **Figure 6-1** shows the **Main** screen. **Table 6-1** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-1 Main screen



Table 6-1 Parameters on the Main screen

Parameter	Description
BIOS Version	Indicates the BIOS version.
Release Date	Indicates the compiling date of the BIOS.
Product Name	Indicates the product name. **NOTE** The value is dynamically obtained from the BMC. If no information is obtained, the message **To be filled by O.E.M.** is displayed.
System Number	Indicates the product serial number. **NOTE** The value is dynamically obtained from the BMC. If no information is obtained, the message **To be filled by O.E.M.** is displayed.
Processor Type	Indicates the processor model.
Node Number	Indicates the number of processors that a server has been installed with.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Processor Core Count	Indicates the number of cores of a single processor. **NOTE** The number of physical cores of a single processor varies depending on the processor model.
TDP	Thermal design power, which is the heat released when the processor reaches the maximum load.
Total Memory	Indicates the total memory capacity that a server has been installed with.
System Memory Speed	Displays the current memory speed.
Cache RAM	Indicates the cache.
Language	Indicates the system language. The menu options are as follows: ● English ● Chinese ● Japanese **NOTE** The default language is **English**.
System Date	Indicates the current system date. The system date is in the format of *mm/dd/yyyy*. Select the month, day, or year to be set and press **Enter**.
System Time	Indicates the current BIOS time. The system time is in the format of *HH:MM:SS* in the 24-hour system. Select the hour, minute, or second to be set and press **Enter**.

6.2 Advanced

The **Advanced** screen provides advanced BIOS configuration options. **Figure 6-2** shows the **Advanced** screen. **Table 6-2** describes the parameters.

NOTE

When the server is configured with a RAID controller card or PCIe device, the **Advanced** screen displays the setup menus of the RAID controller card or the PCIe device. The displayed setup menus vary depending on different RAID controller cards or PCIe devices. For details, see the corresponding RAID controller card or PCIe device manual.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-2 Advanced screen



Table 6-2 Parameters on the Advanced screen

Parameter	Description
Platform Information	Displays the platform information.
Peripheral Configuration	Provides access to configure peripheral devices.
Video Configuration	Provides access to adjust the display settings.
ACPI Table or Features Control	Provides access to ACPI table or function configurations.
Socket Configuration	Provides access to CPU, memory, I/O, and power management configurations.
BMC Configuration	Provides access to configure BMC settings.
PCH-IO Configuration	Provides access to the PCH configurations.
Misc Configuration	Provides access to other miscellaneous configurations.
Console Redirection Configuration	Provides access to serial port redirection configurations.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
PXE Configuration	Provides access to network configurations.
ME Configuration	Provides access to management engine (ME) configurations.
NVMe Information	Displays NVMe device details.
System Event Log	Provides access to the event management.

6.2.1 Platform Information

This screen displays platform-related version information, including the PCH version, ACM version, and PMC firmware version. **Figure 6-3** shows the **Platform Information** screen. **Table 6-3** describes the parameters.

Figure 6-3 Platform Information screen

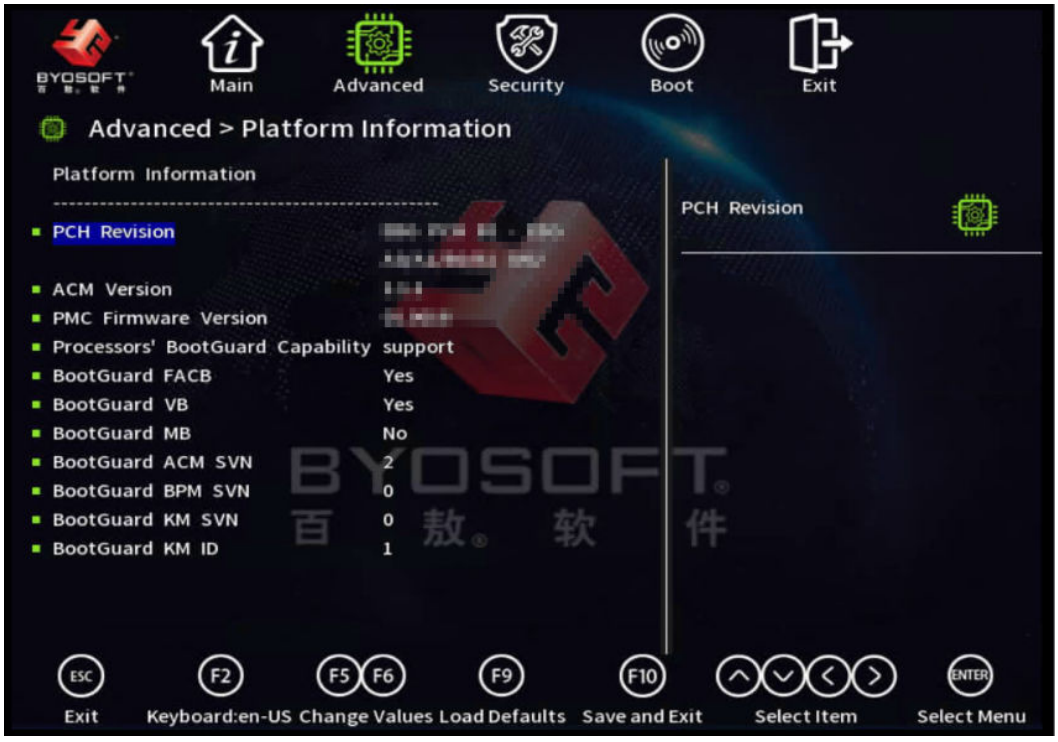


Table 6-3 Parameters on the Platform Information screen

Parameter	Description
PCH Revision	Displays the PCH version.
Acm Version	Displays the ACM version.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
PMC Firmware Version	Displays the PMC firmware version.
Processors' BootGuard Capability	Displays whether the BootGuard function is supported.
BootGuard FACB	Displays the BootGuard FACB information.
BootGuard VB	Displays the BootGuard VB information.
BootGuard MB	Displays the BootGuard MB information.
BootGuard ACM SVN	Displays the BootGuard ACM SVN information.
BootGuard BPM SVN	Displays the BootGuard BPM SVN information.
BootGuard KM SVN	Displays the BootGuard KM SVN information.
BootGuard KM ID	Displays the BootGuard KM ID information.

6.2.2 Peripheral Configuration

On the **Peripheral Configuration** screen, you can set peripheral devices. **Figure 6-4** shows the **Peripheral Configuration** screen. **Table 6-4** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-4 Peripheral Configuration screen

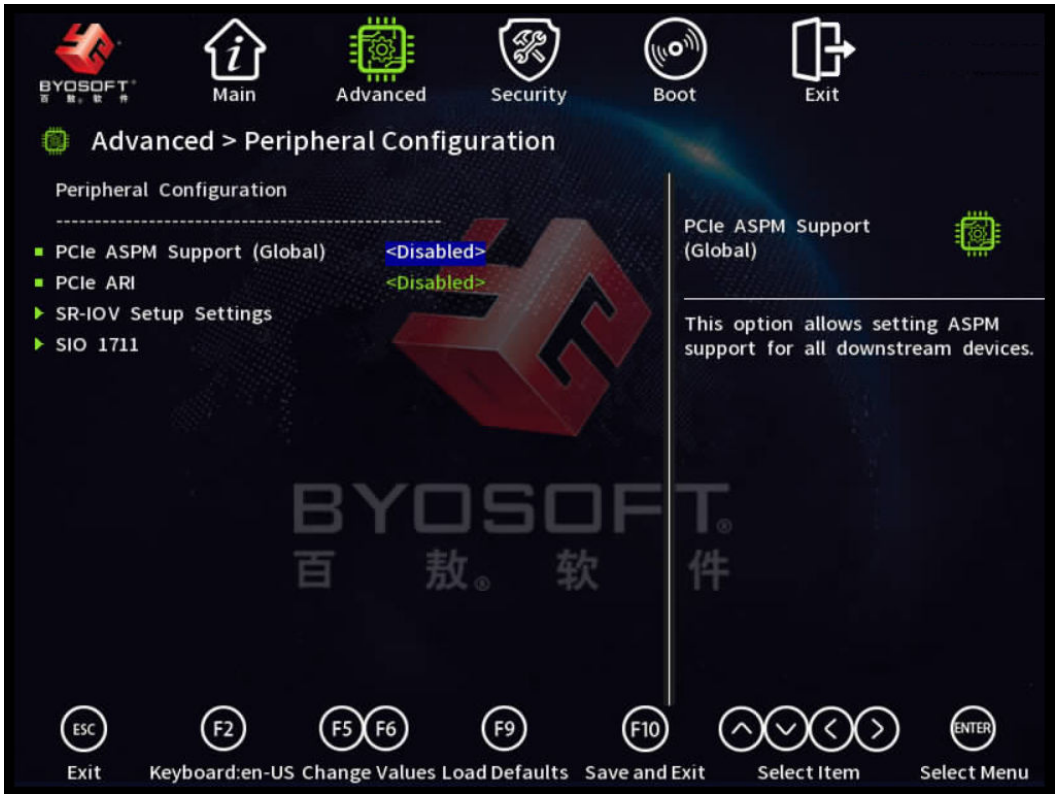


Table 6-4 Parameter on the Peripheral Configuration screen

Parameter	Description	Default Value
PCIe ASPM Support (Global)	Enables dynamic power management for all PCIe devices. The menu options are as follows: • **L1 Only**: Enters L1 mode only. • **Per Individual port**: Sets the mode separately for each port. • Disabled	Disabled
PCIe ARI	Enables or disables the alternative routing ID interpretation (ARI) technology for each PCIe card. The menu options are as follows: • Enabled • Disabled	Disabled

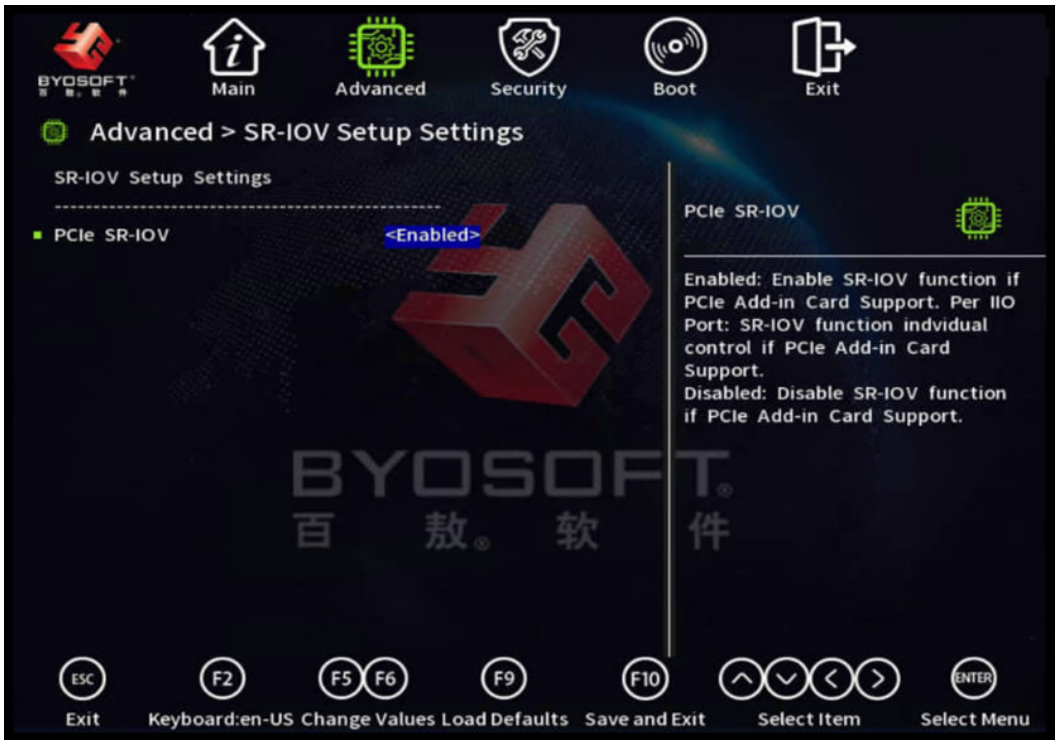
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SR-IOV Setup Settings	Indicates SR-IOV settings.	-
SIO 1711	Indicates SIO 1711 settings.	-

6.2.2.1 SR-IOV Setup Settings

On the **SR-IOV Setup Settings** screen, you can configure SR-IOV. **Figure 6-5** shows the **SR-IOV Setup Settings** screen. **Table 6-5** describes the parameters.

Figure 6-5 SR-IOV Setup Settings screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-5 Parameters on the SR-IOV Setup Settings screen

Parameter	Description	Default Value
PCIe SR-IOV	Enables or disables the SR-IOV function of the PCIe card. The menu options are as follows: ● **Enabled**: Enables the SR-IOV function of the PCIe card. ● **Disabled**: Disables the SR-IOV function of the PCIe card. ● **Per IIO Port**: Individually controls the SR-IOV function depending on the IIO SR-IOV option of each IIO port. **NOTE** Per IIO Port configuration applies only to endpoints directly attached under the CPU Root Port. This setting does not apply to devices extended hierarchically through switches (including the switch itself and endpoints installed in switch expansion slots).	Enabled
CPU 1 Port DMI	Enables or disables the SR-IOV function of CPU 1 port 0/DMI. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **PCIe Device SR-IOV Technology** is set to **Per IIO Port**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CPU *X* Port *Y*	Enables or disables the SR-IOV function of the CPU *X* port *Y*. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is available when **PCIe SR-IOV** is set to **Per IIO Port**. ● *X* indicates the physical slot number of the CPU. For 2288 V7, G5500 V7, and G8600 V7, the value is **1** or **2**. For 5885H V7 and 2488H V7, the value ranges from 1 to 4. *Y* indicates the port number. The parameter list varies depending on the server configuration.	Enabled

6.2.2.2 SIO 1711

On the **SIO 1711** screen, you can set the features related to SIO 1711. **Figure 6-6** shows the **SIO 1711** screen. **Table 6-6** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-6 SIO 1711 screen



Table 6-6 Parameters on the SIO 1711 screen

Parameter	Description	Default Value
UART 1	Configures the serial port using the option. The menu options are as follows: ● **Enabled**: user configuration ● **Disabled**: no configuration	Enabled
Base I/O Address	Indicates the serial port output option. You can configure the address of the serial port device using this option. The menu options are as follows: ● 3F8 ● 2F8	3F8

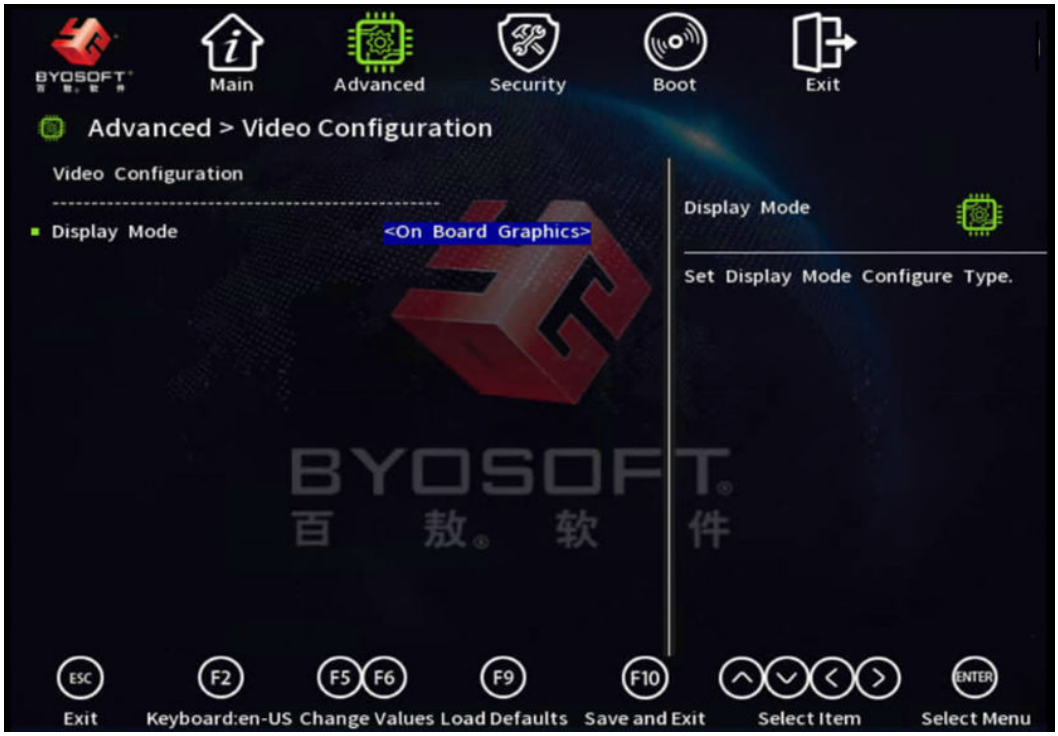
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Interrupt	Interrupts the configuration. The menu options are as follows: • IRQ3 • IRQ4	IRQ4

6.2.3 Video Configuration

On the **Video Configuration** screen, you can set video parameters. **Figure 6-7** shows the **Video Configuration** screen. **Table 6-7** describes the parameters.

Figure 6-7 Video Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-7 Parameter on the Video Configuration screen

Parameter	Description	Default Value
Display Mode	Sets the display mode. The menu options are as follows: • **Plug-in Graphics**: Use a plug-in video card. • **On Board Graphics**: Use an onboard video card. **NOTE** If G5500 V7 is in legacy mode, the **On Board Graphics** function is used if you seclect any of both options.	On Board Graphics

6.2.4 ACPI Table or Features Control

On the **ACPI Table or Features Control** screen, you can configure the ACPI table or set related features. **Figure 6-8** shows the **ACPI Table or Features Control** screen. **Table 6-8** describes the parameters.

Figure 6-8 ACPI Table or Features Control screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-8 Parameters on the ACPI Table or Features Control screen

Parameter	Description	Default Value
SPCR Table Support	Sets whether serial port redirection works after POST. This function takes effect only in DOS and GRUB. The menu options are as follows: • Enabled • Disabled	Enabled

6.2.5 Socket Configuration

On the **Socket Configuration** screen, you can set CPU-related features. **Figure 6-9** shows the **Socket Configuration** screen. **Table 6-9** describes the parameters.

Figure 6-9 Socket Configuration screen



Table 6-9 Parameter on the Peripheral Configuration screen

Parameter	Description
Processor Configuration	Provides access to processor CFR configurations.

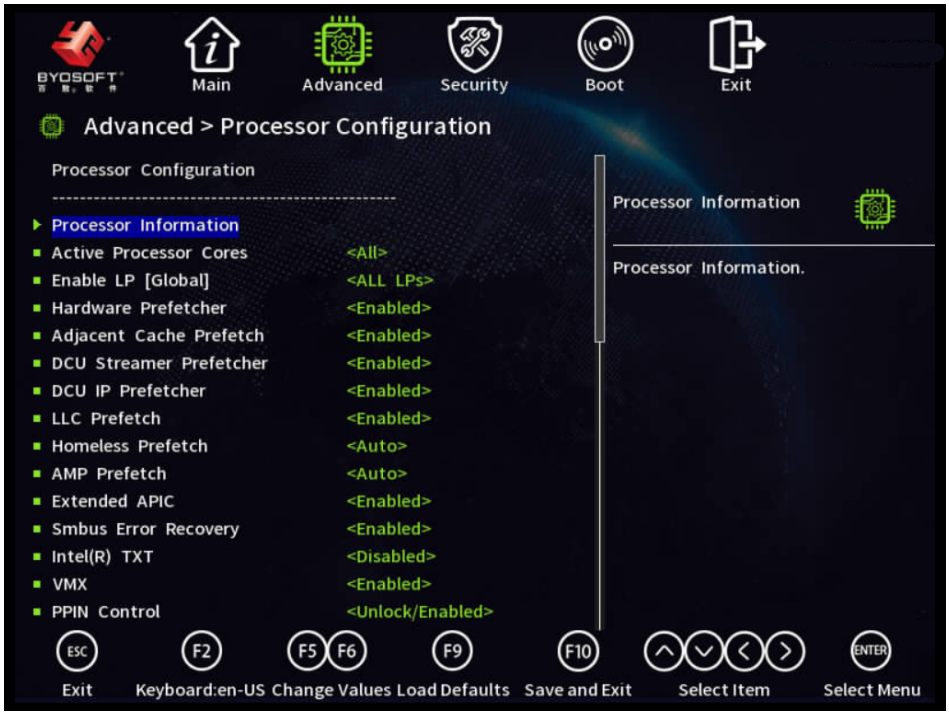
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Common RefCode Configuration	Provides access to common RefCode configurations.
Uncore Configuration	Provides access to uncore configurations.
Memory Configuration	Provides access to memory configurations.
IIO Configuration	Provides access to I/O configurations.
Advanced Power Management Configuration	Provides access to advanced power management configurations.

6.2.5.1 Processor Configuration

On the **Processor Configuration** screen, you can set processor-related parameters. **Figure 6-10**, **Figure 6-11**, and **Figure 6-12** show the **Processor Configuration** screen. **Table 6-10** describes the parameters.

Figure 6-10 Processor Configuration screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-11 Processor Configuration screen 2

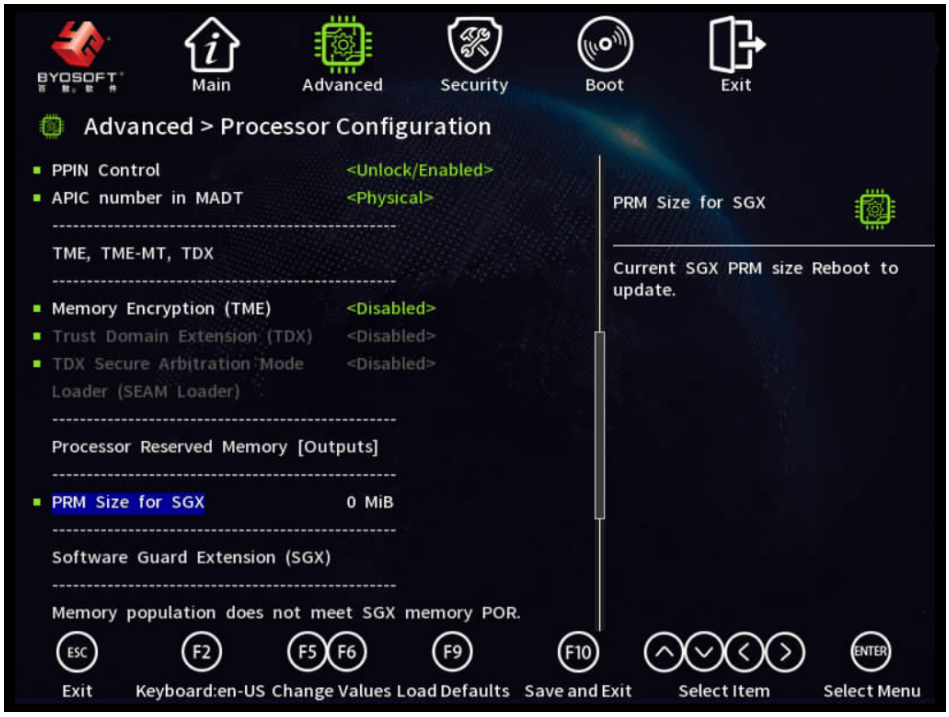
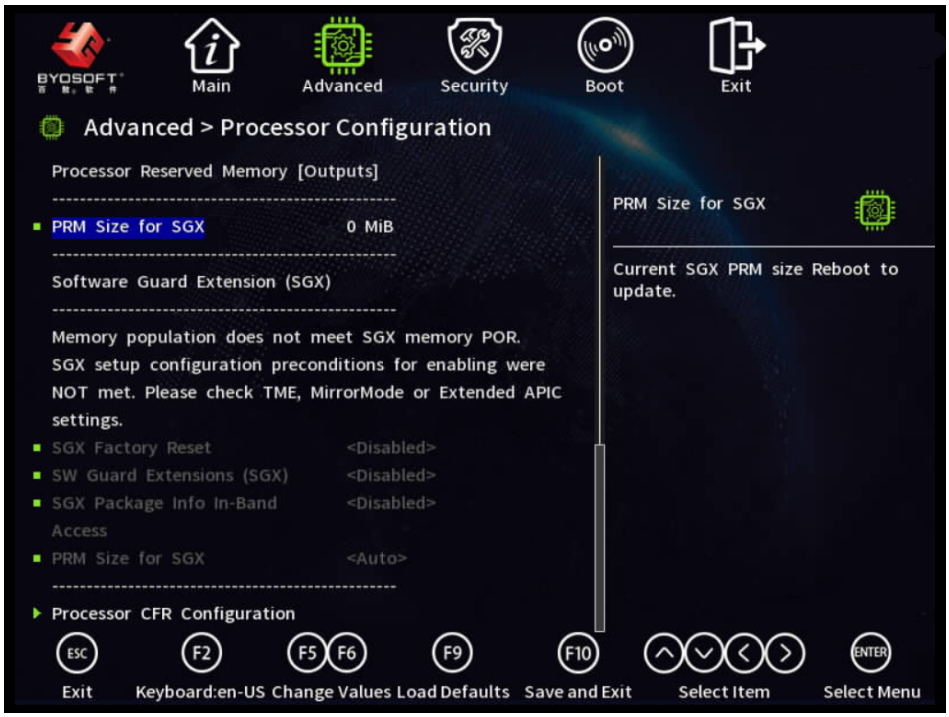


Figure 6-12 Processor Configuration screen 3



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-10 Parameters on the Processor Configuration screen

Parameter	Description	Default Value
Processor Information	Queries detailed CPU configurations in the current environment.	-
Active Processor Cores	Sets the number of CPU cores that can be used. The value can be **All**, **1**, or **2** to **N-1**. (*N* indicates the maximum number of physical cores supported by the CPU.)	All
Enable LP [Global]	Enables or disables the processor hyper-threading feature. If this function is enabled, each physical processor core functions as two logical processor cores. If this function is disabled, each physical processor core functions as only one logical processor core. Enabling this function increases the number of logical processor cores and improves system performance. The menu options are as follows: ● Single LP ● ALL LPs	ALL LPs

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Hardware Prefetcher	Enables or disables the hardware prefetcher function. Enables or disables Hardware Prefetcher. When this feature is enabled, the CPU prefetches instructions or data from the memory to the L2 cache before processing the instructions or data. This feature helps reduce the memory access time and eliminate potential performance bottlenecks. In most environments, this feature needs to be enabled to achieve optimal performance. For some workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Adjacent Cache Prefetch	Enables or disables adjacent cache prefetcher function. When this feature is enabled, the system regards the data adjacent to the required data is also required, and reads the adjacent data in advance to improve data access performance. When the system uses sequential memory access, this feature improves data access efficiency. When the system uses random memory access, you are advised to disable this feature. The menu options are as follows: ● Enabled ● Disabled	Enabled
DCU Streamer Prefetcher	Enables or disables DCU Streamer Prefetcher. This feature may affect system performance depending on the applications running on the server. In most environments, this feature needs to be enabled to achieve optimal performance. For some scenarios with high workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DCU IP Prefetcher	Enables or disables the DCU IP prefetcher function. This feature may affect system performance depending on the applications running on the server. In most environments, this feature needs to be enabled to achieve optimal performance. For some scenarios with high workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The menu options are as follows: ● Enabled ● Disabled	Enabled
LLC Prefetch	Enables or disables the L3 cache prefetcher function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Homeless Prefetch	Enables or disables the Homeless prefetcher feature on all threads. The menu options are as follows: ● Enabled ● Disabled ● Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
L1 Next Page Prefetcher	Enables or disables the next page prefetcher feature of the L1 cache. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **SierraForest**.	Enabled
AMP Prefetch	Enables or disables the MLC AMP prefetcher. The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** ● G8600 V7 The Auto option is supported only in BIOS versions 01.02.04.03 and later. ● G5500 V7 The Auto option is supported only in BIOS versions 01.02.03.02 and later. ● 5885H V7 and 2488H V7 The Auto option is supported only in BIOS versions 01.02.02.02 and later. ● 2288 V7 The Auto option is supported only in BIOS versions 01.02.04.01 and later.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Extended APIC	Enables or disables the extended advanced programmable interrupt controller (APIC) feature. If the total number of CPU cores exceeds 256, you are advised to enable this option to enable the OS to support the CPU multi-core feature more efficiently. The menu options are as follows: ● Enabled ● Disabled	Enabled
Smbus Error Recovery	Enables or disables the SMBus error recovery function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Intel(R) TXT	Enables or disables the Intel(R) TXT function. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
VMX	Enables or disables CPU virtualization technology. When this option is enabled, the virtualization layer or OS that supports this option can use the hardware capabilities of Intel virtualization technology. Some virtualization layers require the Intel virtualization technology. You can keep this feature enabled when the virtualization layer or OS does not support this feature. The menu options are as follows: ● Enabled ● Disabled **NOTE** When **Intel(R) TXT** is set to **Enabled**, this parameter is grayed out and cannot be edited.	Enabled
PPIN Control	Specifies whether to unlock and enable the PPIN control. The menu options are as follows: ● Lock/Disabled ● Unlock/Enabled	Unlock/Enabled
APIC number in MADT	Sets whether the number of local APICs or X2APICs that are physically enabled is reported or the maximum number of supported local APICs or X2APICs is reported in the MADT. The menu options are as follows: ● Physical ● Maximum	Physical

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory Encryption (TME)	Enables or disables the total memory encryption (TME). The menu options are as follows: ● Enabled ● Disabled	Disabled
Total Memory Encryption (TME) Bypass	Enable or disable Total Memory Encryption (TME). The menu options are as follows: ● Auto ● Enabled ● Disabled **NOTE** ● This parameter is supported only in BIOS versions 01.02.08.09 and later. ● This parameter is visible when **Memory Encryption (TME)** is set to **Enabled**.	Disabled
Total Memory Encryption Multi-Tenant (TME-MT)	Enable or disable Total Memory Encryption - Multi-Tenant (TME-MT). The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in BIOS versions 01.02.08.09 and later. ● This parameter is visible when **Memory Encryption (TME)** is set to **Enabled**. ● This parameter is configurable when **Limit CPU PA to 46 bits** is set to **Disabled** in the **Socket Configuration** > **Uncore Configuration** > **Uncore General Configuration** page.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory integrity	Enables or disables the TME-MT integrity function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in BIOS versions 01.02.08.09 and later. ● This parameter is visible when **Memory Encryption (TME)** is set to **Enabled**. ● This parameter is configurable when **Limit CPU PA to 46 bits** is set to **Disabled** in the **Socket Configuration** > **Uncore Configuration** > **Uncore General Configuration** page.	Disabled
Key stock amount	Displays the amount of key stock. **NOTE** This parameter is visible when **Memory Encryption (TME)** is set to **Enabled**.	-
TME-MT key ID bits	Displays the number of bits in the TME-MT key ID. **NOTE** This parameter is visible when **Memory Encryption (TME)** is set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Trust Domain Extension (TDX)	Enables or disables the trust domain extension (TDX). The menu options are as follows: **NOTE** This parameter option is grayed out when any of the following configuration conditions are met: ● **TdxCapability** is **SECURITY_API_INCAPABLE** ● **EnableMktme** is set to **Disabled** ● **MirrorMode** is set to **Enabled** ● **Extended APIC** is set to **Disabled** ● **Memory integrity** is set to **Disabled**, and **LiIntegrityCapability** is **SECURITY_API_INCAPABLE** ● Enabled ● Disabled	Disabled
TDX Secure Arbitration Mode Loader (SEAM Loader)	Enables or disables the TDX Secure Arbitration Mode Loader (SEAM Loader) function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is supported only in BIOS versions 01.02.08.09 and later.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Disable excluding Mem below 1MB in CMR	Enables or disables the function to include memory region below 1 MB in the Convertible Memory Range (CMR). The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** ● This parameter is supported only in BIOS versions 01.02.08.09 and later. ● This parameter is visible when **Total Memory Encryption Multi-Tenant (TME-MT)** and **Trust Domain Extension (TDX)** are set to **Enabled**.	Auto
TME-MT/TDX key split	Sets the number of bits used by TDX in the TME-MT/TDX key split, and the rest of bits will be used by TME-MT. The value ranges from 1 to 0x7. **NOTE** ● This parameter is supported only in BIOS versions 01.02.08.09 and later. ● This parameter is visible when **Total Memory Encryption Multi-Tenant (TME-MT)** and **Trust Domain Extension (TDX)** are set to **Enabled**.	1
TME-MT Keys:	Displays the number of keys designated for TME-MT usage. **NOTE** This parameter is visible when **Memory Encryption (TME)** and **Trust Domain Extension (TDX)** are set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TDX keys:	Displays the number of keys designated for TDX usage. **NOTE** This parameter is visible when **Total Memory Encryption Multi-Tenant (TME-MT)** and **Trust Domain Extension (TDX)** are set to **Enabled**.	-
PRM Size	Specifies the total PRM size, which is applicable to all technologies requesting PRM. The menu options are as follows: ● No valid PRMRR size ● 128M ● 256M ● 512M ● 1G ● 2G ● 4G ● 8G ● 16G ● 32G ● 64G ● 128G ● 256G ● 512G	- **NOTE** There is no default value. Refer to the actual situation.
SGX Factory Reset	Restores the SGX to factory settings and performs the SGX factory reset in subsequent startups: Delete all registration data and force the initial platform to build a process if SGX is enabled. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SW Guard Extensions (SGX)	Enables or disables the Software Guard Extensions (SGX). The menu options are as follows: ● Enabled ● Disabled	Disabled
SGX Package Info In-Band Access	Enables or disables the in-band access to Software Guard Extensions (SGX) package information. The menu options are as follows: ● Enabled ● Disabled	Disabled
SGX PRM Size	Specifies the SGX PRM size. The menu options are as follows: ● No valid PRMRR size ● 128M ● 256M ● 512M ● 1G ● 2G ● 4G ● 8G ● 16G ● 32G ● 64G ● 128G ● 256G ● 512G	- **NOTE** There is no default value. Refer to the actual situation.
Processor CFR Configuration	Provides access to the processor CFR configurations.	-

6.2.5.1.1 Processor Information

On the **Processor Information** screen, you can view information about each CPU. **Figure 6-13** shows the **Processor Information** screen. **Table 6-11** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

The displayed information varies according to the CPU model of the server.

Figure 6-13 Processor Information screen

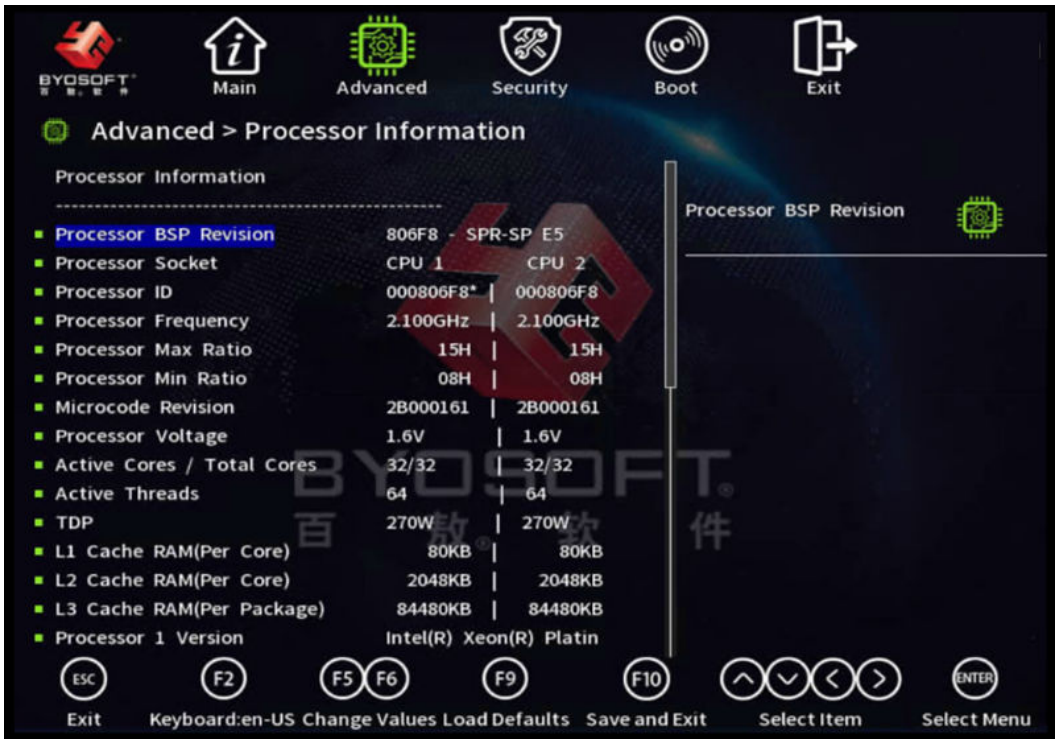


Table 6-11 Parameters on the Processor Information screen

Parameter	Description
Processor BSP Revision	Displays the CPU model information.
Processor Socket	Displays the CPU physical slot number.
Processor ID	Displays the CPU ID information.
Processor Frequency	Displays the CPU frequency information.
Processor Max Ratio	Specifies the maximum CPU frequency ratio.
Processor Min Ratio	Specifies the minimum CPU frequency ratio.
Microcode Revision	Displays the microcode version.
Processor Voltage	Displays the CPU voltage.
Active Cores/Total Cores	Displays the number of enabled cores/ total cores.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Active Threads	Displays the number of enabled threads.
TDP	Displays the heat released when the processor reaches its maximum load.
L1 Cache RAM(Per Core)	Displays the L1 cache capacity of each core.
L2 Cache RAM(Per Core)	Displays the L2 cache capacity of each core.
L3 Cache RAM(Per Package)	Displays the L3 cache capacity.
Processor *X* Version	Displays the model and frequency of CPU *X*. **NOTE** *X* indicates the physical slot number of the CPU. For 2288 V7, G5500 V7, and G8600 V7, the value is **1** or **2**. For 2488H V7 and 5885H V7, the value ranges from 1 to 4.

6.2.5.1.2 Processor CFR Configuration

On the **Processor CFR Configuration** screen, you can view the processor CFR configurations. **Figure 6-14** shows the **Processor CFR Configuration** screen. **Table 6-12** describes the parameters.

NOTE

The parameters displayed on the screen vary depending on the product model.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-14 Processor CFR Configuration screen

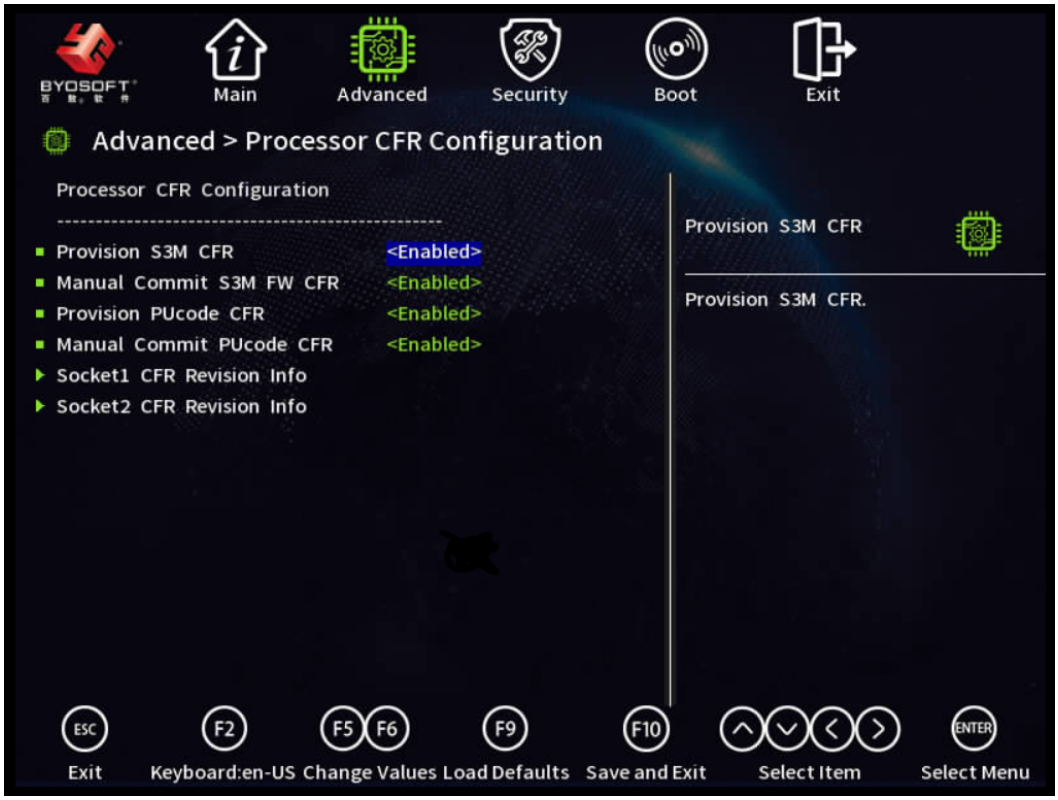


Table 6-12 Parameters on the Processor CFR Configuration screen

Parameter	Description	Default Value
Provision S3M CFR	Enables or disables the Provision S3M CFR. The menu options are as follows: ● Enabled ● Disabled	Enabled
Manual Commit S3M FW CFR	Enables or disables the manual submission of S3M FW CFR. The menu options are as follows: ● Enabled ● Disabled	Enabled
Provision PUcode CFR	Enables or disables the Provision PUcode CFR. The menu options are as follows: ● Enabled ● Disabled	Enabled

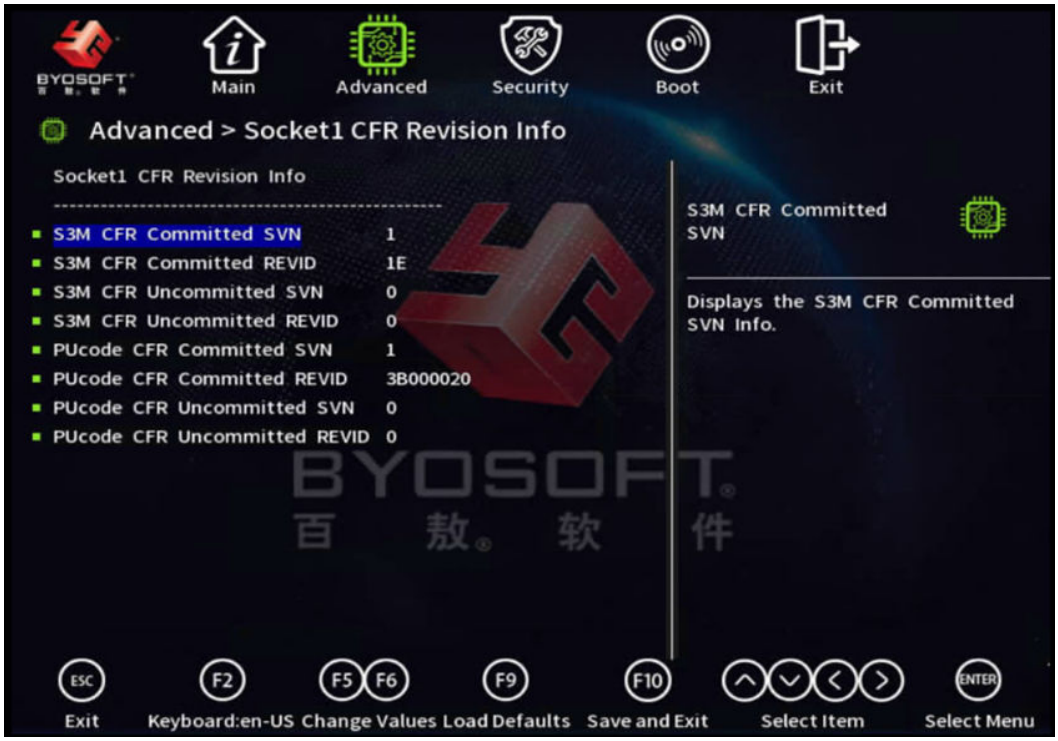
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Manual Commit PUcode CFR	Enables or disables the manual submission of PUcode CFR. The menu options are as follows: • Enabled • Disabled	Enabled
Socket*X* CFR Revision Info	Displays the Socket CFR revision information. **NOTE** *X* indicates the slot number of the CPU. This parameter is displayed when the CPU is installed. The value of *X* ranges from 1 to 4 or from 1 to 2. Refer to the actual situation.	-

?.1. Socket1 CFR Revision Info

Figure 6-15 shows the **Socket1 CFR Revision Info** screen. Table 6-13 describes the parameters.

Figure 6-15 Socket1 CFR Revision Info screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-13 Parameters on the Socket0 CFR Revision Info screen

Parameter	Description
S3M CFR Committed SVN	Displays the SVN information that has been submitted by the S3M CFR.
S3M CFR Committed REVID	Displays the REVID information that has been submitted by the S3M CFR.
S3M CFR UnCommitted SVN	Displays the SVN information that has not been submitted by the S3M CFR.
S3M CFR UnCommitted REVID	Displays the REVID information that has not been submitted by the S3M CFR.
PUcode CFR Committed SVN	Displays the SVN information that has been submitted by the PUcode CFR.
PUcode CFR Committed REVID	Displays the REVID information that has been submitted by the PUcode CFR.
PUcode CFR UnCommitted SVN	Displays the SVN information that has not been submitted by the PUcode CFR.
PUcode CFR UnCommitted REVID	Displays the REVID information that has not been submitted by the PUcode CFR.

6.2.5.2 Common RefCode Configuration

On the **Common RefCode Configuration** screen, you can configure features, such as memory MMIO and NUMA. **Figure 6-16** shows the **Common RefCode Configuration** screen. **Table 6-14** describes the parameters.

NOTE

The displayed information varies according to the product model.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-16 Common RefCode Configuration screen

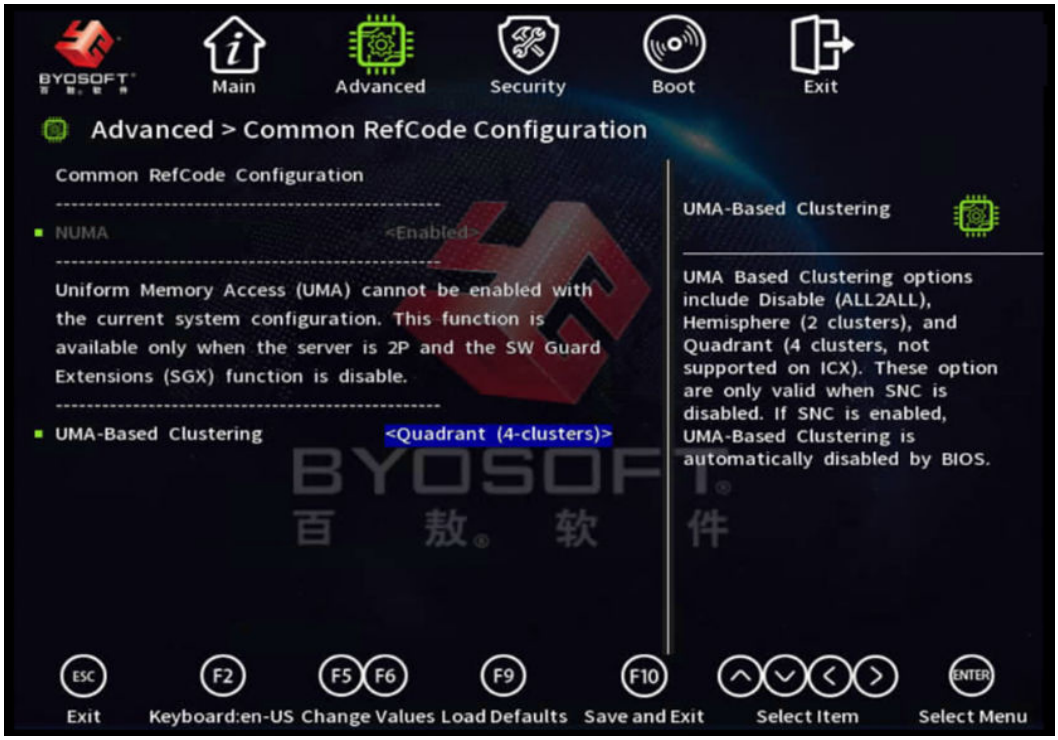


Table 6-14 Parameters on the Common RefCode Configuration screen

Parameter	Description	Default Value
NUMA	Enables or disables the NUMA function of the system. NUMA is supported by all OS platforms. In most cases, enabling this feature improves the performance of some workloads. Disabling this feature requires that all nodes have the same memory capacity. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter can be edited when two CPUs are configured.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
UMA-Based Clustering	Sets the UMA-Based Clustering function. This option is valid only when the SNC is disabled. If SNC is enabled, the BIOS automatically disables this option. The menu options are as follows: ● Disable (All2All): disable ● Hemisphere (2-clusters): dichotomy ● Quadrant (4-clusters): quartering **NOTE** This parameter is unavailable when the CPU type is **Sapphire Rapids-SP** or **Emerald Rapids-SP** and HBM is supported.	Quadrant (4-clusters)

6.2.5.3 Uncore Configuration

On the **Uncore Configuration** screen, you can set uncore parameters. **Figure 6-17** shows the **Uncore Configuration** screen. **Table 6-15** describes the parameters.

Figure 6-17 Uncore Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

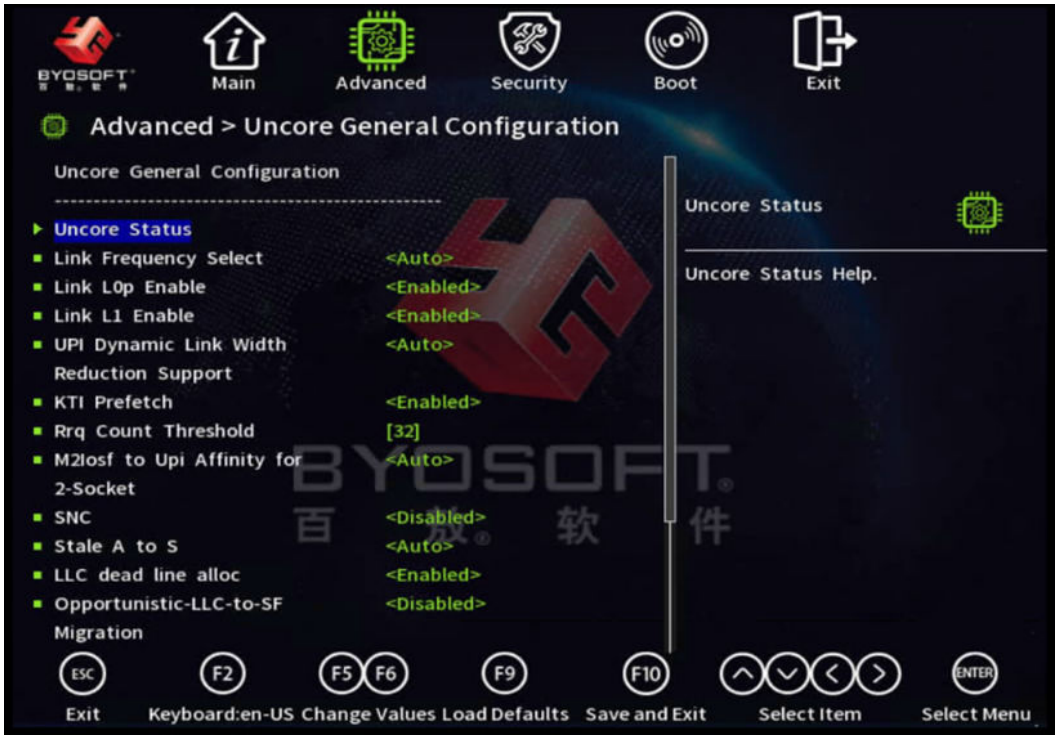
Table 6-15 Parameters on the Uncore Configuration screen

Parameter	Description
Uncore General Configuration	Provides access to common uncore configurations.
Uncore Per Socket Configuration	Provides access to Uncore Per Socket configurations. **NOTE** This parameter is supported only by the G8600 V7 and G5500 V7.

6.2.5.3.1 Uncore General Configuration

On the **Uncore General Configuration** screen, you can configure some common features of the uncore. **Figure 6-18** and **Figure 6-19** show the **Uncore General Configuration** screen. **Table 6-16** describes the parameters.

Figure 6-18 Uncore General Configuration screen 1



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-19 Uncore General Configuration screen 2



Table 6-16 Parameters on the Uncore General Configuration screen

Parameter	Description	Default Value
Uncore Status	Displays the uncore status.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Link Frequency Select	Allows you to select the UPI link rate. When the CPU type is SPR, the menu options are as follows: ● 12.8GT/s ● 14.4GT/s ● 16.0GT/s ● Auto ● **Use Per Link Setting**: Uses the per link settings. When the CPU type is EMR, the menu options are as follows: ● 12.8GT/s ● 14.4GT/s ● 16.0GT/s ● 20.0GT/s ● Auto ● **Use Per Link Setting**: Uses the per link settings. **NOTE** The 20.0 GT/s option is displayed only when **CpuType** is set to **EmeraldRapids-SP**.	Auto
Link L0p Enable	UPI energy saving option. If the L0p option is enabled, the bandwidth of the eight UPI physical channels with low usage will be reduced to x8. When the UPI is not connected and the UPI is set to automatic mode, this function is disabled. In other cases, this function is enabled automatically. The menu options are as follows: ● Disabled ● Enabled ● Auto	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Link L1 Enable	UPI energy saving option. If the L1 option is enabled, UPI is allowed to enter the L1 state when it is idle. In this case, UPI does not generate transmission. The access and exit of L1 are controlled by the PCU. When the UPI is not connected, this function is disabled automatically. In other cases, this function is enabled automatically. The menu options are as follows: ● Disabled ● Enabled ● Auto	Enabled
UPI Dynamic Link Width Reduction Support	Specifies the UPI failover support. The menu options are as follows: ● Disabled ● Enabled ● Auto	Auto
KTI Prefetch	Allows you to set the KTI prefetch function. The menu options are as follows: ● Disabled ● Enabled ● Auto	Enabled
Rrq Count Threshold	Allows you to set the Rrq count threshold. The value ranges from 0 to 32.	32

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
M2Iosf to Upi Affinity for 2-Socket	Allows you to select the optimal UPI for different M2Iosf traffic to enhance performance. Otherwise, all available UPI links are selected. The menu options are as follows: ● Disabled ● Enabled ● Auto **NOTE** This parameter is available when two CPUs are configured.	Auto
SNC	Sets the Sub-NUMA Clustering (SNC) function, which is a mode that reduces the latency of the last level cache (LLC) to local memory. Assume that one CPU can access one memory cluster of its own. In a case of two CPUs, when the SNC is enabled, each CPU can access two memory clusters, but the speed of accessing the memory cluster of its own is fast, and the speed of accessing the external memory cluster is slow. If the SNC is disabled, each CPU can access only one memory cluster of its own. The menu options are as follows: ● Auto ● Disabled ● Enable SNC2 (2-clusters) ● Enable SNC4 (4-clusters)	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Stale A to S	Allows you to set the memory SnoopAll(A) status and Shared(S) status conversion function. Enabling this option reduces the cross-CPU memory access delay. The menu options are as follows: ● Auto ● Enabled ● Disabled	Auto
LLC dead line alloc	Allows you to set the LLC dead line allocation function. The processor marks the row replaced by the MLC as **dead**, indicating that the row will not be read again. This function is used to set the allocation policy for the data marked **dead** in the LLC. The menu options are as follows: ● **Auto**: automatic ● **Enabled**: Allows the LLC to fill dead lines into the LLC if there is free space. ● **Disabled**: The dead lines are dropped and are never filled into the LLC, saving the LLC space.	Enabled
Opportunistic-LLC-to-SF Migration	Allows you to control the Opportunistic-LLC-to-SF migration function. The menu options are as follows: ● Auto ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MBA BW Calibration Profiles	Allows you to select the MBA BW throttling curve. The menu options are as follows: ● Linear BW shaping ● Biased BW shaping ● Legacy BW shaping ● Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MMIO High Base	Allows you to configure the high base address of the memory mapped I/O (MMIO). Adjust this parameter based on requirements of the connected PCIe device for the MMIO high base resources above 4 GB. Improper configuration may cause the system startup failure or abnormal device resource allocation. Do not modify this parameter. The menu options are as follows: ● 56 TB ● 40 TB ● 32 TB ● 24 TB ● 16 TB ● 13 TB ● 4 TB ● 3.5 TB ● 2 TB ● 1 TB ● 512 GB **NOTE** ● The value of this parameter is related to MMIO high granularity size. Refer to the actual situation. ● When the MMIOH base is 56T and the MMIOH granularity size is set to 1024 GB, there may be insufficient space for all stack allocations.	13 TB (2288 V7/G5500 V7/G8600 V7) 32 TB (2488H V7)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MMIO High Granularity Size	Specifies the I/O high base granularity size. By default, the size of MMIO resources allocated to each stack is equal to the I/O high base granularity. Adjust this parameter based on requirements of the connected PCIe device for the MMIO high base resources above 4 GB. So, exercise caution when modifying the parameter. When a large number of PCIe devices (especially GPU devices) are connected, you may need to increase the value to enlarge the MMIO high base space to ensure that the MMIO high base resources of PCIe devices are properly allocated. The menu options are as follows: ● 1 GB ● 4 GB ● 16 GB ● 64 GB ● 256 GB ● 1024 GB **NOTE** ● When the MMIOH start address is 56T and the MMIOH unit size is set to 1024 GB, there may be insufficient space for all stack allocations. ● If the value of **MMIO High Granularity Size** is less than or equal to **4 GB**, the BIOS adds 4 GB MMIOH resources.	1024 GB (G8600 V7/ G5500 V7) 256 GB (5885H V7/2488H V7) 64 GB (2288 V7)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Limit CPU PA to 46 bits	Limits the length of CPU physical addresses to 46 bits to support the earlier Hyper-v. If this option is enabled, TME-MT is automatically disabled. When the option is set to **Disabled**, some OSs, such as Windows 2019, cannot be entered. The menu options are as follows: ● Enabled ● Disabled	Enabled
MCTP Bus Owner Selection	Allows you to select the MCTP bus owner. The menu options are as follows: ● PCH SPS as Bus Owner (Proxy) ● CPU as Bus Owner **CAUTION** If this parameter is set to **CPU as BUS owner**, the OS breaks down.	PCH SPS as Bus Owner (Proxy)

Figure 6-20 shows the **Uncore Status** screen. **Table 6-17** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-20 Uncore Status screen

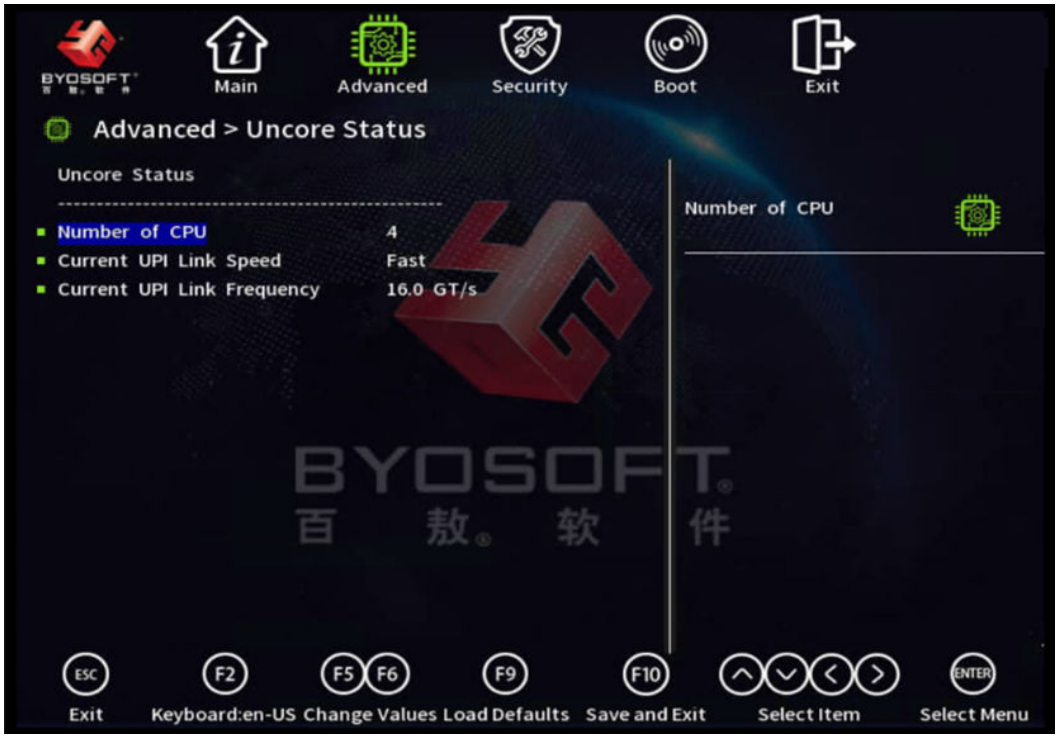


Table 6-17 Parameters on the Uncore Status screen

Parameter	Description
Number of CPU	Displays the current number of CPUs.
Current UPI Link Speed	Displays the current UPI link speed. **NOTE** **Slow or 1s Configuration** is displayed when only one processor is installed.
Current UPI Link Frequency	Displays the current UPI link frequency value. **NOTE** **Unknown or 1s configuration** is displayed when only one processor is installed.

6.2.5.3.2 Uncore Per Socket Configuration

This parameter is supported only by the G8600 V7 and G5500 V7.

On the **Uncore Per Socket Configuration** screen, you can configure **Uncore Per Socket**. Figure 6-21 shows the **Uncore Per Socket Configuration** screen. Table 6-18 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-21 Uncore Per Socket Configuration screen

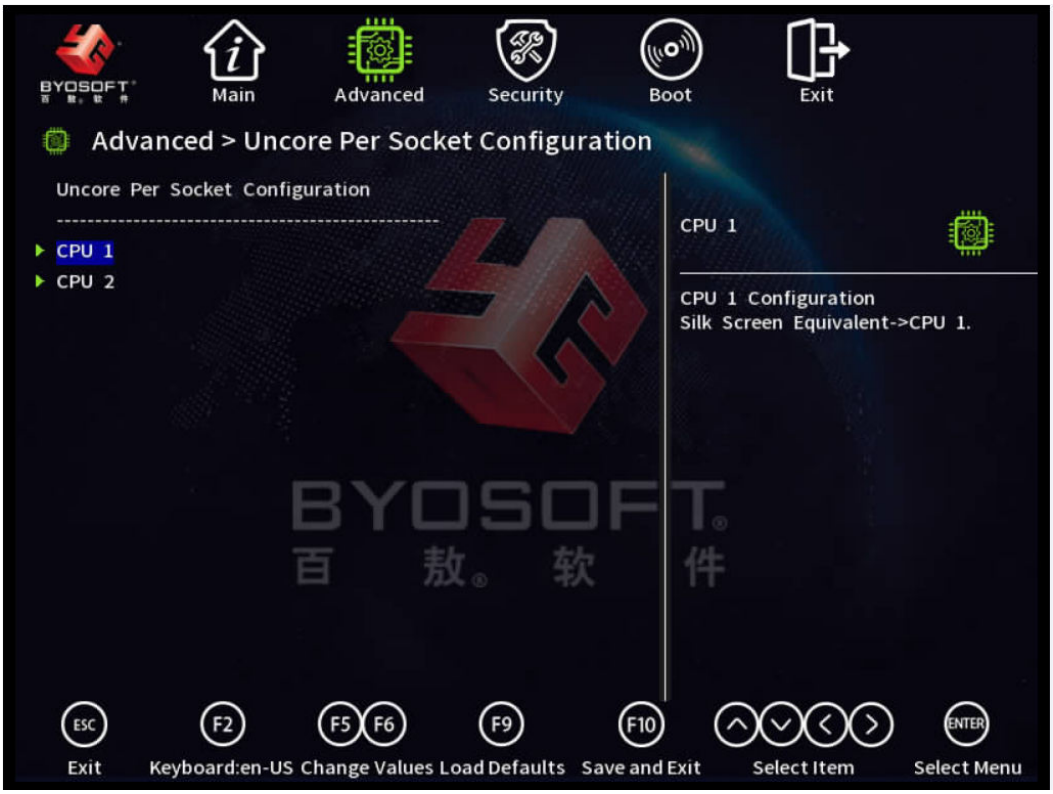


Table 6-18 Parameters on the Uncore Per Socket Configuration screen

Parameter	Description
CPU *X*	Specifies the configurations of CPU *X*.

Figure 6-22 shows the CPU *X* screen (CPU 1 is used as an example). **Table 6-19** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-22 CPU X screen

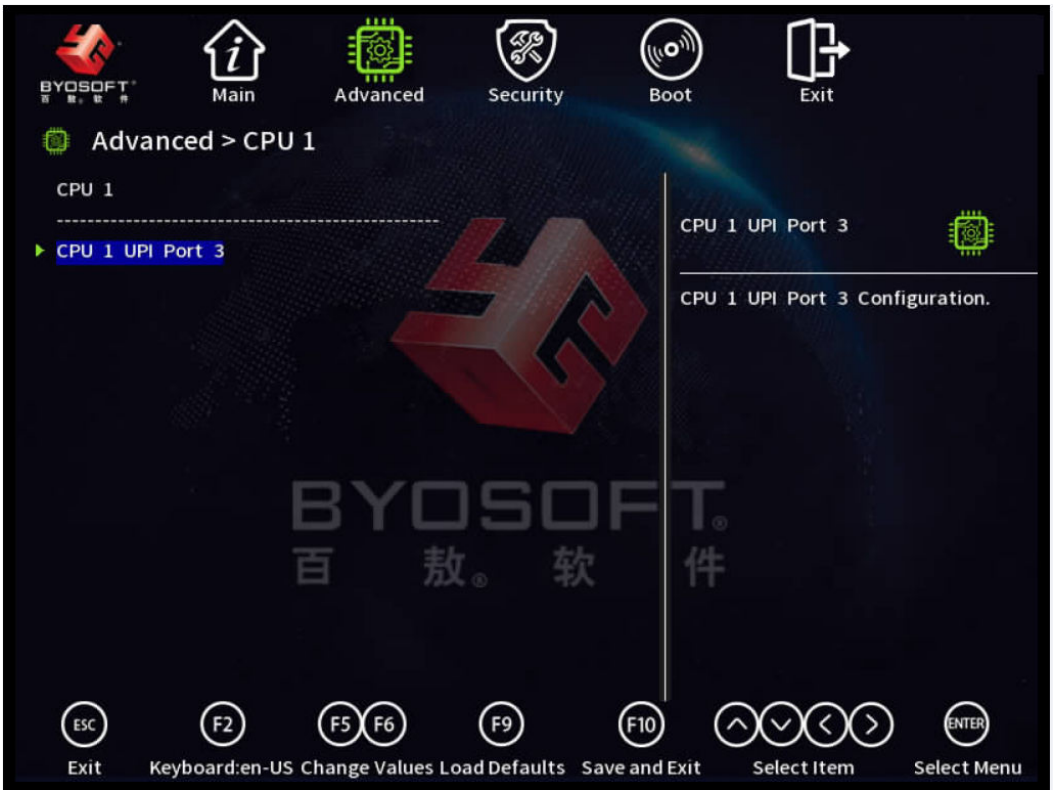


Table 6-19 Parameters on the CPU *X* screen

Parameter	Description
CPU *X* UPI Port 3	Specifies the configurations of CPU X UPI port 3.

Figure 6-23 shows the CPU *X* UPI Port 3 screen. **Table 6-20** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-23 CPU *X* UPI Port 3 screen

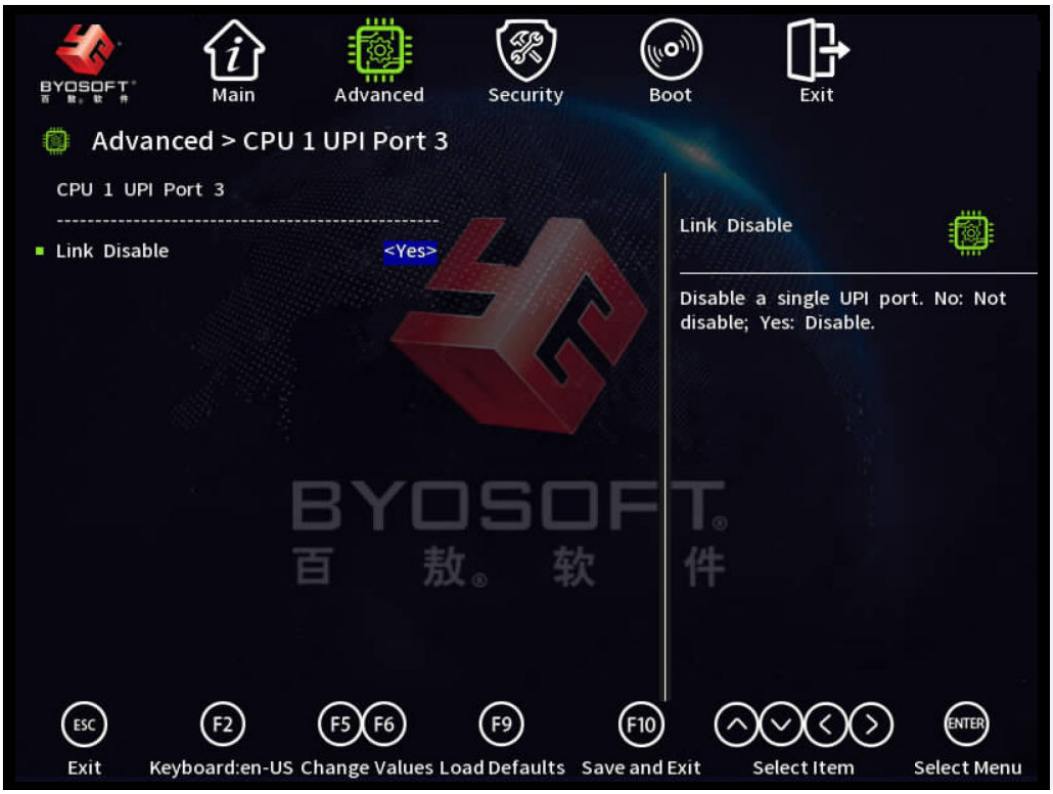


Table 6-20 Parameters on the CPU *X* UPI Port 3 screen

Parameter	Description	Default Value
Link Disable	Disables the UPI link. The menu options are as follows: ● Yes: Disables the UPI link. ● No: Enables the UPI link.	Yes

6.2.5.4 Memory Configuration

On the **Memory Configuration** screen, you can set memory-related parameters. **Figure 6-24** and **Figure 6-25** show the **Memory Configuration** screen. **Table 6-21** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-24 Memory Configuration screen 1

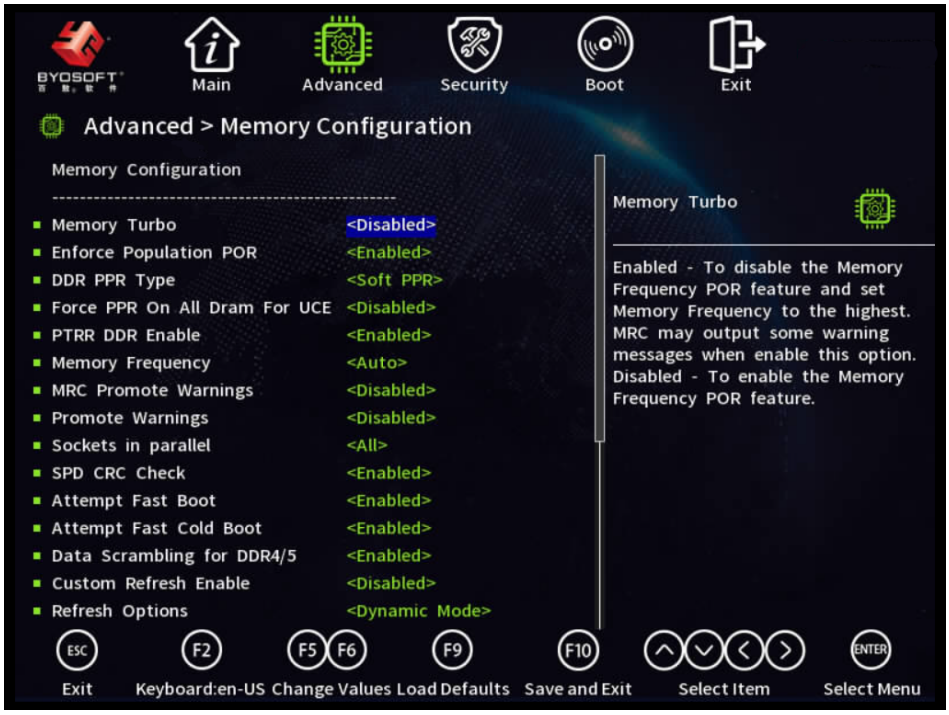
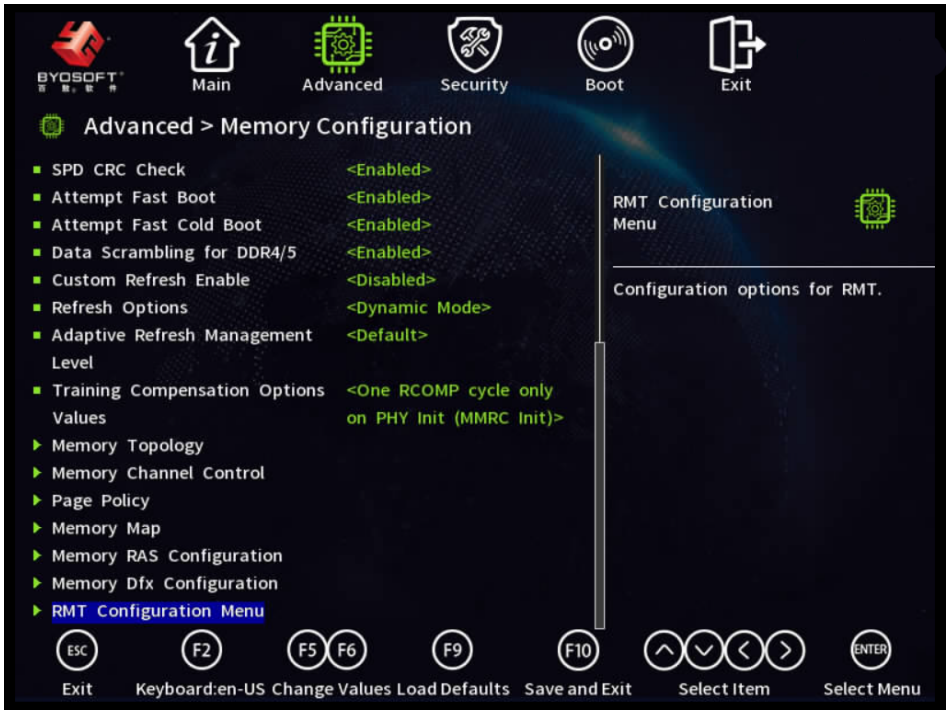


Figure 6-25 Memory Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-21 Parameters on the Memory Configuration screen

Parameter	Description	Default Value
Memory Turbo	Enables or disables the memory acceleration. The menu options are as follows: ● Disabled ● Enabled	Disabled
Enforce Population POR	Enables or disables the memory forced population Plan of Record (POR). If this function is enabled, Memory Reference Code (MRC) forcibly requires the memory module insertion to meet the POR requirements. (verified and officially supported by Intel). The memory module insertion configuration not meeting the requirements will be degraded to the supported configuration.The menu options are as follows: ● Disabled ● Enabled	Enabled
DDR PPR Type	Selects the DDR PPR type. The menu options are as follows: ● PPR Disabled ● Hard PPR ● Soft PPR	Soft PPR
Force PPR On All Dram For UCE	Enables or disables the force PPR on all dram for UCE. The menu options are as follows: ● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
HBM Memory Test	Selects the HBM memory test type. The menu options are as follows: ● Disable HBM Memory Test ● Enable HBM Memory Test **NOTE** This parameter is available when the CPU model is **HBM SKU**.	Enable HBM Memory Test
HBM PPR Type	Selects the HBM post package repair type. The menu options are as follows: ● PPR Disabled ● Hard PPR ● Soft PPR **NOTE** This parameter is available when the CPU model is **HBM SKU**.	PPR Disabled
PTRR DDR Enable	Enables or disables support for the PTRR in DDR. The menu options are as follows: ● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory Frequency	Allows you to set the maximum memory speed in MT/s. If you force to disable the POR, users' device will be able to run at a higher frequency than that supported by memory (restricted to processors). When the CPU type is SPR, the menu options are as follows: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 When the CPU type is EMR, the menu options are as follows: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 ● 5200 ● 5600 **NOTE** When **Memory Turbo** is set to **Enabled**, this parameter is grayed out.	Auto
MRC Promote Warnings	Determines whether to elevate the MRC warning to the system level. The menu options are as follows: ● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Promote Warnings	Determines whether to elevate the warning to the system level. The menu options are as follows: ● Disabled ● Enabled	Disabled
PMem MediaStatus Exception	Enables or disables the PMem media status exception. The menu options are as follows: ● Disabled ● Enabled **NOTE** This parameter is supported only by the 2288 V7.	Enabled
Sockets in parallel	Selects the number of parallel sockets. The menu options are as follows: ● ALL ● 1 ● 2 ● 4	ALL
SPD CRC Check	Enables or disables the SPD CRC function. The menu options are as follows: ● Disabled ● Enabled	Enabled
Attempt Fast Boot	Enables or disables the attempt fast boot function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Attempt Fast Cold Boot	Enables or disables the attempt fast cold boot function. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Data Scrambling for PMem	Selects the data scrambling for PMem. The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** This parameter is supported only by the 2288 V7.	Auto
Data Scrambling for DDR4/5	Selects the data scrambling for DDR4/5. The menu options are as follows: ● Enabled ● Disabled	Enabled
Enable fADR	Enables or disables the fADR function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the CPU model is **SPR CPU**.	Disabled
Custom Refresh Enable	Enables or disables the custom memory refresh feature. The menu options are as follows: ● Enabled ● Disabled	Disabled
Custom Refresh Rate	Sets the custom memory refresh rate. The value ranges from 20 to 40. **NOTE** This parameter is available when **Custom Refresh Enable** is set to **Enabled**.	20
Refresh Options	Selects the memory refresh mode. The menu options are as follows: ● Dynamic Mode ● Static 2x Mode	Static 2x Mode (5885H V7/2488H V7) Dynamic Mode (2288 V7/ G8600 V7/G5500 V7)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Adaptive Refresh Management Level	Selects the adaptive refresh management level. The menu options are as follows: ● Default ● Level A ● Level B ● Level C	Default
Training Compensation Options Values	Provides options for issuing the RCOMP at specific points in training. The menu options are as follows: ● One RCOMP cycle only on PHY Init (MMRC Init) ● One RCOMP cycle after every JEDEC Init ● One RCOMP cycle right before every training step	One RCOMP cycle only on PHY Init (MMRC Init)
Memory Topology	Provides access to the memory topology.	-
Memory Channel Control	Provides access to memory channel control configurations. **NOTE** This parameter is not supported by the 2288 V7.	-
Page Policy	Provides access to the page policy configurations.	-
Memory Map	Provides access to memory mapping configurations.	-
Memory RAS Configuration	Provides access to memory RAS configurations.	-
PMem Configuration	Provides access to PMem configurations. **NOTE** This parameter is supported only by the 2288 V7.	-

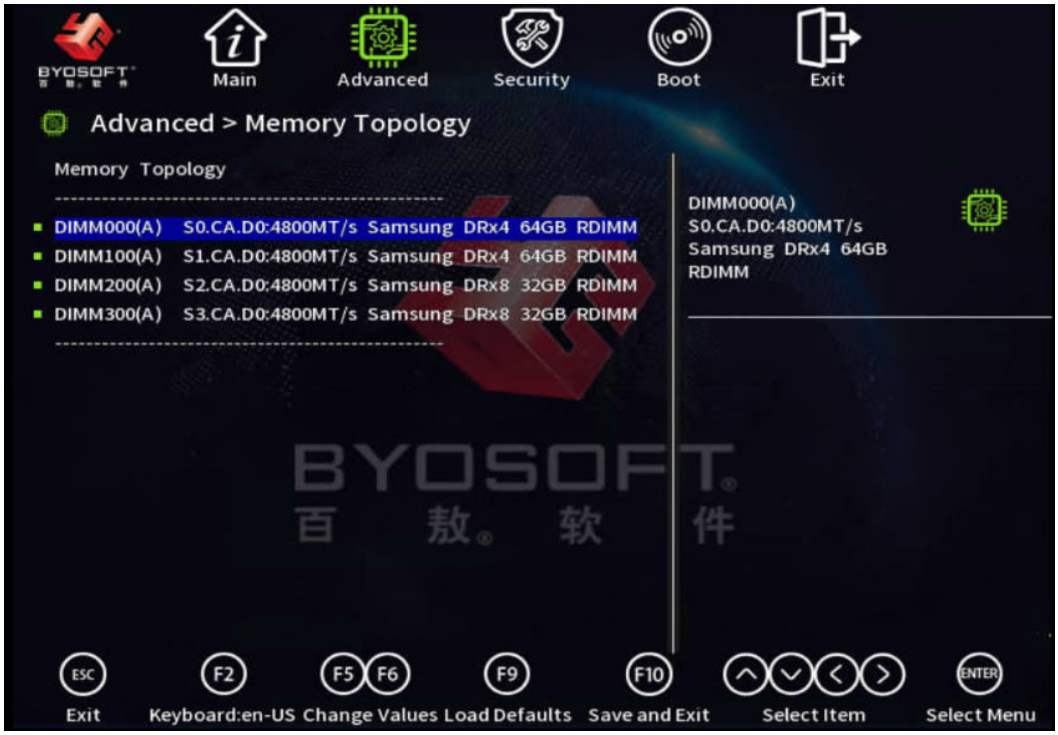
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Memory Dfx Configuration	Provides access to memory DFX configurations.	-
BSSA Configuration Menu	Provides access to BSSA configurations.	-

6.2.5.4.1 Memory Topology

On the **Memory Topology** screen, you can view the model and position of the memory installed on the mainboard. **Figure 6-26** shows the **Memory Topology** screen. **Table 6-22** describes the parameters.

Figure 6-26 Memory Topology screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-22 Parameters on the **Memory Topology** screen

Parameter	Description
DIMMxyz(N)	Displays the topology and presence Information of the memory. ● *x* indicates the slot number of the CPU, which is the actual CPU slot number minus 1. ● *y* indicates the memory channel. The value ranges from 0 to 7. ● *z* indicates the slot number of the memory. ● *N* indicates the silkscreen of the memory. **NOTE** ● "Not Present" is displayed if no memory module is installed in the slot. ● For example, the memory module name DIMM000(A) S0.CA.D0:4800MT/s Samsung DRx4 64GB RDIMM indicates that the DIMM is located in CPU 1 (S0), channel A (CA), and the first slot (D0), the frequency is 4800 MT/s, the vendor is Samsung, the granularity bit width is DRx8, and the capacity is 32 GB. ● *x* indicates the physical slot number of the CPU. The value ranges from 0 to 3.

6.2.5.4.2 Memory Channel Control

On the **Memory Channel Control** screen, you can enable or disable the control function of the CPU channel. **Figure 6-27** shows the **Memory Channel Control** screen. **Table 6-23** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-27 Memory Channel Control screen

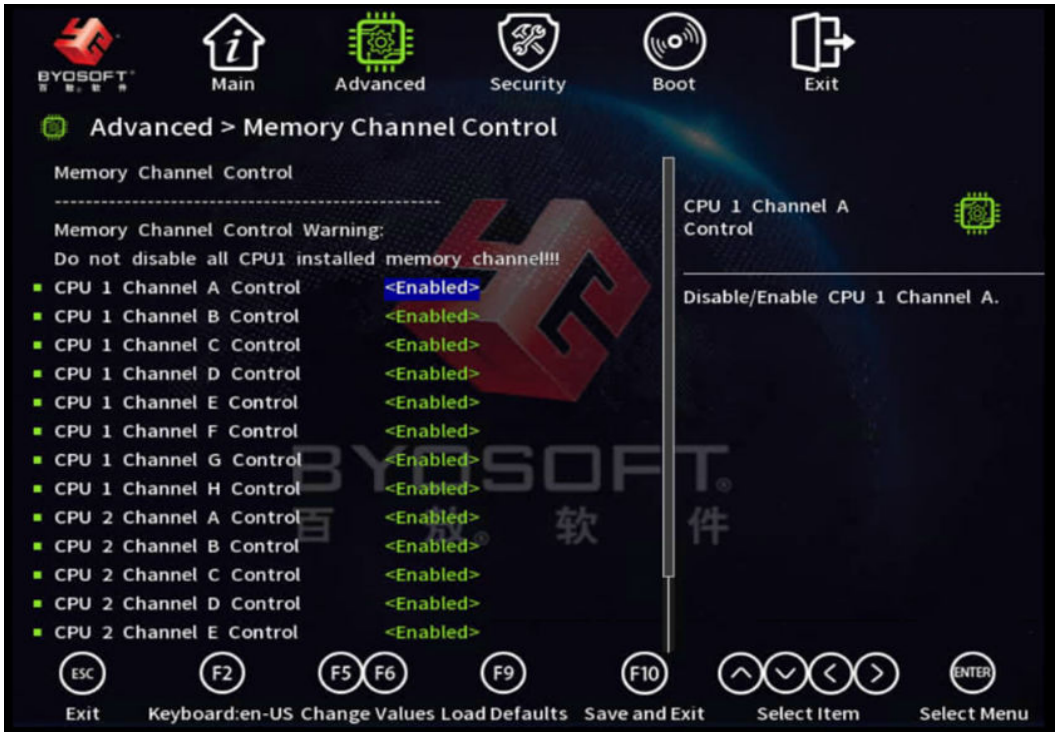


Table 6-23 Parameters on the Memory Channel Control screen

Parameter	Description	Default Value
CPU n Channel m Control	Enables or disables memory *m* channel of CPU *n*. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● *n* indicates the physical slot number of the CPU, and the value ranges from 1 to 4. *m* indicates the channel number, and the value ranges from A to H. ● At least one channel inserted with DIMM must be enabled for CPU1. Otherwise, the system cannot be powered on.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.4.3 Page Policy

On the **Page Policy** screen, you can set the page management policy. **Figure 6-28** shows the Page Policy screen. **Table 6-24** describes the parameters.

Figure 6-28 Page Policy screen

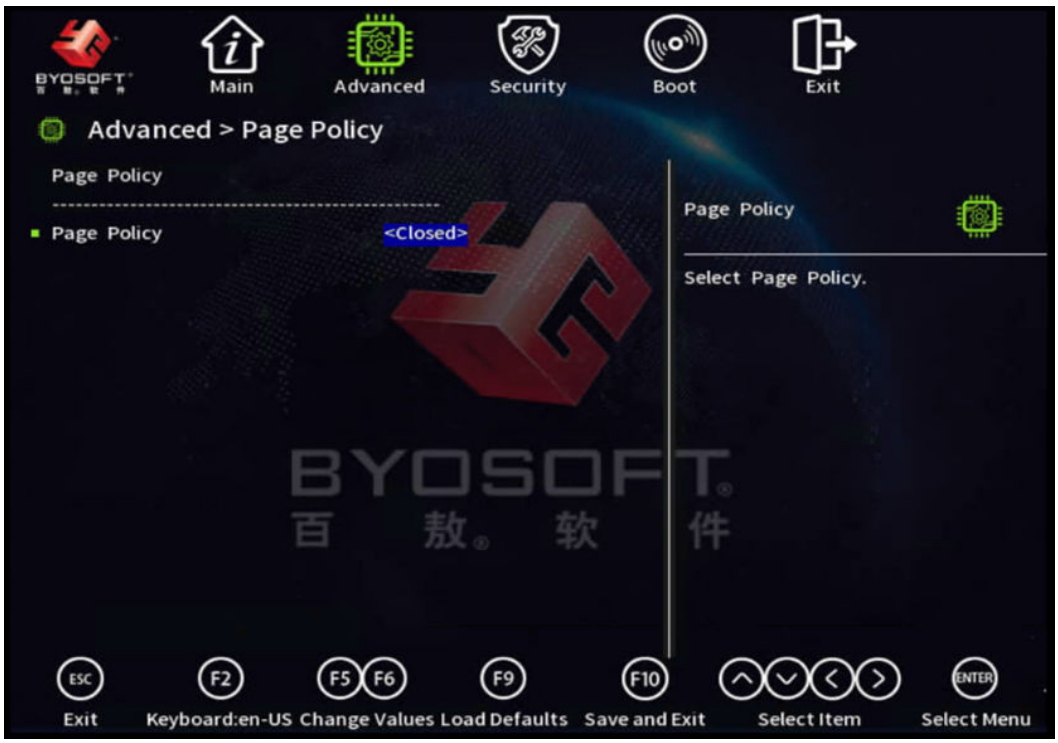


Table 6-24 Parameters on the Page Policy screen

Parameter	Description	Default Value
Page Policy	Sets the page management policy. The menu options are as follows: • **Closed**: Disables the page management policy. • **Adaptive**: Indicates the adaptive mode.	Closed

6.2.5.4.4 Memory Map

On the **Memory Map** screen, you can set the volatile memory mode and the eADR function. **Figure 6-29** shows the **Memory Map** screen. **Table 6-25** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-29 Memory Map screen

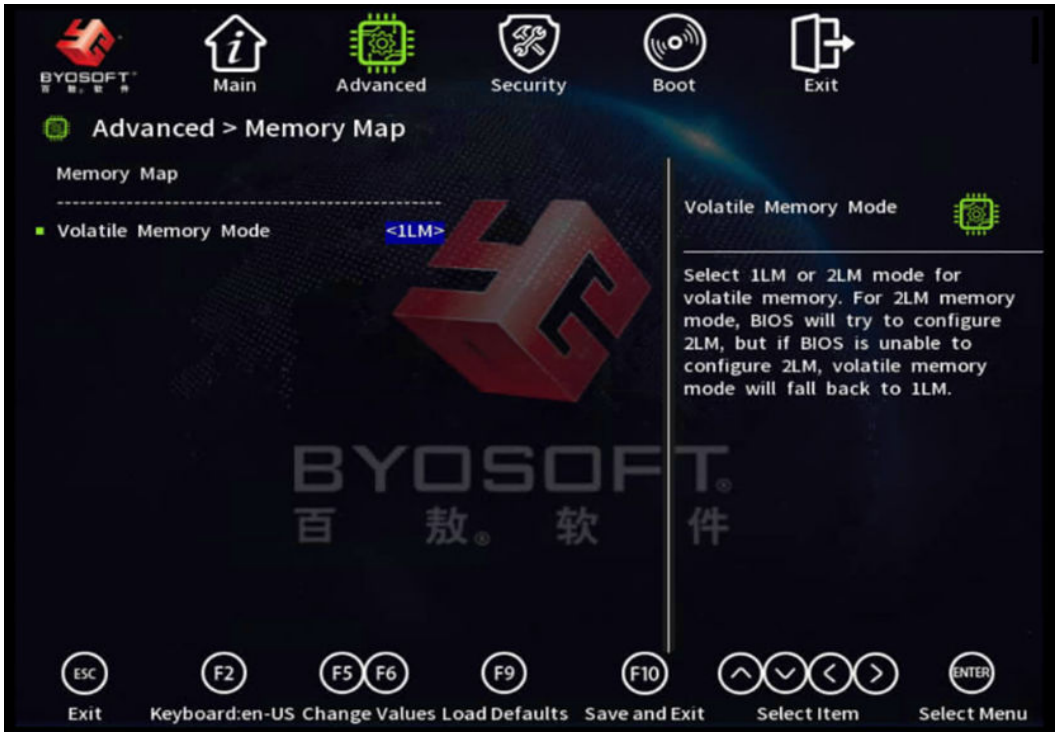


Table 6-25 Parameters on the Memory Map screen

Parameter	Description	Default Value
Volatile Memory Mode	Enables or disables the 1LM or 2LM memory mode. The menu options are as follows: ● 1LM ● 2LM **NOTE** If the CPU does not support HBM, only **1LM** is available.	1LM

6.2.5.4.5 Memory RAS Configuration

On the **Memory RAS Configuration** screen, you can set memory RAS-related functions. **Figure 6-30** shows the **Memory RAS Configuration** screen. **Table 6-26** describes the parameters.

NOTE

The parameters displayed on this screen vary depending on the memory configuration of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-30 Memory RAS Configuration screen

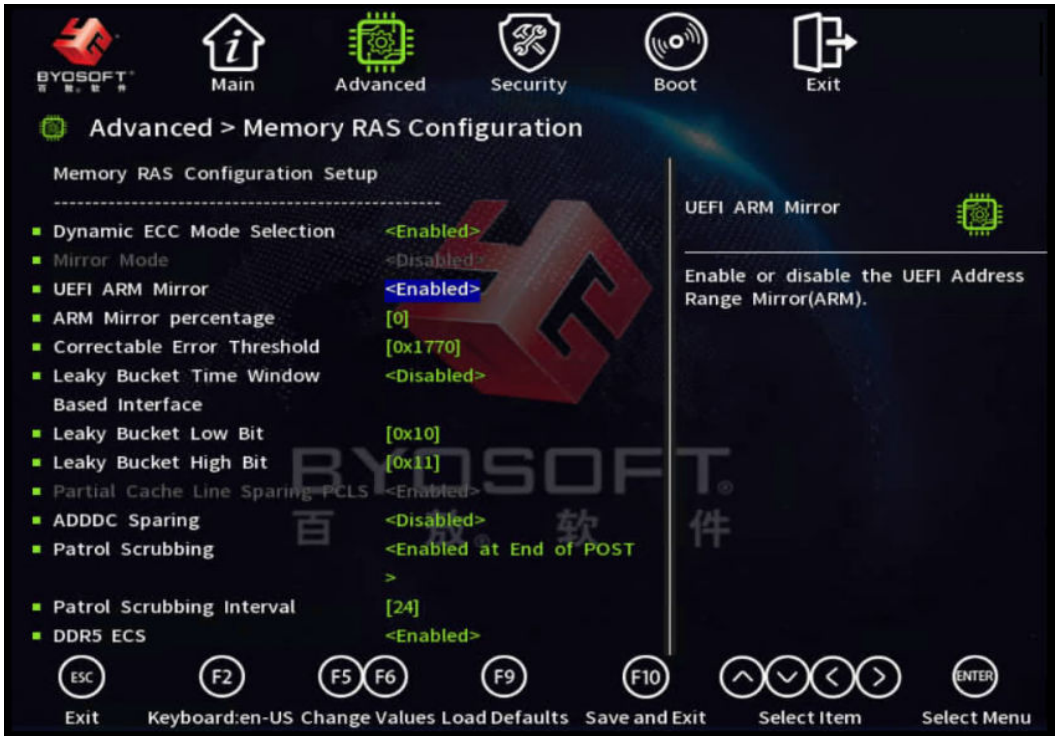


Table 6-26 Parameters on the Memory RAS Configuration screen

Parameter	Description	Default Value
Dynamic ECC Mode Selection	Sets the dynamic ECC mode. The menu options are as follows: ● Disabled ● Enabled ● Enable + Allow Partial Poison Mode	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Mirror Mode	Sets the mirroring mode. The menu options are as follows: ● **Disabled**: The mirroring mode is not set. ● **Full Mirror Mode**: Indicates the full mirroring mode. ● **Partial Mirror Mode**: Indicates the partial mirroring mode. **NOTE** ● This parameter is unavailable when DIMMs are not installed in the mirror mode. ● This parameter is unavailable when **UEFI ARM Mirror** is set to **Enabled** or **ADDDC Sparing** is set to **Enabled**.	Disabled
Partial Mirror 1 Size (GB)	Sets the unit capacity in the partial mirroring mode, in GB. The value ranges from 0 to 4095. **NOTE** This parameter is available when **Mirror Mode** is set to **Partial Mirror Mode**.	0
Mirror TAD0	Enables mirroring on the entire memory of TAD0. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is unavailable when DIMMs are not installed in the mirror mode. ● This parameter is unavailable when **Mirror Mode** is set to **Partial Mirror Mode** or **ADDDC Sparing** is set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
UEFI ARM Mirror	Enables or disables the UEFI address range mirroring. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is unavailable when DIMMs are not installed in the mirror mode. ● This parameter is available only when **ADDDC Sparing** is set to **Disabled** and **Mirror Mode** is set to **Disabled**.	Disabled
ARM Mirror percentage	Inputs the mirroring percentage. **1275** stands for 12.75%. The value ranges from 0 to 5000. **NOTE** This parameter is unavailable when **UEFI ARM Mirror** is set to **Disabled**.	0
Correctable Error Threshold	Set the correctable error threshold for sparing and leaky buckets. The value ranges from 0 to 0x7FFF.	0x1770
Leaky Bucket Time Window Based Interface	Enables or disables the leaky bucket time window-based screen. The menu options are as follows: ● Enabled ● Disabled	Disabled
Leaky Bucket Low Bit	Sets the low bits of the leaky bucket. The value ranges from 0x1 to 0x29. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Disabled**.	0x10

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Leaky Bucket High Bit	Sets the high leaky bits of the leaky bucket. The value ranges from 0x1 to 0x29. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Disabled**.	0x11
Leaky Bucket Time Window Based Interface Hour	Specifies the leaky bucket time window based on hour (0 to 3744). The value ranges from 0 to 3744. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	24
Leaky Bucket Time Window Based Interface Minute	Specifies the leaky bucket time window based on minute (0 to 60). The value ranges from 0 to 60. **NOTE** This parameter is available when **Leaky Bucket Time Window Based Interface** is set to **Enabled**.	0
Partial Cache Line Sparing PCLS	Enables or disables the partial cache line sparing (PCLS). The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
ADDDC Sparing	Enables or disables the ADDDC reservation function. If performance is preferred, it is recommended that the ADDDC reservation function be disabled. If reliability is preferred, it is recommended that X4 memory be used and the ADDDC reservation function be enabled. The menu options are as follows: ● Enabled ● Disabled **NOTE** When x8 memory is used, the ADDDC function is not supported.	Disabled
Patrol Scrubbing	Enables or disables the patrol scrubbing function. The menu options are as follows: ● Enabled at End of POST ● Disabled	Enabled at End of POST
Patrol Scrubbing Interval	Sets the time interval (in hours) for the patrol scrubbing to be performed. The value ranges from 0 to 24.	24
DDR5 ECS	Enables or disables the DDR5 error check and scrubbing (ECS) function. The menu options are as follows: ● Enabled ● Disabled	Enabled

6.2.5.4.6 PMem Configuration

On the **PMem Configuration** screen, you can set PMem-related functions. **Figure 6-31** and **Figure 6-32** show the **PMem Configuration** screen. **Table 6-27** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

Only the 2288 V7 supports this screen.

Figure 6-31 PMem Configuration screen 1

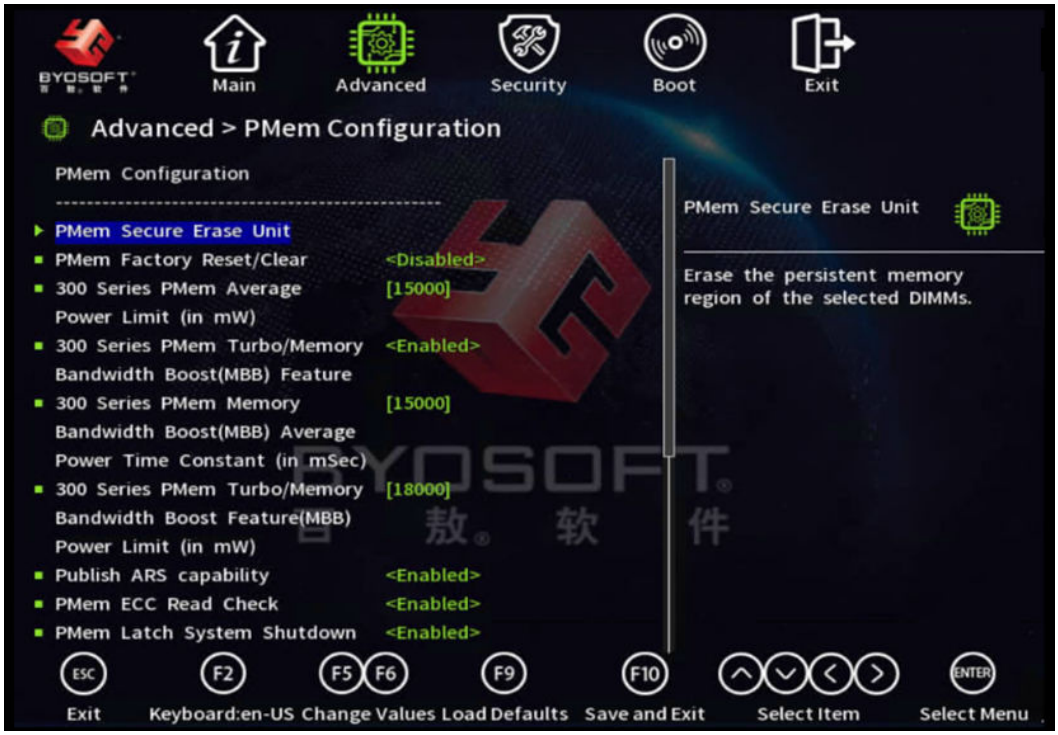


Figure 6-32 PMem Configuration screen 2

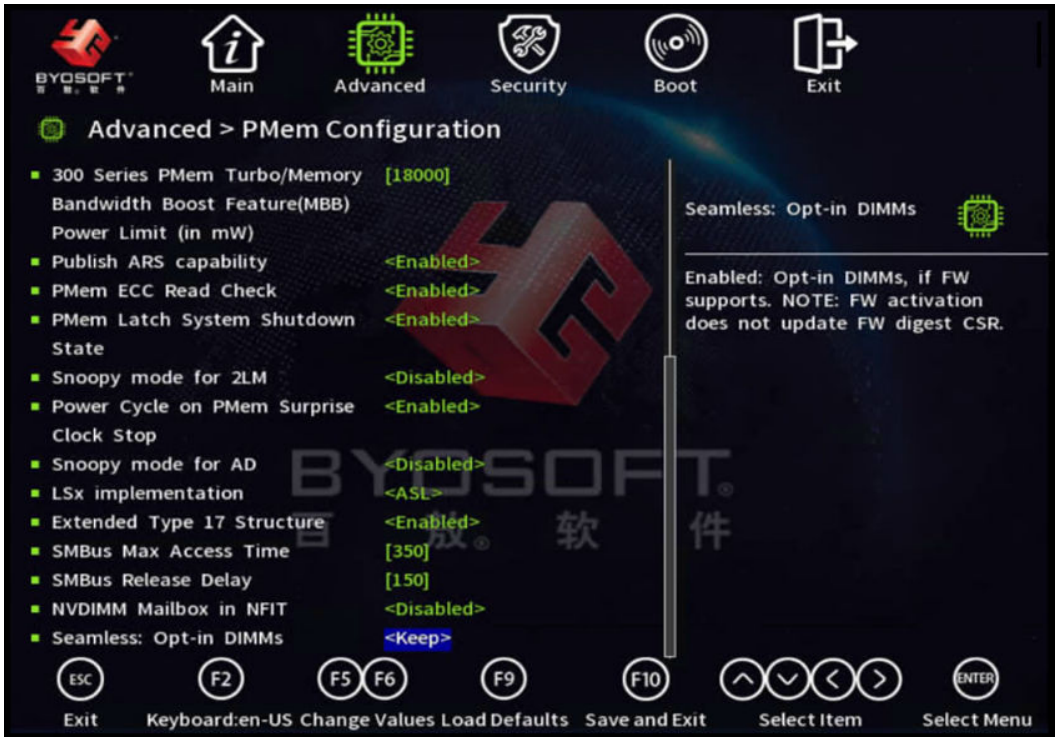


Table 6-27 Parameter on the PMem Configuration screen

Parameter	Description	Default Value
PMem Secure Erase Unit	Provides access to PMem secure erase tool settings.	-
PMem Factory Reset/ Clear	Enables or disables the PMem factory reset/clear. The menu options are as follows: ● Enabled ● Disabled	Disabled
300 Series PMem Average Power Limit (in mW)	Specifies the 300 series PMem average power limit (in mW). The power limit must be a multiple of 250 mW, which is equal to or larger than 10000 mW. The minimum value is **0**. The maximum value is **65535**.	15000
300 Series PMem Turbo/ Memory Bandwidth Boost(MBB) Feature	Enables or disables the 200 series PMem turbo/ memory bandwidth boost (MBB) function. The menu options are as follows: ● Enabled ● Disabled	Enabled
300 Series PMem Memory Bandwidth Boost(MBB) Average Power Time Constant (in mSec)	Specifies the 300 Series PMem memory bandwidth boost (MBB) average power time constant (in milliseconds). The valid range is from 1000 milliseconds to 120,000 milliseconds (which must be in an increment of 1000 milliseconds). The minimum value is **0**. The maximum value is **4294967295**.	15000

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
300 Series PMem Turbo/ Memory Bandwidth Boost Feature(MBB) Power Limit (in mW)	Specifies the 300 series PMem turbo/memory bandwidth boost (MBB) power limit (in mW). The valid range of turbo power limit starts from 15,000 mW. The minimum value is **0**. The maximum value is **65535**.	18000
Publish ARS capability	Enables or disables the public address range inspection capability for the OS. The menu options are as follows: ● Enabled ● Disabled	Enabled
PMem CMD Time	Selects the PMem command time. The menu options are as follows: ● Auto ● 1N ● 2N **NOTE** This parameter is available when the CPU model is not **Sapphire Rapids-SP** or **Emerald Rapids-SP**.	Auto
PMem ECC Read Check	Enables or disables the PMem ECC read check function. The menu options are as follows: ● Enabled ● Disabled	Enabled
PMem Latch System Shutdown State	Enables or disables the PMem latch system shutdown state function. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Snoopy mode for 2LM	Enables or disables the 2LM snoopy mode. Enabling new 2LM specific features to avoid the catalog to update from non-NUMA optimized workloads to the remote storage. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when only one CPU is configured.	Disabled
Power Cycle on PMem Surprise Clock Stop	Enables or disables the power-off restart policy when the PMem clock stops unexpectedly. The menu options are as follows: ● Enabled ● Disabled	Enabled
Snoopy mode for AD	Enables or disables the AD snoopy mode. Enabling this function to avoid the catalog to update from non-NUMA optimized workloads to the DDRT memory. The menu options are as follows: ● Enabled ● Disabled	Disabled
LSx implementation	Selects the implementation mode of LSx. The menu options are as follows: ● ASL ● SWSMI	ASL

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Extended Type 17 Structure	Enables or disables the extended Type 17 SMBIOS structure. The menu options are as follows: ● Enabled ● Disabled	Enabled
SMBus Max Access Time	Specifies the SMBus maximum access time, which is the maximum time (in milliseconds) that the UEFI mgmt driver is allowed to use the SMBus. The value ranges from 0 to 512.	350
SMBus Release Delay	Specifies the SMBus release delay, which is the release delay after the UEFI management driver accesses the SMBus. The value ranges from 0 to 512.	150
NVDIMM Mailbox in NFIT	Enables or disables the NVDIMM mailbox register released in the NFIT structure. The menu options are as follows: ● Enabled ● Disabled	Disabled
Seamless: Opt-in DIMMs	Sets the seamless selective memory opt-in policy. The menu options are as follows: ● Keep ● Enabled ● Disabled	Keep

Figure 6-33 shows the **PMem Secure Erase Unit** screen. **Table 6-28** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-33 PMem Secure Erase Unit screen

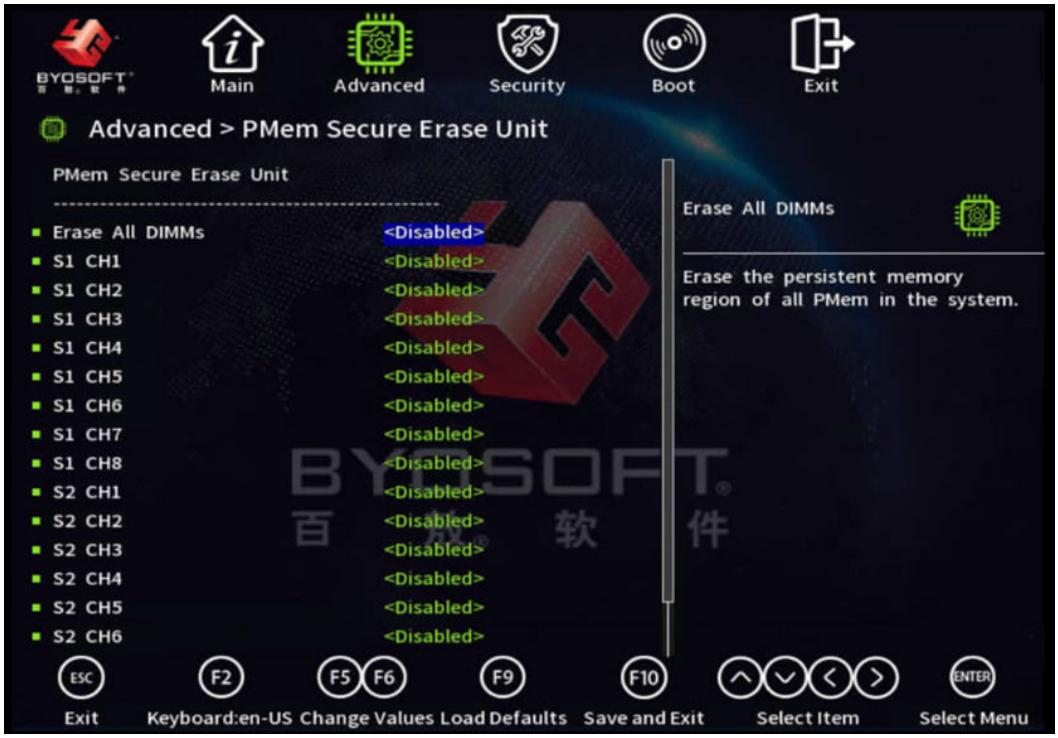


Table 6-28 Parameters on the PMem Secure Erase Unit screen

Parameter	Description	Default Value
Erase All DIMMs	Enables or disables the function of erasing the intrinsic memory area of all PMems in the system. The menu options are as follows: ● Enabled ● Disabled	Disabled
Sx CHy	Erases the intrinsic memory area of PMem on CPU *x* channel *y*. The menu options are as follows: ● Enabled ● Disabled **NOTE** *x* indicates the slot number of the CPU. *y* indicates the memory channel. The value ranges from 0 to 7.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.4.7 Memory Dfx Configuration

On the **Memory Dfx Configuration** screen, you can set memory Dfx-related functions. **Figure 6-34** shows the **Memory Dfx Configuration** screen. **Table 6-29** describes the parameters.

Figure 6-34 Memory Dfx Configuration screen

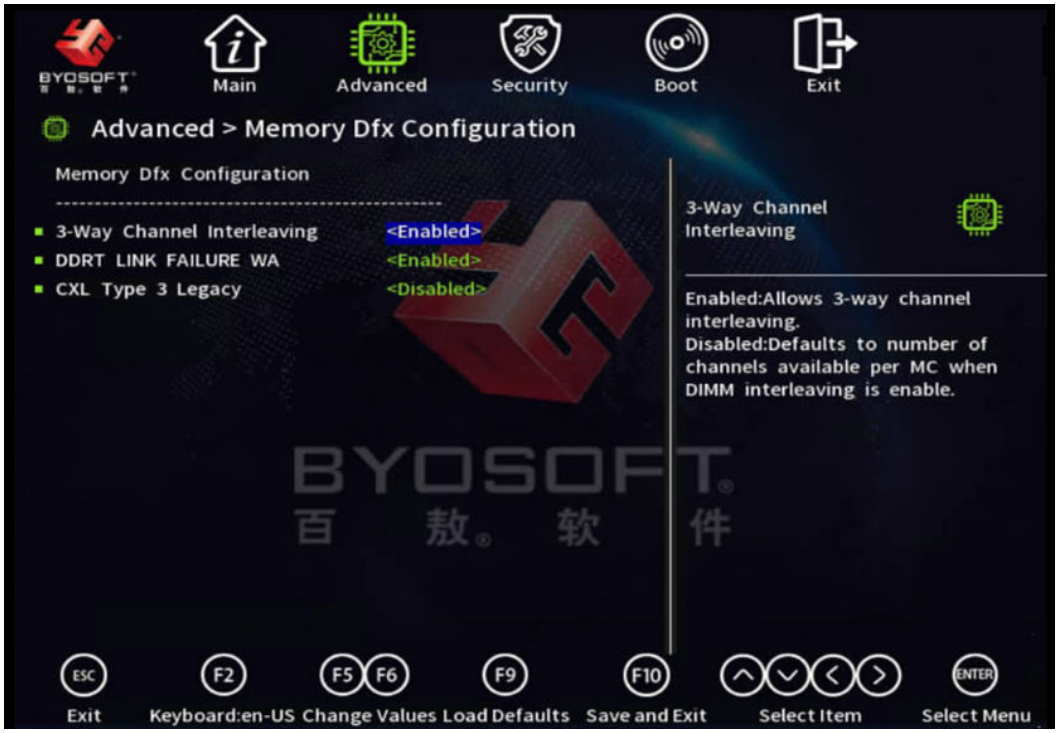


Table 6-29 Parameters on the Memory Dfx Configuration screen

Parameter	Description	Default Value
3-Way Channel Interleaving	Enables or disables the 3-way channel interleaving. The menu options are as follows: ● Enabled ● Disabled	Enabled
DDRT LINK FAILURE WA	Enables or disables the application DDRT link troubleshooting method. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CXL Type 3 Legacy	Enables or disables legacy mode for CXL3 devices. The menu options are as follows: • Enabled • Disabled	Disabled

6.2.5.4.8 BSSA Configuration Menu

On the **BSSA Configuration Menu** screen, you can configure the BSSA. **Figure 6-35** shows the **BSSA Configuration Menu** screen. **Table 6-30** describes the parameters.

Figure 6-35 BSSA Configuration Menu screen

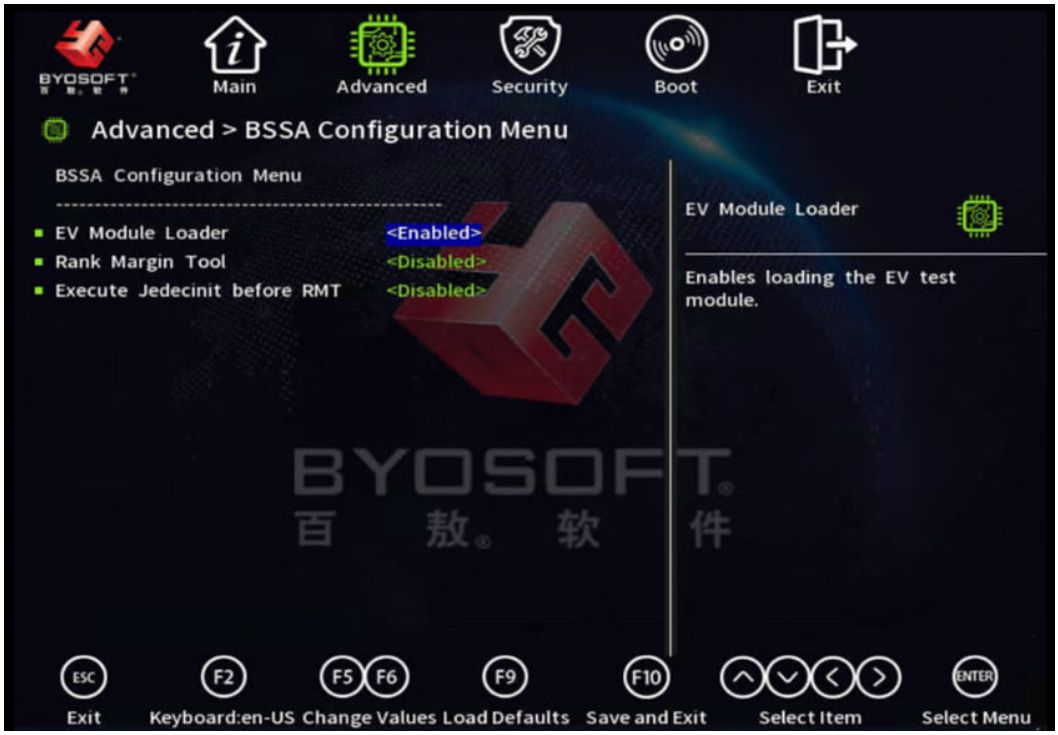


Table 6-30 Parameters on the BSSA Configuration Menu screen

Parameter	Description	Default Value
EV Module Loader	Enables or disables the EV module loader. The menu options are as follows: • Enabled • Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Rank Margin Tool	Enables or disables the rank margin tool. The menu options are as follows: ● Enabled ● Disabled	Disabled
Per CA Lane Margining	Enables or disables each CA lane margin function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **BSSA Rank Margin Tool** is set to **Enabled**.	Enabled
Scrambler	Enables or disables the scrambler during the RMT test. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **BSSA Rank Margin Tool** is set to **Enabled**.	Enabled
RMT Supress Serial Message Log	Enables or disables the RMT suppression serial message logging function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **BSSA Rank Margin Tool** is set to **Enabled**.	Enabled
Execute Jedecinit before RMT	Executes the **Jedecinit** command before the Rank Margin Tool. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.5 IIO Configuration

On the **IIO Configuration** screen, you can configure PCIe slots, including the link speed and maximum load of PCIe ports. **Figure 6-36** shows the **IIO Configuration** screen. **Table 6-31** describes the parameters.

Figure 6-36 IIO Configuration screen



Table 6-31 Parameters on the IIO Configuration screen

Parameter	Description	Default Value
Socket *X* Configuration	Provides access to CPU configurations, which is used to set the link speed, Max Payload Size, and ASPM settings of the PCIe device on CPU *X*, and to display the link status, maximum link, and current link speed of the current PCIe port. **NOTE** *X* indicates the physical slot number of the CPU. For 2288 V7, G5500 V7, and G8600 V7, the value is **1** or **2**. For 2488H V7 and 5885H V7, the value ranges from 1 to 4.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Intel(R) Virtualization for Directed I/O (VT-d)	Provides access to Intel virtualization-related configurations. Intel VT-d technology switch settings are used to improve system security and reliability and improve the performance of I/O devices in virtual environments.	-
IIO Stack IO Resource Configuration	Provides access to I/O stack and I/O resource configurations.	-
Intel(R) VMD technology	Provides access to Intel(R) VMD technology configurations. **NOTE** This parameter is available only in UEFI mode.	-
IIO DFX Configuration	Provides access to I/O DFX-related configurations.	-
IIO Global Performance Tuning	Provides access to I/O global performance adjustment configurations.	-
MultiCast Enable	Specifies whether to enable the multicast. The menu options are as follows: ● Enabled ● Disabled	Disabled
MC BaseAddress Range	Selects the MC base address range. The menu options are as follows: ● Auto ● Below_4G **NOTE** This parameter is available when **MultiCast Enable** is set to **Enabled**.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
MC Index Position	Selects the MC index position. The menu options are as follows: ● 12 ● 20 **NOTE** This parameter is available when **MultiCast Enable** is set to **Enabled**.	12
MC Num Group	Selects the MC Num group. The menu options are as follows: ● 1 ● 8 ● 32 ● 64 **NOTE** This parameter is available when **MultiCast Enable** is set to **Enabled**.	8
Skip Halt On DMI Degradation	Selects whether to skip pauses due to DMI degradation. The menu options are as follows: ● Enabled ● Disabled	Disabled
Rx Clock WA	Enables or disables the receiver clock. The menu options are as follows: ● Enabled ● Disabled	Disabled
PCI 64-Bit Resource Allocation	Enables or disables the PCI 64-bit resource allocation function. This option is automatically enabled when the server restarts when some PCIe devices that require more than 4 GB memory resources are used. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Completion Timeout	Selects whether the completion timeout is controlled by each port independently or globally. The menu options are as follows: ● Per-Port ● Global	Per-Port
PCIe Completion Timeout Value	Sets the PCIe completion timeout value. The menu options are as follows: ● 50us to 50ms ● 50us to 100us ● 1ms to 10ms ● 16ms to 55ms ● 65ms to 210ms ● 260ms to 900ms ● 1s to 3.5s ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **PCIe Completion Timeout** is set to **Per-Port**.	260ms to 900ms

6.2.5.5.1 Socket X Configuration

On the **Socket X Configuration** screen, you can configure CPU-related features. The following uses the **Socket 1 Configuration** screen as an example. **Figure 6-37** shows the **Socket 1 Configuration** screen. **Table 6-32** describes the parameters.

NOTE

The parameters on the displayed screen vary depending on the bandwidth configuration and used port of the server.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-37 Socket 1 Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-32 Parameters on the Socket 1 Configuration screen

Parameter	Description	Default Value
IOUx (IIO PCIe Port y)	Select the bandwidth of PCIe port y corresponding to IOUx. The options are as follows: ● Auto ● x4x4x4x4 ● x4x4x8 ● x8x4x4 ● x8x8 ● x16 ● x2x2x4x8 ● x4x2x2x8 ● x8x2x2x4 ● x2x2x4x4x4 ● x4x2x2x4x4 ● x4x4x2x2x4 ● x2x2x2x2x8 ● x2x2x2x2x4x4 ● x2x2x4x2x2x4 ● x4x2x2x2x2x4 ● x2x2x2x2x2x2x4 ● x8x4x2x2 ● x4x4x4x2x2 ● x8x2x2x2x2 ● x2x2x4x4x2x2 ● x4x2x2x4x2x2 ● x4x4x2x2x2x2 ● x2x2x2x2x4x2x2 ● x2x2x4x2x2x2x2 ● x4x2x2x2x2x2x2 ● x2x2x2x2x2x2x2x2	-
Port *X*	Provides access to Port *X* configurations. **NOTE** According to different server configurations, the Port configuration menu lists displayed are different. Refer to the actual situation.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

The parameters displayed on the Port *X* setting screens are the same. Port 1A is used as an example here.

Figure 6-38 shows the **Port 1A** screen. **Table 6-33** describes the parameters.

Figure 6-38 Port 1A screen



Table 6-33 Parameters on the Port 1A screen

Parameter	Description	Default Value
PCIe Port	Sets the enabling status of the PCIe port. The menu options are as follows: ● Auto ● Enabled ● Disabled	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Link Speed	Selects the link speed of the PCIe port. The menu options are as follows: ● Auto ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s) ● Gen 4 (16 GT/s) ● Gen 5 (32 GT/s)	Auto
PCIe Port DeEmphasis Level	Sets the PCIe port de-emphasis level. The menu options are as follows: ● -3.5 dB ● -6.0 dB	-3.5 dB
PCIe Port Link Status	Displays the link status of the current PCIe port.	-
PCIe Port Link Max Width	Displays the maximum bandwidth of the PCIe port link.	-
PCIe Port Link Speed	Displays the link speed of the current PCIe port.	-
PCIe Port Max Payload Size	Sets the supported maximum payload size field in the device function register of the PCIe port. The menu options are as follows: ● Auto ● 128B ● 256B ● 512B	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Completion Timeout Value	Sets the PCIe completion timeout value. The menu options are as follows: ● 50us to 50ms ● 50us to 100us ● 1ms to 10ms ● 16ms to 55ms ● 65ms to 210ms ● 260ms to 900ms ● 1s to 3.5s ● Disabled **NOTE** This parameter can be edited when **PCIe Completion Timeout** is set to **Per-Port**.	260ms to 900ms
PCIe ASPM Support	Sets the dynamic power management function of the PCIe device connected to the corresponding port. The menu options are as follows: ● **L1 Only**: Enters L1 mode only. ● **Disabled**: Disables this function. **NOTE** This parameter is available when **PCIe ASPM Support (Global)** is set to **Per Individual port** on the **Miscellaneous Configuration** screen.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

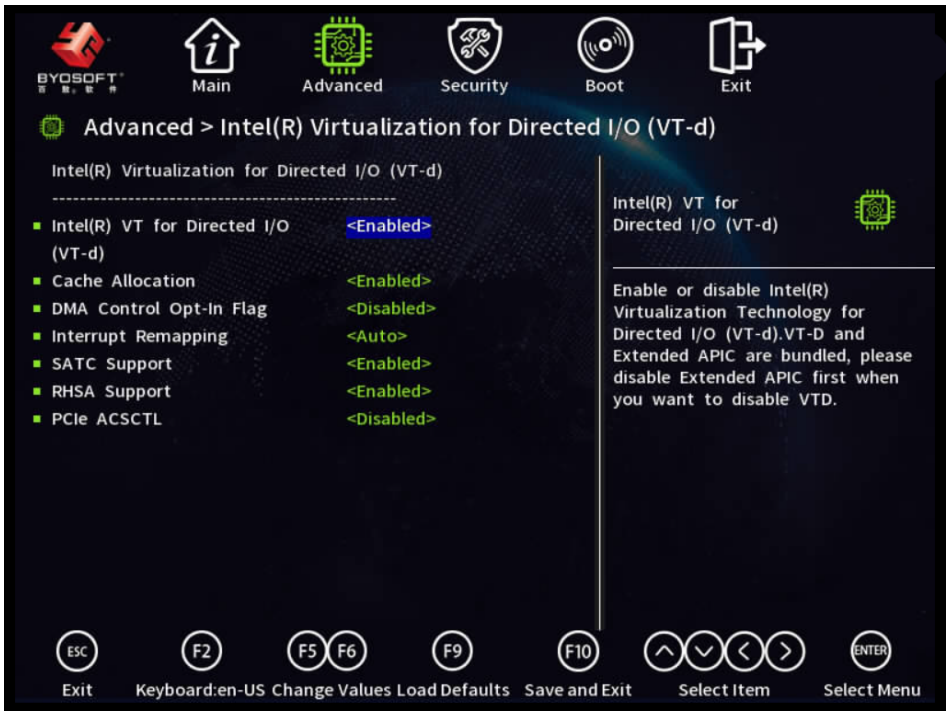
Parameter	Description	Default Value
PCIe Port L1 Exit Latency	Sets the time required for the port to complete the transition from L1 to L0. The menu options are as follows: ● <1uS ● 1uS - 2uS ● 2uS - 4uS ● 4uS - 8uS ● 8uS - 16uS ● 16uS - 32uS ● 32uS - 64uS ● >64uS **NOTE** This parameter is grayed out and cannot be edited when **PCIe ASPM Support** is set to **Disabled**.	8uS-16uS
PCIe 10-bit Tag Support	Selects the PCIe 10-bit label support. The menu options are as follows: ● Disabled ● Auto ● Force Enable	Auto
MCTP	Enables or disables the MCTP menu. The menu options are as follows: ● Enabled ● Disabled	Enabled
Equalization Bypass To Highest Rate	Enables or disables the equalization bypass to highest rate function. The menu options are as follows: ● Enabled ● Disabled	Enabled
CXL Drift Buffer	Enables or disables the CXL drift buffer. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.5.2 Intel(R) Virtualization for Directed I/O (VT-d)

On the **Intel(R) Virtualization for Directed I/O (VT-d)** screen, you can set virtualization-related parameters. **Figure 6-39** shows the **Intel(R) Virtualization for Directed I/O (VT-d)** screen. **Table 6-34** describes the parameters.

Figure 6-39 Intel(R) Virtualization for Directed I/O (VT-d) screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-34 Parameters on the Intel(R) Virtualization for Directed I/O (VT-d) screen

Parameter	Description	Default Value
Intel(R) VT for Directed I/O (VT-d)	Enables or disables Intel VT for Directed I/O (VT-d). The VT-d feature enables the virtual machine manager (VMM) to manage multiple VMs by using one physical I/O device. The menu options are as follows: ● **Enabled**: Enables the Intel VT-d feature. ● **Disabled**: Disables the Intel VT-d feature. **NOTE** ● This parameter can be set but will not take effect when **Extended APIC** is set to Enabled. ● To disable the **VT-D** parameter, you need to set **Extended APIC** to **Disabled** first.	Enabled
Cache Allocation	Enables or disables the cache allocation. The menu options are as follows: ● Enabled ● Disabled	Enabled
DMA Control Opt-In Flag	Enables or disables the DMA control opt-in flag. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **Intel(R) VT for Directed I/O (VT-d)** is set to **Disabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Interrupt Remapping	Enables or disables the interrupt remapping function. The menu options are as follows: ● Enabled ● Disabled ● Auto **NOTE** This parameter is grayed out and cannot be edited when **Intel(R) VT for Directed I/O (VT-d)** is set to **Disabled**.	Auto
SATC Support	Enables or disables the SATC support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **Intel(R) VT for Directed I/O (VT-d)** is set to **Disabled**.	Enabled
RHSA Support	Enables or disables the RHSA support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **Intel(R) VT for Directed I/O (VT-d)** is set to **Disabled**.	Enabled
PCIe ACSCTL	Enables or disables the overwrite of PCI Access Control Services Control register in PCI root ports. The menu options are as follows: ● Enabled ● Disabled	The default value of this parameter varies depending on the server model: ● G8600 V7 and G5500 V7 Disabled ● 2288 V7, 2488H V7, and 5885H V7 Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.5.3 IIO Stack IO Resource Configuration

On the **IIO Stack IO Resource Configuration** screen, you can configure IO stack IO resources. **Figure 6-40** shows the **IIO Stack IO Resource Configuration** screen. **Table 6-35** describes the parameters.

Figure 6-40 IIO Stack IO Resource Configuration screen

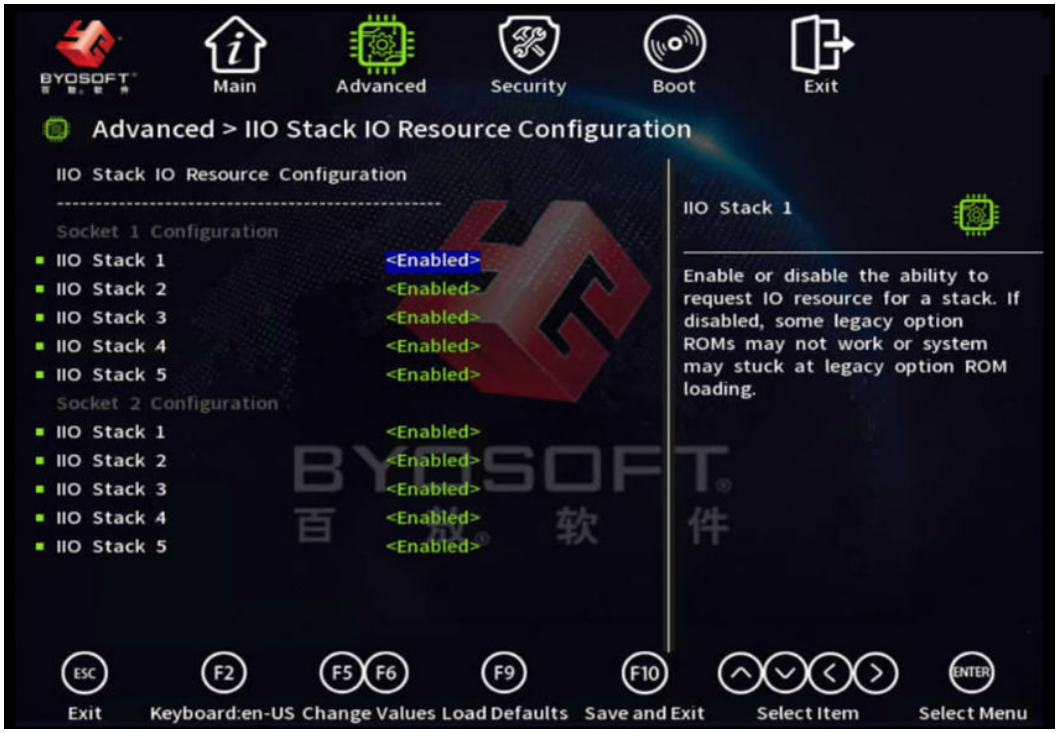


Table 6-35 Parameters on the IIO Stack IO Resource Configuration screen

Parameter	Description	Default Value
IIO Stack *X*	Enables or disables the function for the CPU stack to request I/O resources. • Enabled • Disabled **NOTE** The value of *X* ranges from 1 to 5.	Enabled

6.2.5.5.4 Intel(R) VMD technology

On the **Intel(R) VMD technology** screen, you can configure the VMD feature of the PCIe device. **Figure 6-41** shows the **Intel(R) VMD technology** screen. **Table 6-36** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-41 Intel(R) VMD technology screen



Table 6-36 Parameters on the Intel(R) VMD technology screen

Parameter	Description	Default Value
Intel(R) VMD Config	Specifies whether to enable the VMD function of the PCIe device. The menu options are as follows: • **Enabled**: Enables the VMD function of the PCIe device. • **Disabled**: Disables the VMD function of the PCIe device.	Disabled

6.2.5.5.5 IIO DFX Configuration

On the **IIO DFX Configuration** screen, you can configure the global I/O performance. **Figure 6-42** shows the **IIO DFX Configuration** screen. **Table 6-37** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-42 IIO DFX Configuration screen

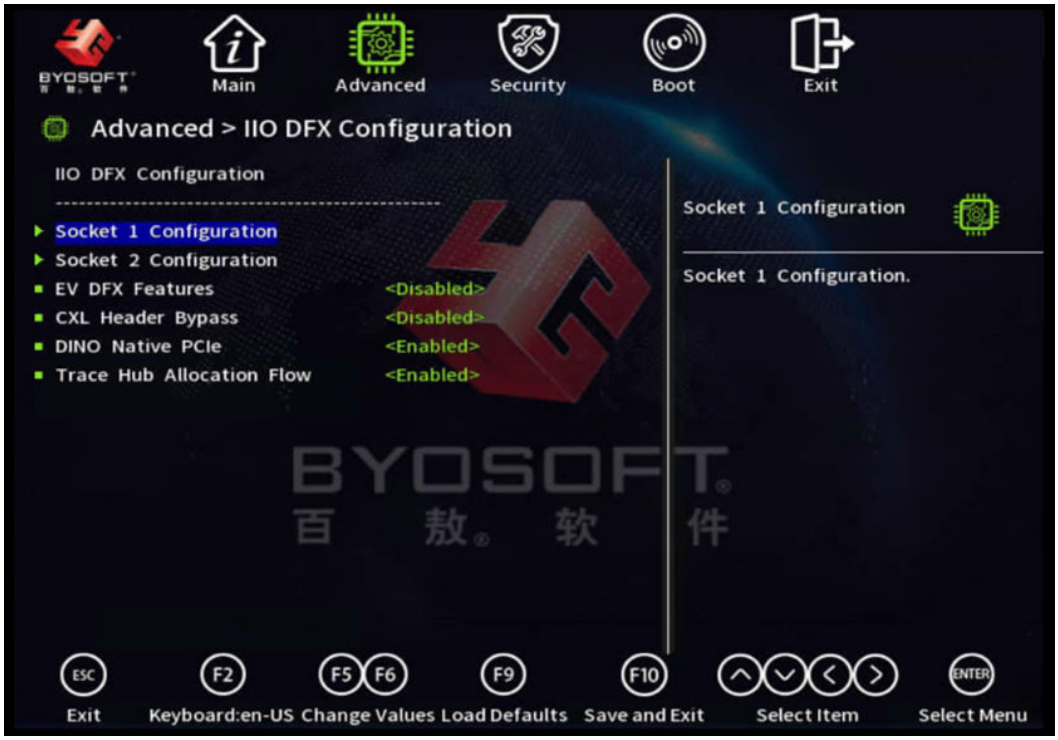


Table 6-37 Parameters on the IIO DFX Configuration screen

Parameter	Description	Default Value
Socket *X* Configuration	Provides access to Socket *X* configurations, which is used to set the link speed, Max Payload Size, and ASPM settings of the PCIe device on CPU *X*, and to display the link status, maximum link, and current link speed of the current PCIe port. **NOTE** The displayed menus are related to the number of CPUs installed on the server.	-
EV DFX Features	Enables or disables the EV DFX function. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CXL Header Bypass	Enables or disables the CXL header bypass function. The menu options are as follows: • Enabled • Disabled	Disabled
DINO Native PCIe	Enables or disables the DINO native PCIe function. The menu options are as follows: • Enabled • Disabled	Enabled
Trace Hub Allocation Flow	Enables or disables the track center allocation flow function. The menu options are as follows: • Enabled • Disabled	Enabled

Figure 6-43 shows the **Socket x Configuration** screen (the **Socket 1 Configuration** screen is used as an example). Table 6-38 describes the parameters.

Figure 6-43 Socket 1 Configuration screen



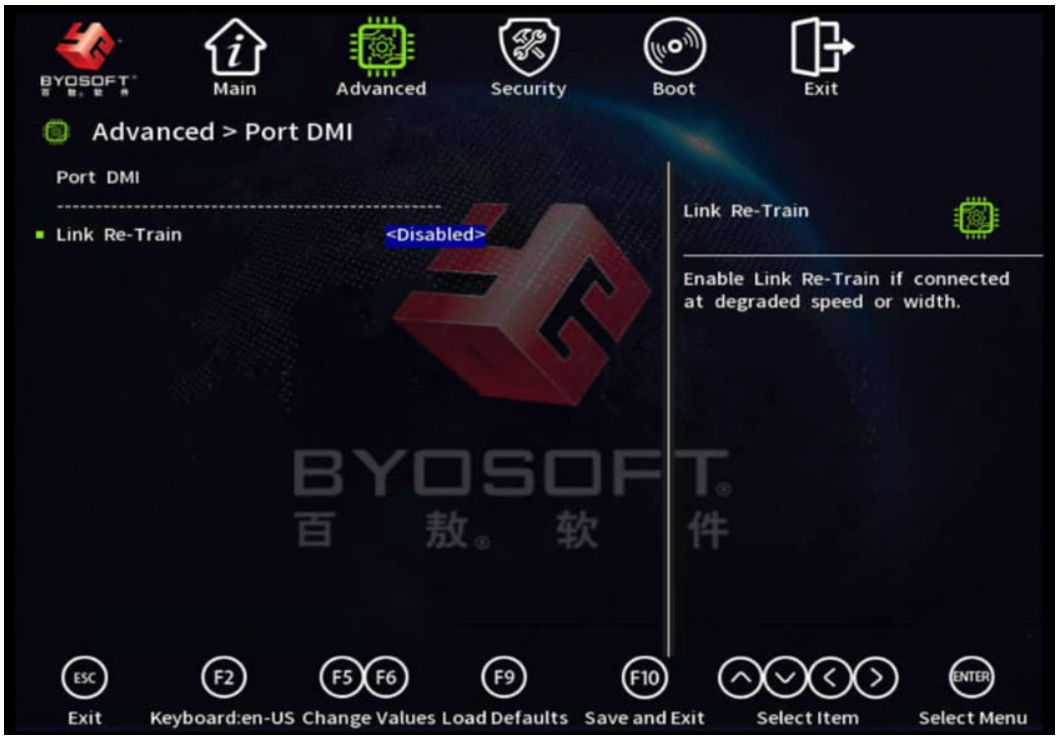
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-38 Parameters on the Socket 1 Configuration screen

Parameter	Description	Default Value
Port *X*	Provides access to Port *X* configurations. **NOTE** According to different server configurations, the Port configuration menu lists displayed are different. Refer to the actual situation.	-

Figure 6-44 shows the **Port X** screen (the **Port DMI** screen is used as an example). **Table 6-39** describes the parameters.

Figure 6-44 Port DMI screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-39 Parameters on the Port DMI screen

Parameter	Description	Default Value
Link Re-Train	Specifies the link retraining. Enable this function if the connection speed or width decreases. The menu options are as follows: • Enabled • Disabled	Disabled

6.2.5.5.6 IIO Global Performance Tuning

On the **IIO Global Performance Tuning** screen, you can configure the global I/O performance. **Figure 6-45** shows the **IIO Global Performance Tuning** screen. **Table 6-40** describes the parameters.

Figure 6-45 IIO Global Performance Tuning screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

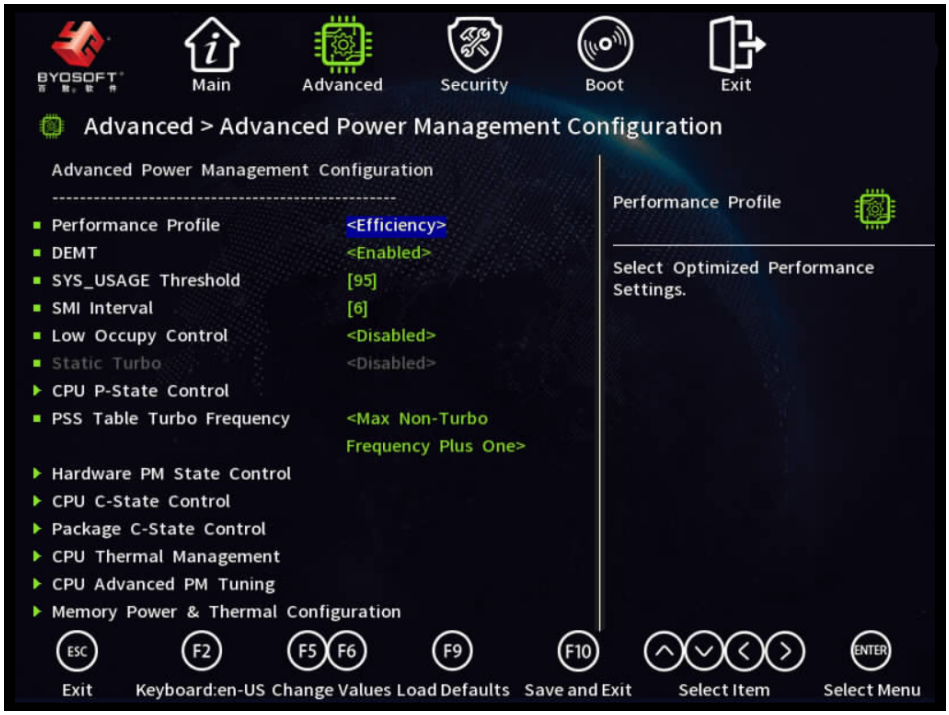
Table 6-40 Parameters on the IIO Global Performance Tuning screen

Parameter	Description	Default Value
Retimer Low Latency Mode	Selects the retimer low delay mode. The menu options are as follows: • Disabled • Enabled • 16GT/s Only • 32GT/s Only	Enabled

6.2.5.6 Advanced Power Management Configuration

On the **Advanced Power Management Configuration** screen, you can configure advanced settings for the power supply of the processor. **Figure 6-46** shows the **Advanced Power Management Configuration** screen. **Table 6-41** describes the parameters.

Figure 6-46 Advanced Power Management Configuration screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-41 Parameters on the Advanced Power Management Configuration screen

Parameter	Description	Default Value
Performance Profile	Select an energy efficiency test scenario. The menu options are as follows: ● **Custom**: Specifies the user-defined mode. ● **Efficiency**: Recommended for the high energy efficiency ratio. ● **Performance**: Performance priority. ● **Load Balance**: Power load balance. ● **High RAS**: Recommended for the high reliability mode. ● **HPC**: Recommended for high-performance computing. ● **General Computing**: Recommended for CPU general computing. ● **Low Latency**: Recommended for real-time transaction and low latency. ● **Server Side Java**: Recommended for high-performance Java on the server side. ● **Memory Throughput**: Recommended for high-performance memory. ● **I/O Throughput**: Recommended for high-performance storage. ● **Energy Saving**: Recommended for low power consumption. ● **NFV**: Recommended configuration for	Custom

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
	network function virtualization (NFV).	
DEMT	Enables or disables the dynamic energy management technology (DEMT) mode. This mode controls the processor performance and the power state based on processor workload. Enabling this option may have a negative impact on performance, depending on the workload. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**. ● This parameter is grayed out and cannot be edited when **Static Turbo** is set to **Auto** or **Manual**.	Disabled
SYS_USAGE Threshold	Sets the SYS_USAGE threshold. Controls the CPU usage that triggers frequency modulation when DEMT is enabled. **NOTE** ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled** or **DEMT** is set to **Disabled**. ● This parameter is grayed out and cannot be edited when **Static Turbo** is set to **Auto** or **Manual**.	95

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
SMI Interval	Sets the system management interrupt (SMI) interval. Controls the interval at which the BIOS monitors the CPU usage when the DEMT is enabled. **NOTE** ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled** or **DEMT** is set to **Disabled**. ● This parameter is grayed out and cannot be edited when **Static Turbo** is set to **Auto** or **Manual**.	6
Low Occupy Control	Enables or disables the low usage control function. When this function is enabled and the CPU usage is low for a long time, the DEMT function is disabled, which saves more energy. When this function is disabled, DEMT remains on. The menu options are as follows: **NOTE** ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled** or **DEMT** is set to **Disabled**. ● This parameter is grayed out and cannot be edited when **Static Turbo** is set to **Auto** or **Manual**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Static Turbo	Selects the static turbo policy to be applied by the BIOS. The menu options are as follows: ● Disabled ● **Manual**: The frequency is the selected frequency. ● **Auto**: The frequency range is from the selected frequency to the turbo frequency. **NOTE** This parameter is grayed out and cannot be edited when **DEMT** is set to **Enabled**.	Disabled
CPU Frequency Select	You need to select the frequency value between the fundamental frequency and the turbo frequency, in 100 MHz. When the input value is less than the fundamental frequency, set the value based on the fundamental frequency. When the input value is greater than the supported maximum turbo frequency, set the value based on the maximum turbo frequency. **NOTE** This parameter is available when **Static Turbo** is set to **Manual** or **Auto**.	50
PSS Table Turbo Frequency	Select the ACPI _PSS table turbo frequency. The default is the maximum non-turbo frequency plus 1MHz. ● Max Non-Turbo Frequency Plus One ● Max Turbo Frequency	Max Non-Turbo Frequency Plus One

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CPU P-State Control	Provides access to CPU P status control configurations, which controls the turbo mode and enables the Enhanced Intel SpeedStep Technology function.	-
Hardware PM State Control	Provides access to hardware PM status control configurations.	-
Frequency Prioritization	Provides access to frequency priority configurations.	-
CPU C-State Control	Provides access to the CPU C-state configurations, which allows you to control power consumption when the CPU is idle.	-
Package C-State Control	Provides access to CPU Package C state configurations. **NOTE** This menu is parameter when **Hardware P-State** is set to **Disabled** or **Out of Band Mode**.	-
CPU Thermal Management	Provides access to CPU temperature control configurations.	-
CPU Advanced PM Tuning	Provides access to CPU advanced PM adjustment configurations.	-
Memory Power & Thermal Configuration	Provides access to memory power and thermal configurations. Displays and provides options to change memory settings.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.6.1 CPU P-State Control

On the **CPU P-State Control** screen, you can configure CPU P state functions. Figure 6-47 shows the **CPU P-State Control** screen. Table 6-42 describes the parameters.

Figure 6-47 CPU P-State Control screen



Table 6-42 Parameters on the CPU P-State Control screen

Parameter	Description	Default Value
AVX License Pre-Grant Override	Enables or disables AVX ICCP pre-grant level override. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
AVX ICCP pre-grant level	Specifies the pre-grant AVX levels. The menu options are as follows: ● 128 Heavy ● 256 Light ● 256 Heavy ● 512 Light ● 512 Heavy **NOTE** This parameter is unavailable when **AVX License Pre-Grant Override** is set to **Disabled**.	128 Heavy
AVX P1	Selects the AVX P1 level. The menu options are as follows: ● Nominal ● Level 1 ● Level 2 **NOTE** This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	Nominal
Intel SST-PP	Specifies the Intel speed select technology (SST). The menu options are as follows: ● Auto ● Level 0 ● Level 3 ● Level 4 **NOTE** This parameter is not displayed in the following cases: ● The CPU feature is not supported. ● **SpeedStep (Pstates)** is set to **Disabled**. ● **AVX P1** is set to **Nominal** and **Dynamic SST-PP** is set to **Enabled**.	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Dynamic SST-PP	Enables or disables the dynamic SST-PP. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is not displayed in the following cases: ● The CPU feature is not supported. ● **SpeedStep (Pstates)** is set to **Disabled**. ● **Hardware P-State** is set to **Disabled** or **Out of Band Mode**. ● **AVX P1** is not set to **Nominal**.	Disabled
Activate SST-BF	Allows SST-BF to be enabled. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is not displayed in the following cases: ● SST-BF is not supported by all CPU models. ● **Hardware P-State** is set to **Disabled** or **Out of Band Mode**. ● **AVX P1** is not set to **Nominal**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Configure SST-BF	Allows BIOS to configure SST-BF high priority cores so that SW does not need to be configured. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is not displayed in the following cases: ● SST-BF is not supported by all CPU models. ● **Hardware P-State** is set to **Disabled** or **Out of Band Mode**. ● **AVX P1** is not set to **Nominal**. This parameter can be edited in the following cases: **Activate SST-BF** is set to **Enabled** and **Hardware P-State** is set to **Native Mode with No Legacy Support**.	Enabled
SpeedStep (Pstates)	Enables or disables EIST (P state). The menu options are as follows: ● Enabled ● Disabled **NOTE** Whether this parameter is displayed depends on the CPU feature. If the SpeedStep technology is disabled on the CPU, this parameter is unavailable.	Enabled
EIST PSD Function	Selects the PSD function. The menu options are as follows: ● HW_ALL ● SW_ALL **NOTE** This parameter cannot be edited when **SpeedStep (Pstates)** is set to **Disabled**.	HW_ALL

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Boot performance mode	Enables the boot performance mode. The menu options are as follows: ● Max Performance ● Max Efficiency ● Set by intel Node Manager **NOTE** This parameter cannot be edited when **SpeedStep (Pstates)** is set to **Disabled**.	Max Performance
Energy Efficient Turbo	Enables or disables the energy saving turbo mode. The menu options are as follows: ● Enabled ● Disabled	Enabled
Turbo Mode	Enables or disables the processor acceleration mode. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● If the CPU does not support Turbo Mode, this parameter is disabled and cannot be edited. ● This parameter is unavailable when **SpeedStep (Pstates)** is set to **Disabled**.	Enabled
CPU Flex Ratio Override	Enables or disables the CPU frequency reset function in non-Turbo mode. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
CPU Core Flex Ratio	Sets the processor core frequency in non-Turbo mode when the reset function is enabled. **NOTE** This parameter can be edited when **CPU Flex Ratio Override** is set to **Enabled**.	23

6.2.5.6.2 Hardware PM State Control

On the **Hardware PM State Control** screen, you can configure the hardware P state. Figure 6-48 shows the **Hardware PM State Control** screen. Table 6-43 describes the parameters.

Figure 6-48 Hardware PM State Control screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-43 Parameters on the Hardware PM State Control screen

Parameter	Description	Default Value
Hardware P-State	Specifies the Hardware P-State function control switch. The menu options are as follows: ● **Disabled**: Selects the P state (traditional P state) based on the OS request for the hardware. ● **Native Mode**: Specifies the local mode. The hardware PM register is directly accessed through the OS to configure the CPU. This mode supports both the traditional ACPI table and the new ACPI specifications. ● **Out of Band Mode**: Specifies the out-of-band mode. The OS cannot access the Hardware PM register and can only configure the CPU in out-of-band mode through the BMC. ● **Native Mode with No Legacy Support**: Same as Native Mode, but this mode only supports the new ACPI specifications.	Disabled
EPP Enable	Specifies the energy performance preference (EPP) control switch. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **Hardware P-State** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
EPP profile	Selects the energy preference policy. The menu options are as follows: ● **Performance**: Performance priority. ● **Balanced Performance**: Balanced performance. ● **Balanced Power**: Balanced power consumption. ● **Power**: Energy saving. **NOTE** ● This parameter is available when **Hardware P-State** is set to **Out of Band Mode**. ● This parameter is grayed out and cannot be edited when **EPP Enable** is set to **Disabled**.	Balanced Performance
Intel(R) Turbo Boost Max Technology 3.0	Enables or disables the Intel turbo boost max technology 3.0 support. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when the system supports the Intel turbo boost max technology 3.0.	Enabled

6.2.5.6.3 Frequency Prioritization

On the **Frequency Prioritization** screen, you can control the frequency priority. **Figure 6-49** shows the **Frequency Prioritization** screen. **Table 6-44** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-49 Frequency Prioritization screen



Table 6-44 Parameters on the Frequency Prioritization screen

Parameter	Description	Default Value
SST-CP	Enables or disables the SST-CP function, which will activate the per-core power budget when enabled. The menu options are as follows: • Disabled • Enabled	Disabled

6.2.5.6.4 CPU C-State Control

On the **CPU C-State Control** screen, you can configure the C state of the CPU. **Figure 6-50** shows the **CPU C-State Control** screen. **Table 6-45** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-50 CPU C-State Control screen



Table 6-45 Parameters on the CPU C-State Control screen

Parameter	Description	Default Value
Enable Monitor MWAIT	Enables or disables the Monitor/MWAIT feature. The menu options are as follows: ● Enabled ● Disabled ● Auto	Disabled
CPU C6 report	Sets the feature that reports CPU C6 (ACPI C3) to the OS. The menu options are as follows: ● Auto ● Enabled ● Disabled	Disabled
Enhanced Halt State (C1E)	Enables or disables the Enhanced Halt State (C1E) conversion function. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
C1E OS Indicator	Enables or disables the CPU global C1E indicator for the OS. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter can be edited when **Enable Monitor MWAIT** is not set to **Disabled**.	Disabled
C6 OS Indicator	Enables or disables the CPU C6 status indicator for the OS. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter can be edited when **Enable Monitor MWAIT** is set to **Enabled** and **CPU C6 report** is set to **Enabled**.	Disabled

6.2.5.6.5 Package C-State Control

On the **Package C-State Control** screen, you can configure the Package C state function of the CPU. **Figure 6-51** shows the **Package C-State Control** screen. **Table 6-46** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-51 Package C-State Control screen



Table 6-46 Parameters on the Package C-State Control screen

Parameter	Description	Default Value
Package C State	Specifies the Package C State restriction option. The menu options are as follows: ● **C0/C1 state**: Set the state to **C0/C1**. ● **C2 state**: Set the state to **C2**. ● **C6(Non-Retention State)**: Sets the state to **C6(Non-Retention State)**. ● **C6(Retention State)**: Set the state to **C6(Retention State)**. ● **No Limit**: Sets the mode to **No Limit**. ● Auto	C0/C1 state

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PC6 Persistent Memory Regulatory Test Mode	Controls PC6 persistent memory regulatory test mode. The menu options are as follows: • Disabled • Enabled	Disabled
Pkg C-state SA Power Management Control	Specifies options related to Pkg C-state SA power management control.	-

Figure 6-52 shows the **Pkg C-state SA Power Management Control** screen. Table 6-47 describes the parameters.

Figure 6-52 Pkg C-state SA Power Management Control screen

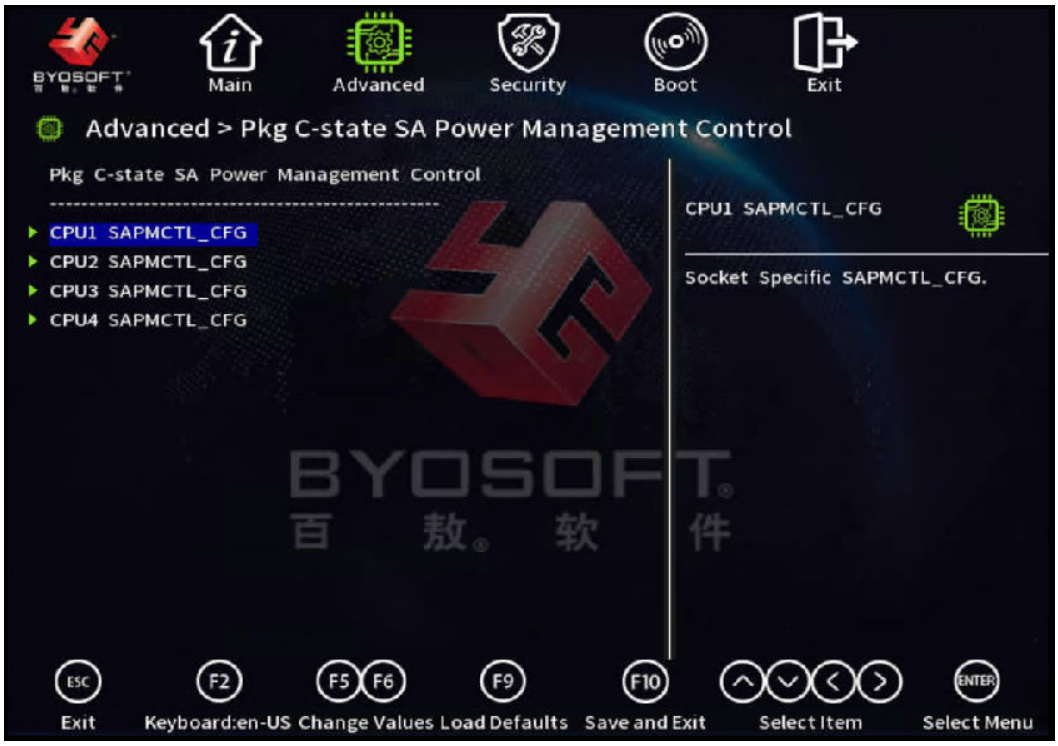


Table 6-47 Parameters on the Pkg C-state SA Power Management Control screen

Parameter	Description	Default Value
CPUx SAPMCTL_CFG	Specifies the processor-specific SAPMCTL_CFG.	-

Figure 6-53 shows the **CPU1 SAPMCTL_CFG** screen. Table 6-48 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-53 CPU1 SAPMCTL_CFG screen

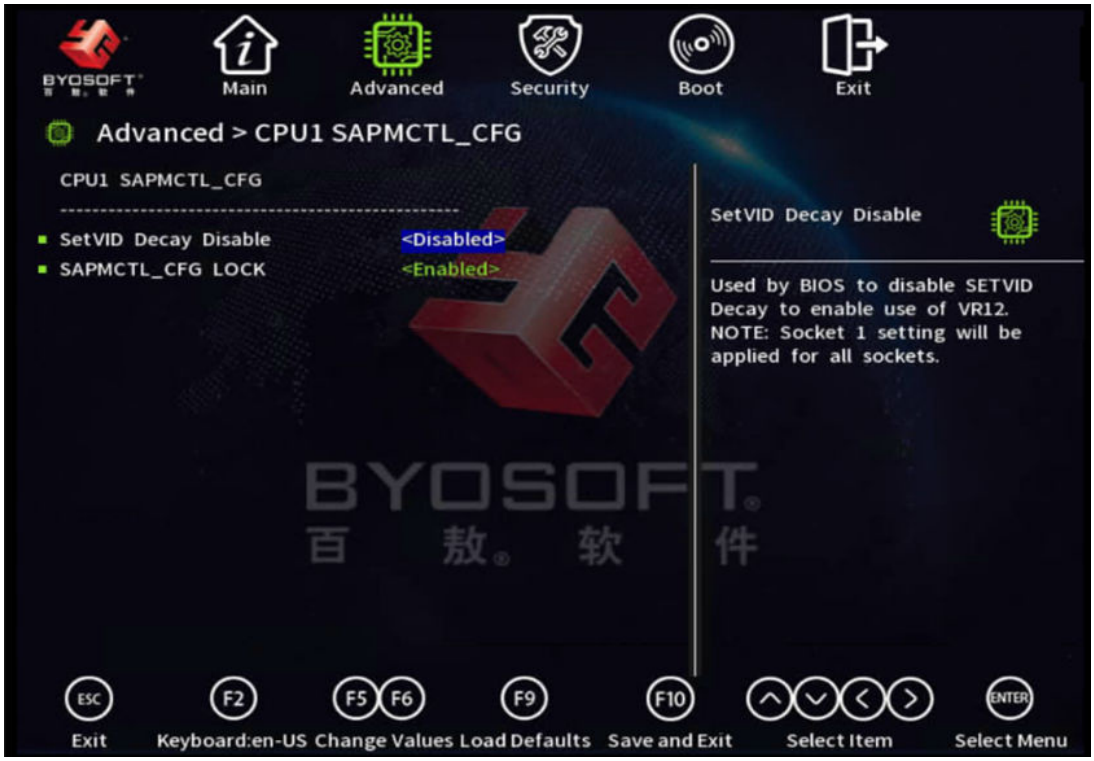


Table 6-48 Parameters on the CPU1 SAPMCTL_CFG screen

Parameter	Description	Default Value
SetVID Decay Disable	Specifies the processor-specific SAPMCTL_CFG, which is used by the BIOS to disable SETVID attenuation to enable VR12. The menu options are as follows: ● Enabled ● Disabled **NOTE** The settings for socket 1 apply to all sockets.	Disabled
SAPMCTL_CFG LOCK	Sets to lock various PM registers. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.6.6 CPU Thermal Management

On the **CPU Thermal Management** screen, you can configure the CPU temperature. Figure 6-54 shows the **CPU Thermal Management** screen. Table 6-49 describes the parameters.

Figure 6-54 CPU Thermal Management screen

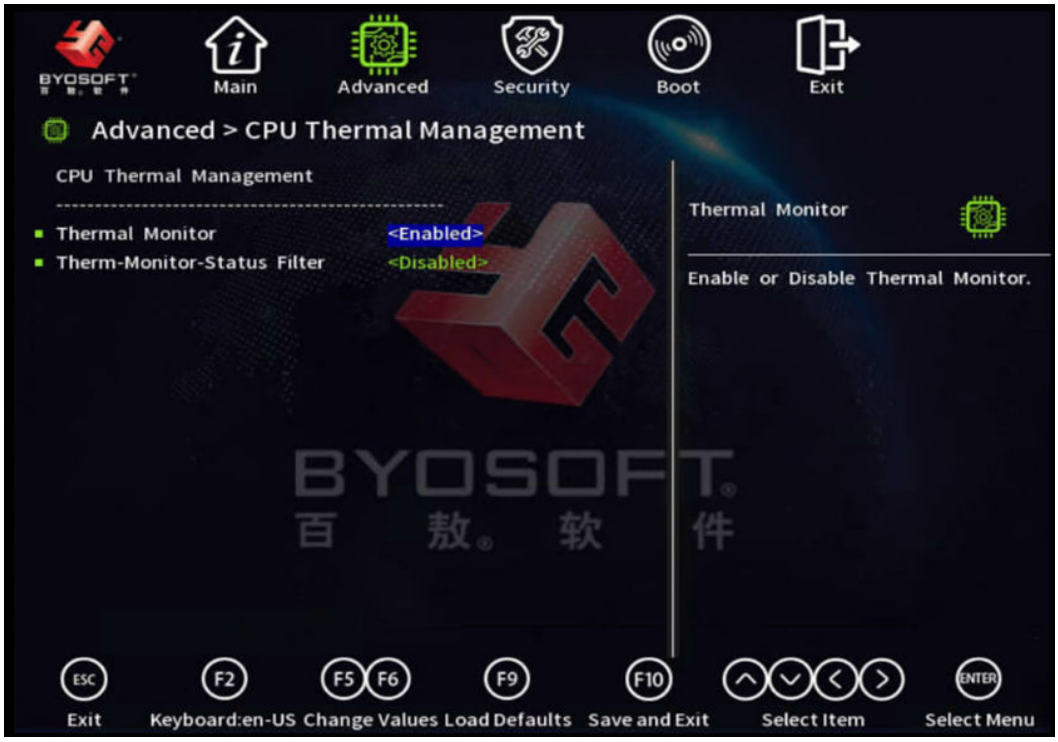


Table 6-49 Parameters on the CPU Thermal Management screen

Parameter	Description	Default Value
Thermal Monitor	Enables or disables the thermal monitor. The menu options are as follows: ● Enabled ● Disabled	Enabled
Therm-Monitor-Status Filter	Enables the **therm_monitor_status(IA32_THERM_STATUS[0])** based report of the filter. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.5.6.7 CPU Advanced PM Tuning

On the **CPU Advanced PM Tuning** screen, you can configure advanced CPU PM tuning. **Figure 6-55** shows the **CPU Advanced PM Tuning** screen. **Table 6-50** describes the parameters.

Figure 6-55 CPU Advanced PM Tuning screen

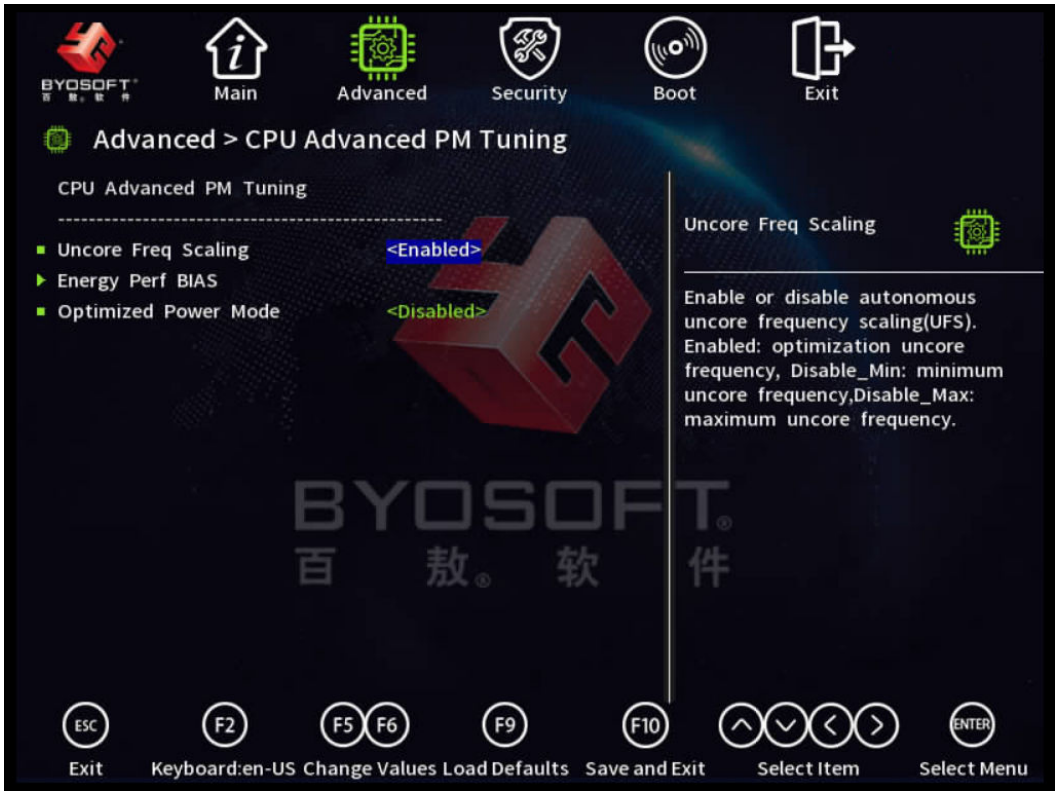


Table 6-50 Parameters on the CPU Advanced PM Tuning screen

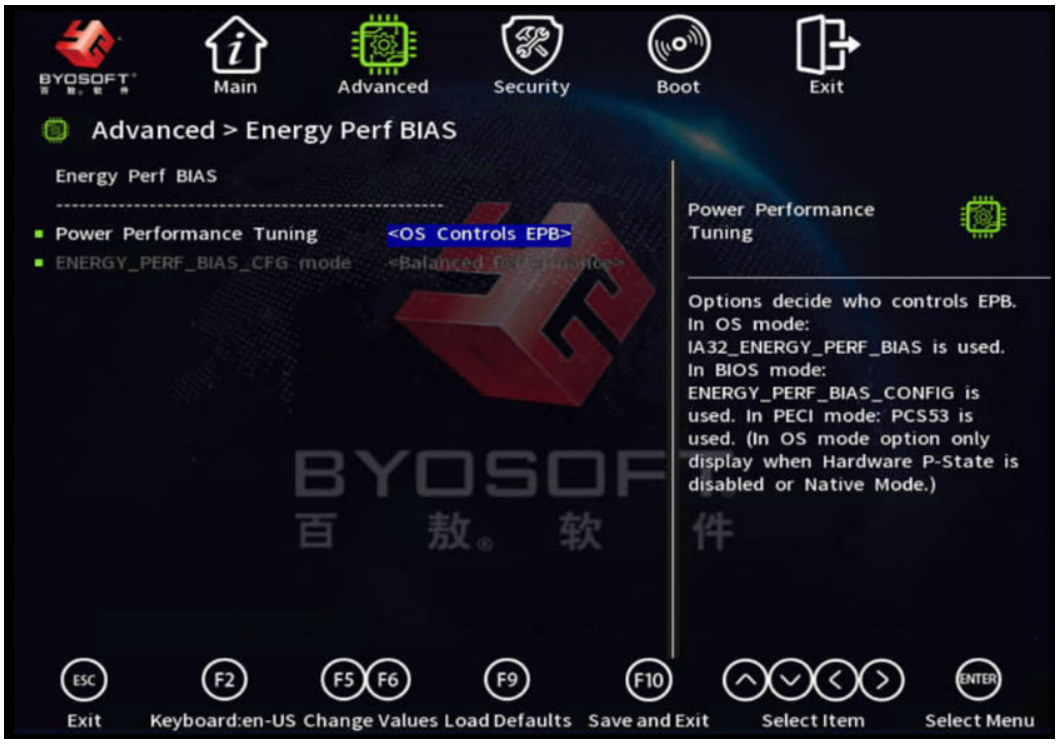
Parameter	Description	Default Value
Uncore Freq Scaling	Selects the uncore frequency scaling mode. The menu options are as follows: • Enabled • Disabled_Max • Disabled_Min	Enabled
Energy Perf BIAS	Provides access to performance bias configurations.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Optimized Power Mode	Enables or disables the optimized power mode. The menu options are as follows: ● Enabled ● Disabled	Disabled

Figure 6-56 shows the **Energy Perf BIAS** screen. Table 6-51 describes the parameters.

Figure 6-56 Energy Perf BIAS screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-51 Parameters on the Energy Perf BIAS screen

Parameter	Description	Default Value
Power Performance Tuning	Sets the power performance tuning function. The menu options are as follows: ● **OS Controls EPB**: Use IA32_ENERGY_PERF_BIAS in OS mode. ● **BIOS Controls EPB**: Uses ENERGY_PERF_BIAS_CONFIG in BIOS mode. ● **PECI Controls EPB**: PECI controls EPB. **NOTE** The **OS Controls EPB** option is hidden when **Hardware P-State** is set to **Out of Band Mode** or **Native Mode with No Legacy Support**.	OS Controls EPB

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
ENERGY_PERF_BIAS_CFG mode	Sets the ENERGY_PERF_BIAS_CONFIG mode. Configures power performance tuning. The CPU adjusts the internal operation of the processor according to the setting to meet the requirements of high performance or energy saving. This setting is available only when the energy efficiency adjustment is set to BIOS control energy efficiency policy. Selecting any one of them will overwrite the CPU performance adjustment configuration in the OS. The menu options are as follows: ● **Balanced Performance**: Balanced performance mode. ● **Performance**: Performance priority mode. ● **Balanced Power**: Balanced power mode. ● **Power**: Energy saving priority mode. **NOTE** This parameter can be configured when **Power Performance Tuning** is set to **BIOS Controls EPB**.	Balanced Performance

6.2.5.6.8 Memory Power & Thermal Configuration

On the **Memory Power & Thermal Configuration** screen, you can perform the memory power and thermal configurations. **Figure 6-57** shows the **Memory Power & Thermal Configuration** screen. **Table 6-52** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-57 Memory Power & Thermal Configuration screen

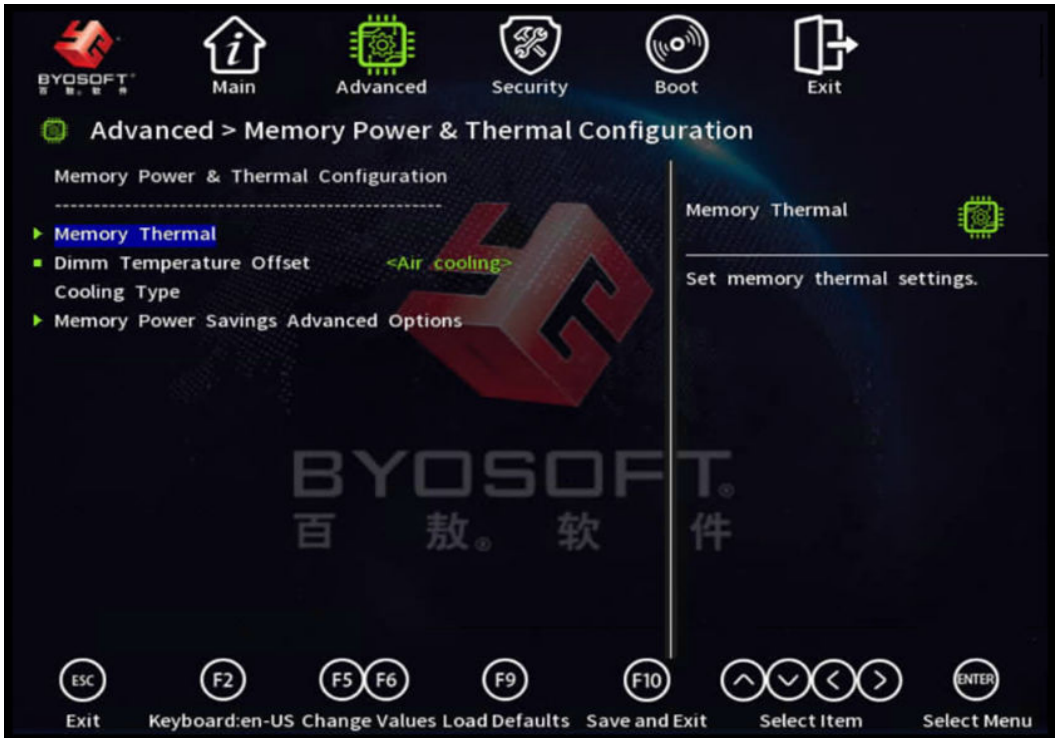


Table 6-52 Parameters on the Memory Power & Thermal Configuration screen

Parameter	Description	Default Value
Memory Thermal	Provides access to memory thermal energy configurations.	-
Dimm Temperature Offset Cooling Type	Specifies the memory temperature compensation for different cooling types. The menu options are as follows: ● Air cooling ● Liquid cooling (tube) ● Immersion cooling	Air cooling
Memory Power Savings Advanced Options	Provides access to advanced options for the memory power saving.	-

Figure 6-58 shows the **Memory Thermal** screen. Table 6-53 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-58 Memory Thermal screen



Table 6-53 Parameters on the Memory Thermal screen

Parameter	Description	Default Value
Throttling Mode	Sets the thermal energy throttling mode. The menu options are as follows: ● **Disabled**: Disables the throttling mode. ● **CLTT**: CLTT mode.	CLTT

Figure 6-59 shows the **Memory Power Savings Advanced Options** screen. **Table 6-54** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-59 Memory Power Savings Advanced Options screen

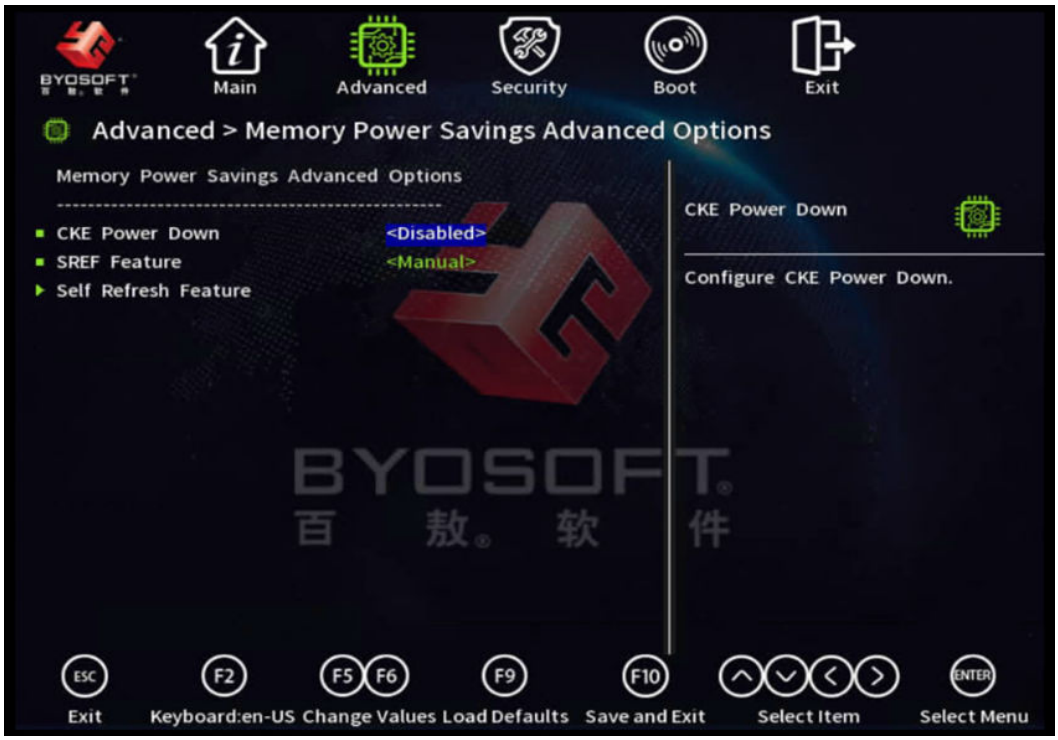


Table 6-54 Parameters on the Memory Power Savings Advanced Options screen

Parameter	Description	Default Value
CKE Power Down	Enables or disables the CKE power-down function. The menu options are as follows: ● Enabled ● Disabled	Disabled
CKE Feature	Provides access to CKE function settings. **NOTE** This parameter is available when **CKE Power Down** is set to **Enabled**.	-
SREF Feature	Sets the method for configuring the SREF feature. The menu options are as follows: ● **Auto**: Automatically configures the self-refresh function. ● **Manual**: Manually configures the self-refresh function.	Manual

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Self Refresh Feature	Provides access to self-refresh function settings. **NOTE** This parameter is available when **SREF Feature** is set to **Manual**.	-

Figure 6-60 shows the **CKE function** screen. **Table 6-55** describes the parameters.

Figure 6-60 CKE Feature screen



Table 6-55 Parameters on the CKE Feature screen

Parameter	Description	Default Value
CKE Idle Timer	Sets the CKE idle timer, in nanoseconds. The minimum value is **20**. **NOTE** This parameter is unavailable when **CKE Power Down** is set to **Disabled**.	20

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PPD	To enable or disable the pre-charge power down (PPD) function. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
	NOTE This parameter is unavailable when **CKE Power Down** is set to **Disabled**. When **CKE Power Down** is set to **Enabled**, the displayed information varies depending on the server model, as follows: ● 2288 V7 1. This option is visible for versions 01.02.02.02 and earlier, and versions 01.02.04.01 to 01.02.04.02. 2. This option is not visible for versions 01.02.04.02 and later, and this function does not take effect. ● 5885H V7 and 2488H V7 1. This option is visible for versions 01.02.02.02 and earlier. 2. This option is not visible for versions 01.02.03.03 and later, and this function does not take effect. ● G5500 V7 1. This option is available for versions prior to 01.02.03.02. 2. For versions between 01.02.03.02 and 01.02.04.03 (excluding 01.02.04.03), this option is available for SPR CPUs but not for EMR CPUs. 3. For versions 01.02.04.03 and later, this option is not available, and this function does not take effect. ● G8600 V7 1. This option is available for versions prior to 01.02.04.03. 2. For versions between 01.02.04.03 and 01.02.05.03, this option is not	

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-61 shows the **Self Refresh Feature** screen. Table 6-56 describes the parameters.

Figure 6-61 Self Refresh Feature screen



Table 6-56 Parameters on the Self Refresh Feature screen

Parameter	Description	Default Value
CK in SR	Sets the CK action during self-refresh. The menu options are as follows: • Driven • Pulled Low	Pulled Low

6.2.6 BMC Configuration

The **BMC Configuration** screen contains BMC-related information (such as BMC version and current status) and functions (such as setting the power-on policy, and configuring network and watchdog). Figure 6-62 shows the **BMC Configuration** screen. Table 6-57 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-62 BMC Configuration screen

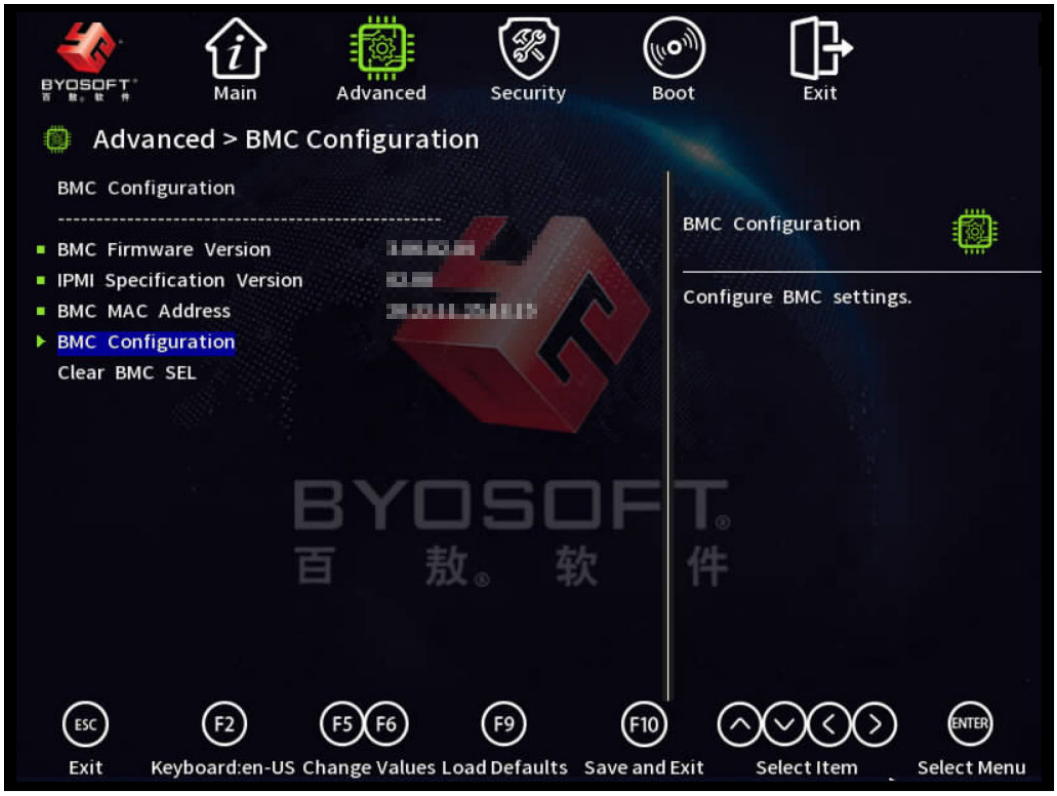


Table 6-57 Parameters on the BMC Configuration screen

Parameter	Description	Default Value
BMC Version	Displays the BMC version.	-
IPMI Specification Version	Displays the IPMI specifications version.	-
BMC MAC Address	Displays the BMC MAC address.	-
BMC Configuration	Provides access to BMC configurations.	-
Clear BMC SEL	Clears the BMC SEL.	-

6.2.6.1 BMC Configuration

On the **BMC Configuration** screen, you can configure the power-on policy, network, and watchdog. **Figure 6-63** and **Figure 6-64** show the **BMC Configuration** screen. **Table 6-58** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-63 BMC Configuration screen 1

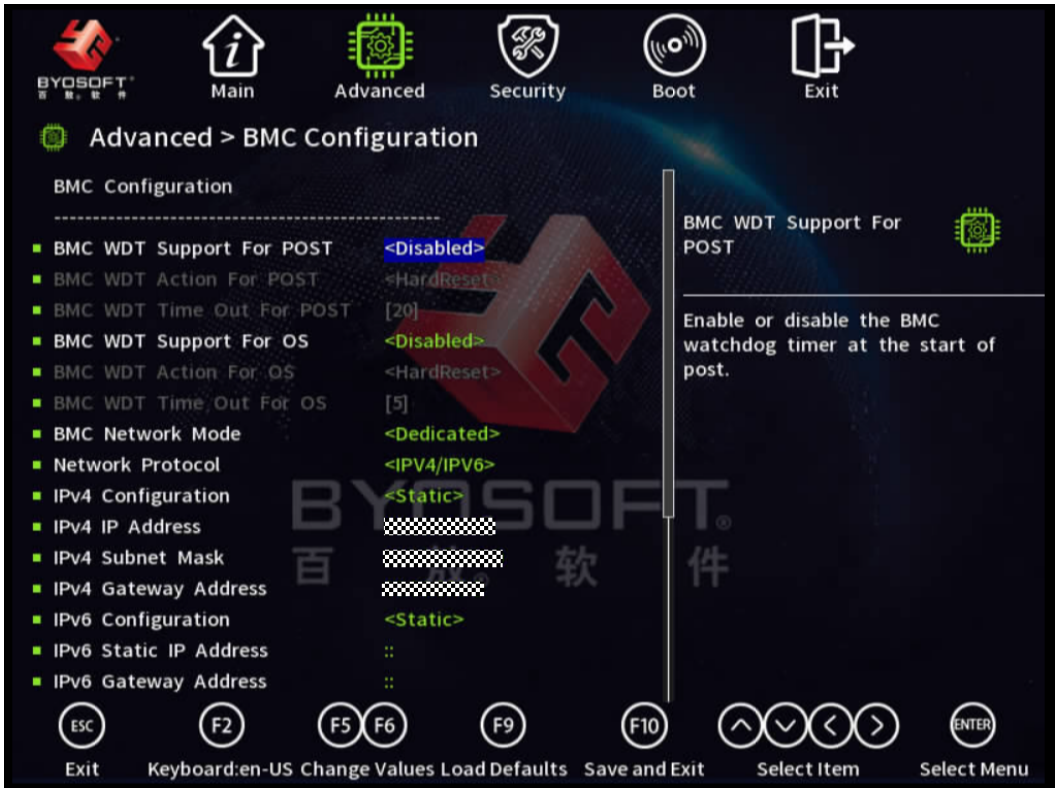
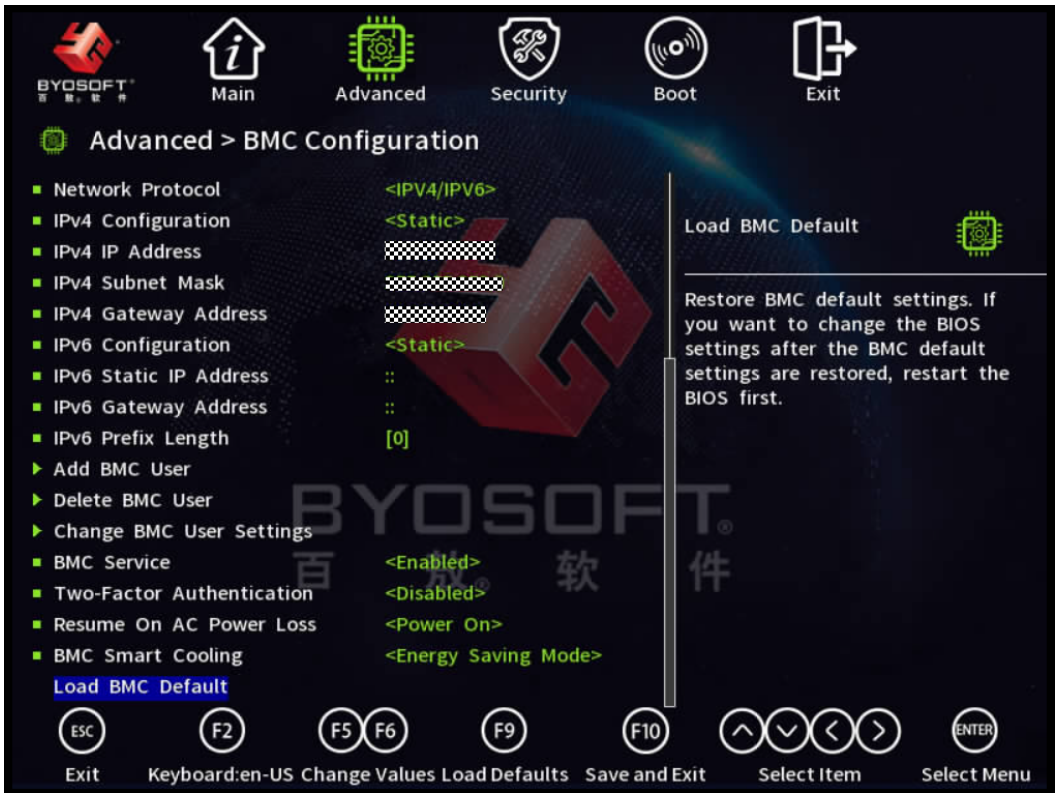


Figure 6-64 BMC Configuration screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-58 Parameters on the BMC Configuration screen

Parameter	Description	Default Value
BMC WDT Support For POST	Enables or disables the BMC watchdog for POST. The menu options are as follows: ● Enabled ● Disabled	Disabled
BMC WDT Action For POST	Sets the BMC watchdog timeout action for POST. The menu options are as follows: ● **No Action**: No operation is performed. ● **Hard Reset**: Forcibly resets. ● **Power Down**: Powers off the system. ● **Power Cycle**: Powers off and restarts the system. **NOTE** This parameter can be configured when **BMC WDT Support For POST** is set to **Enabled**.	Hard Reset
BMC WDT Time Out For POST	Sets the BMC watchdog timeout interval for POST, in minutes. The value ranges from 18 to 25. **NOTE** This parameter can be configured when **BMC WDT Support For POST** is set to **Enabled**.	20
BMC WDT Support For OS	Enables or disables the BMC watchdog for OS. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC WDT Action For OS	Sets the BMC watchdog timeout action for OS. The menu options are as follows: ● **No Action**: No operation is performed. ● **Hard Reset**: Forcibly resets. ● **Power Down**: Powers off the system. ● **Power Cycle**: Powers off and restarts the system. **NOTE** This parameter can be configured when **BMC WDT Support For OS** is set to **Enabled**.	Hard Reset
BMC WDT Time Out For OS	Sets the BMC watchdog timeout interval for OS, in minutes. The value ranges from 2 to 8. **NOTE** This parameter can be configured when **BMC WDT Support For OS** is set to **Enabled**.	5

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC Network Mode	Sets the working mode of the BMC network port. The menu options are as follows: ● **Dedicated**: Dedicated mode. You can access the BMC only through the management network port. ● **Auto**: Adaptive mode. The BMC can be accessed through the management network port or the service network port of the server. ● **PCIe Shared**: PCIe NIC sharing mode. You can access the BMC only through the network port of the PCIe NIC. ● **Onboard Shared**: OCP NIC sharing mode. You can access the BMC only through the network port of the OCP NIC. **NOTE** For details about how to set G5500 V7 parameters, see **Step 5**.	Dedicated
Vlan Id	Specifies the VLAN ID. The value can be **0** (disabling the VLAN) or from 1 to 4094 (enabling the VLAN). **NOTE** This parameter is available when **BMC Network Mode** is set to **PCIe Shared**, **Onboard OCP Shared**, or **Auto**.	0

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
NCSI NIC Port Select	Sets the NCSI network port of the NIC to be used. The menu options are as follows: ● Port1 ● Port2 ● Port3 ● Port4 **NOTE** ● This parameter is available when **BMC Network Mode** is set to **PCIe Shared**. ● The value of this parameter varies depending on the NIC configuration.	Port1
NCSI OCP Port Select	Sets the NCSI network port of the OCP NIC to be used. The menu options are as follows: ● Port1 ● Port2 **NOTE** ● This parameter is available when **BMC Network Mode** is set to **Onboard OCP Shared**. ● The value of this parameter varies depending on the NIC configuration.	Port1
Network Protocol	Enables or disables the IPv4/IPv6 Internet protocol support. The menu options are as follows: ● IPV4 ● IPV6 ● IPV4/IPV6	**NOTE** The default value of this parameter depends on the BMC policy.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPv4 Configuration	Sets the IPv4 configuration mode. The menu options are as follows: ● Static ● DHCP **NOTE** ● **IPv4 IP Address**, **IPv4 Subnet Mask**, **IPv4 Gateway Address** are grayed out and cannot be edited when this parameter is set to **DHCP**. ● This option is hidden when **Network Protocol** is set to **IPV6**.	Static
IPv4 IP Address	When IPv4 configuration mode is set to a static address, you can set this parameter for an IPv4 IP address. When the IPv4 configuration mode is set to the dynamic configuration, the automatically assigned IPv4 IP address is displayed. **NOTE** ● The IP address cannot be all zeros or empty. ● This option is hidden when **Network Protocol** is set to **IPV6**.	-
IPv4 Subnet Mask	When the IPv4 configuration mode is a static address, you can set this parameter for an IPv4 IP mask. When the IPv4 configuration mode is set to the dynamic configuration, the current IPv4 IP mask is displayed. **NOTE** This option is hidden when **Network Protocol** is set to **IPV6**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPv4 Gateway Address	When the IPv4 configuration mode is a static address, you can set this parameter for an IPv4 IP gateway. When the IPv4 configuration mode is set to the dynamic configuration, the current default IPv4 IP gateway is displayed. **NOTE** ● The gateway cannot be set to all **0** or empty. ● This option is hidden when **Network Protocol** is set to **IPV6**.	-
IPv6 Configuration	Sets the IPv6 configuration mode. The menu options are as follows: ● Static ● DHCP **NOTE** ● **IPv6 Static IP Address**, **IPv6 Gateway Address**, **IPv6 Prefix Length** are grayed out and cannot be edited when this parameter is set to **DHCP**. ● This option is hidden when **Network Protocol** is set to **IPV4**.	DHCP
IPv6 Static IP Address	When IPv6 configuration mode is set to a static address, you can set this parameter for an IPv6 IP address. When the IPv6 configuration mode is set to the dynamic configuration, the automatically assigned IPv6 IP address is displayed. **NOTE** This option is hidden when **Network Protocol** is set to **IPV4**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPv6 Gateway Address	When the IPv6 configuration mode is a static address, you can set this parameter for an IPv6 IP gateway. When the IPv6 configuration mode is set to the dynamic configuration, the current default IPv6 IP gateway is displayed. **NOTE** This option is hidden when **Network Protocol** is set to **IPV4**.	-
IPv6 Prefix Length	When IPv6 configuration mode is set to a static address, you can set this parameter for the IPv6 prefix length. When the IPv6 configuration mode is set to the dynamic configuration, the current IPv6 prefix length is displayed. **NOTE** This option is hidden when **Network Protocol** is set to **IPV4**.	-
Add BMC User	Adds the BMC user.	-
Delete BMC User	Deletes the BMC user.	-
Change BMC User Settings	Changes the BMC user settings.	-
BMC Service	Enables or disables the BMC SSH service. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Two-Factor Authentication	Enables or disables the two-factor authentication function. After this function is enabled, all CLI interfaces of the BMC cannot be used. You can only log in to the BMC WebUI. A menu under the BIOS is added to enable and disable the function in emergency situations. The menu options are as follows: ● Enabled ● Disabled	Disabled
Resume On AC Power Loss	Sets the power-on policy. The menu options are as follows: ● **Power Off**: After being powered on, the PSU of the server keeps the state entered before the power-off. If the server OS is started before the power-off, it automatically powers on after the power supply is connected. If the server OS is shut down before the power-off, it will not be started after the power supply is connected. ● **Last State**: The OS is not powered on after the PSU of the server is powered on. ● **Power On**: The OS automatically starts after the PSU of the server is powered on.	Power Off **NOTE** The default value of this parameter depends on the BMC policy.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC Smart Cooling	Sets the BMC speed adjustment mode. The menu options are as follows: ● **Energy Saving Mode**: Evaluates the current load and heat dissipation of the system and controls the fan speed at a balanced point to minimize the system power consumption. ● **Low Noise Mode**: Minimizes the fan speed and reduces the noise while the heat dissipation requirements are met. ● **High Performance Mode**: Increases the fan speed to ensure the heat dissipation capability of key components and keep low the temperature to maximize the overall performance of the server system. ● **Custom Mode**: Provides a custom interface. You can set the target CPU temperature, target speed adjustment temperature at air outlets, and fan speed corresponding to each temperature areas of air intakes.	Energy Saving Mode
CPU Temp. Threshold	Sets the target CPU temperature. The value ranges from 50 to *xx*. **NOTE** This parameter is available when **BMC Smart Cooling** is set to **Custom Mode**.	- **NOTE** Displays the current BMC settings.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Fan Speed Rate *X*	Configures the fan speed rate. The value ranges from 20 to 100. **NOTE** ● This parameter is available when **BMC Smart Cooling** is set to **Custom Mode**.	- **NOTE** The default value of this parameter depends on the BMC policy.
Load BMC Default	Restores the BMC IP address, user name, and password.	-

6.2.6.1.1 Add BMC User

On the **Add BMC User** screen, you can add a BMC user. **Figure 6-65** shows the **Add BMC User** screen. **Table 6-59** describes the parameters.

Figure 6-65 Add BMC User screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-59 Parameters on the Add BMC User screen

Parameter	Description	Default Value
BMC User ID	Sets the BMC user ID. The value ranges from 2 to 17.	-
BMC User Name	Sets the BMC user name. **NOTE** ● The username contains 1 to 16 characters. ● The value can contain letters, digits, and special characters. ● The value cannot start with a number sign (#), plus sign (+), or hyphen (-). ● The value cannot contain spaces or the following special characters: :<>&, '"/\%	-

BMC User Password	Sets the BMC user password.
	NOTE
	The password complexity requirements are as follows:
	● Contain 8 to 20 characters.
	● Contain at least two types of the following characters:
	  ● Uppercase letters A to Z
	  ● Lowercase letters a to z
	  ● Digits 0 to 9
	● Contain at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/?
	● Cannot be the same as the username or the username in reverse order.
		-

BMC User Status	Sets the BMC user state.	Enabled

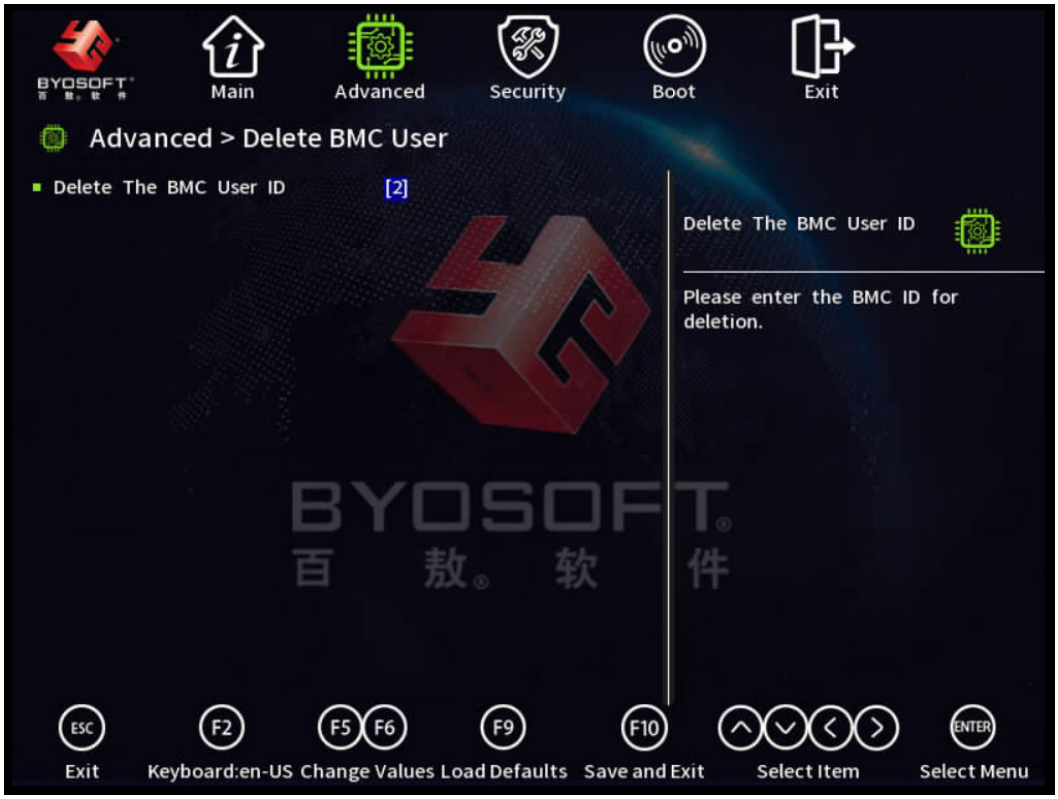
 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC User Rights	Sets the BMC user rights. The menu options are as follows: • **Administrator**: Specifies the administrator. • **Operator**: Specifies the operator. • **Common User**: Specifies the common user. • **No Access**: Specifies that the BMC is not accessible.	Administrator
Save	Saves the BMC user settings.	-

6.2.6.1.2 Delete BMC User

On the **Delete BMC User** screen, you can delete a BMC user. **Figure 6-66** shows the **Delete BMC User** screen. **Table 6-60** describes the parameters.

Figure 6-66 Delete BMC User screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-60 Parameters on the Delete BMC User screen

Parameter	Description	Default Value
Delete The BMC User ID	Enters the BMC user ID to be deleted.	-

6.2.6.1.3 Change BMC User Settings

On the **Change BMC User Settings** screen, you can modify the BMC user settings. **Figure 6-67** shows the **Change BMC User Settings** screen. **Table 6-61** describes the parameters.

Figure 6-67 Change BMC User Settings screen

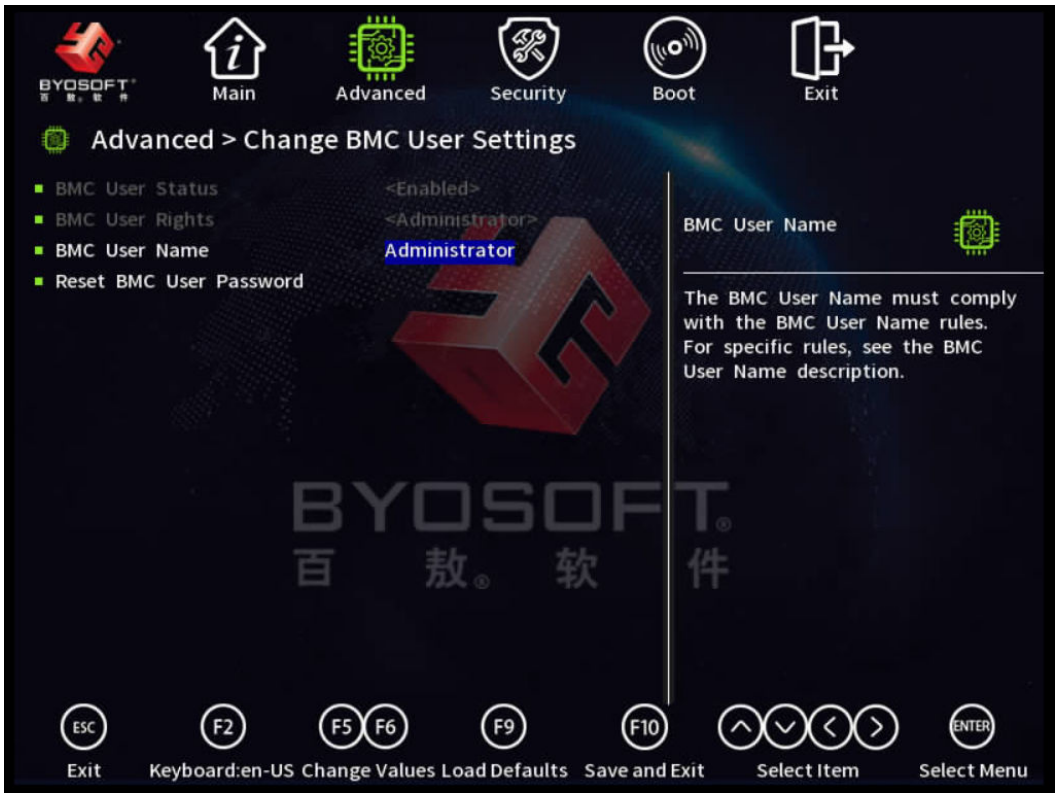


Table 6-61 Parameters on the Change BMC User Settings screen

Parameter	Description	Default Value
BMC User Status	Sets the BMC user state when **UserID** is set to **2**. **NOTE** This parameter cannot be configured when there is only one user.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BMC User Rights	Sets the BMC user rights when **UserID** is set to **2**. The menu options are as follows: ● **Administrator**: Specifies the administrator. ● **Operator**: Specifies the operator. ● **Common User**: Specifies the common user. ● **No Access**: Specifies that the BMC is not accessible. **NOTE** This parameter cannot be configured when there is only one user.	Administrator
BMC User Name	Displays or modifies the BMC user name when **UserID** is set to **2**. **NOTE** ● The username contains 1 to 16 characters. ● The value can contain letters, digits, and special characters. ● The value cannot start with a number sign (#), plus sign (+), or hyphen (-). ● The value cannot contain spaces or the following special characters: :<>&, '"/\%	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Reset BMC User Password	Modifies the BMC user password when **UserID** is set to **2**. **NOTE** The password complexity requirements are as follows: ● Contain 8 to 20 characters. ● Contain at least two types of the following characters: ● Uppercase letters A to Z ● Lowercase letters a to z ● Digits 0 to 9 ● Contain at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? ● Cannot be the same as the username or the username in reverse order.	-

6.2.7 PCH-IO Configuration

On the **PCH-IO Configuration** screen, you can configure PCI Express, SATA and USB functions. **Figure 6-68** shows the **PCH-IO Configuration** screen. **Table 6-62** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-68 PCH-IO Configuration screen



Table 6-62 Parameters on the PCH-IO Configuration screen

Parameter	Description
PCI Express Configuration	Provides access to PCI Express configurations.
SATA And RST Configuration	Provides access to SATA and RST configurations.
USB Configuration	Provides access to USB configurations.

6.2.7.1 PCI Express Configuration

On the **PCI Express Configuration** screen, you can independently configure each of the 16 PCI Express root ports. **Figure 6-69** shows the **PCI Express Configuration** screen. **Table 6-63** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-69 PCI Express Configuration screen

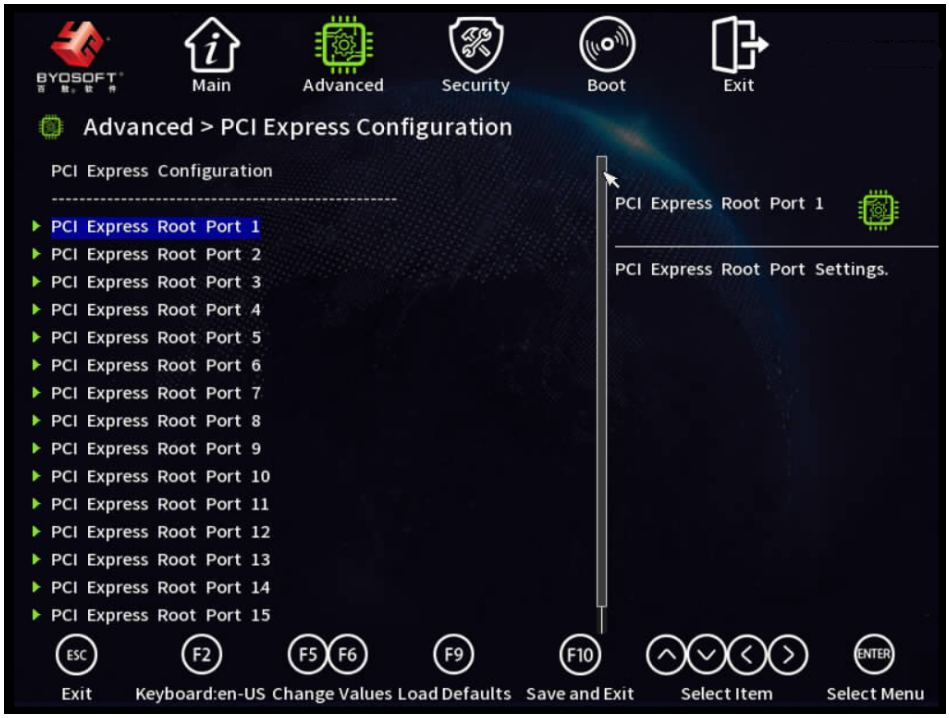


Table 6-63 Parameters on the PCI Express Configuration screen

Parameter	Description
PCI Express Root Port *X*	Provides access to PCI Express Root Port configurations.

6.2.7.1.1 PCI Express Root Port X

On the **PCI Express Root Port *X*** screen, you can enable or disable the control service extension feature. **Figure 6-70** shows the **PCI Express Root Port *X*** screen. **Table 6-64** describes the parameters.

Figure 6-70 PCI Express Root Port *X* screen

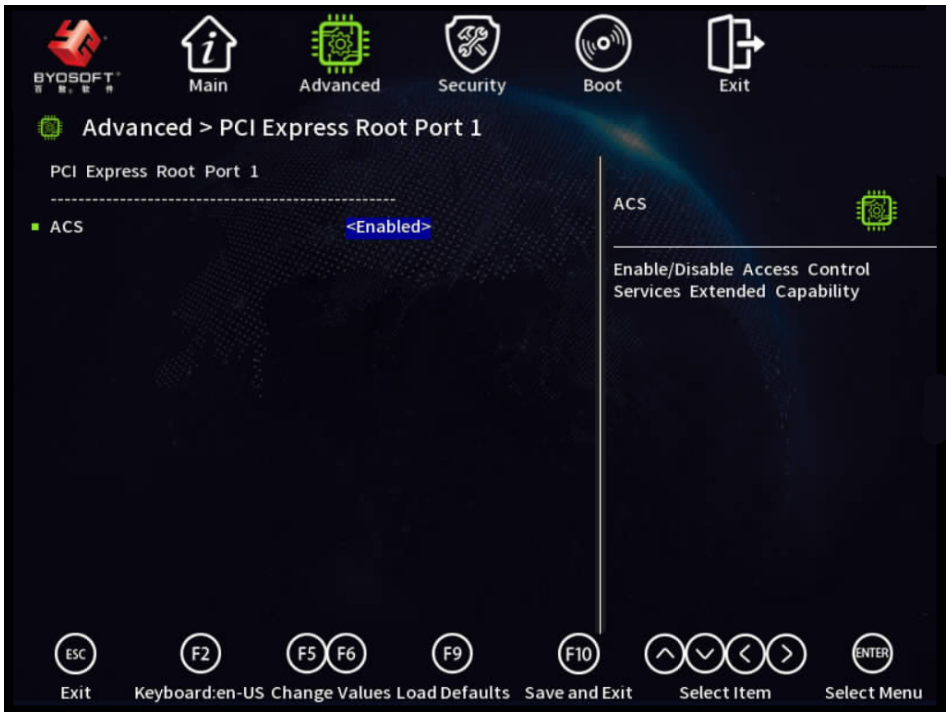


Table 6-64 Parameters on the PCI Express Root Port *X* screen

Parameter	Description	Default Value
ACS	Enable or disable Access Control Services Extended Capability. The menu options are as follows: • Disabled • Enabled **NOTE** Only BIOS 01.02.08.09 and later versions support this parameter.	The default value of this parameter varies depending on the server model: • G8600 V7 and G5500 V7 Disabled • 2288 V7, 2488H V7, and 5885H V7 Enabled

6.2.7.2 SATA And RST Configuration

On the **SATA And RST Configuration** screen, you can configure the SATA (including the SATA controllers and drive interfaces) and disable the specified ports using the three controllers. Multiple SATA interfaces can be configured. If the server supports the Intel VROC (SATA RAID) function, you need to set the RAID mode to the SATA mode to configure the Intel VROC (SATA RAID). There are three groups of SATA information on this screen, which are the specific information about the drives of the three controllers. If there is no drive under the controller, this screen is empty. **Figure 6-71** shows the **SATA And RST Configuration** screen. **Table 6-65** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-71 SATA And RST Configuration screen

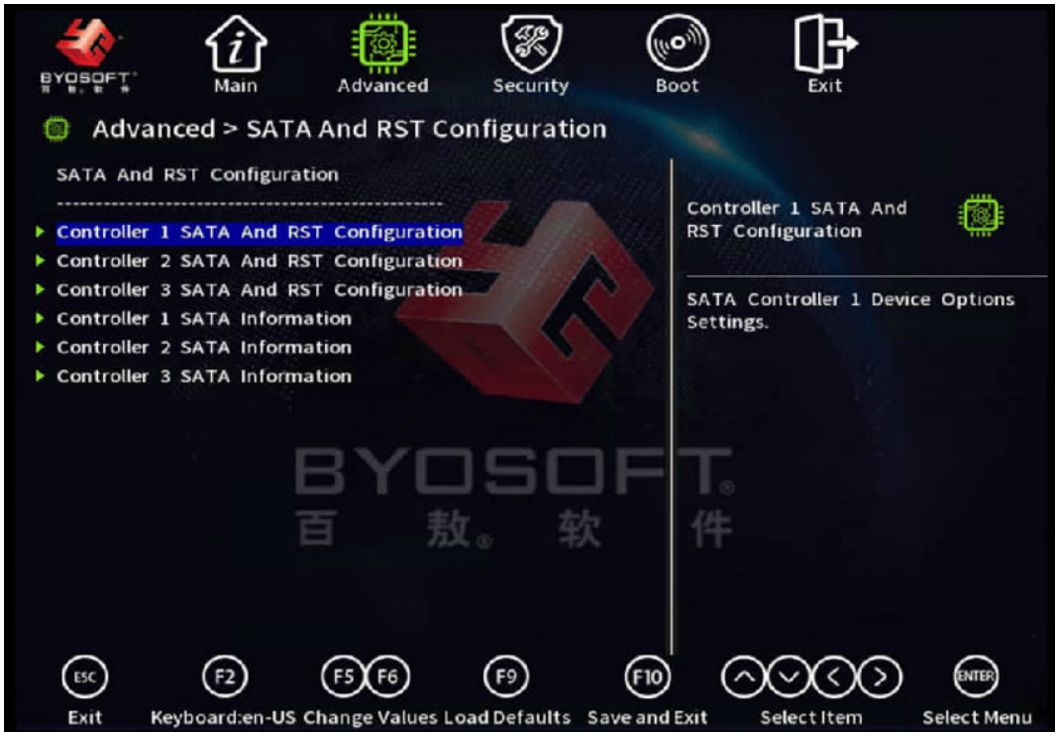


Table 6-65 Parameters on the SATA And RST Configuration screen

Parameter	Description
Controller *X* SATA And RST Configuration	Provides access to SATA and RST configurations of controller X.
Controller *X* SATA Information	Specifies the SATA information of controller X.

6.2.7.2.1 Controller 1 SATA And RST Configuration

On this screen, you can configure the SATA ports controlled by controller 1. **Figure 6-72** shows the **Controller 1 SATA And RST Configuration** screen. **Table 6-66** describes the parameters.

Figure 6-72 Controller 1 SATA And RST Configuration screen

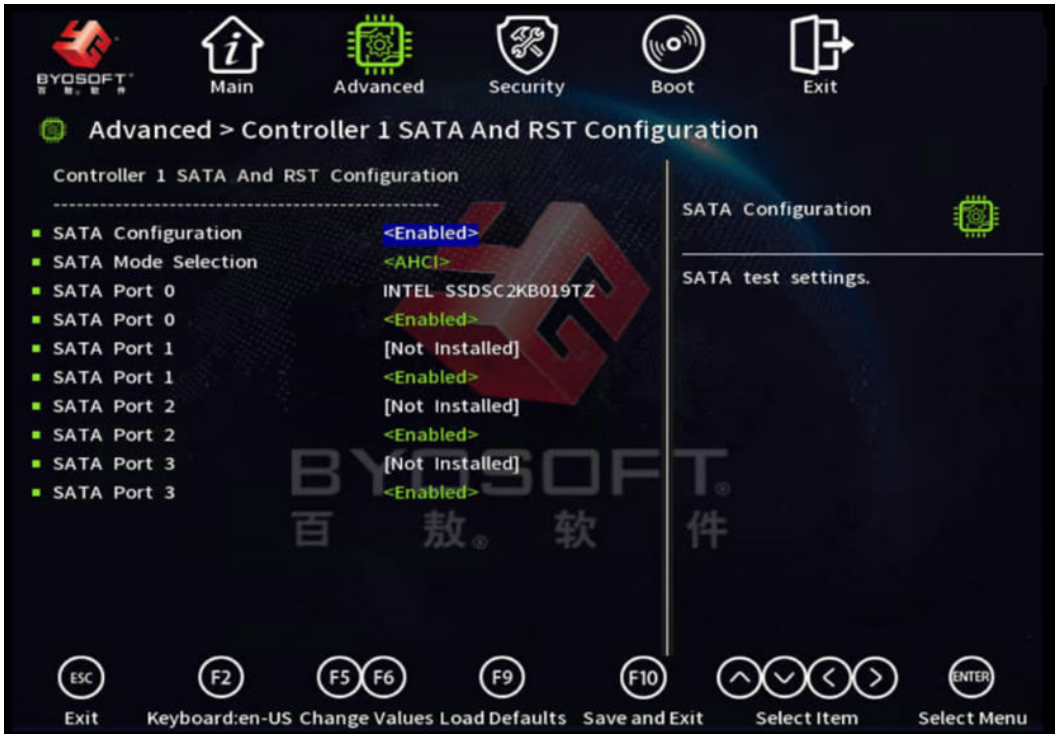


Table 6-66 Parameters on the Controller 1 SATA And RST Configuration screen

Parameter	Description	Default Value
SATA Configuration	Enables or disables the SATA controller. The menu options are as follows: ● Enabled ● Disabled	Enabled
SATA Mode Selection	Sets the working mode of the drive controller. The menu options are as follows: ● AHCI ● RAID **NOTE** ● This parameter is unavailable when **SATA Configuration** is set to **Disabled**. ● To configure Intel VROC (SATA RAID), you must set this parameter to **RAID**.	AHCI

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
RAID Device ID	Sets the device ID function in RAID mode. The menu options are as follows: ● Client ● Alternate ● Server **NOTE** This parameter is available when **SATA Configuration** is set to **Enabled** and **SATA Mode Selection** is set to **RAID**.	Server
SATA Port *X*	Displays information about the connected SATA drives. If the device is not detected, **Not Installed** is displayed. If the device is detected, the device information is displayed. **NOTE** The value of *X* ranges from 0 to 7, which depends on the hardware design. The unused SATA ports are not displayed.	-
SATA Port *X*	Enables or disables the SATA port. The menu options are as follows: ● Enabled ● Disabled **NOTE** The value of *X* ranges from 0 to 7, which depends on the hardware design. The unused SATA ports are not displayed.	Enabled

6.2.7.2.2 Controller 1 SATA Information

On this screen, you can view the SATA information of controller 1. **Figure 6-73** shows the **Controller 1 SATA Information** screen. **Table 6-67** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-73 Controller 1 SATA Information screen

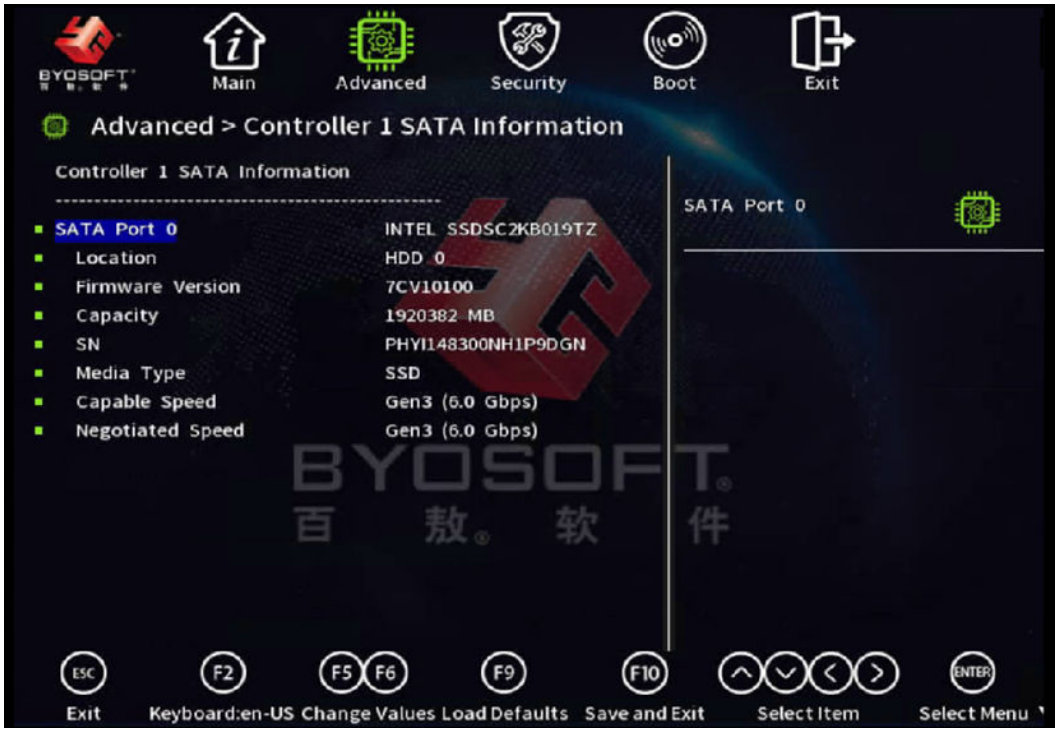


Table 6-67 Parameters on the Controller 1 SATA Information screen

Parameter	Description
SATA Port n	Displays the manufacturer information about the drive connected to the port.
Location	Displays the position of the drive.
Firmware Version	Displays the firmware version of the drive.
Capacity	Displays the drive capacity.
SN	Displays the serial number.
Media Type	Displays the media type.
Capable Speed	Indicates the supported speed.
Negotiated Speed	Displays the negotiated speed.

6.2.7.3 USB Configuration

On the **USB Configuration** screen, you can view the number of current USB devices, control USB ports, and disable specified ports by configuring related options. **Figure 6-74** shows the **USB Configuration** screen. **Table 6-68** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-74 USB Configuration screen

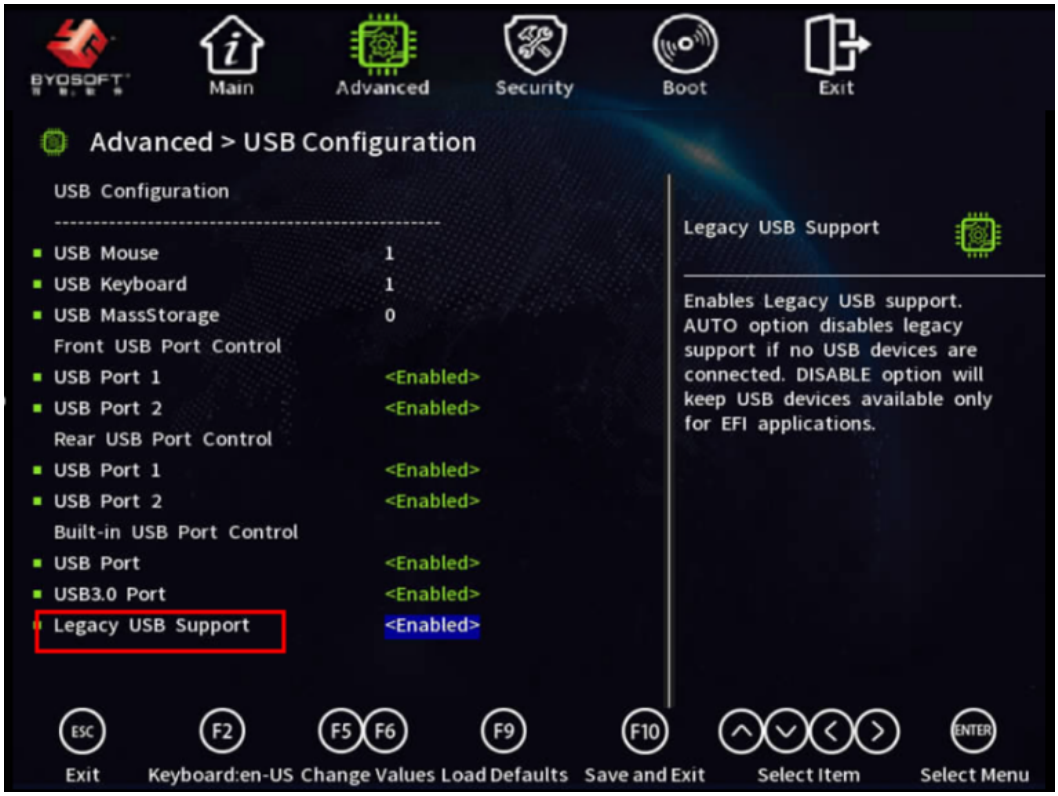


Table 6-68 Parameter on the USB Configuration screen

Parameter	Description	Default Value
USB Mouse	Displays the number of currently valid mouses. The value **0** indicates that no valid device is detected.	The value is displayed as the number that is actually read. Example: USB Mouse 1
USB Keyboard	Displays the number of currently valid keyboards. The value **0** indicates that no valid device is detected.	The value is displayed as the number that is actually read. Example: USB Keyboard 1
USB MassStorage	Displays the number of valid USB storage devices. The value **0** indicates that no valid device is detected.	The value is displayed as the number that is actually read. Example: USB MassStorage 2

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Front USB Control ● USB Port 1 ● USB Port 2	Specifies the USB ports on the front panel. Enables or disables this USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the front panel of the server.	Enabled
Rear USB Control ● USB Port 1 ● USB Port 2	Specifies the USB ports on the rear panel. Enables or disables this USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the rear panel of the server.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Built-in USB Control ● USB Port	Specifies the built-in USB port. Enables or disables this USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports correspond to the built-in USB 3.0 ports of the server.	Enabled
USB3.0 Port	Enable or disable this USB3.0 Physical Connector (physical port). Once disabled, any USB3.0 devices plug into the connector will not be detected by BIOS or OS. The menu options are as follows: ● Enabled ● Disabled **NOTE** Only G8600 V7 supports this parameter.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Legacy USB Support	Legacy USB support function. The options are: ● **Enabled**: Supports legacy USB devices. ● **Disabled**: Does not support legacy USB devices. The server ensures USB device availability only in UEFI mode. ● **Auto**: If a USB device is connected, the function will be enabled; if no USB device is connected, the function will be disabled. **NOTE** Only BIOS 01.02.08.05 and later versions support this parameter.	Enabled

6.2.8 Misc Configuration

On the **Misc Configuration** screen, you can set the serial port debugging switch and spread spectrum functions. **Figure 6-75** shows the **Misc Configuration** screen. **Table 6-69** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-75 Misc Configuration screen

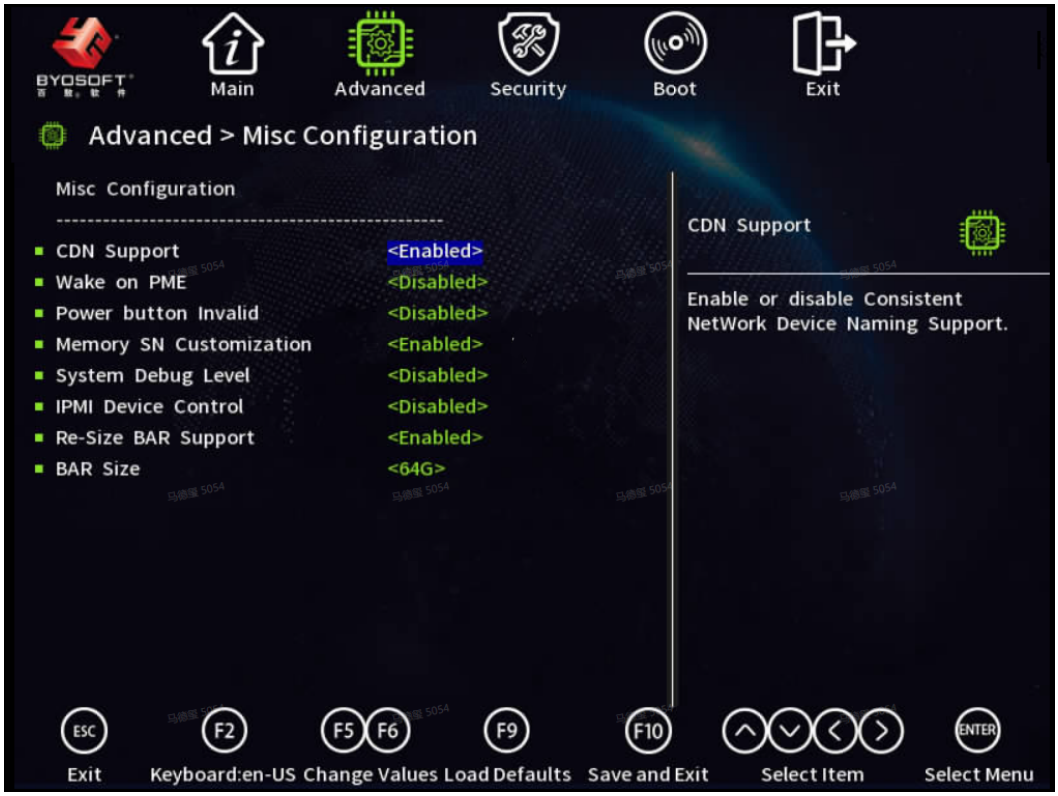


Table 6-69 Parameters on the Misc Configuration screen

Parameter	Description	Default Value
CDN Support	Enables or disables the consistent network device naming (CDN) support function. The menu options are as follows: • Enabled • Disabled	Enabled
Wake On PME	Enables or disables the Wake On Power Management Event (PME) function. Controls the network wakeup function. The menu options are as follows: • Enabled • Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Power button Invalid	Enables or disables the power button invalid function. The menu options are as follows: ● Enabled ● Disabled **NOTE** When this parameter is set to **Enabled**, the power button is locked. You cannot use the power button to power on or off the server. You need to use the server management software to power on or off the server.	Disabled
Memory SN Customization	Enables or disables the memory serial number customization function. ● Disabled ● Enabled	Disabled
System Debug Level	Sets the output type of the serial port debugging information. The menu options are as follows: ● **Enabled**: Outputs all information. ● **Disabled**: Outputs OEM or error information.	Disabled
IPMI Device Control	Controls the IPMI device to report ACPI. The menu options are as follows: ● Enabled ● Disabled	Disabled
Re-Size BAR Support	Enables or disables the PCIe resizable BAR capability supported. The options are as follows: ● Disabled ● Enabled **NOTE** Only BIOS 01.02.08.05 and later versions support this parameter.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
BAR Size	Choose the BAR size for the PCIe device. **Auto** means max of Re-size BAR supported each PCIe Device. This option will not take effect if the PCIe card does not support the Resizable BAR feature. The options are as follows: ● Auto ● 8G ● 16G ● 32G ● 64G **NOTE** ● This parameter is available when **Re-Size BAR Support** is set to **Enabled**. ● Only BIOS 01.02.08.05 and later versions support this parameter.	Auto

6.2.9 Console Redirection Configuration

On the **Console Redirection Configuration** screen, you can set parameters related to the serial port, for example, enable the redirection function of the serial port. **Figure 6-76** shows the **Console Redirection Configuration** screen. **Table 6-70** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-76 Console Redirection Configuration screen

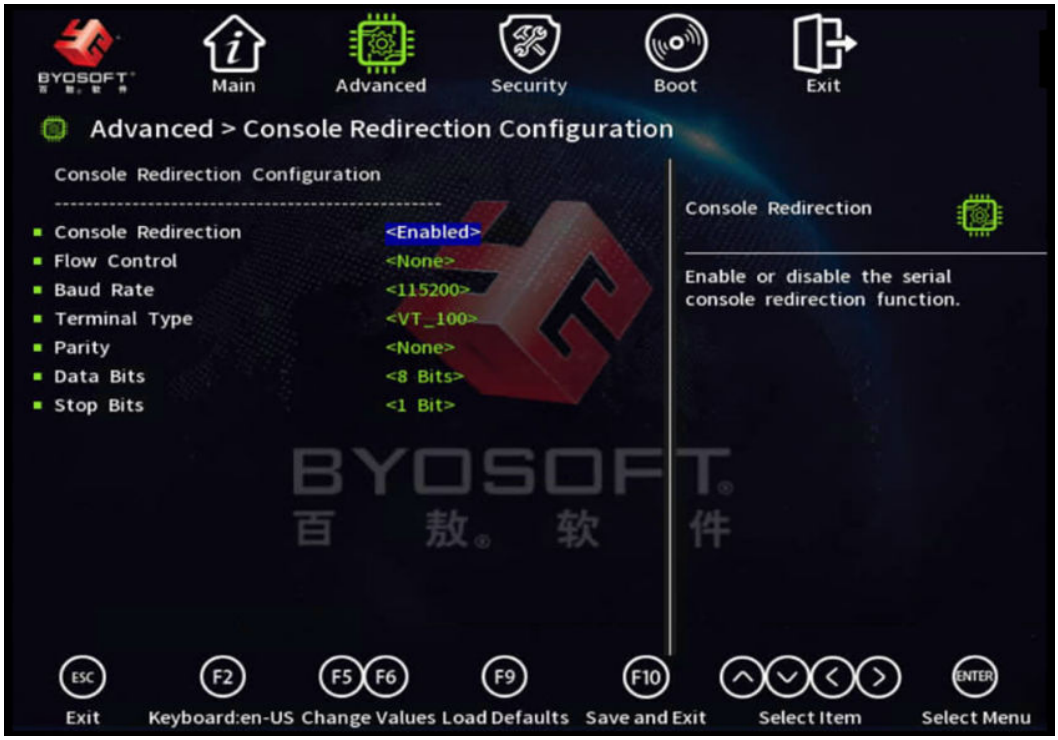


Table 6-70 Parameters on the Console Redirection Configuration screen

Parameter	Description	Default Value
Console Redirection	Enables or disables the serial port redirection. This function maps the data of a specified physical or virtual serial port to a specified system serial port. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Flow Control	Sets the control flow of the serial port redirection. The menu options are as follows: ● **None**: Disables the control flow of the serial port redirection. ● **RTS/CTS**: Sends request/Clears request sending. **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	None
Baud Rate	Sets the baud rate for serial port redirection. The menu options are as follows: ● 1200 ● 2400 ● 4800 ● 9600 ● 19200 ● 38400 ● 57600 ● 115200 **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	115200

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Terminal Type	Specifies the emulation type selected in the terminal program. The emulation type selected in the terminal program must be the same as the emulation type in BIOS. The menu options are as follows: ● VT_100 ● VT_100+ ● VT_UTF8 ● PC_ANSI ● LOG_TERM **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	VT_100
Parity	Sets the serial port redirection check. A parity check bit can be sent along with data bits to detect data transmission errors. The menu options are as follows: ● **None**: Disables The check function is disabled. ● **Even**: Sends even bits with data bits to detect data transmission errors. If the number of 1s in data bits is even, the parity check bit is **0**. ● **Odd**: Sends odd bits with data bits to detect data transmission errors. If the number of 1s in data bits is odd, the parity check bit is **0**. **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	None

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Data Bits	Specifies the data length of serial port redirection. The menu options are as follows: ● 7 Bits ● 8 Bits **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	8 Bits
Stop Bits	Sets the stop bit of the serial port redirection. A stop bit indicates the end of a serial data packet (the start bit indicates the start). The standard setting is 1 stop bit, and communication with slow devices may require more than 1 stop bit. The menu options are as follows: ● 1 Bit ● 2 Bit **NOTE** This parameter is unavailable when **Console Redirection** is set to **Disabled**.	1 Bit

6.2.10 PXE Configuration

On the **PXE Configuration** screen, you can control the PXE function of the NIC. **Figure 6-77** shows the **Misc Configuration** screen. **Table 6-71** describes the parameters.

NOTE

The displayed screen varies depending on the NIC configuration.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-77 PXE Configuration screen



Table 6-71 Parameters on the PXE Configuration screen

Parameter	Description	Default Value
Slot PXE Control	Enables or disables the PXE function of the PCIe NIC. The menu options are as follows: ● Enabled ● Disabled	Enabled
SLOT*X* PXE Configuration	All controllable PXE ports on slot *X* are in this group. **NOTE** ● This parameter is displayed only when a PCIe NIC is installed in the corresponding CPU slot. ● This parameter is unavailable when **Slot PXE Control** is set to **Disabled**.	-
FLEXIO n PXE Configuration	All controllable PXE ports on FlexIO *n* are in this group.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-78 shows the **SLOT X PXE Configuration** screen. Table 6-72 describes the parameters.

Figure 6-78 SLOTX PXE Configuration screen

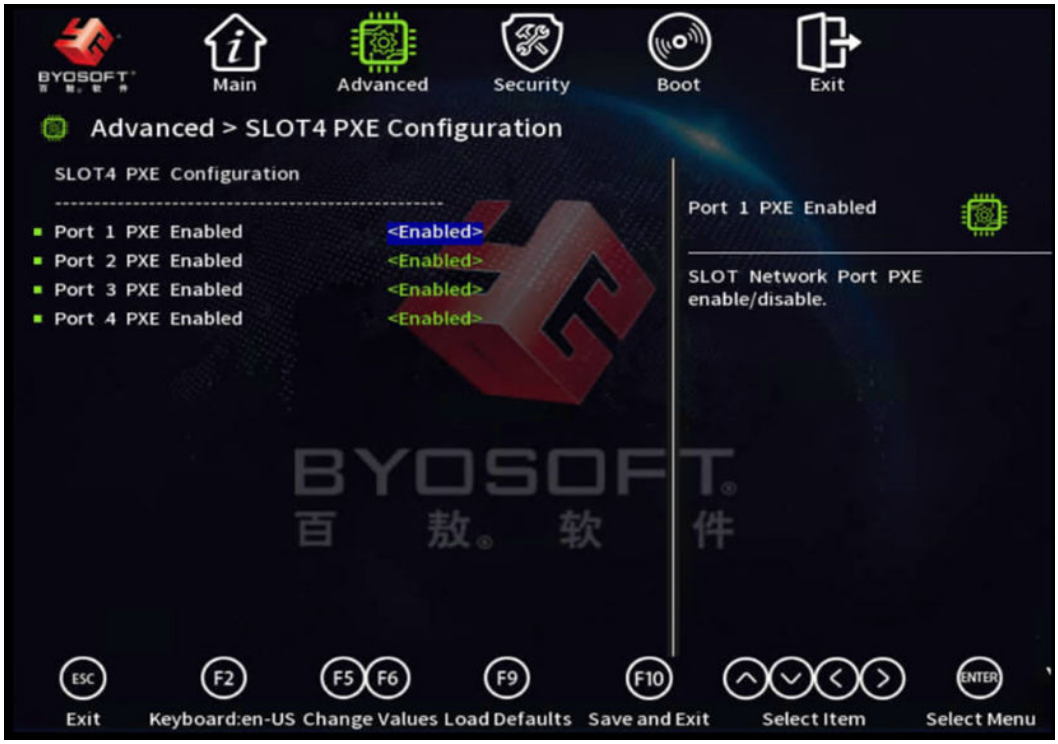


Table 6-72 Parameters on the SLOTX PXE Configuration screen

Parameter	Description	Default Value
Port n PXE Enabled	Enables or disables the PXE function of SLOT X port *n*. The menu options are as follows: • Enabled • Disabled **NOTE** This parameter is displayed only when a PCIe NIC is installed in the corresponding CPU slot.	Enabled

Figure 6-79 shows the **FlexIO *n* PXE Configuration** screen. Table 6-73 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-79 FlexIO *n* PXE Configuration screen

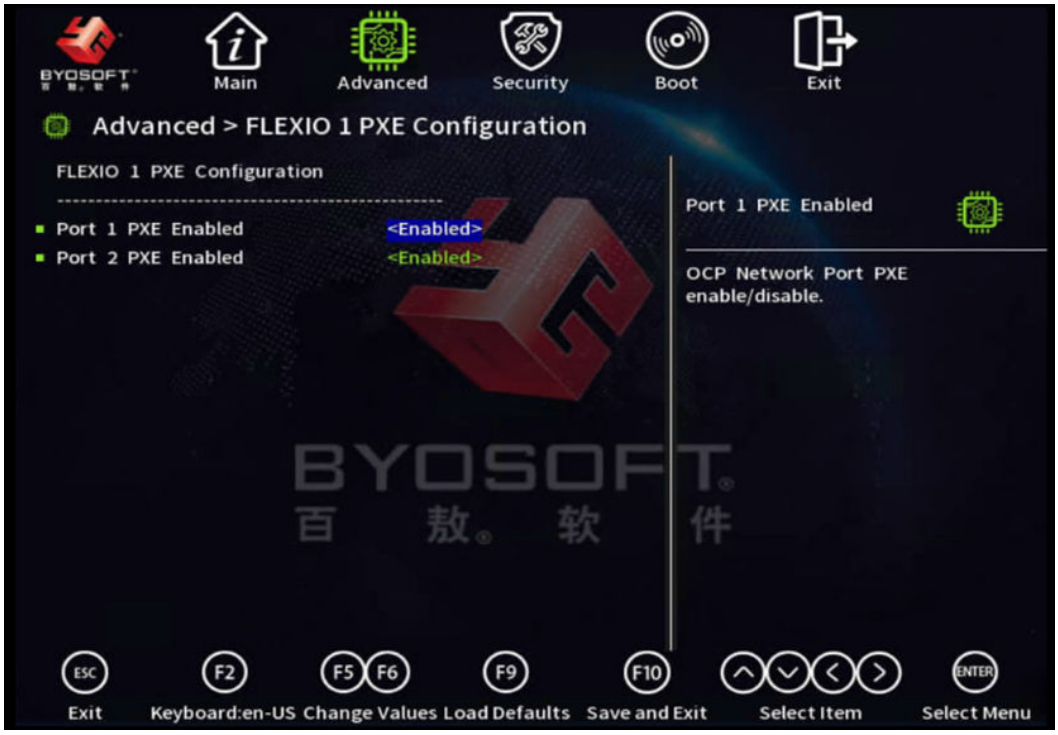


Table 6-73 Parameters on the FlexIO *n* PXE Configuration screen

Parameter	Description	Default Value
Port n PXE Enabled	Enables or disables the PXE function of the OCP NIC port *X*. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is displayed only when an OCP NIC is configured.	Enabled **NOTE** ● A maximum of one OCP NIC is displayed on the 2288 V7, 5885H V7, 2488H V7, and G8600 V7 servers, two OCP NICs on the 2288H V7 server, and three OCP NICs on the G5500 V7 server. ● All default values of network ports are set to **Enabled** in UEFI mode. ● In legacy mode, only the first network port of the OCP NIC is enabled by default. That is, the default value of **Flex IO 1 Port 1** is **Enabled**, and the default value of **Flex IO 1 Port 2** is **Disabled**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.11 ME Configuration

On the **ME Configuration** screen, you can learn about the features of the current ME. **Figure 6-80** shows the **ME Configuration** screen. **Table 6-74** describes the parameters.

Figure 6-80 ME Configuration screen



Table 6-74 Parameters on the ME Configuration screen

Parameter	Description
Server ME Configuration	Specifies the technical specifications of the server ME.

Figure 6-81 shows the **Server ME Configuration** screen. **Table 6-75** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-81 Server ME Configuration screen

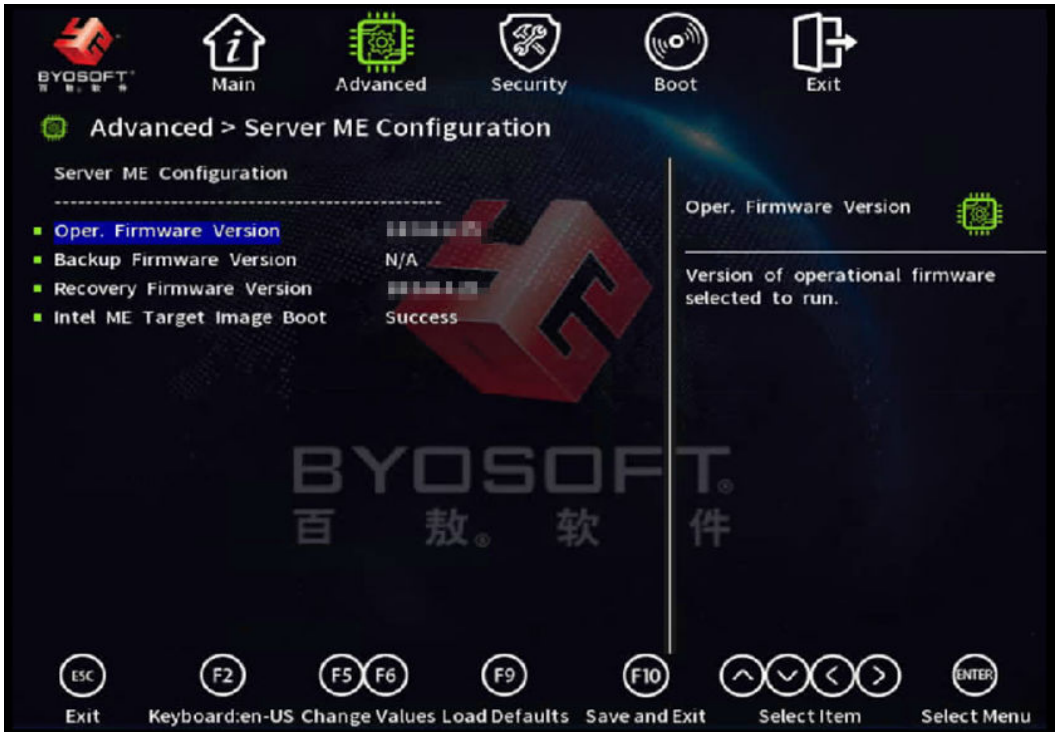


Table 6-75 Parameters on the Server ME Configuration screen

Parameter	Description
Oper. Firmware Version	Displays the version of the operating ME firmware.
Backup Firmware Version	Displays the backup firmware version.
Recovery Firmware Version	Displays the version of the restored ME firmware. This parameter runs when the ME is in recovery mode.
Intel ME Target Image Boot	Displays the current running status of the ME.

6.2.12 NVMe Information

On the **NVMe Information** screen, you can view information about the NVMe drives. **Figure 6-82** or **Figure 6-83** shows the **NVMe Information** screen. **Table 6-76** describes the parameters.

NOTE

The NVMe drive information is displayed only when **Intel(R) VMD Config** is set to **Disabled**.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-82 NVMe Information screen 1

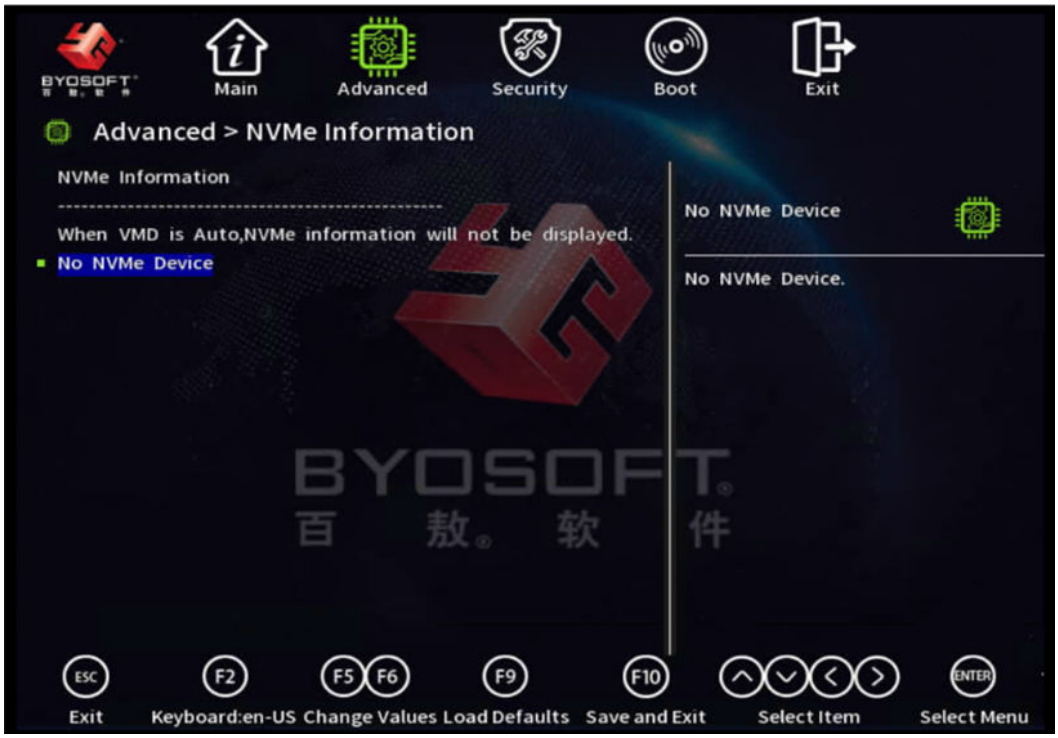
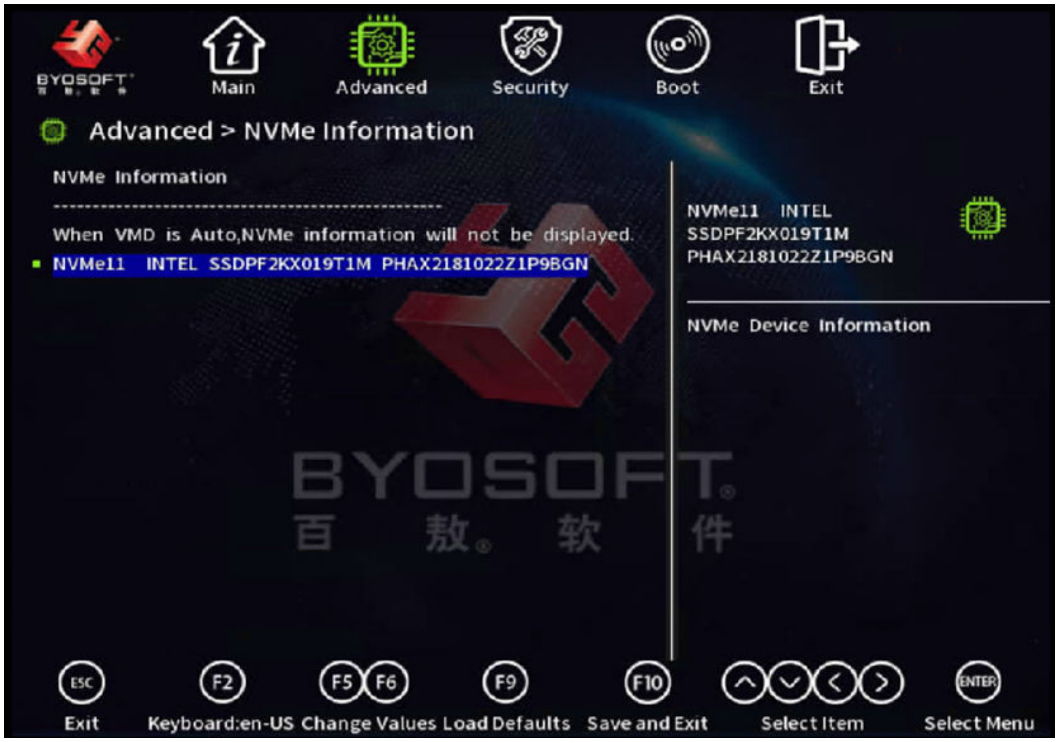


Figure 6-83 NVMe Information screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

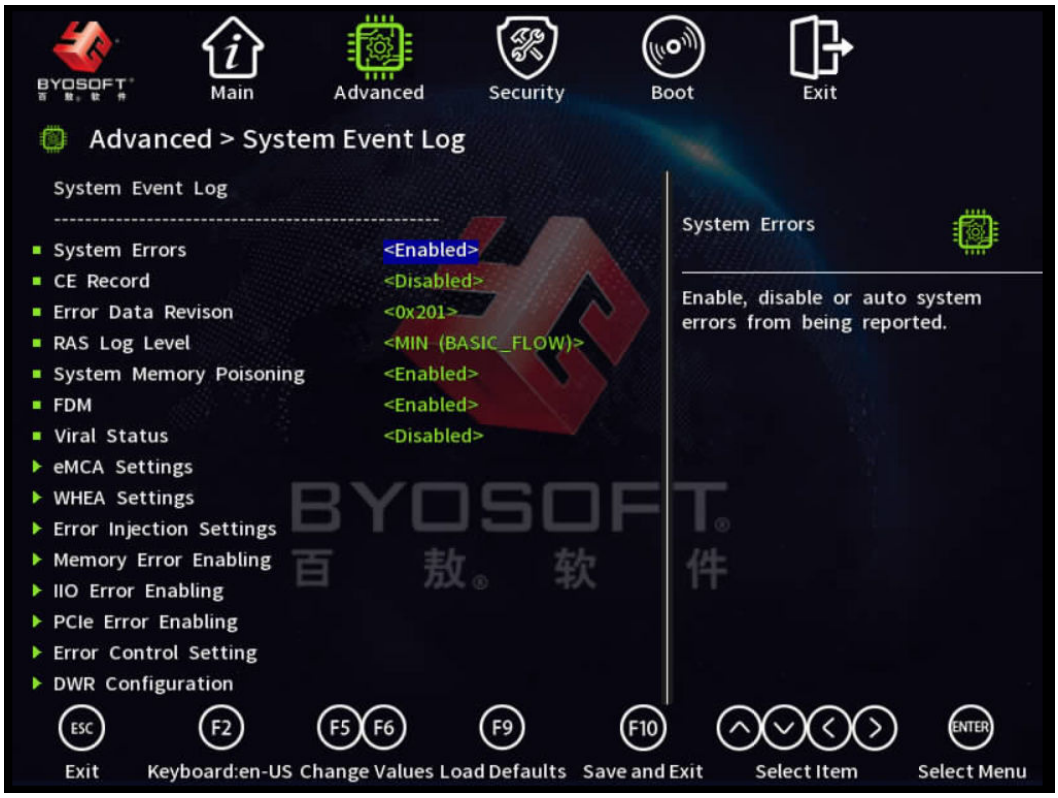
Table 6-76 Parameters on the NVMe Information screen

Parameter	Description
NVMe*X*	Displays details about the NVMe drives. **NOTE** • The name displayed varies depending on the NVMe drives. • **No NVMe Device** is displayed if no NVMe drive is installed.

6.2.13 System Event Log

On the **System Event Log** screen, you can configure the event log function, including system error logging and system memory poisoning configuration. **Figure 6-84** shows the **System Event Log** screen. **Table 6-77** describes the parameters.

Figure 6-84 System Event Log screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-77 Parameters on the System Event Log screen

Parameter	Description	Default Value
System Errors	Enables or disables the function of recording system errors. After enabling this function, errors can be rectified. Uncorrectable errors are reported to the BMC and OS. The menu options are as follows: ● Enabled ● Disabled ● Auto	Enabled
CE Record	Enables or disables the CE record. The menu options are as follows: ● Enabled ● Disabled	Disabled
Error Data Revison	Sets the fault data version. The menu options are as follows: ● 0x201 ● 0x300	0x201
RAS Log Level	Sets the RAS log level. The menu options are as follows: ● None ● MIN (BASIC_FLOW) ● MID (BASIC_FLOW, FUNC_FLOW) ● MAX (BASIC_FLOW, FUNC_FLOW, REG)	MIN (BASIC_FLOW)

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
System Memory Poisoning	Enables or disables the system memory poisoning function. After this function is enabled, if an error is detected, the system marks the error message with a poisoning label and does not trigger the error immediately. The interrupt is triggered only when the error data is used. The menu options are as follows: ● Enabled ● Disabled	Enabled
FDM	Enables or disables the fault diagnosis management (FDM) function. The FDM provides automatic troubleshooting capabilities covering the entire system, including fault data collection, fault data analysis, and fault diagnosis and location. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available only when **System Errors** is set to **Enabled**.	Enabled
Viral Status	Enables or disables the virus status. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available only when **System Errors** is set to **Enabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Clear Viral Status	Enables or disables the function of clearing virus status. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is available when **System Errors** and **Viral Status** are set to **Enabled**.	Disabled
eMCA Settings	Provides access to eMCA settings. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled** or **Auto**.	-
WHEA Settings	Provides access to WHEA configurations. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled** or **Auto**.	-
Error Injection Settings	Provides access to error injection configurations. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled** or **Auto**.	-
Memory Error Enabling	Provides access to memory error configurations. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled**.	-
IIO Error Enabling	Displays or modifies I/O error options. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled**.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIe Error Enabling	Provides access to PCIe error configurations. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled**.	-
Error Control Setting	Provides access to patrol scrub error type setting. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled**.	-
DWR Configuration	Provides access to DWR configurations. **NOTE** This parameter can be edited when **System Errors** is set to **Enabled**.	-

6.2.13.1 eMCA Settings

On the **eMCA Settings** screen, you can set eMCA functions. **Figure 6-85** shows the **eMCA Settings** screen. **Table 6-78** describes the parameters.

Figure 6-85 eMCA Settings screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-78 Parameters on the eMCA Settings screen

Parameter	Description	Default Value
eMCA Logging Support	Enables or disables the logging function of the enhanced machine check architecture (eMCA). After this function is enabled, an area is allocated in the memory to store the MCBank register data and incorrect DIMM data for OS access and an uncorrectable error may trigger an SMI interruption. The menu options are as follows: ● Enabled ● Disabled	Enabled
LMCE Support	Enable or disable local MCE firmware support. The menu options are as follows: ● Enabled ● Disabled	Enabled
eMCA CMCI-SMI Morphing	Enables or disables the eMCA CMCI-SMI mapping. The menu options are as follows: ● eMCA Gen 2 CSMI ● Disabled **NOTE** This parameter is unavailable when **eMCA Logging Support** is set to **Disabled**.	eMCA Gen 2 CSMI
Opportunistic Spare Core	Enables or disables the opportunity spare core. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **eMCA Logging Support** is set to **Disabled**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.13.2 WHEA Settings

On the **WHEA Settings** screen, you can enable or disable the Windows hardware error architecture (WHEA) function. **Figure 6-86** shows the **WHEA Settings** screen. **Table 6-79** describes the parameters.

Figure 6-86 WHEA Settings screen



Table 6-79 Parameters on the WHEA Settings screen

Parameter	Description	Default Value
WHEA Support	Enables or disables the WHEA function. This function provides rich hardware error reports for running servers, shortening the average recovery time caused by fatal hardware errors. The menu options are as follows: • Enabled • Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.13.3 Error Injection Settings

On the **Error Injection Settings** screen, you can set the error injection function. Figure 6-87 shows the **Error Injection Settings** screen. Table 6-80 describes the parameters.

Figure 6-87 Error Injection Settings screen

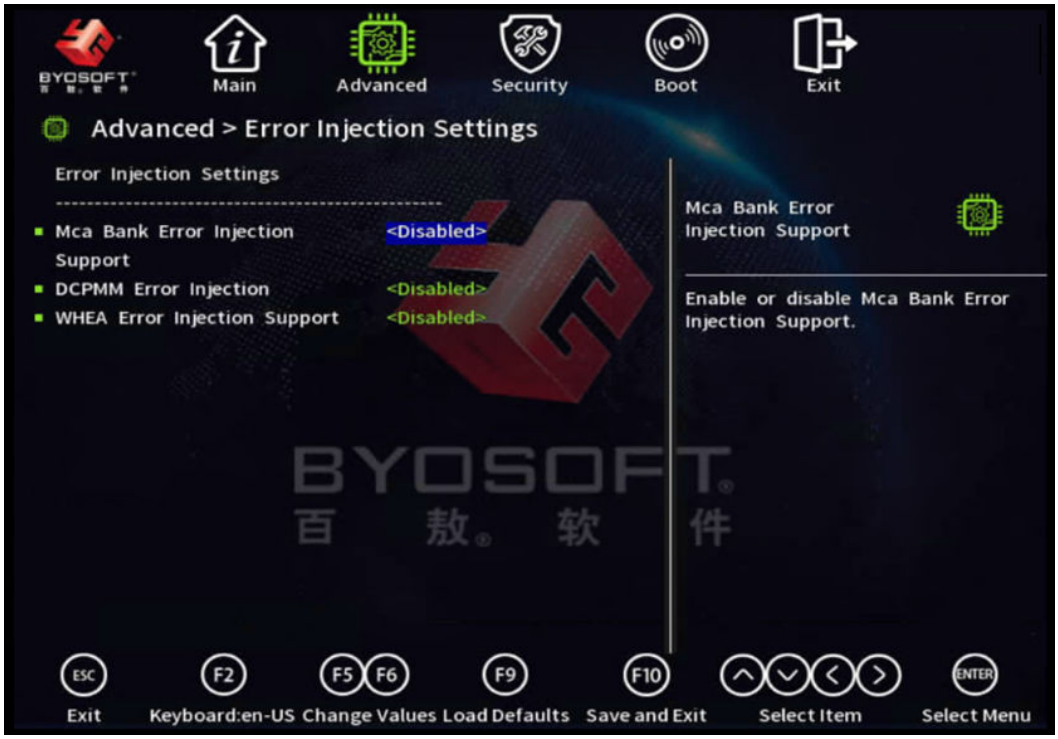


Table 6-80 Parameters on the Error Injection Settings screen

Parameter	Description	Default Value
Mca Bank Error Injection Support	Enables or disables the MCA Bank error injection. The menu options are as follows: ● Enabled ● Disabled	Disabled
DCPMM Error Injection	Enables or disables the DCPMM error injection. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
WHEA Error Injection Support	Enables or disables the WHEA error injection. The menu options are as follows: • Enabled • Disabled	Disabled

6.2.13.4 Memory Error Enabling

On the **Memory Error Enabling** screen, you can enable or disable the memory error detection and correction function. **Figure 6-88** shows the **Memory Error Enabling** screen. **Table 6-81** describes the parameters.

Figure 6-88 Memory Error Enabling screen

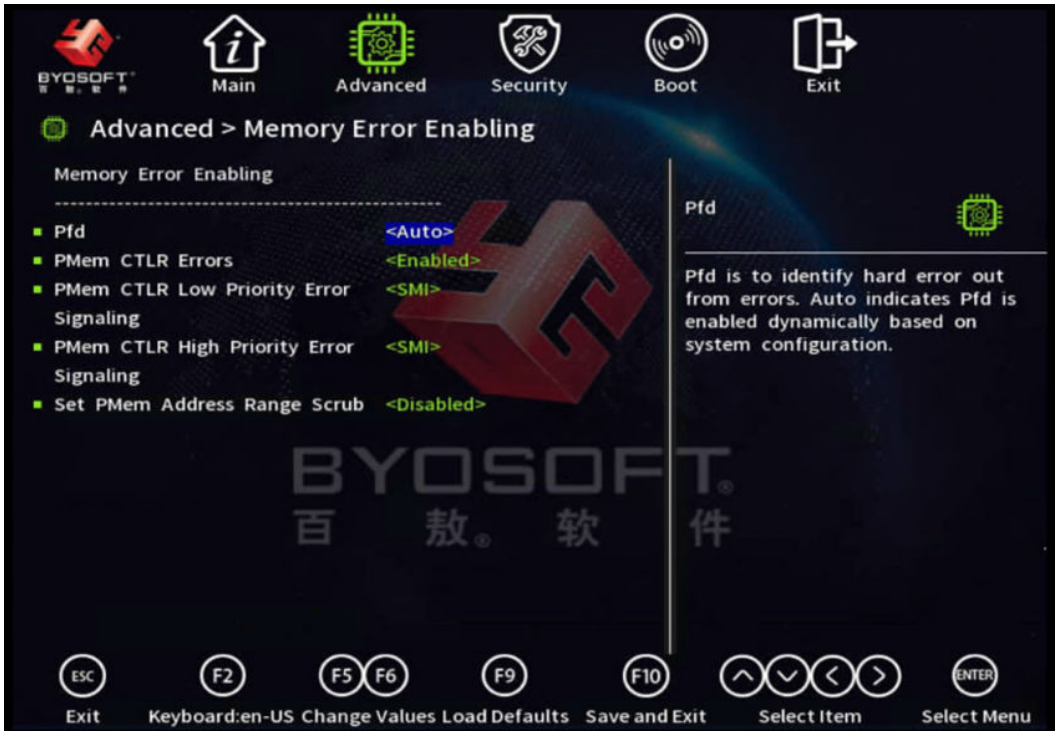


Table 6-81 Parameters on the Memory Error Enabling screen

Parameter	Description	Default Value
Pfd	identifies hard faults from faults. The menu options are as follows: • Auto • Enabled • Disabled	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PMem CTLR Errors	Enables or disables PMem CTLR error reporting and logging. The menu options are as follows: ● Enabled ● Disabled **NOTE** Only the 2288 V7 supports this parameter.	Enabled
PMem CTLR Low Priority Error Signaling	Sets the signal selection function for PMem CTLR low-priority errors. The menu options are as follows: ● Disabled ● SMI ● ERR0# Pin **NOTE** Only the 2288 V7 supports this parameter.	SMI
PMem CTLR High Priority Error Signaling	Sets the signal selection function for PMem CTLR high-priority errors. The menu options are as follows: ● Disabled ● SMI ● ERR0# Pin **NOTE** Only the 2288 V7 supports this parameter.	SMI
Set PMem Address Range Scrub	Enables or disables the PMem DIMM physical address range inspection. The menu options are as follows: ● Enabled ● Disabled **NOTE** Only the 2288 V7 supports this parameter.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.13.5 IIO Error Enabling

On the **IIO Error Enabling** screen, you can set I/O functions. **Figure 6-89** shows the **IIO Error Enabling** screen. **Table 6-82** describes the parameters.

Figure 6-89 IIO Error Enabling screen



Table 6-82 Parameters on the IIO Error Enabling screen

Parameter	Description	Default Value
OS Native AER Support	Enables or disables the OS-controlled advanced error reporting (AER) error handling function. By default, the Intel firmware preferentially controls AER error handling. If the OS needs to control AER errors, set this parameter to **Enabled**. The menu options are as follows: • **Enabled**: The OS controls the AER error handling. • **Disabled**: The firmware controls the AER error handling.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IIO MCA Support	Enables or disables the I/O MCA support. The menu options are as follows: ● Enabled ● Disabled	Disabled
IIO eDPC Support	Enables or disables the eDPC support. The menu options are as follows: ● Disabled ● On Fatal Error ● On Fatal and Non-Fatal Errors	Disabled
IIO eDPC Interrupt	Enables or disables the I/O eDPC interruption. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Enabled
IIO eDPC ERR_COR Message	Enables or disables the I/O eDPC ERR_COR message. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Enabled
PCIe Poison TLP Egress Blocking	Enables or disables the PCIe Poison TLP egress blocking function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is unavailable when **IIO eDPC Support** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PCIE Error	Enables or disables PCIe errors. The menu options are as follows: • Enabled • Disabled	Enabled

6.2.13.6 PCIe Error Enabling

On the **PCIe Error Enabling** screen, you can set PCIe error functions. **Figure 6-90** shows the **PCIe Error Enabling** screen. **Table 6-83** describes the parameters.

Figure 6-90 PCIe Error Enabling screen



Table 6-83 Parameters on the PCIe Error Enabling screen

Parameter	Description	Default Value
Corrected Error	Enables or disables the correctable error function. The menu options are as follows: • Enabled • Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Uncorrected Error	Enables or disables the uncorrectable error function. The menu options are as follows: ● Enabled ● Disabled	Enabled
Fatal Error	Enables or disables the fatal error function. The menu options are as follows: ● Enabled ● Disabled	Enabled
PCIe Corrected Error Threshold Counter	Enables or disables the PCIe correction error threshold counter. The menu options are as follows: ● Enabled ● Disabled	Disabled
PCIe Corrected Error Threshold	Sets the PCIe corrected error threshold. The minimum value is **0**. The maximum value is **0xffffffff**. The default value is **1**.	1
PCIe ECRC Error	Enables or disables the PCIe ECRC error. The menu options are as follows: ● Enabled ● Disabled	Disabled
PCIe Surprise Link Down Error	Enables or disables the PCIe unexpected link disconnection error. The menu options are as follows: ● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.2.13.7 Error Control Setting

On the **Error Control Setting** screen, you can select the patrol scrub error type. Figure 6-91 shows the **Error Control Setting** screen. Table 6-84 describes the parameters.

Figure 6-91 Error Control Setting screen

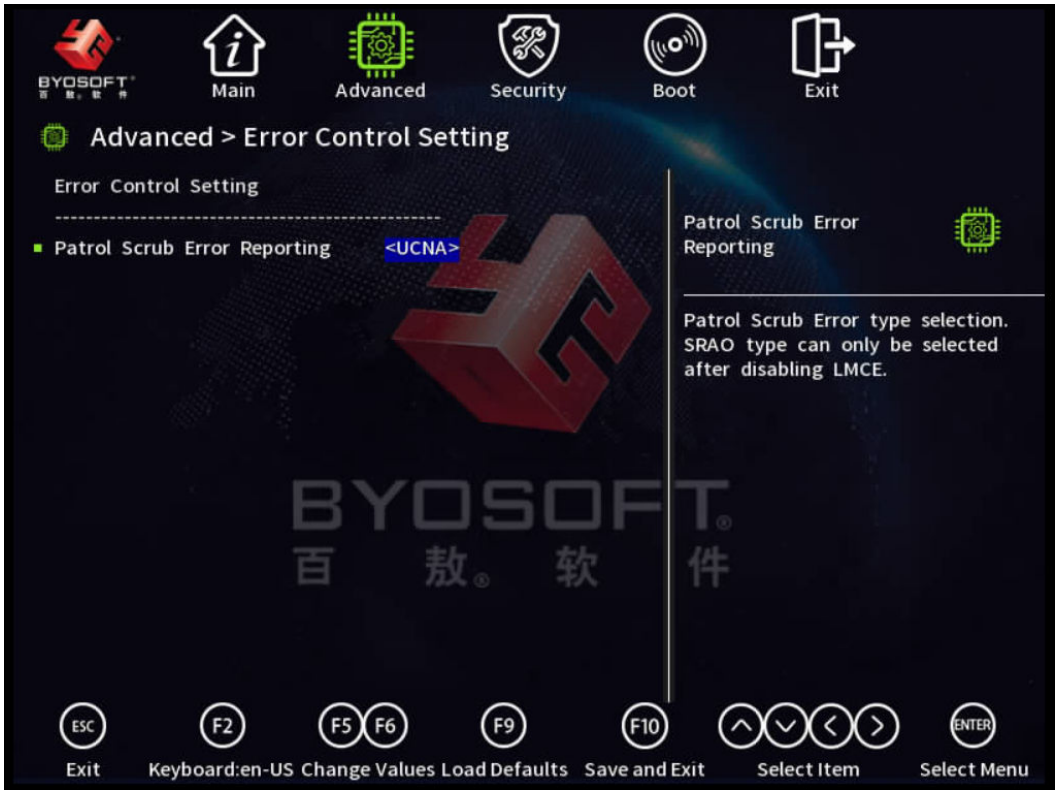


Table 6-84 Parameters on the Error Control Setting screen

Parameter	Description	Default Value
Patrol Scrub Error Reporting	Allows you to select the patrol scrub error type. The menu options are as follows: • UCNA • SRAO **NOTE** This parameter is available when **System Memory Poisoning** is set to **Enabled**.	UCNA

6.2.13.8 DWR Configuration

On the **DWR Configuration** screen, you can set DWR-related functions. Figure 6-92 shows the **DWR Configuration** screen. Table 6-85 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-92 DWR Configuration screen

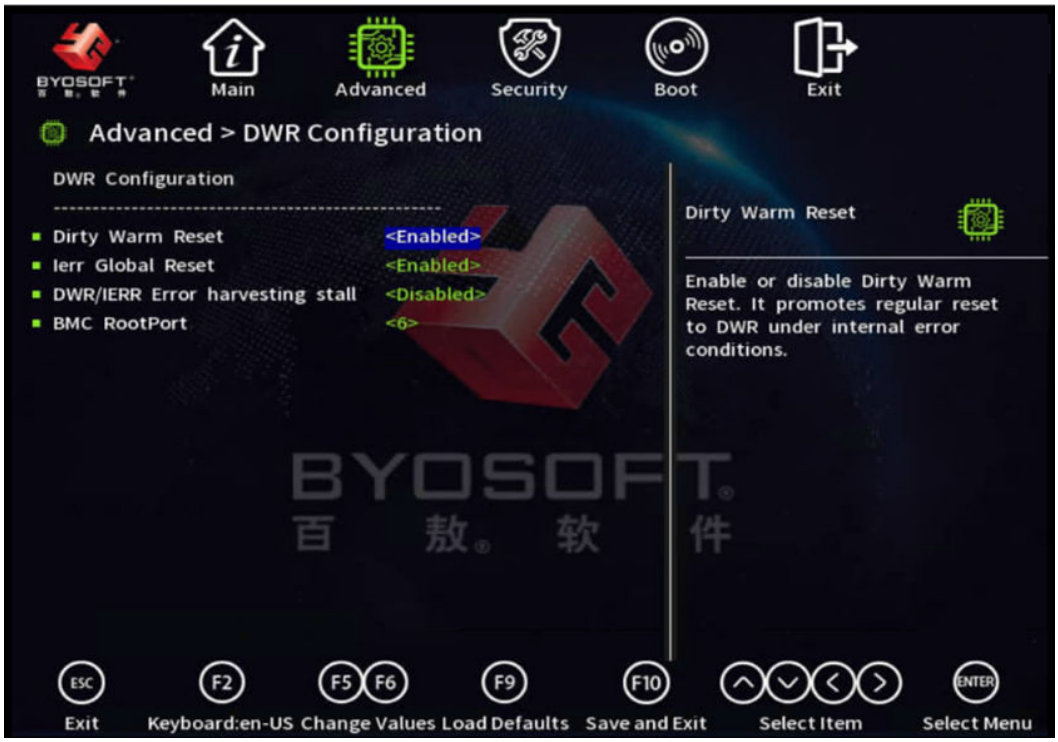


Table 6-85 Parameter on the DWR Configuration screen

Parameter	Description	Default Value
Dirty Warm Reset	Enables or disables DWR. The function promotes regular resets of DWR under internal error conditions. The menu options are as follows: ● Enabled ● Disabled	Enabled
Ierr Global Reset	Enables or disables the IERR global reset. The menu options are as follows: ● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
DWR/IERR Error harvesting stall	Enables or disables the DWR/IERR error harvesting stall. After this function is enabled, if a DWR/IERR error is captured, the system automatically processes the error. After this function is disabled, the system logs the error but does not process it. The menu options are as follows: ● Enabled ● Disabled	Disabled
BMC RootPort	Specifies the root port to which the BMC is connected. The menu options are as follows: ● 6 ● 12	6

6.3 Security

On the **Security** screen  , you can set the trusted platform module (TPM)/trusted cryptography module (TCM) function, the BIOS administrator, or the common user password.

- **Figure 6-93** shows the **Security** screen if no TPM or TCM is installed on the server.
- **Figure 6-94** shows the **Security** screen if a TPM 2.0 is installed on the server.
- **Figure 6-95** shows the **Security** screen if a TCM is installed on the server.

Table 6-86 describes the parameters on the screen.

TPM is a security chip that complies with the TPM specification. It can effectively protect the server and prevent unauthorized users from accessing the server. The TPM specification is formulated by the Trusted Computing Group (TCG).

TCM uses the cryptographic algorithm and engine developed by China to build a security chip.

Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-93 Security screen 1



Figure 6-94 Security screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-95 Security screen 3



Table 6-86 Parameters on the Security screen

Parameter	Description	Default Value
TPM Device	Dynamically displays the detected TPM/TCM device type. If no device is detected, **Not Present** is displayed.	-
TPM State	TPM Status. The menu options are as follows: ● Disabled ● Enabled **NOTE** ● If set to **Disabled**, the system will not respond to any TPM commands, and the status options will be hidden. If set to **Enabled**, you must save your settings and reboot before modifying the following options. ● This parameter is only supported in BIOS versions 01.02.08.09 and later.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TPM2 Active PCR Hash Algorithm	Displays the PCR hash algorithms activated by TPM 2.0. **NOTE** This parameter is available when the TPM 2.0 is installed.	-
TPM2 Hardware Supported Hash Algorithm	Displays the hash algorithms supported by the TPM 2.0 hardware. **NOTE** This parameter is available when the TPM 2.0 is installed.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TPM2 Operation	Dynamically displays the option values in the TPM operation menu. The menu options are as follows: ● **No Action**: No action is required. ● **TPM2 ClearControl(NO) + Clear**: Deletes all TPM contexts associated with a specific owner by running the **ClearControl** and **Clear** commands. ● **TPM2 PCR_Allocate (Algorithm IDs)**: The firmware shall check that each PCR bank supports all requested hash algorithms and must ensure that at least one PCR bank is active. ● **TPM2 ChangeEPS**: Replaces the current endorsement primary seed (EPS) with the value in RNG and sets the endorsement hierarchy control to its default initialization value. ● **TCG2 LogAllDigests**: Queries the TPM to determine which hash algorithms are supported and which PCR banks are currently active, and distributes all supported PCR data. **NOTE** This parameter is available when the TPM 2.0 is installed.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
TCM Enable Status	Displays the enabling status of the TCM. **NOTE** This parameter is available when the TCM is installed.	-
TCM Activated Status	Displays the activation status of the TCM. **NOTE** This parameter is available when the TCM is installed.	-
TCM Owned Status	Specifies the TCM owner status. **NOTE** This parameter is available when the TCM is installed.	-
TCM State	Enables or disables the TCM security device. The menu options are as follows: ● Disable ● Enable **NOTE** ● This parameter is available when the TCM is installed. ● After setting this parameter, restart the OS for the setting to take effect.	Disable

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Pending Operation	Sets the pending operation. The menu options are as follows: ● **None**: No task is to be processed. ● **ACTIVATE**: Activates the TCM. ● **DEACTIVATE**: Deactivates the TCM. ● **TCM Clear**: Clears the TCM. **NOTE** ● This parameter is available when the TCM is installed. ● This parameter can be set when **TCM State** is set to **Enable**.	None
Supervisor Password	Displays the status of the BIOS administrator password. ● **Not Installed**: The password of the BIOS administrator is not set. ● **Installed**: The password of the BIOS administrator has been set.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
User Password	Displays the status of the common BIOS user password. ● **Not Installed**: The password of a common BIOS user is not set. ● **Installed**: The password of a common BIOS user has been set. **NOTE** On the **Setup Utility** screen, a common user can only view menu options, set or change their own password (that is, editing the **Set User Password** option on the **6.3 Security** screen and **Save Changes & Exit** option on the **6.5 Exit** screen). Other options are grayed out and cannot be edited.	-
Delete Password Support	Enables or disables the function of deleting passwords. This parameter can be configured when the BIOS login password is set. The menu options are as follows: ● Enabled ● Disabled	Disabled
Saved password record numbers	Sets the number of historical password groups. The value ranges from 5 to 10. This password cannot be used as a new password. This setting takes effect after you save it.	5

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Set Supervisor Password	Sets the BIOS administrator password. **NOTE** ● The password must contain at least 8 to 16 characters, including at least two types of the following characters: uppercase letters, lowercase letters, and digits, as well as at least one space or one special character. ● Cannot be the same as the latest five passwords and cannot be set to the default password. ● After setting the BIOS administrator password, the **Delete Supervisor Password** parameter is displayed. ● Before changing the BIOS administrator password, you need to enter the current BIOS administrator password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it. ● The default BIOS password is **Admin@9000**. You must change the default password when you log in to the BIOS for the first time.	Admin@9000

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Delete Supervisor Password	Clears the BIOS administrator password that has been set. **NOTE** ● Clearing the BIOS password reduces system security. Exercise caution when performing this operation. ● This parameter is available when the BIOS administrator password has been set and **Delete Password Support** is set to **Enabled**. ● Before clearing the BIOS administrator password, you need to enter the current BIOS administrator password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Set User Password	Sets the common BIOS user password. **NOTE** ● The password must contain at least 8 to 16 characters, including at least two types of the following characters: uppercase letters, lowercase letters, and digits, as well as at least one space or one special character. ● The new password cannot be the same as the latest five passwords. ● After setting the common BIOS user password, the **Delete User Password** parameter is displayed. ● Before changing the BIOS administrator password, you need to enter the current BIOS administrator password or the common user password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it. ● The default BIOS password is **Admin@9000** (administrator password). You are advised to change the default password when you log in to the BIOS for the first time.	-

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Delete User Password	Clears the common BIOS user password that has been set. **NOTE** ● This parameter is available when a common BIOS user password is set and **Delete Password Support** is set to **Enabled**. ● To perform this operation, you need to enter the correct BIOS administrator password or the common user password. If you enter an incorrect password for three consecutive times, the server will be locked. You can restart the server to unlock it.	-
Power On Password	Enables or disables the power-on password. The menu options are as follows: ● **Enabled**: A password is required for power-on. ● **Disabled**: No password is required for power-on.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Simple Password	Enables or disables the simple password function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● After the simple password function is enabled, the password complexity is not verified. The password must contain 8 to 16 characters. ● Enabling the simple password function reduces system security. Exercise caution when enabling this function.	Disabled
Password Expiration Day	Sets the password expiration time. The menu options are as follows: ● 0 day ● 30 days ● 60 days ● 90 days ● 180 days ● 360 days **NOTE** **0 day** means that the password never expires.	180days
Weak Password Dictionary	Displays the list of weak passwords. You can add or delete password strings on this screen. There are 25 weak passwords by default.	-
TLS Certificate Manager	Provides access to TLS authentication configurations.	-

6.3.1 Weak Password Dictionary

On the screen, you can add or delete password strings. **Figure 6-96** shows the **Weak Password Dictionary** screen. **Table 6-87** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-96 Weak Password Dictionary screen



Table 6-87 Parameters on the Weak Password Dictionary screen

Parameter	Description
Add Weak Password	Enters the password string to be added to the weak password dictionary. **NOTE** • Strings in the weak password dictionary cannot be used as passwords. • A maximum of 100 password strings can be set.
Remove Weak Password	Enters the password string to be removed from the weak password dictionary. After the password string is removed, you can use this string as a password.
Weak Password List	Displays weak passwords that have been added. When there is no weak password, no content is displayed.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.3.2 TLS Certificate Manager

On the **TLS Certificate Manager** screen, you can manage server certificates, such as importing and deleting certificates. **Figure 6-97** shows the **TLS Certificate Manager** screen. **Table 6-88** describes the parameters.

Figure 6-97 TLS Certificate Manager screen



Table 6-88 Parameters on the TLS Certificate Manager screen

Parameter	Description
CA Manager	Manages server certificates.
CRL Manager	Manages the server certificate revocation list (CRL).
Client Cert Configuration	Provides access to client certificate configurations. **NOTE** This menu is not supported currently. The parameter is grayed and cannot be edited.

6.3.2.1 CA Manager

On the **CA Manager** screen, you can import or delete certificates. **Figure 6-98** shows the **CA Manager** screen. **Table 6-89** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-98 CA Manager screen



Table 6-89 Parameters on the CA Manager screen

Parameter	Description
Import Certificate	Imports certificates. Import a certificate (example): 1. Use the storage medium to place the certificate in the root directory of the server. 2. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **CA Manager** > **Import Certificate** > **Eroll Cert Using File**. 3. Select **xFusion.cer**, press **Enter**, and select **Yes**. 4. Select **Delete Certificate** to enter the certificate deletion screen. If the certificate information is displayed, the certificate is imported successfully. **NOTE** • Certificates can be imported only in UEFI mode. • Only certificates with the DER code in FAT16/FAT32 format are supported.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Delete Certificate	Deletes certificates. Select the certificate and press **Enter** to enter screen for deleting a certificate. Delete a certificate (example): 1. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **CA Manager** > **Delete Certificate**. 2. Select **xFusion.cer**, **press Enter**, and select **Yes**. 3. If no certificate information is displayed on the certificate deletion screen, the certificate is deleted successfully.

6.3.2.1.1 Import Certificate

Figure 6-99 shows the **Import Certificate** screen. **Table 6-90** describes the parameters.

Figure 6-99 Import Certificate screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-90 Parameters on the Import Certificate screen

Parameter	Description
Eroll Cert Using File	Uses the file to register the certificate. Select the file and press **Enter**. Select a proper file to register the certificate.
Cert GUID	Enters the GUID of the certificate in the format.
Commit Changes and Exit	Commits your changes and exits the menu.
Discard Changes and Exit	Exits the menu without saving the file.

Figure 6-100 shows the **Eroll Cert Using File** screen.

NOTE

The information displayed on the screen varies depending on the configuration of the server. If no file is identified, no content is displayed on the screen.

Figure 6-100 Eroll Cert Using File screen



6.3.2.1.2 Delete Certificate

Figure 6-101 or **Figure 6-102** shows the **Delete Certificate** screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

NOTE

If certificates exist, the certificate list is automatically displayed on this screen. If no certificate exists, no content is displayed on this screen.

Figure 6-101 Delete Certificate screen 1



Figure 6-102 Delete Certificate screen 2



6.3.2.2 CRL Manager

On the **CRL Manager** screen, you can import or delete certificates. **Figure 6-103** shows the **CRL Manager** screen. **Table 6-91** describes parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-103 CRL Manager screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-91 Parameters on the CRL Manager screen

Parameter	Description
Import Cert Revocation List	Import the CRL. Import a certificate (example): 1. Use the storage medium to place the certificate in the root directory of the server. 2. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **CRL Manager** > **Import Cert Revocation List** > **Eroll Cert Using File**. 3. Select **xFusion.cer**, press **Enter**, and select **Yes**. 4. Select **Delete Cert Revocation List** to enter the certificate deletion screen. If the certificate information is displayed, the certificate is imported successfully. **NOTE** • Certificates can be imported only in UEFI mode. • Only certificates with the DER code in FAT16/FAT32 format are supported.
Delete Cert Revocation List	Deletes the CRL. Select a CRL and press **Enter** to enter the screen for deleting a CRL. Delete a certificate (example): 1. Enter the BIOS and choose **Security** > **TLS Certificate Manager** > **CRL Manager** > **Delete Cert Revocation List**. 2. Select **xFusion.cer**, **press Enter**, and select **Yes**. 3. If no certificate information is displayed on the certificate deletion screen, the certificate is deleted successfully.

6.3.2.2.1 Import Cert Revocation List

Figure 6-104 shows the **Import Cert Revocation List** screen. **Table 6-92** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-104 Import Cert Revocation List screen



Table 6-92 Parameters on the Import Cert Revocation List screen

Parameter	Description
Eroll Cert Using File	Uses the file to register the certificate. Select the file and press **Enter**. Select a proper file to register the certificate.
Cert GUID	Enters the GUID of the certificate in the format.
Commit Changes and Exit	Commits your changes and exits the menu.
Discard Changes and Exit	Exits the menu without saving the file.

Figure 6-105 shows the **Eroll Cert Using File** screen.

NOTE

The information displayed on the screen varies depending on the configuration of the server. If no file is identified, no content is displayed on the screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-105 Eroll Cert Using File screen



6.3.2.2.2 Delete Cert Revocation List

Figure 6-106 or Figure 6-107 shows the **Delete Cert Revocation List** screen.

NOTE

If certificates exist, the certificate list is automatically displayed on this screen. If no certificate exists, no content is displayed on this screen.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-106 Delete Cert Revocation List screen 1



Figure 6-107 Delete Cert Revocation List screen 2



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

6.4 Boot

On the **Boot** screen , you can set the boot mode, boot method, and boot device of the server. **Figure 6-108** and **Figure 6-109** show the **Boot** screen. **Table 6-93** describes the parameters.

Figure 6-108 Boot screen (UEFI mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-109 Boot screen (legacy mode)



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-93 Parameters on the Boot screen

Parameter	Description	Default Value
Boot Type	Set the boot mode of the system. The menu options are as follows: ● LegacyBoot ● UEFIBoot	UEFIBoot

Parameter	Description	Default Value
	NOTE ● If the OS has been installed in Legacy or UEFI mode on the server, you cannot access the OS after switching the boot mode. You need to switch to the boot mode selected during installation. Only the ESXi OS supports normal boot after switching between Legacy and UEFI modes. If the OS needs to be reinstalled, select the UEFI or legacy mode. ● For some OSs, if the capacity of the drive or the RAID array for installing the OS is greater than 2 TB, set **Boot Type** to **UEFI Boot**. For details, see the release notes of the OS. ● If the OS is to be installed on an NVMe drive, you can set **Boot Type** to only **UEFI Boot**. ● In legacy mode, the Option ROM uses a fixed 128 KB memory address space. When a large number of devices are configured on the server, some devices in legacy mode may not have sufficient Option ROM space. As a result, the device functions are abnormal. For example, the OS cannot be booted on the RAID, the NIC fails to be started in PXE mode, or the GPU cannot be properly displayed. Based on this limitation, it is highly recommended that the UEFI mode be used. If the legacy mode is required, you are advised to disable the serial port redirection or NIC PXE function based on the actual service scenario to ensure that [illegible] properly started. For details, see **3.2.12 Setting PXE for a NIC** and **3.2.20 Setting Serial Port Redirection**.	

Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
OEM Fast Boot	Enables or disables the OEM fast boot function. The menu options are as follows: ● Enabled ● Disabled	Disabled
Boot Fail Policy	Selects the operation to be performed after the boot fails. The menu options are as follows: ● **Boot Retry**: Attempts to reboot. ● **Cold Boot**: Cold boot. ● **None**: No operation is performed.	Boot Retry
PXE Retry Count	Sets the times of repeated boots from the PXE. The value ranges from 1 to 99. ● **99** indicates that the PXE is repeatedly booted. ● The values 1 to 98 indicate the times of repeated boots from the PXE. When the repeated boot times reaches the set value, the BIOS automatically attempts to boot from another bootable device. **NOTE** This parameter is unavailable when **Boot Fail Policy** is set to **Cold Boot** or **None**.	1
PXE Boot to LAN	Enables or disables the PXE boot function of the LAN. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is supported only in legacy mode.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PXE Timeout Control	Sets the number of DHCP connection timeout retries during the PXE boot. The menu options are as follows: ● Disabled ● 1 ● 2 ● 3 ● 4 **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is unavailable when **Network Stack** is set to **Disabled**. ● When this parameter is set to **1**, **2**, **3**, or **4**, the maximum duration is 4s, 12s, 28s, or 60s respectively. If this parameter is set as **Disabled**, the maximum duration is 60s by default.	Disabled
Network Stack	Enables or disables the network stack function. The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is supported only in UEFI mode.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
PXE Boot Capability	Sets the PXE boot network. The menu options are as follows: ● UEFI:IPv4 ● UEFI:IPv6 ● UEFI:IPv4/IPv6 ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is unavailable when **Network Stack** is set to **Disabled**.	UEFI:IPv4
IPv4 PXE	Enables or disables the IPv4 PXE function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled** and **PXE Boot Capability** is set to **UEFI:IPv4** or **UEFI:IPv4/IPv6**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
IPv6 PXE	Enables or disables the IPv6 PXE function. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is available when **Network Stack** is set to **Enabled** and **PXE Boot Capability** is set to **UEFI:IPv6** or **UEFI:IPv4/IPv6**.	Disabled
HTTPS Boot Capability	Selects the HTTPS boot function. The menu options are as follows: ● HTTPS:IPv4 ● HTTPS:IPv6 ● HTTPS:IPv4/IPv6 ● Disabled **NOTE** ● This parameter is supported only in UEFI mode. ● This parameter is unavailable when **Network Stack** is set to **Disabled**.	HTTPS:IPv4

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Boot Override	Sets the first priority boot device. The menu options are as follows: ● **Disabled**: Disables this function. ● **PCIE SSD First**: PCIe SSD as priority. ● **iSCSI First**: iSCSI as priority. ● **FC First**: Fiber Channel as priority. ● **FCOE First**: Fibre Channel over Ethernet as priority. ● **PCH Direct First**: PCH pass-through device as priority. ● **RAID First**: RAID as priority. ● **USB First**: USB as priority. ● **Local Disk Boot Only**: Local drive as priority. **NOTE** After this option is set, the system starts from the boot device set in **Boot Override**. If the boot fails, the system starts according to the boot sequence set in **Boot Sequence**.	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
USB Boot	Enables or disables the boot function of the external USB device. The menu options are as follows: ● **Enabled**: allows booting from external USB devices (such as virtual a CD-ROM drive, a floppy drive, and a physical USB CD-ROM drive). ● **Disabled**: It is forbidden to boot from external USB devices (such as a virtual CD-ROM drive, a floppy drive, and a physical USB CD-ROM drive).	Enabled
SP Boot	Enables or disables the boot function of the smart deployment tool Smart Provisioning (SP). The menu options are as follows: ● Enabled ● Disabled **NOTE** This parameter is grayed out and cannot be edited when **USB Boot** is set to **Disabled**.	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Sync Order	Enables or disables the synchronization sequence function. The menu options are as follows: • **Disabled**: invalid. • **Sync Boot Order**: Synchronizes the boot sequence on the **Setup Utility** screen to the boot list on the **Boot Manager** screen. • **Sync Boot Device Type Order**: Synchronizes the boot list on the **Boot Manager** screen to the boot sequence on the **Setup Utility** screen. **NOTE** This parameter is supported only in UEFI mode.	Disabled
Boot Sequence	Sets the boot sequence of the system boot items.	-
UEFI	Sets the boot devices in UEFI mode. **NOTE** This parameter is supported only in UEFI mode.	-
Legacy	Sets the boot devices in legacy mode. **NOTE** This parameter is supported only in legacy mode.	-

6.4.1 Boot Sequence

On the **Boot Sequence** screen, you can set the boot sequence of the system boot options. Figure 6-110 shows the **Boot Sequence** screen. Table 6-94 describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-110 Boot Sequence screen



NOTE

- Press the ↑ and ↓ keys to select the boot device.
- Press **F5** (move down)/**F6** (move up) to change the boot sequence.
- The default boot sequence is **Hard Disk Drive** > **DVD-ROM Drive** > **PXE** > **Others**.

Table 6-94 Parameters on the Boot Sequence screen

Parameter	Description	Default Value
Hard Disk Drive	Change Hard Disk Drive boot order. The menu options are as follows: ● Disabled ● Enabled	Enabled
DVD-ROM Drive	Change DVD-ROM Drive boot order. The menu options are as follows: ● Disabled ● Enabled	Enabled
PXE	Change PXE boot order. The menu options are as follows: ● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description	Default Value
Others	Change Other Device boot order. The menu options are as follows: • Disabled • Enabled	Enabled

6.4.2 UEFI/Legacy

NOTE

If **Boot Type** is set to **UEFI**, **UEFI** is displayed. If **Boot Type** is set to **Legacy**, **Legacy** is displayed.

On the **UEFI/Legacy** screen, you can set the boot device of the system. **Figure 6-111** shows the **UEFI/Legacy** screen. **Table 6-95** describes the parameters.

NOTE

If the server does not have boot devices such as drives, NICs, CD/DVD-ROM drives, or images, the **UEFI** or **Legacy** screen does not display the corresponding boot items. The boot items displayed on the screen are subject to the actual situation.

Figure 6-111 UEFI Boot/Legacy Boot screen



 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Table 6-95 Parameters on the UEFI Boot/Legacy Boot screen

Parameter	Description
HDD Device	Sets the drive boot devices. **NOTE** • Press the ↑ and ↑ keys to select the boot device. • Press **F5** (move down)/**F6** (move up) to change the boot sequence.
DVD-ROM Device	Sets the DVD-ROM boot devices. **NOTE** • Press the ↑ and ↑ keys to select the boot device. • Press **F5** (move down)/**F6** (move up) to change the boot sequence.
PXE Device	Sets the PXE boot devices. **NOTE** • Press the ↑ and ↑ keys to select the boot device. • Press **F5** (move down)/**F6** (move up) to change the boot sequence.
Other Device	Sets other boot devices. **NOTE** • Press the ↑ and ↑ keys to select the boot device. • Press **F5** (move down)/**F6** (move up) to change the boot sequence.

6.5 Exit

On the **Exit** screen , you can control the function of saving and exiting after BIOS parameters modification. **Figure 6-112** shows the **Exit** screen. **Table 6-96** describes the parameters.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Figure 6-112 Exit screen



Table 6-96 Parameters on the Exit screen

Parameter	Description
Save Changes & Exit	Saves all the modifications and exits the BIOS. **NOTE** You can also press **F10** to save the changes and exit the BIOS.
Save Changes Without Exiting	Saves all the modifications without exiting the BIOS.
Discard Changes & Exit	Discards all the modifications and exits the BIOS.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Description
Load Factory Defaults	Restores factory default values. **NOTE** ● Except for the following information that cannot be restored, the other BIOS parameters will be restored to default values of the current BIOS version. Modify related parameters again if the service requires special configurations on the BIOS parameters. ● Date and time information on the **Main** screen ● BIOS password and BIOS startup logo ● All parameters (except watchdog-related parameters) on the **BMC Configuration** screen under the **Advanced** screen ● All parameters on the **Device Manager** and **Administer Secure Boot** screens in UEFI mode ● Press **F9** to restore factory settings or custom settings.
Discard Changes Without Exiting	Discards the modification.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

A FAQ

A.1 Restrictions on Boot Devices in Legacy Mode

NOTE

Boot devices are divided into four types: HDD (RAID belongs to this type), PXE, CD-DVD (DVD-ROM drive), and others (floppy drive and others).

In legacy real mode, the available memory space is only 1 MB, and the 1 MB space is divided into different address spaces according to functions. In the specific implementation of the product, the legacy Bootable can obtain only less than 4 KB memory space. This limits the number of boot devices.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

B Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Main				
Language	Language	Sets the language of the current BIOS.	• en-US • ja-JP • zh-CN	en-US

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Time Zone	TimeZone	Sets the time zone of system time. **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	• UTC-12:00 • UTC-11:00 • UTC-10:00 • UTC-09:30 • UTC-09:00 • UTC-08:00 • UTC-07:00 • UTC-06:00 • UTC-05:00 • UTC-04:00 • UTC-03:30 • UTC-03:00 • UTC-02:30 • UTC-02:00 • UTC-01:00 • UTC+00:00 • UTC+01:00 • UTC+02:00 • UTC+03:00 • UTC+03:30 • UTC+04:00 • UTC+04:30 • UTC+05:00 • UTC+05:30 • UTC+05:45 • UTC+06:00 • UTC+06:30 • UTC+07:00 • UTC+08:00 • UTC+08:45 • UTC+09:00 • UTC+09:30 • UTC+10:00 • UTC+10:30 • UTC+11:00 • UTC+12:00 • UTC+12:45 • UTC+13:00	UTC+00:00

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
			• UTC+13:45 • UTC+14:00	
Daylight Saving Time	Daylight	Enables or disables the daylight saving time of system time. **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	• Disabled • Enabled	Disabled
Synchronize Time Zone With BMC	SyncTimeZoneWithBmc	Enables or disables the synchronize the system time zone from BMC at boot time, and set the BMC time zone when the system time zone is changed by user. **NOTE** Only BIOS 01.01.08.03 and later versions support this parameter.	• Disabled • Enabled	Disabled
./Advanced/Peripheral Configuration/SR-IOV Setup Settings				
PCIe SR-IOV	SriovEnablePolicy	Sets the SR-IOV function of the PCIe card.	• Disabled • Enabled • Per IIO Port	Enabled
CPU1 Port 1A	SriovEnable1	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU1 Port 1E	SriovEnable5	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 2A	SriovEnable9	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 3A	SriovEnable17	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4A	SriovEnable25	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4E	SriovEnable29	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 5A	SriovEnable33	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 5E	SriovEnable37	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 1A	SriovEnable58	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU2 Port 1E	SriovEnable62	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 2A	SriovEnable66	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 3A	SriovEnable74	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 3E	SriovEnable78	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 4A	SriovEnable82	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 4C	SriovEnable84	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 4E	SriovEnable86	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 4G	SriovEnable88	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU2 Port 5A	SriovEnable90	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5E	SriovEnable94	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
./Advanced/Peripheral Configuration				
PCIe ARI	ARIEnable	Enables or disables ARI of the PCIe card.	• Disabled • Enabled	Disabled
PCIe ASPM Support (Global)	PcieAspmControl	Sets the PCIe ASPM Support (Global) function.	• Disabled • Per individual port • L1 Only	Disabled
Degrade 64-bit PCI MMIO BARs	DegradeResource	Enables or disables the 64-bit PCI MMIO BARs function.	• Disabled • Enabled	Disabled
./Advanced/Peripheral Configuration/SIO 1711				
UART 1	Uart1Enable	Enables or disables the BMC serial port function.	• Disabled • Enabled	Enabled
Base I/O Address	Uart1IoAddress	Sets the base address of the BMC serial port.	• 3F8 • 2F8	3F8
./Advanced/Video Configuration				
Display Mode	DisPlayMode	Sets the video card mode.	• On Board Graphics • Plug-in Graphics	On Board Graphics
./Advanced/ACPI Table or Features Control				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SPCR Table Support	ACPISpcr	Enables or disables the SPCR table function.	• Disabled • Enabled	Enabled
Windows SOL Input	WinSolWA	Enables or disables redirection input of the serial port in the Windows OS.	• Disabled • Enabled	Disabled
./Advanced/Misc Configuration				
System Debug Level	SysDbgLevel	Enables or disables the system debug level.	• Disabled • Enabled	Disabled
CDN Support	CdnSupport	Enables or disables the function of CDN.	• Disabled • Enabled	Enabled
IPMI Device Control	IpmiDevControl	Enables or disables ACPI reporting on the IPMI device.	• Disabled • Enabled	Disabled
Wake on PME	WakeOnPME	Enables or disables the PME function.	• Disabled • Enabled	Disabled
Power Button Invalid	PowerButtonInvalid	Enables or disables the function of powering off the server through the power button, which does not affect Forced Power Off (Power Button Override Function).	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Power Supply Module Customize	PwrModulePartnum	Enables or disables the display of the power supply model in the power supply module part number.	• Disabled • Enabled	Disabled
Kernel Black Box	BlackBoxEn	Enables or disables the kernel black box. **NOTE** This function is supported only in FusionOS.	• Disabled • Enabled	Disabled
Memory SN Customization	MemorySNCustomize	Enables or disables the memory serial number customization function. **NOTE** Only BIOS 01.01.08.03 and later versions support this parameter.	• Disabled • Enabled	Disabled
Re-Size BAR Support	PcieResizableBarSupport	Enables or disables the PCIe resizable BAR capability supported. **NOTE** Only BIOS 01.01.08.08 and later versions support this parameter.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
BAR Size	PcieResizableBarSize	Choose the BAR size for the PCIe device. **Auto** means max of Re-size BAR supported each PCIe Device. This option will not take effect if the PCIe card does not support the Resizable BAR feature. **NOTE** ● This parameter is available when **Re-Size BAR Support** is set to **Enabled**. ● Only BIOS 01.01.08.08 and later versions support this parameter.	● Auto ● 8G ● 16G ● 32G ● 64G	Auto
./Advanced/System Event Log				
System Errors	SystemErrorEn	Sets the function of recording system errors.	● Disabled ● Enabled ● Auto	Enabled
System Memory Poisoning	PoisonEn	Enables or disables the memory poisoning function.	● Disabled ● Enabled	Enabled
FDM	FDMSupport	Enables or disables the FDM function.	● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CE Record	CeReportToOs	Enables or disables the CE record.	• Disabled • Enabled	Disabled
Memory CE Record	MemoryCeReport	Enables or disables the memory CE record. **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	• Enabled • Disabled	Enabled
PCIe CE Record	PcieCeReport	Enables or disables the PCIe CE record. **NOTE** Only BIOS 01.01.06.13 and later versions support this parameter.	• Enabled • Disabled	Enabled
Error Data Revison	ErrorDataRevison	Sets the compatible error data version.	• 0x201 • 0x300	0x201
System Cloaking	CloakingEn	Enables or disables the system cloaking function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Disabled
./Advanced/System Event Log/eMCA Settings				
eMCA Logging Support	EmcaEn	Enables or disables the eMCA logging function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
eMCA CMCI-SMI Morphing	EmcaCsmiEn	Enables or disables the eMCA CMCI-SMI mapping.	• Disabled • eMCA Gen 2 CSMI	eMCA Gen 2 CSMI
./Advanced/System Event Log/WHEA Settings				
WHEA Support	WheaSupportEn	Enables or disables the WHEA function.	• Disabled • Enabled	Enabled
WHEA Log Memory Error	WheaLogMemoryEn	Enables or disables the WHEA log memory error function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Enabled
WHEA Log Processor Error	WheaLogProcEn	Enables or disables the WHEA log processor error function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Enabled
WHEA Log PCI Error	WheaLogPciEn	Enables or disables the WHEA log PCI error function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Enabled
./Advanced/System Event Log/Error Injection Settings				

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
ME Seg Error Injection Support	MeSegErrorInjEn	Enables or disables the ME Seg error injection support function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Disabled
./Advanced/System Event Log/IIO Error Enabling				
OS Native AER Support	OsNativeAerSupport	Enables or disables the AER function controlled by the OS.Enables or disables the AER function controlled by the OS.	• Disabled • Enabled	Disabled
IIO MCA Support	IoMcaEn	Enables or disables the I/O MCA support function.	• Disabled • Enabled	Disabled
IIO eDPC Support	EdpcEn	Sets the I/O eDPC support function.	• Disabled • Enabled • On Fatal and Non-Fatal Errors	Disabled
IIO eDPC Interrupt	EdpcInterrupt	Enables or disables the I/O eDPC interrupt function.	• Disabled • Enabled	Disabled **NOTE** For BIOS versions earlier than 01.01.06.03 it is **Enabled** by default.

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO eDPC ERR_COR Message	EdpcErrCorMsg	Enables or disables the I/O eDPC ERR_COR function.	• Disabled • Enabled	Enabled
PCIe Error	PcieErrEn	Enables or disables PCIe error detection.	• Disabled • Enabled	Enabled
./Advanced/System Event Log/PCIe Error Enabling				
Corrected Error	PcieCorrErrEn	Enables or disables the PCIe correctable error detection.	• Disabled • Enabled	Enabled
Uncorrected Error	PcieUncorrErrEn	Enables or disables the PCIe uncorrectable error detection.	• Disabled • Enabled	Enabled
Fatal Error	PcieFatalErrEn	Enables or disables the PCIe fatal error detection.	• Disabled • Enabled	Enabled
PCIe Corrected Error Threshold Counter	PcieCorErrCntr	Enables or disables the PCIe correction error threshold counter.	• Disabled • Enabled	Disabled
PCIe Corrected Error Threshold	PcieCorErrThres	Sets the PCIe correction error threshold.	0 to 0xffffffff	1
PCIe Surprise Link Down Error	PcieAerSurpriseLinkDownEn	Enables or disables unexpected PCIe link disconnection.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Processor Configuration/Per-Socket Information				
Active Processor Cores	ProcessorActiveCore	Sets the number of physical cores for each CPU to be used.	• All • 1 • 2 to *N-1* **NOTE** *N* indicates the maximum number of physical CPU cores supported by the CPU.	All
Enable LP [Global]	ProcessorHyperThreadingDisable	Enables or disables the hyper-threading function of the Intel processor.	• Single LP • ALL LPs	ALL LPs
Hardware Prefetcher	MlcStreamerPrefetcherEnable	Enables or disables the hardware prefetcher function.	• Disabled • Enabled	Enabled
Adjacent Cache Prefetch	MlcSpatialPrefetcherEnable	Enables or disables the adjacent cache prefetch function.	• Disabled • Enabled	Enabled
DCU Streamer Prefetcher	DCUStreamerPrefetcherEnable	Enables or disables the DCU streamer prefetching function.	• Disabled • Enabled	Enabled
DCU IP Prefetcher	DCUIPPrefetcherEnable	Enables or disables the DCU IP prefetching function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
LLC Prefetch	LlcPrefetchEnable	Enables or disables the L3 cache prefetch feature.	• Disabled • Enabled	Enabled
Homeless Prefetch	HomelessPrefetchEnable	Enables or disables Homeless Prefetch on all threads.	• Disabled • Enabled • Auto	Auto
Extended APIC	ProcessorX2apic	Enables or disables the extended APIC feature.	• Disabled • Enabled	Enabled
Intel(R) TXT	ProcessorLtsxEnable	Enables or disables the Intel(R) TXT function.	• Disabled • Enabled	Disabled
VMX	ProcessorVmxEnable	Enables or disables CPU virtualization technology. **NOTE** This function takes effect after the server restart.	• Disabled • Enabled	Enabled
Enable SMX	ProcessorSmxEnable	Enables or disables the SMX function. **NOTE** • This parameter is unavailable when **Intel(R) TXT** is set to **Enabled**. • Only BIOS 01.01.03.13 and later versions support this parameter.	• Disabled • Enabled	Enabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
APIC number in MADT	AcpiApicReport	Sets whether the number of local APICs or X2APICs that are physically enabled is reported or the maximum number of supported local APICs or X2APICs is reported in the MADT.	• Physical • Maximum	Physical
Memory Encryption (TME)	EnableTme	Enables or disables the TME.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Memory integrity	EnableGlobalIntegrity	Enables or disables the TME-MT integrity function.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
		NOTE ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable under the following conditions: ● The CPU model is Emerald Rapids. ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC. ● **Memory Encryption (TME)** is set to **Enabled**. ● **Limit CPU PA to 46 bits** is set to **Disabled** in the **Socket Configuration > Uncore Configuration > Uncore General Configuration**		

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Trust Domain Extension (TDX)	EnableTdx	Enables or disables the Trust Domain Extension (TDX) function. **NOTE** ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable under the following conditions: ● The CPU model is Emerald Rapids. ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC. ● **Total Memory Encryption Multi-Tenant (TME-MT)** is set to **Enabled**.	● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
TDX Secure Arbitration Mode Loader (SEAM Loader)	EnableTdxSeamldr	Enables or disables the TDX Secure Arbitration Mode Loader (SEAM Loader) function.	• Disabled • Enabled	Disabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
		NOTE ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable under the following conditions: ● The CPU model is Emerald Rapids. ● The memory insertion method is 1DPC (DIMM Per Channel) or 2DPC. ● **Total Memory Encryption Multi-Tenant (TME-MT)** is set to **Enabled**.		

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Disable excluding Mem below 1MB in CMR	DfxTdxDisable1MbCmrExclude	Enables or disables the function to include memory region below 1 MB in the CMR. **NOTE** ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable when **Trust Domain Extension (TDX)** is set to **Enabled**.	● Disabled ● Enabled ● Auto	Auto

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
TME-MT/TDX key split	KeySplit	Sets the number of bits used by TDX in the TME-MT/TDX key split, and the rest of bits will be used by TME-MT. **NOTE** ● Only BIOS 01.01.03.16 and later versions support this parameter. ● This parameter is configurable when **Trust Domain Extension (TDX)** is set to **Enabled**.	1 to 7	1
./Advanced/Socket Configuration/Processor Configuration/In Field Scan (IFS)				
Enable SAF	EnableSaf	Enables or disables the SAF function.	● Disabled ● Enabled	Disabled
./Advanced/Socket Configuration/Common RefCode Configuration				
NUMA	NumaEn	Enables or disables the NUMA architecture of the system.	● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
UMA-Based Clustering	UmaBasedClustering	Sets the UMA-Based Clustering function. **NOTE** The setting of this function is valid only when SNC is disabled. If SNC is enabled, the BIOS automatically disables the UMA-based cluster.	• Disable (All2All) • Hemisphere (2-clusters) • Quadrant (4-clusters)	Quadrant (4-clusters)
./Advanced/Socket Configuration/Uncore Configuration/Uncore General Configuration				
Link Speed Mode	QpiLinkSpeedMode	Sets the UPI link speed mode. **NOTE** Only BIOS 01.01.06.08 and later versions support this parameter.	• Slow • Fast	Fast
Link Frequency Select	QpiLinkSpeed	Sets the UPI link frequency.	• 12.8GT/s • 14.4GT/s • 16GT/s • 20GT/s • Auto • Use Per Link Setting	Auto
Link L0p Enable	KtiLinkL0pEn	Sets the UPI energy saving option.	• Disabled • Enabled • Auto • Full L0p Enable	Auto
Link L1 Enable	KtiLinkL1En	Sets the UPI energy saving option.	• Disabled • Enabled • Auto	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
KTI Prefetch	KtiPrefetchEn	Sets the KTI prefetch function.	• Disabled • Enabled • Auto	Enabled
SNC	SncEn	Sets the SNC function.	• AUTO • Disabled • Enable SNC2 (2-clusters) • Enable SNC4 (4-clusters)	Disabled
Stale AtoS	StaleAtoSOptEn	Enables or disables the switching between the SnoopAll (A) state and the Shared (S) state of the memory.	• Disabled • Enabled • Auto	Auto
MMIO High Base	MmiohBase	Sets the high base address of the MMIO.	• 56T • 40T • 32T • 24T • 16T • 13T • 4T • 3.5T • 2T • 1T • 512G	13T
MMIO High Granularity Size	MmiohSize	Sets the I/O high base granularity size.	• 1G • 4G • 16G • 64G • 256G • 1024G	64G

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Limit CPU PA to 46 bits	CpuPaLimit	Enables or disables the limit on the CPU physical address to 46 bits to support earlier versions of Hyper-V.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Memory Configuration				
Memory Turbo	EnforceDdrMemoryFreqPor	Enables or disables memory overclocking.	• Disabled • Enabled	Disabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Memory Frequency	DdrFreqLimit	Sets the DDR frequency in MT/s.	The CPU type is SPR: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 The CPU type is EMR: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 ● 5200 ● 5600 **NOTE** ● When **Memory Turbo** is set to **Enabled**, this parameter is grayed out. ● Only BIOS version 01.01.03.05 and later supports EMR CPUs.	Auto
SPD CRC Check	spdCrcCheck	Enables or disables the SPD CRC function.	● Disabled ● Enabled	Enabled
Attempt Fast Boot	AttemptFastBoot	Enables or disables the fast boot function.	● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Attempt Fast Cold Boot	AttemptFastBootCold	Enables or disables the fast cold boot function.	• Disabled • Enabled	Enabled
Custom Refresh	CustomRefreshRateEn	Enables or disables the custom refresh function.	• Disabled • Enabled	Disabled
Custom Refresh Rate	CustomRefreshRate	Sets the custom memory refresh rate.	20 to 40	20
Refresh Options	refreshMode	Sets the memory self-refresh frequency mode.	• Dynamic Mode • Static 2x Mode	Dynamic Mode
./Advanced/Socket Configuration/Memory Configuration/Memory Channel Control				
CPU 1 Channel A Control	TotalChannel0	Enables or disables memory channel A of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel B Control	TotalChannel1	Enables or disables memory channel B of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel C Control	TotalChannel2	Enables or disables memory channel C of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel D Control	TotalChannel3	Enables or disables memory channel D of CPU 1.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 1 Channel E Control	TotalChannel4	Enables or disables memory channel E of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel F Control	TotalChannel5	Enables or disables memory channel F of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel G Control	TotalChannel6	Enables or disables memory channel G of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel H Control	TotalChannel7	Enables or disables memory channel H of CPU 1.	• Disabled • Enabled	Enabled
CPU 2 Channel A Control	TotalChannel8	Enables or disables memory channel A of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel B Control	TotalChannel9	Enables or disables memory channel B of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel C Control	TotalChannel10	Enables or disables memory channel C of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel D Control	TotalChannel11	Enables or disables memory channel D of CPU 2.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 2 Channel E Control	TotalChannel12	Enables or disables memory channel E of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel F Control	TotalChannel13	Enables or disables memory channel F of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel G Control	TotalChannel14	Enables or disables memory channel G of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel H Control	TotalChannel15	Enables or disables memory channel H of CPU 2.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Memory Configuration/Page Policy				
Page Policy	PagePolicy	Sets the page management policy.	• Closed • Adaptive	Closed
./Advanced/Socket Configuration/Memory Configuration/Memory Map				
Volatile Memory Mode	volMemMode	Enables the 1LM or 2LM memory mode.	• 1LM • 2LM	1LM
./Advanced/Socket Configuration/Memory Configuration/Memory RAS Configuration				
Mirror Mode	MirrorMode	Sets the memory mirroring mode.	• Disabled • Full Mirror Mode • Partial Mirror Mode	Disabled
UEFI ARM Mirror	PartialMirrorUefi	Enables or disables the UEFI ARM mirroring mode.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
ARM Mirror percentage	PartialMirrorUefiPercent	Sets the ARM image percentage. 1275 represents 12.75%.	0 to 5000	0
Correctable Error Threshold	spareErrTh	Sets the correctable error threshold.	1 to 0x7FFF	0x1770
Leaky Bucket Time Window Based Interface	leakyBktTimeWindow	Enables or disables the interface based on the leaky bucket time window.	• Disabled • Enabled	Disabled
Leaky Bucket Low Bit	leakyBktLo	Sets the low bit of the leaky bucket.	0x1 to 0x29	0x10
Leaky Bucket High Bit	leakyBktHi	Sets the high bit of the leaky bucket.	0x1 to 0x29	0x11
Leaky Bucket Time Window Based Interface Hour	leakyBktHour	Sets the leaky bucket time window based on hour.	0 to 3744	24
Leaky Bucket Time Window Based Interface Minute	leakyBktMinute	Sets the leaky bucket time window based on minute.	0 to 60	0
Partial Cache Line Sparing PCLS	PclsEn	Enables or disables the partial cache line sparing (PCLS).	• Disabled • Enabled	Enabled
ADDDC Sparing	ADDDCEn	Enables or disables the ADDDC reservation function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Enable ADDDC Error Injection	AdddcErrInjEn	Enables or disables the ADDDC error injection function. **NOTE** BIOS 01.01.03.06 and later versions support this parameter.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Memory Configuration/PMem Configuration/PMem Secure Erase Unit				
Erase All DIMMs	setSecureEraseAllDIMMs	Enables or disables the function of erasing the intrinsic memory area of all PMems in the system.	• Disabled • Enabled	Disabled
S1 CH0	setSecureEraseSktCh0	Erases the intrinsic memory area of PMem on CPU 1 channel 0.	• Disabled • Enabled	Disabled
S1 CH1	setSecureEraseSktCh1	Erases the intrinsic memory area of PMem on CPU 1 channel 1.	• Disabled • Enabled	Disabled
S1 CH2	setSecureEraseSktCh2	Erases the intrinsic memory area of PMem on CPU 1 channel 2.	• Disabled • Enabled	Disabled
S1 CH3	setSecureEraseSktCh3	Erases the intrinsic memory area of PMem on CPU 1 channel 3.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
S1 CH4	setSecureEraseSktCh4	Erases the intrinsic memory area of PMem on CPU 1 channel 4.	• Disabled • Enabled	Disabled
S1 CH5	setSecureEraseSktCh5	Erases the intrinsic memory area of PMem on CPU 1 channel 5.	• Disabled • Enabled	Disabled
S1 CH6	setSecureEraseSktCh6	Erases the intrinsic memory area of PMem on CPU 1 channel 6.	• Disabled • Enabled	Disabled
S1 CH7	setSecureEraseSktCh7	Erases the intrinsic memory area of PMem on CPU 1 channel 7.	• Disabled • Enabled	Disabled
S2 CH0	setSecureEraseSktCh8	Erases the intrinsic memory area of PMem on CPU 2 channel 0.	• Disabled • Enabled	Disabled
S2 CH1	setSecureEraseSktCh9	Erases the intrinsic memory area of PMem on CPU 2 channel 1.	• Disabled • Enabled	Disabled
S2 CH2	setSecureEraseSktCh10	Erases the intrinsic memory area of PMem on CPU 2 channel 2.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
S2 CH3	setSecureEraseSktCh11	Erases the intrinsic memory area of PMem on CPU 2 channel 3.	• Disabled • Enabled	Disabled
S2 CH4	setSecureEraseSktCh12	Erases the intrinsic memory area of PMem on CPU 2 channel 4.	• Disabled • Enabled	Disabled
S2 CH5	setSecureEraseSktCh13	Erases the intrinsic memory area of PMem on CPU 2 channel 5.	• Disabled • Enabled	Disabled
S2 CH6	setSecureEraseSktCh14	Erases the intrinsic memory area of PMem on CPU 2 channel 6.	• Disabled • Enabled	Disabled
S2 CH7	setSecureEraseSktCh15	Erases the intrinsic memory area of PMem on CPU 2 channel 7.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Memory Configuration/PMem Configuration				
PMem Factory Reset/Clear	FactoryResetClear	Enables or disables the PMem Factory Reset/Clear function.	• Disabled • Enabled	Disabled
Publish ARS capability	NgnArsPublish	Enables or disables the address range inspection capability open to the OS.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PMem ECC Read Check	NgnEccRdChk	Enables or disables the PMem ECC read check function.	● Disabled ● Enabled	Enabled
PMem Latch System Shutdown State	LatchSystemShutdownState	Enables or disables the PMem latch shutdown function.	● Disabled ● Enabled	Enabled
Snoopy mode for 2LM	EliminateDirectoryInFarMemory	Enables or disables the snoopy mode for 2LM.	● Enabled ● Disabled	Disabled
Enable power cycle policy	NvmdimmPowerCyclePolicy	Enables or disables the power restart mechanism.	● Enabled ● Disabled	Enabled
Snoopy mode for AD	DisableDirForAppDirect	Enables or disables the APP Direct (AD) mode.	● Disabled ● Enabled	Disabled
LSx implementation	LsxImplementation	Sets the ACPI method implementation mode.	● SWSMI ● ASL	ASL
Extended Type 17 Structure	ExtendedType17	Enables or disables the extended type 17 structure.	● Disabled ● Enabled	Enabled
SMBus Max Access Time	NvdimmSmbusMaxAccessTime	Sets the maximum SMBus access time.	0 to 512	350
SMBus Release Delay	NvdimmSmbusReleaseDelay	Sets the SMBus release delay.	0 to 512	150
NVDIMM Mailbox in NFIT	NfitPublishMailboxStructs	Enables or disables the NVDIMM mailbox in NFIT.	● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Memory Configuration/BSSA Configuration Menu				
Rank Margin Tool	EnableRMT	Enables or disables Rank Margin Tool (RMT).	• Disabled • Enabled	Disabled
Scrambler	RMTScrambler	Enables or disables the scrambler during the RMT test.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/Socket1/2 Configuration/Port 1A/1B/1C/1D/1E/1F/1G/1H/2A/2B/2C/2D/2E/2F/2G/2H/3A/3B/3C/3D/3E/3F/3G/3H/4A/4B/4C/4D/4E/4F/4G/4H/5A/5B/5C/5D/5E/5F/5G/5H/ **NOTE** • The values of **index** from **Socket1 Configuration/Port 1A** to **Socket1 Configuration/Port 5H** are 1 to 40 in sequence. • The values of **index** from **Socket2 Configuration/Port 1A** to **Socket2 Configuration/Port 5H** are 58 to 97 in sequence.				
PCIe Port	PciePortEnable*index*	Sets the PCIe port parameters.	• Auto • Disabled • Enabled • Only Disable Boot Driver	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PCIe Link Speed	PciePortLinkSpeed*index*	Sets the link speed of a PCIe port.	• Auto • Gen 1 (2.5 GT/s) • Gen 2 (5 GT/s) • Gen 3 (8 GT/s) • Gen 4 (16 GT/s) • Gen 5 (32 GT/s) **NOTE** BIOS versions above 01.01.06.07 do not support setting to Gen 5 via Redfish.	Auto
PCIe Port DeEmphasis Level	DeEmphasis*index*	Sets de-emphasis for a PCIe port.	• -6.0 dB • -3.5 dB	-6.0 dB
Data Link Feature Exchange	PcieDataLinkFeatureExchangeEnable*index*	Enables or disables the data link function negotiation in the data link feature capabilities register (DLFCAP).	• Disabled • Enabled	Enabled
PCIe Port Max Payload Size	PcieMaxPayload*index*	Sets the maximum payload size for a PCIe port.	• 128B • 256B • 512B • Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PCIe Completion Timeout Value	PcieCtoValue*index*	Sets the timeout period of PCIe transfer completion.	• 50us to 50ms • 50us to 100us • 1ms to 10ms • 16ms to 55ms • 65ms to 210ms • 260ms to 900ms • 1s to 3.5s • Disabled	260ms to 900ms
PCIe ASPM Support	PcieAspm*index*	Sets the dynamic power management function of the PCIe device connected to the corresponding port.	• Disabled • L1 Only	Disabled
PCIe Port L1 Exit Latency	PcieL1Latency*index*	Sets the time required by this port to complete the transition from L1 to L0.	• <1uS • 1uS - 2uS • 2uS - 4uS • 4uS - 8uS • 8uS - 16uS • 16uS - 32uS • 32uS - 64uS • >64uS	8uS - 16uS
MCTP	MctpEn*index*	Enables or disables the MCTP function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/IIO Configuration/IOAT Configuration/ Sck1/2 IOAT Config **NOTE** ● The values of **index** from **DINO 0 Items** to **DINO 3 Items** of **Sck1 IOAT Config** are 0 to 3 in sequence. ● The values of **index** from **DINO 0 Items** to **DINO 3 Items** of **Sck2 IOAT Config** are 4 to 7 in sequence.				
CPM	CpmEn*index*	Enables or disables CPM.	● Disabled ● Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket 1 Configuration				
IIO Stack 1	IioStackIoResource1	Enables or disables the default I/O resources of the request stack.	● Disabled ● Enabled	Enabled
IIO Stack 2	IioStackIoResource2	Enables or disables the default I/O resources of the request stack.	● Disabled ● Enabled	Enabled
IIO Stack 3	IioStackIoResource3	Enables or disables the default I/O resources of the request stack.	● Disabled ● Enabled	Enabled
IIO Stack 4	IioStackIoResource4	Enables or disables the default I/O resources of the request stack.	● Disabled ● Enabled	Enabled
IIO Stack 5	IioStackIoResource5	Enables or disables the default I/O resources of the request stack.	● Disabled ● Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket2 Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO Stack 1	IioStackIoResource13	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 2	IioStackIoResource14	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 3	IioStackIoResource15	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 4	IioStackIoResource16	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 5	IioStackIoResource17	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/Intel Virtualization for Directed I/O (VT-d)				
Intel VT for Directed I/O (VT-d)	VTdSupport	Enables or disables the VT-d feature.	• Enabled • Disabled	Enabled
Opt-Out Illegal MSI Mitigation	IllegalMsiMitigation	Enables or disables exiting illegal MSI mitigation.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
DMA Control Opt-In Flag	DmaCtrlOptIn	Enables or disables DMA_CTRL_PLATFORM_OPT_IN_FLAG in the ACPI's DMAR table.	• Disabled • Enabled	Disabled
Interrupt Remapping	InterruptRemap	Enables or disables the VT-d interrupt remapping function.	• Auto • Enabled • Disabled	Auto
./Advanced/Socket Configuration/IIO Configuration/Intel(R) VMD technology				
Intel(R) VMD Config	VMDConfigEnable	Enables or disables the volume management device (VMD) function for PCIe devices.	• Disabled • Enabled	Disabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Surprise Hot Plug Support	SurpriseHotPlugSupport	Enables or disables the surprise hot plug function of NVMe drives. **NOTE** ● This parameter is supported only in BIOS 01.01.03.13 and later. ● iBMC version matching requirements: The iBMC version is 3.07.03.17 or later. ● CPLD version matching requirements: The drive backplane (BC15NHBC) CPLD version is 1.06 or later.	● Disabled ● Enabled	Disabled
./Advanced/Socket Configuration/IIO Configuration/IIO DFX Configuration/ Socket1/2 Configuration/Port DMI/1A/1B/1C/1D/1E/1F/1G/1H/2A/2B/2C/2D/2E/2F/2G/2H/3A/3B/3C/3D/3E/3F/3G/3H/4A/4B/4C/4D/4E/4F/4G/4H/5A/5B/5C/5D/5E/5F/5G/5H/ **NOTE** ● The value of **index** of **Socket1 Configuration/Port DMI** is **0**. ● The values of **index** from **Socket1 Configuration/Port 1A** to **Socket1 Configuration/Port 5H** are 1 to 40 in sequence. ● The values of **index** from **Socket2 Configuration/Port 1A** to **Socket2 Configuration/Port 5H** are 58 to 97 in sequence.			

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Link Re-Train	DfxLinkRetrainEn*index*	Enables the link retraining function when the link speed or bandwidth decreases.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/IIO Configuration/IIO Global Performance Tuning				
Retimer Low Latency Mode	RetimerLowLatencyMode	Sets the re-timer low latency mode.	• Disabled • Enabled • 16GT/s Only • 32GT/s Only	Enabled
./Advanced/Socket Configuration/IIO Configuration				
PCI 64-Bit Resource Allocation	Pci64BitResourceAllocation	Enables or disables the PCI 64-bit resource allocation function. This option is automatically enabled when the server restarts when some PCIe devices that require more than 4 GB memory resources are used.	• Disabled • Enabled	Enabled
PCIe Completion Timeout	PcieCtoGlobal	Sets whether the completion timeout is controlled by each port independently or globally.	• Per-Port • Global	Per-Port

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PCIe Completion Timeout Value	PcieCtoGlobalValue	Sets the timeout period of PCIe transfer completion.	• 50us to 50ms • 50us to 100us • 1ms to 10ms • 16ms to 55ms • 65ms to 210ms • 260ms to 900ms • 1s to 3.5s • Disabled	260ms to 900ms
PCIe ENQCMD and ENQCMDS	PcieEnqCmdSupport	Whether to enable PCIe ENQ request support.	• No • Yes	No
./Advanced/Socket Configuration/Advanced Power Management Configuration				
Performance Profile	BenchMarkSelection	Select an energy efficiency test scenario.	• Custom • Efficiency • Performance • Load Balance • High RAS • HPC • General Computing • Low Latency • Server Side Java • Memory Throughput • I/O Throughput • Energy Saving • NFV	Custom

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Static Turbo	StaticTurbo	Sets the static turbo policy to be applied by the BIOS.	• Disabled • Manual • Auto	Disabled
CPU Frequency Select	FreqSelect	You need to select the frequency value between the fundamental frequency and the turbo frequency, in 100 MHz. When the input value is less than the fundamental frequency, set the value based on the fundamental frequency. When the input value is greater than the supported maximum turbo frequency, set the value based on the maximum turbo frequency.	12 to 50	50
DEMT	PowerSaving	Enables or disables the Dynamic Energy Management Technology (DEMT) mode.	• Disabled • Enabled	Disabled
SYS_USAGE Threshold	SystemCpuUsage	Sets the **SYS_USAGE** threshold.	50 to 99	95

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SMI Interval	TcoTimeout	Sets the SMI interval in 0.6s.	2 to 10	6
Low Occupy Control	LowOccupyControl	Enables or disables the low usage control function.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU P-State Control				
AVX License Pre-Grant Override	AvxLicensePreGrant	Enables or disables AVX ICCP pre-grant level override.	• Disabled • Enabled	Disabled
AVX P1	AvxP1Level	Sets the AVX P1 level.	• Nominal • Level 1 • Level 2	Nominal
Intel SST-PP	IssTdpLevel	Sets the Intel speed select technology (SST).	• Auto • Level 0 • Level 1 • Level 2 • Level 3 • Level 4	Auto
Dynamic SST-PP	DynamicIss	Enables or disables the dynamic SST-PP.	• Disabled • Enabled	Disabled
SpeedStep (Pstates)	ProcessorEist Enable	Enables or disables EIST (P state).	• Disabled • Enabled	Enabled
EIST PSD Function	ProcessorEist PsdFunc	Sets the PSD function.	• HW_ALL • SW_ALL	HW_ALL
Energy Efficient Turbo	EETurboDisable	Enables or disables the energy saving turbo mode.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Turbo Mode	TurboMode	Enables or disables the processor acceleration mode.	• Disabled • Enabled	Enabled
PSS Table Turbo Frequency	PSSTableTurboFrequency	Select the ACPI _PSS table turbo frequency. The default is the maximum non-turbo frequency plus 1MHz. **NOTE** Only BIOS version 01.01.03.05 and later supports this parameter.	• Max Non-Turbo Frequency Plus One • Max Turbo Frequency	Max Non-Turbo Frequency Plus One
CPU Flex Ratio Override	ProcessorFlexibleRatioOverrideEnable	Enables or disables the CPU frequency reset function in non-Turbo mode.	• Disabled • Enabled	Disabled
CPU Core Flex Ratio	ProcessorFlexibleRatio	Sets the processor core frequency in non-Turbo mode	0 to 100	23
./Advanced/Socket Configuration/Advanced Power Management Configuration/Hardware PM State Control				
Hardware P-State	ProcessorHWPMEnable	Sets the Hardware P-State function control switch.	• Disabled • Native Mode • Out of Band Mode • Native Mode with No Legacy Support	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
EPP Enable	ProcessorEPPEnable	Enables or disables the energy performance preference (EPP) control switch.	• Disabled • Enabled	Enabled
EPP Profile	ProcessorEppProfile	Sets the energy preference policy.	• Performance • Balanced Performance • Balanced Power • Power	Balanced Performance
./Advanced/Socket Configuration/Advanced Power Management Configuration/UCP				
UFMT	UncoreRatioEn	Enables or disables the Uncore Frequency Management Technology (UFMT) mode.	• Enabled • Disabled	Disabled
UR0	UncoreRatio0	Specifies the maximum uncore ratio limit when the workload reaches 0%.	0 to 36	8
UR1	UncoreRatio1	Specifies the maximum uncore ratio limit when the workload reaches 1%.	0 to 36	8
UR2	UncoreRatio2	Specifies the maximum uncore ratio limit when the workload reaches 2%.	0 to 36	8

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
UR3	UncoreRatio3	Specifies the maximum uncore ratio limit when the workload reaches 3%.	0 to 36	36
UR4	UncoreRatio4	Specifies the maximum uncore ratio limit when the workload reaches 4%.	0 to 36	36
UR5	UncoreRatio5	Specifies the maximum uncore ratio limit when the workload reaches 5%.	0 to 36	36
UR6	UncoreRatio6	Specifies the maximum uncore ratio limit when the workload reaches 6%.	0 to 36	36
UR7	UncoreRatio7	Specifies the maximum uncore ratio limit when the workload reaches 7%.	0 to 36	36
UR8	UncoreRatio8	Specifies the maximum uncore ratio limit when the workload reaches 8%.	0 to 36	36
UR9	UncoreRatio9	Specifies the maximum uncore ratio limit when the workload reaches 9%.	0 to 36	36

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
UR10	UncoreRatio10	Specifies the maximum uncore ratio limit when the workload reaches 10%.	0 to 36	36
UR20	UncoreRatio11	Specifies the maximum uncore ratio limit when the workload reaches 20%.	0 to 36	36
UR30	UncoreRatio12	Specifies the maximum uncore ratio limit when the workload reaches 30%.	0 to 36	36
UR40	UncoreRatio13	Specifies the maximum uncore ratio limit when the workload reaches 40%.	0 to 36	36
UR50	UncoreRatio14	Specifies the maximum uncore ratio limit when the workload reaches 50%.	0 to 36	36
UR60	UncoreRatio15	Specifies the maximum uncore ratio limit when the workload reaches 60%.	0 to 36	36
UR70	UncoreRatio16	Specifies the maximum uncore ratio limit when the workload reaches 70%.	0 to 36	36

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
UR80	UncoreRatio17	Specifies the maximum uncore ratio limit when the workload reaches 80%.	0 to 36	36
UR90	UncoreRatio18	Specifies the maximum uncore ratio limit when the workload reaches 90%.	0 to 36	36
UR100	UncoreRatio19	Specifies the maximum uncore ratio limit when the workload reaches 100%.	0 to 36	36
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU C-State Control				
Enable Monitor MWAIT	MonitorMWait	Enables, disables, or automatically sets the MONITOR MWAIT instruction.	• Disabled • Enabled • Auto	Disabled
CPU C6 Report	C6Enable	Sets the feature of reporting CPU C6 (ACPI C3) information to the OS.	• Disabled • Enabled • Auto	Disabled
Enhanced Halt State (C1E)	ProcessorC1eEnable	Enables or disables the enhanced halt state (C1E) function.	• Disabled • Enabled	Disabled
C1E OS Indicator	CSOSIndicator	Enables or disables the CPU global C1E-state indicator of the OS.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
C6 OS Indicator	C6OSIndicator	Enables or disables the CPU C6 status indicator of the OS.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Package C-State Control				
Package C-State	PackageCState	Sets the deep energy saving.	• C0/C1 State • C2 State • C6(Non-Retention State) • C6(Retention State) • No Limit • Auto	C0/C1 State
./Advanced/Socket Configuration/Advanced Power Management Configuration/Package C-State Control/Pkg C-state SA Power Management Control/CPU1 SAPMCTL_CFG				
SAPMCTL_CFG LOCK	SapmCtlLock0	Enables or disables the SA power management control lock.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Package C-State Control/Pkg C-state SA Power Management Control/CPU2 SAPMCTL_CFG				
SAPMCTL_CFG LOCK	SapmCtlLock1	Enables or disables the SA power management control lock.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU Advanced PM Tuning				
Uncore Freq Scaling	UncoreFreqScaling	Sets the non-core frequency scaling function.	• Disabled • Enabled • Manual	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Uncore Freq	InputUncoreFreq	Uncore frequency input by the user.	0 to 127	127
Input Min Uncore Freq	InputMinUncoreFreq	Minimum input uncore frequency.	0 to 127	0
Input Max Uncore Freq	InputMaxUncoreFreq	Maximum input uncore frequency.	0 to 127	127
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU Advanced PM Tuning/Energy Perf BIAS				
Power Performance Tuning	PwrPerfTuning	Sets the power performance tuning function.	• OS Controls EPB • BIOS Controls EPB • PECI Controls EPB	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	AltEngPerfBIAS	Sets the ENERGY_PERF_BIAS_CFG mode.	• Performance • Balanced Performance • Balanced Power • Power	Balanced Performance
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU Advanced PM Tuning				
Optimized Power Mode	OptimizedPowerMode	Enables or disables the optimized power mode.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Thermal				
Throttling Mode	thermalthrottlingsupport	Sets the thermal energy throttling mode.	• Disabled • CLTT	CLTT

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options				
CKE Power Down	CkeProgramming	Enables or disables the CKE power-down function.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options/CKE Feature				
CKE Idle Timer	CkeIdleTimer	Sets the CKE idle timer, in nanoseconds. **NOTE** This parameter is applicable to the servers which CPU type is SPR.	0 to 255	20
CKE Idle Timer	CkeIdleTimerEmr	Sets the CKE idle timer, in nanoseconds. **NOTE** This parameter is applicable to the servers which CPU type is EMR.	0 to 255	160
PPD	PpdEn	Enables or disables the pre-charge power down (PPD) function. **NOTE** BIOS 01.01.06.03 and later versions do not support setting this parameter through Redfish.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options				
SREF Feature	SrefProgramming	Sets the self-refresh mode, which is used to retain data in sleep mode in low-power mode.	• Auto • Manual	Manual
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options/Self Refresh Feature				
CK in SR	CkMode	Sets the clock behavior during self-refresh.	• Driven • Pulled Low	Pulled Low
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 1 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** value is **Disabled**.				
SATA Controller(s)	PchSata0	Enables or disables the SATA controller.	• Enabled • Disabled	Enabled
SATA Mode Selection	SataInterfaceMode0	Sets the working mode of the SATA controller.	• AHCI • RAID	AHCI
RAID Device ID	RaidDeviceId0	Sets the device ID in RAID mode.	• Client • Alternate • Server	Server
SATA Port 0	SataPortController00	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 1	SataPortController01	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 2	SataPortController02	Enables or disables the SATA port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController03	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController04	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController05	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController06	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController07	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 2 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** value is **Disabled**.				
SATA Controller(s)	PchSata1	Enables or disables the SATA controller.	• Enabled • Disabled	Enabled
SATA Mode Selection	SataInterfaceMode1	Sets the working mode of the SATA controller.	• AHCI • RAID	AHCI
RAID Device ID	RaidDeviceId1	Sets the device ID in RAID mode.	• Client • Alternate • Server	Server
SATA Port 0	SataPortController10	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 1	SataPortController11	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 2	SataPortController12	Enables or disables the SATA port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController13	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController14	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController15	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController16	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController17	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 3 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** value is **Disabled**.				
SATA Controller(s)	PchSata2	Enables or disables the SATA controller.	• Enabled • Disabled	Enabled
SATA Mode Selection	SataInterfaceMode2	Sets the working mode of the SATA controller.	• AHCI • RAID	AHCI
RAID Device ID	RaidDeviceId2	Sets the device ID in RAID mode.	• Client • Alternate • Server	Server
SATA Port 0	SataPortController20	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 1	SataPortController21	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 2	SataPortController22	Enables or disables the SATA port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController23	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController24	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController25	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController26	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController27	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/BMC Configuration/BMC Configuration				
BMC WDT Support For POST	BMCWDTEnable	Enables or disables the BMC watchdog timer at the start of POST.	• Disabled • Enabled	Disabled
BMC WDT Time Out For POST	BMCWDTTimeout	Sets the maximum duration (in minutes) allowed for the system BIOS to start.	18 to 25	20
BMC WDT Action For POST	BMCWDTAction	Sets the action to be taken after the watchdog timer times out.	• No Action • Hard Reset • Power Down • Power Cycle	Hard Reset
BMC WDT Support For OS	OSWDTEnable	Enables or disables the watchdog timer on the OS.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
BMC WDT Time Out For OS	OSWDTTimeout	Sets the maximum time allowed for loading the OS completely, in minutes.	2 to 8	5
BMC WDT Action For OS	OSWDTAction	Sets the action to be taken after the watchdog timer times out.	• No Action • Hard Reset • Power Down • Power Cycle	Hard Reset
./Advanced/Console Redirection Configuration				
Console Serial Redirect	CREnable	Enables or disables the serial port redirection.	• Disabled • Enabled	Enabled
Terminal Type	GlobalTerminalType	Sets the simulation type. The BIOS simulation type must match the mode selected in the terminal program.	• VT_100 • VT_100+ • VT_UTF8 • PC_ANSI • LOG_TERM • TTY_TERM • LINUX_TERM • XTERM_R6 • VT_400 • SCO_TERM	VT_100

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Baud Rate	GlobalBaudRate	Sets the baud rate for serial port redirection.	• 115200 • 57600 • 38400 • 19200 • 9600 • 4800 • 2400 • 1200	115200
Data Bits	GlobalDataBits	Sets the data length of serial port redirection.	• 7 Bits • 8 Bits	8 Bits
Parity	GlobalParity	Sets serial port redirection verification.	• None • Even • Odd • Mark • Space	None
Stop Bits	GlobalStopBits	Sets the stop bit of the serial port redirection function.	• 1 Bit • 2 Bit	1 Bit
Flow Control	GlobalFlowControl	Sets the control flow of the serial port redirection.	• None • RTS/CTS • XON/XOFF **NOTE** 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7 does not support the **RTS/CTS** option only in BIOS 01.01.08.07 and later versions.	None
./Advanced/PXE Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Slot PXE Control	SlotLanPortSetting	Enables or disables the PXE function of all external PCIe NICs.	• Disabled • Enabled	Enabled
CPU1 First SLOT Port 1	SlotLanPortControl0	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 1.	• Disabled • Enabled	Enabled
CPU1 First SLOT Port 2	SlotLanPortControl1	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 1.	• Disabled • Enabled	Enabled
CPU1 First SLOT Port 3	SlotLanPortControl2	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 1.	• Disabled • Enabled	Enabled
CPU1 First SLOT Port 4	SlotLanPortControl3	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 1.	• Disabled • Enabled	Enabled
CPU2 First SLOT Port 1	SlotLanPortControl4	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 2.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU2 First SLOT Port 2	SlotLanPortControl5	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 2.	• Disabled • Enabled	Enabled
CPU2 First SLOT Port 3	SlotLanPortControl6	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 2.	• Disabled • Enabled	Enabled
CPU2 First SLOT Port 4	SlotLanPortControl7	Enables or disables the PXE function of the first PCIe slot port corresponding to the CPU 2.	• Disabled • Enabled	Enabled
FLEX IO 1-1 Port 1	PXE1Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 1-1 Port 2	PXE2Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 1-2 Port 1	PXE3Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 1-2 Port 2	PXE4Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
FLEX IO 2 Port 1	PXE5Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 2 Port 2	PXE6Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 2 Port 3	PXE7Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
FLEX IO 2 Port 4	PXE8Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
./Security				
Simple Password	SimplePassWord	Enables or disables the simple password function.	• Disabled • Enabled	Disabled
Password Expiration Date	PWDExpirationDate	Sets the validity period of the password.	• 0 day • 30 days • 60 days • 90 days • 180 days • 360 days	180 days

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
MOR State	MorState	Enables or disables the MOR (Memory Overwrite Request) feature. **NOTE** 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7 supports this parameter only in BIOS 01.01.08.07 and later versions.	• Disabled • Enabled	Disabled
./Boot				
Boot Type	BootType	Sets the system boot type.	• Legacy Boot Type • UEFI Boot Type	UEFI Boot Type
Network Stack	PxeBootToLan	Enables or disables the network stack function.	• Disabled • Enabled	Enabled
PXE Boot capability	PxeBootCapability	Sets the PXE boot network.	• Disabled • UEFI:IPv4 • UEFI:IPv6 • UEFI:IPv4/IPv6	UEFI:IPv4
IPv4 PXE	Ipv4Pxe	Enables or disables the IPv4 PXE function.	• Disabled • Enabled	Enabled
IPv6 PXE	Ipv6Pxe	Enables or disables the IPv6 PXE function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
HTTP(s) Boot Capability	HttpNetworkProtocol	Sets the HTTPS boot network.	• Disabled • HTTP(s):IPv4 • HTTP(s):IPv6 • HTTP(s):IPv4/IPv6	HTTP(s):IPv4
HTTP Support	HttpEnable	Specifies whether to allow the HTTP connection.	• Disabled • Enabled	Disabled
Boot Fail Policy	NoBootReset	Sets the operation to be performed after the boot fails.	• None • Boot Retry • Cold Boot	Boot Retry
PXE Retry Count	PxeRetryCount	Sets the times of repeated boots from the PXE.	1 to 99	1
PXE Timeout Control	PxeTimeoutRetryControl	Sets the number of DHCP connection retries due to timeout occurring when each enabled port is booted from the PXE.	• Disabled • TimeoutRetryCount1 • TimeoutRetryCount2 • TimeoutRetryCount3 • TimeoutRetryCount4	Disabled
SP Boot	SPBoot	Enables or disables the boot function of Smart Provisioning (SP).	• Disabled • Enabled	Enabled
USB Boot	UsbBoot	Enables or disables the boot function of the external USB device.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
OEM Fast Boot	OemFastBoot	Enables or disables the BIOS fast boot function.	• Disabled • Enabled	Disabled
Sync Order	SyncOrder	Sets the synchronization sequence function.	• Disabled • Sync Boot Order • Sync Boot Device Type Order	Disabled
Boot Override	BootOverride	Sets the first priority boot device.	• PCIe SSD First • iSCSI First • FC First • FCOE First • PCH Direct First • RAID First • USB First • Local Disk Boot Only • Disabled	Disabled
OEM Secure Boot	OemSecureBoot	Enables or disables the OEM Secure Boot. **NOTE** This function is only supported in UEFI mode. The Redfish interface can only be used to enable this function.	• Disabled • Enabled	Disabled
./Boot/Boot Sequence				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
-	BootTypeOrder0	Sets the boot sequence of the system boot option 1.	• HardDiskDrive • DVDROMDrive • PXE • Others • Disabled	HardDiskDrive
-	BootTypeOrder1	Sets the boot sequence of the system boot option 2.	• HardDiskDrive • DVDROMDrive • PXE • Others • Disabled	DVDROMDrive
-	BootTypeOrder2	Sets the boot sequence of the system boot option 3.	• HardDiskDrive • DVDROMDrive • PXE • Others • Disabled	PXE
-	BootTypeOrder3	Sets the boot sequence of the system boot option 4.	• HardDiskDrive • DVDROMDrive • PXE • Others • Disabled	Others

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

C Redfish Out-of-Band Configurations on the Eagle Stream Platform (Only for 2288 V7/2488H V7/5885H V7/G5500 V7/G8600 V7)

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Main				
Language	Language	Sets the language of the current BIOS.	• en-US • ja-JP • zh-CN	en-US
./Advanced/Peripheral Configuration/SR-IOV Setup Settings				
PCIe SR-IOV	SriovEnablePolicy	Sets the SR-IOV function of the PCIe card.	• Disabled • Enabled • Per IIO Port	Enabled
CPU1 Port DMI	PcieSriov[0]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 1A	PcieSriov[1]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 2A	PcieSriov[9]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU1 Port 2C	PcieSriov[11]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 2E	PcieSriov[13]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 2G	PcieSriov[15]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 3A	PcieSriov[17]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 3E	PcieSriov[21]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4A	PcieSriov[25]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4B	PcieSriov[26]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4C	PcieSriov[27]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU1 Port 4D	PcieSriov[28]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4E	PcieSriov[29]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 4G	PcieSriov[31]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU1 Port 5A	PcieSriov[33]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 1A	PcieSriov[58]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 2A	PcieSriov[66]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 3A	PcieSriov[74]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 3C	PcieSriov[76]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU2 Port 3E	PcieSriov[78]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 3G	PcieSriov[80]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5A	PcieSriov[90]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5B	PcieSriov[91]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5C	PcieSriov[92]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5D	PcieSriov[93]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5E	PcieSriov[94]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5F	PcieSriov[95]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU2 Port 5G	PcieSriov[96]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU2 Port 5H	PcieSriov[97]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1A	PcieSriov[115]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1B	PcieSriov[116]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1C	PcieSriov[117]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1D	PcieSriov[118]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1E	PcieSriov[119]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1F	PcieSriov[120]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU3 Port 1G	PcieSriov[121]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 1H	PcieSriov[122]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 2A	PcieSriov[123]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 2E	PcieSriov[127]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 3A	PcieSriov[131]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 3E	PcieSriov[135]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 5A	PcieSriov[147]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 5C	PcieSriov[149]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU3 Port 5E	PcieSriov[151]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU3 Port 5G	PcieSriov[153]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1A	PcieSriov[172]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1B	PcieSriov[173]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1C	PcieSriov[174]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1D	PcieSriov[175]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1E	PcieSriov[176]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1F	PcieSriov[177]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU4 Port 1G	PcieSriov[178]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 1H	PcieSriov[179]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2A	PcieSriov[180]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2B	PcieSriov[181]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2C	PcieSriov[182]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2D	PcieSriov[183]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2E	PcieSriov[184]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2F	PcieSriov[185]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU4 Port 2G	PcieSriov[186]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 2H	PcieSriov[187]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 3A	PcieSriov[188]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
CPU4 Port 4A	PcieSriov[196]	Enables or disables the SR-IOV function of the port.	• Disabled • Enabled	Enabled
./Advanced/Peripheral Configuration				
PCIe ARI	ARIEnable	Enables or disables ARI of the PCIe card.	• Disabled • Enabled	Disabled
PCIe ASPM Support (Global)	SystemPcieGlobalAspm	Sets the PCIe ASPM Support (Global) function.	• Disabled • Per individual port • L1 Only	Disabled
./Advanced/Peripheral Configuration/SIO 1711				
UART 1	DeviceEnable	Enables or disables the BMC serial port function.	• Disabled • Enabled	Enabled
Base I/O Address	COMBaseAddress	Sets the base address of the BMC serial port.	• 3F8 • 2F8	3F8
Interrupt	DeviceIrq	Interrupts the configuration.	• IRQ3 • IRQ4	IRQ4

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Video Configuration				
Display Mode	VideoSelect	Sets the video card mode.	• On Board Graphics • Plug-in Graphics	On Board Graphics
./Advanced/ACPI Table or Features Control				
SPCR Table Support	CRAfterPost	Enables or disables the SPCR table function.	• Disabled • Enabled	Enabled
./Advanced/Misc Configuration				
System Debug Level	SysDbgLevel	Enables or disables the system debug level.	• Disabled • Enabled	Disabled
IPMI Device Control	IpmiDevCtrl	Enables or disables ACPI reporting on the IPMI device.	• Disabled • Enabled	Disabled
CDN Support	CdnSupport	Enables or disables the function of CDN.	• Disabled • Enabled	Enabled
Power button Invalid	FrontPanelLock	Enables or disables the power button invalid function. **NOTE** When this parameter is set to **Enabled**, the power button is locked. You cannot use the power button to power on or off the server. You need to use the server management software to power on or off the server.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Memory SN Customization	MemorySNCustomize	Enables or disables the memory serial number customization function.	• Disabled • Enabled	Disabled
Wake on PME	WakeOnLanSupport	Enables or disables the PME function.	• Disabled • Enabled	Disabled
Re-Size BAR Support	PcieResizableBarSupport	Enables or disables the PCIe resizable BAR capability supported. **NOTE** Only BIOS 01.02.08.05 and later versions support this parameter.	• Enabled • Disabled	Disabled
BAR Size	PcieResizableBarSize	Choose the BAR size for the PCIe device. **NOTE** Only BIOS 01.02.08.05 and later versions support this parameter.	• Auto • 8G • 16G • 32G • 64G	Auto
./Advanced/System Event Log				
System Errors	SystemErrorEn	Sets the function of recording system errors.	• Disabled • Enabled • Auto	Enabled
System Memory Poisoning	PoisonEn	Enables or disables the memory poisoning function.	• Disabled • Enabled	Enabled
FDM	FDMSupport	Enables or disables the FDM function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Clear Viral Status	ClearViralStatus	Enables or disables the function of clearing virus status. **NOTE** This parameter is available when **System Errors** and **Viral Status** are set to **Enabled**.	• Enabled • Disabled	Disabled
CE Record	CeReportToOs	Enables or disables the CE record.	• Disabled • Enabled	Disabled
Error Data Revison	ErrorDataRevison	Sets the compatible error data version.	• 0x201 • 0x300	0x201
./Advanced/System Event Log/eMCA Settings				
eMCA Logging Support	EmcaEn	Enables or disables the eMCA logging function.	• Disabled • Enabled	Enabled
eMCA CMCI-SMI Morphing	EmcaCsmiEn	Enables or disables the eMCA CMCI-SMI mapping.	• Disabled • eMCA Gen 2 CSMI	eMCA Gen 2 CSMI
./Advanced/System Event Log/WHEA Settings				
WHEA Support	WheaSupportEn	Enables or disables the WHEA function.	• Disabled • Enabled	Enabled
./Advanced/System Event Log/IIO Error Enabling				
OS Native AER Support	OsNativeAerSupport	Enables or disables the AER function controlled by the OS.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO MCA Support	IoMcaEn	Enables or disables the I/O MCA support function.	• Disabled • Enabled	Disabled
IIO eDPC Support	EdpcEn	Sets the I/O eDPC support function.	• Disabled • On Fatal Error • On Fatal and Non-Fatal Errors	Disabled
IIO eDPC Interrupt	EdpcInterrupt	Enables or disables the I/O eDPC interrupt function.	• Disabled • Enabled	Enabled
IIO eDPC ERR_COR Message	EdpcErrCorMsg	Enables or disables the I/O eDPC ERR_COR function.	• Disabled • Enabled	Enabled
PCIe Error	PcieErrEn	Enables or disables PCIe error detection.	• Disabled • Enabled	Enabled
./Advanced/System Event Log/PCIe Error Enabling				
Corrected Error	PcieCorrErrEn	Enables or disables the PCIe correctable error detection.	• Disabled • Enabled	Enabled
Uncorrected Error	PcieUncorrErrEn	Enables or disables the PCIe uncorrectable error detection.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Fatal Error	PcieFatalErrEn	Enables or disables the PCIe fatal error detection.	• Disabled • Enabled	Enabled
PCIe Corrected Error Threshold Counter	PcieCorErrCntr	Enables or disables the PCIe correction error threshold counter.	• Disabled • Enabled	Disabled
PCIe Corrected Error Threshold	PcieCorErrThres	Sets the PCIe correction error threshold.	0 to 0xffffffff	1
PCIe ECRC Error	PcieAerEcrcEn	Enables or disables the PCIe ECRC error function.	• Disabled • Enabled	Disabled
PCIe Surprise Link Down Error	PcieAerSurpriseLinkDownEn	Enables or disables unexpected PCIe link disconnection.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Processor Configuration				
Homeless Prefetch	HomelessPrefetchEnable	Enables or disables the Homeless prefetcher feature on all threads.	• Enabled • Disabled • Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
AMP Prefetch	AmpPrefetchEnable	Enables or disables the MLC AMP prefetcher.	• Enabled • Disabled • Auto	Auto

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
			NOTE ● G8600 V7 The Auto option is supported only in BIOS versions 01.02.04.03 and later. ● G5500 V7 The Auto option is supported only in BIOS versions 01.02.03.02 and later. ● 5885H V7 and 2488H V7 The Auto option is supported only in BIOS versions 01.02.02.02 and later. ● 2288 V7 The Auto option is supported only in BIOS versions 01.02.04.01 and later.	

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PPIN Control	PpinControl	Specifies whether to unlock and enable the PPIN control.	• Lock/ Disabled • Unlock/ Enabled	Unlock/ Enabled
Total Memory Encryption (TME) Bypass	EnableTmeBypass	Enable or disable Total Memory Encryption (TME).	• Auto • Enabled • Disabled	Disabled
Total Memory Encryption Multi-Tenant(TME-MT)	EnableMktme	Enable or disable Total Memory Encryption - Multi-Tenant (TME-MT).	• Enabled • Disabled	Disabled
Memory integrity	EnableGlobalIntegrity	Enables or disables the TME-MT integrity function.	• Enabled • Disabled	Disabled
Trust Domain Extension (TDX)	EnableTdx	Enables or disables the trust domain extension (TDX).	• Enabled • Disabled	Disabled
TDX Secure Arbitration Mode Loader (SEAM Loader)	EnableTdxSeamldr	Enables or disables the TDX Secure Arbitration Mode Loader (SEAM Loader) function.	• Disabled • Enabled	Disabled
Disable excluding Mem below 1MB in CMR	DfxTdxDisable1MbCmrExclude	Enables or disables the function to include memory region below 1 MB in the Convertible Memory Range (CMR).	• Enabled • Disabled • Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
TME-MT/TDX key split	KeySplit	Sets the number of bits used by TDX in the TME-MT/TDX key split, and the rest of bits will be used by TME-MT.	1～0x7	1
./Advanced/Socket Configuration/Processor Configuration/Processor Information				
Active Processor Cores	ActiveCpuCores	Sets the number of physical cores for each CPU to be used.	• All • 1 • 2 to *N-1* **NOTE** *N* indicates the maximum number of physical CPU cores supported by the CPU.	All
Enable LP [Global]	ProcessorHyperThreadingDisable	Enables or disables the hyper-threading function of the Intel processor.	• Single LP • ALL LPs	ALL LPs
Hardware Prefetcher	MlcStreamerPrefetcherEnable	Enables or disables the hardware prefetcher function.	• Disabled • Enabled	Enabled
Adjacent Cache Prefetch	MlcSpatialPrefetcherEnable	Enables or disables the adjacent cache prefetch function.	• Disabled • Enabled	Enabled
DCU Streamer Prefetcher	DCUStreamerPrefetcherEnable	Enables or disables the DCU streamer prefetching function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
DCU IP Prefetcher	DCUIPPrefetcherEnable	Enables or disables the DCU IP prefetching function.	• Disabled • Enabled	Enabled
LLC Prefetch	LlcPrefetchEnable	Enables or disables the L3 cache prefetch feature.	• Disabled • Enabled	Enabled
Extended APIC	ProcessorX2apic	Enables or disables the extended APIC feature.	• Disabled • Enabled	Enabled
Intel(R) TXT	ProcessorLtsxEnable	Enables or disables the Intel(R) TXT function.	• Disabled • Enabled	Disabled
VMX	ProcessorVmxEnable	Enables or disables CPU virtualization technology. **NOTE** This function takes effect after the server restart.	• Disabled • Enabled	Enabled
APIC number in MADT	AcpiApicReport	Sets whether the number of local APICs or X2APICs that are physically enabled is reported or the maximum number of supported local APICs or X2APICs is reported in the MADT.	• Physical • Maximum	Physical
Memory Encryption (TME)	EnableTme	Enables or disables the TME.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Processor Configuration/Common RefCode Configuration				
NUMA	NumaEn	Enables or disables the NUMA architecture of the system.	• Disabled • Enabled	Enabled
UMA-Based Clustering	UmaBasedClustering	Sets the UMA-Based Clustering function. **NOTE** The setting of this function is valid only when SNC is disabled. If SNC is enabled, the BIOS automatically disables the UMA-based cluster.	• Disable (All2All) • Hemisphere (2-clusters) • Quadrant (4-clusters)	Quadrant (4-clusters)
./Advanced/Socket Configuration/Uncore Configuration/Uncore General Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Link Frequency Select	QpiLinkSpeed	Sets the UPI link frequency.	The CPU type is SPR: ● 12.8GT/s ● 14.4GT/s ● 16.0GT/s ● Auto ● **Use Per Link Setting** The CPU type is EMR: ● 12.8GT/s ● 14.4GT/s ● 16.0GT/s ● 20.0GT/s ● Auto ● **Use Per Link Setting**	Auto
Link L1 Enable	KtiLinkL1En	Sets UPI energy saving option.	● Disabled ● Enabled ● Auto	Enabled
KTI Prefetch	KtiPrefetchEn	Sets the KTI prefetch function.	● Disabled ● Enabled ● Auto	Enabled
SNC	SncEn	Sets the SNC function.	● Auto ● Disabled ● Enable SNC2 (2-clusters) ● Enable SNC4 (4-clusters)	Disabled
Stale A to S	StaleAtoSOptEn	Set the memory SnoopAll(A) status and Shared(S) status conversion function.	● Disabled ● Enabled ● Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
LLC Dead Line Alloc	LLCDeadLine Alloc	Set the LLC dead line allocation function.	• Disabled • Enabled • Auto	Enabled
MMIO High Base	MmiohBase	Sets the high base address of the MMIO.	• 56T • 40T • 32T • 24T • 16T • 13T • 4T • 3.5T • 2T • 1T • 512G	32T
MMIO High Granularity Size	MmiohSize	Sets the I/O high base granularity size.	• 1G • 4G • 16G • 64G • 256G • 1024G	256G
Limit CPU PA to 46 bits	CpuPaLimit	Enables or disables the limit on the CPU physical address to 46 bits to support earlier versions of Hyper-V.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Memory Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Enforce Population POR	EnforcePopulationPor	Enables or disables the memory forced population Plan of Record (POR). If this function is enabled, Memory Reference Code (MRC) forcibly requires the memory module insertion to meet the POR requirements. (verified and officially supported by Intel). The memory module insertion configuration not meeting the requirements will be degraded to the supported configuration.	• Disabled • Enabled	Enabled
DDR PPR Type	pprType	Sets the DDR PPR type.	• PPR Disabled • Hard PPR • Soft PPR	Soft PPR
Force PPR On All Dram For UCE	ForcePprOnAllDramUce	Enables or disables the force PPR on all dram for UCE.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Memory Frequency	DdrFreqLimit	Sets the DDR frequency in MT/s. **NOTE** When **Memory Turbo** is set to **Enabled**, this parameter is grayed out.	The CPU type is SPR: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 The CPU type is EMR: ● Auto ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 ● 5200 ● 5600	Auto
SPD CRC Check	spdCrcCheck	Enables or disables the SPD CRC function.	● Disabled ● Enabled	Enabled
Attempt Fast Boot	AttemptFastBoot	Enables or disables the fast boot function.	● Disabled ● Enabled	Enabled
Attempt Fast Cold Boot	AttemptFastBootCold	Enables or disables the fast cold boot function.	● Disabled ● Enabled	Enabled
Data Scrambling for DDR4/5	ScrambleEn	Selects the data scrambling for DDR4/5.	● Enabled ● Disabled	Enabled
Custom Refresh Enable	CustomRefreshRateEn	Enables or disables the custom refresh function.	● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Custom Refresh Rate	CustomRefreshRate	Sets the custom memory refresh rate.	20 to 40	20
Refresh Options	refreshMode	Sets the memory self-refresh frequency mode.	• Dynamic Mode • Static 2x Mode	Static 2x Mode
./Advanced/Socket Configuration/Memory Configuration/Memory Channel Control				
CPU 1 Channel A Control	MemChannelEnable[0]	Enables or disables memory channel A of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel B Control	MemChannelEnable[1]	Enables or disables memory channel B of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel C Control	MemChannelEnable[2]	Enables or disables memory channel C of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel D Control	MemChannelEnable[3]	Enables or disables memory channel D of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel E Control	MemChannelEnable[4]	Enables or disables memory channel E of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel F Control	MemChannelEnable[5]	Enables or disables memory channel F of CPU 1.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 1 Channel G Control	MemChannel Enable[6]	Enables or disables memory channel G of CPU 1.	• Disabled • Enabled	Enabled
CPU 1 Channel H Control	MemChannel Enable[7]	Enables or disables memory channel H of CPU 1.	• Disabled • Enabled	Enabled
CPU 2 Channel A Control	MemChannel Enable[8]	Enables or disables memory channel A of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel B Control	MemChannel Enable[9]	Enables or disables memory channel B of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel C Control	MemChannel Enable[10]	Enables or disables memory channel C of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel D Control	MemChannel Enable[11]	Enables or disables memory channel D of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel E Control	MemChannel Enable[12]	Enables or disables memory channel E of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel F Control	MemChannel Enable[13]	Enables or disables memory channel F of CPU 2.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 2 Channel G Control	MemChannel Enable[14]	Enables or disables memory channel G of CPU 2.	• Disabled • Enabled	Enabled
CPU 2 Channel H Control	MemChannel Enable[15]	Enables or disables memory channel H of CPU 2.	• Disabled • Enabled	Enabled
CPU 3 Channel A Control	MemChannel Enable[16]	Enables or disables memory channel A of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel B Control	MemChannel Enable[17]	Enables or disables memory channel B of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel C Control	MemChannel Enable[18]	Enables or disables memory channel C of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel D Control	MemChannel Enable[19]	Enables or disables memory channel D of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel E Control	MemChannel Enable[20]	Enables or disables memory channel E of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel F Control	MemChannel Enable[21]	Enables or disables memory channel F of CPU 3.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 3 Channel G Control	MemChannel Enable[22]	Enables or disables memory channel G of CPU 3.	• Disabled • Enabled	Enabled
CPU 3 Channel H Control	MemChannel Enable[23]	Enables or disables memory channel H of CPU 3.	• Disabled • Enabled	Enabled
CPU 4 Channel A Control	MemChannel Enable[24]	Enables or disables memory channel A of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel B Control	MemChannel Enable[25]	Enables or disables memory channel B of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel C Control	MemChannel Enable[26]	Enables or disables memory channel C of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel D Control	MemChannel Enable[27]	Enables or disables memory channel D of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel E Control	MemChannel Enable[28]	Enables or disables memory channel E of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel F Control	MemChannel Enable[29]	Enables or disables memory channel F of CPU 4.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU 4 Channel G Control	MemChannel Enable[30]	Enables or disables memory channel G of CPU 4.	• Disabled • Enabled	Enabled
CPU 4 Channel H Control	MemChannel Enable[31]	Enables or disables memory channel H of CPU 4.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Memory Configuration/Page Policy				
Page Policy	PagePolicy	Sets the page management policy.	• Closed • Adaptive	Closed
./Advanced/Socket Configuration/Memory Configuration/Memory Map				
Volatile Memory Mode	volMemMode	Enables the 1LM or 2LM memory mode.	• 1LM • 2LM	1LM
./Advanced/Socket Configuration/Memory Configuration/Memory RAS Configuration				
Mirror Mode	MirrorMode	Sets the memory mirroring mode.	• Disabled • Full Mirror Mode • Partial Mirror Mode	Disabled
UEFI ARM Mirror	PartialMirrorUefi	Enables or disables the UEFI ARM mirroring mode.	• Disabled • Enabled	Disabled
ARM Mirror percentage	PartialMirrorUefiPercent	Sets the ARM image percentage. 1275 represents 12.75%.	0 to 5000	0
Correctable Error Threshold	spareErrTh	Sets the correctable error threshold.	0 to 0x7FFF	0x1770

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Leaky Bucket Time Window Based Interface	leakyBktTimeWindow	Enables or disables the interface based on the leaky bucket time window.	• Disabled • Enabled	Disabled
Leaky Bucket Low Bit	leakyBktLo	Sets the low bit of the leaky bucket.	0x1 to 0x29	0x10
Leaky Bucket High Bit	leakyBktHi	Sets the high bit of the leaky bucket.	0x1 to 0x29	0x11
Leaky Bucket Time Window Based Interface Hour	leakyBktHour	Sets the leaky bucket time window based on hour.	0 to 3744	24
Leaky Bucket Time Window Based Interface Minute	leakyBktMinute	Sets the leaky bucket time window based on minute.	0 to 60	0
Partial Cache Line Sparing PCLS	PclsEn	Enables or disables the partial cache line sparing (PCLS).	• Disabled • Enabled	Enabled
ADDDC Sparing	ADDDCEn	Enables or disables the ADDDC reservation function.	• Disabled • Enabled	Enabled
Patrol Scrubbing	PatrolScrub	Enables or disables the patrol scrubbing function.	• Enabled at End of POST • Disabled	Enabled at End of POST

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Patrol Scrubbing Interval	PatrolScrubDuration	Sets the time interval (in hours) for the patrol scrubbing to be performed. The value ranges from 0 to 24.	0~24	24
DDR5 ECS	ErrorCheckScrub	Enables or disables the DDR5 error check and scrubbing (ECS) function.	● Enabled ● Disabled	Enabled
./Advanced/Socket Configuration/Memory Configuration/PMem Configuration/PMem Secure Erase Unit				
Erase All DIMMs	setSecureEraseAllDIMMs	Enables or disables the function of erasing the intrinsic memory area of all PMems in the system.	● Disabled ● Enabled	Disabled
S1 CH0	setSecureEraseSktCh[0]	Erases the intrinsic memory area of PMem on CPU 1 channel 0.	● Disabled ● Enabled	Disabled
S1 CH1	setSecureEraseSktCh[1]	Erases the intrinsic memory area of PMem on CPU 1 channel 1.	● Disabled ● Enabled	Disabled
S1 CH2	setSecureEraseSktCh[2]	Erases the intrinsic memory area of PMem on CPU 1 channel 2.	● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
S1 CH3	setSecureEraseSktCh[3]	Erases the intrinsic memory area of PMem on CPU 1 channel 3.	• Disabled • Enabled	Disabled
S1 CH4	setSecureEraseSktCh[4]	Erases the intrinsic memory area of PMem on CPU 1 channel 4.	• Disabled • Enabled	Disabled
S1 CH5	setSecureEraseSktCh[5]	Erases the intrinsic memory area of PMem on CPU 1 channel 5.	• Disabled • Enabled	Disabled
S1 CH6	setSecureEraseSktCh[6]	Erases the intrinsic memory area of PMem on CPU 1 channel 6.	• Disabled • Enabled	Disabled
S1 CH7	setSecureEraseSktCh[7]	Erases the intrinsic memory area of PMem on CPU 1 channel 7.	• Disabled • Enabled	Disabled
S2 CH0	setSecureEraseSktCh[8]	Erases the intrinsic memory area of PMem on CPU 2 channel 0.	• Disabled • Enabled	Disabled
S2 CH1	setSecureEraseSktCh[9]	Erases the intrinsic memory area of PMem on CPU 2 channel 1.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
S2 CH2	setSecureEraseSktCh[10]	Erases the intrinsic memory area of PMem on CPU 2 channel 2.	• Disabled • Enabled	Disabled
S2 CH3	setSecureEraseSktCh[11]	Erases the intrinsic memory area of PMem on CPU 2 channel 3.	• Disabled • Enabled	Disabled
S2 CH4	setSecureEraseSktCh[12]	Erases the intrinsic memory area of PMem on CPU 2 channel 4.	• Disabled • Enabled	Disabled
S2 CH5	setSecureEraseSktCh[13]	Erases the intrinsic memory area of PMem on CPU 2 channel 5.	• Disabled • Enabled	Disabled
S2 CH6	setSecureEraseSktCh[14]	Erases the intrinsic memory area of PMem on CPU 2 channel 6.	• Disabled • Enabled	Disabled
S2 CH7	setSecureEraseSktCh[15]	Erases the intrinsic memory area of PMem on CPU 2 channel 7.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Memory Configuration/PMem Configuration				
PMem Factory Reset/Clear	FactoryResetClear	Enables or disables the PMem Factory Reset/Clear function.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Publish ARS capability	NgnArsPublish	Enables or disables the address range inspection capability open to the OS.	• Disabled • Enabled	Enabled
PMem CMD Time	NgnCmdTime	Sets the PMem command time.	• Auto • 1N • 2N	Auto
PMem ECC Read Check	NgnEccRdChk	Enables or disables the PMem ECC read check function.	• Disabled • Enabled	Enabled
PMem Latch System Shutdown State	LatchSystemShutdownState	Enables or disables the PMem latch shutdown function.	• Disabled • Enabled	Enabled
Snoopy mode for 2LM	EliminateDirectoryInFarMemory	Enables or disables the snoopy mode for 2LM.	• Enabled • Disabled	Disabled
Power Cycle on PMem Surprise Clock Stop	NvmdimmPowerCyclePolicy	Enables or disables the power-off restart policy when the PMem clock stops unexpectedly.	• Enabled • Disabled	Enabled
Snoopy mode for AD	DisableDirForAppDirect	Enables or disables the APP Direct (AD) mode.	• Disabled • Enabled	Disabled
LSx implementation	LsxImplementation	Sets the ACPI method implementation mode.	• SWSMI • ASL	ASL

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Extended Type 17 Structure	ExtendedType17	Enables or disables the extended type 17 structure.	• Disabled • Enabled	Enabled
SMBus Max Access Time	NvdimmSmbusMaxAccessTime	Sets the maximum SMBus access time.	0 to 512	350
SMBus Release Delay	NvdimmSmbusReleaseDelay	Sets the SMBus release delay.	0 to 512	150
NVDIMM Mailbox in NFIT	NfitPublishMailboxStructs	Enables or disables the NVDIMM mailbox in NFIT.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Memory Configuration/Memory Dfx Configuration				
3-Way Channel Interleaving	DfxMod3Support	Enables or disables the 3-way channel interleaving.	• Enabled • Disabled	Enabled
./Advanced/Socket Configuration/Memory Configuration/RMT Configuration Menu				
Rank Margin Tool	EnableRMT	Enables or disables Rank Margin Tool (RMT).	• Disabled • Enabled	Disabled
Scrambler	RMTScrambler	Enables or disables the scrambler during the RMT test.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/IIO Configuration/Socket 1/2/3/4 Configuration/Port 1A/1B/1C/1D/1E/1F/1G/1H/2A/2B/2C/2D/2E/2F/2G/2H/3A/3B/3C/3D/3E/3F/3G/3H/4A/4B/4C/4D/4E/4F/4G/4H/5A/5B/5C/5D/5E/5F/5G/5H **NOTE** ● The values of **index** from **Socket1 Configuration/Port 1A** to **Socket1 Configuration/Port 5H** are 1 to 40 in sequence. ● The values of **index** from **Socket2 Configuration/Port 1A** to **Socket2 Configuration/Port 5H** are 58 to 97 in sequence. ● The values of **index** from **Socket3 Configuration/Port 1A** to **Socket3 Configuration/Port 5H** are 115 to 154 in sequence. ● The values of **index** from **Socket4 Configuration/Port 1A** to **Socket4 Configuration/Port 5H** are 172 to 211 in sequence.				
PCIe Port	PciePortEnable[*index*]	Sets the PCIe port parameters.	● Auto ● Disabled ● Enabled	Auto
PCIe Link Speed	PciePortLinkSpeed[*index*]	Sets the link speed of a PCIe port.	● Auto ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s) ● Gen 4 (16 GT/s) ● Gen 5 (32 GT/s)	Auto
PCIe Port DeEmphasis Level	DeEmphasis[*index*]	Sets de-emphasis for a PCIe port.	● -6.0 dB ● -3.5 dB	-3.5 dB
PCIe Port Max Payload Size	PcieMaxPayload[*index*]	Sets the maximum payload size for a PCIe port.	● 128B ● 256B ● 512B ● Auto	Auto

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PCIe Completion Timeout Value	PcieCtoValue[*index*]	Sets the timeout period of PCIe transfer completion.	• 50us to 50ms • 50us to 100us • 1ms to 10ms • 16ms to 55ms • 65ms to 210ms • 260ms to 900ms • 1s to 3.5s • Disabled	260ms to 900ms
PCIe ASPM Support	PcieAspm[*index*]	Sets the dynamic power management function of the PCIe device connected to the corresponding port.	• Disabled • L1 Only	Disabled
PCIe Port L1 Exit Latency	PcieL1Latency[*index*]	Sets the time required by this port to complete the transition from L1 to L0.	• <1uS • 1uS - 2uS • 2uS - 4uS • 4uS - 8uS • 8uS - 16uS • 16uS - 32uS • 32uS - 64uS • >64uS	8uS - 16uS
MCTP	MctpEn[*index*]	Enables or disables the MCTP function.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket 1 Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO Stack 1	IioStackLegacylo[0]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 2	IioStackLegacylo[1]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 3	IioStackLegacylo[2]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 4	IioStackLegacylo[3]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 5	IioStackLegacylo[4]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket 2 Configuration				
IIO Stack 1	IioStackLegacylo[5]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 2	IioStackLegacylo[6]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO Stack 3	IioStackLegacyIo[7]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 4	IioStackLegacyIo[8]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 5	IioStackLegacyIo[9]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket 3 Configuration				
IIO Stack 1	IioStackLegacyIo[10]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 2	IioStackLegacyIo[11]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 3	IioStackLegacyIo[12]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 4	IioStackLegacyIo[13]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
IIO Stack 5	IioStackLegacylo[14]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/IIO Stack IO Resource Configuration/Socket 4 Configuration				
IIO Stack 1	IioStackLegacylo[15]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 2	IioStackLegacylo[16]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 3	IioStackLegacylo[17]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 4	IioStackLegacylo[18]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
IIO Stack 5	IioStackLegacylo[19]	Enables or disables the default I/O resources of the request stack.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/IIO Configuration/Intel(R) Virtualization for Directed I/O (VT-d)				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Intel(R) VT for Directed I/O (VT-d)	VTdSupport	Enables or disables Intel VT for Directed I/O (VT-d).	● Disabled ● Enabled	Enabled
DMA Control Opt-In Flag	DmaCtrlOptIn	Enables or disables DMA_CTRL_PLATFORM_OPT_IN_FLAG in the ACPI's DMAR table.	● Disabled ● Enabled	Disabled
Interrupt Remapping	InterruptRemap	Enables or disables the VT-d interrupt remapping function.	● Auto ● Enabled ● Disabled	Auto
PCIe ACSCTL	VtdPciAcsCtlWaEn	Enables or disables the overwrite of PCI Access Control Services Control register in PCI root ports.	● Enabled ● Disabled	The default value of this parameter varies depending on the server model: ● G8600 V7 and G5500 V7 Disabled ● 2288 V7, 2488H V7, and 5885H V7 Enabled
./Advanced/Socket Configuration/IIO Configuration/Intel(R) VMD technology				
Intel(R) VMD Config	SystemVMDConfigEnable	Enables or disables the volume management device (VMD) function for PCIe devices.	● Disabled ● Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/IIO Configuration/IIO DFX Configuration/ Socket1/2/3/4 Configuration/Port 1A/1B/1C/1D/1E/1F/1G/1H/2A/2B/2C/2D/2E/2F/2G/2H/3A/3B/3C/3D/3E/3F/3G/3H /4A/4B/4C/4D/4E/4F/4G/4H/5A/5B/5C/5D/5E/5F/5G/5H **NOTE** ● The value of **index** of **Socket1 Configuration/Port DMI** is **0**. ● The values of **index** from **Socket1 Configuration/Port 1A** to **Socket1 Configuration/Port 5H** are 1 to 40 in sequence. ● The values of **index** from **Socket2 Configuration/Port 1A** to **Socket2 Configuration/Port 5H** are 58 to 97 in sequence. ● The values of **index** from **Socket3 Configuration/Port 1A** to **Socket3 Configuration/Port 5H** are 115 to 154 in sequence. ● The values of **index** from **Socket4 Configuration/Port 1A** to **Socket4 Configuration/Port 5H** are 172 to 211 in sequence.				
./Advanced/Socket Configuration/IIO Configuration/IIO DFX Configuration				
EV DFX Features	DFXEnable	Enables or disables the EV DFX function.	● Enabled ● Disabled	Disabled
Link Re-Train	DfxLinkRetrainEn[*index*]	Enables the link retraining function when the link speed or bandwidth decreases.	● Disabled ● Enabled	Disabled
./Advanced/Socket Configuration/IIO Configuration/IIO Global Performance Tuning				
Retimer Low Latency Mode	RetimerLowLatencyMode	Sets the re-timer low latency mode.	● Disabled ● Enabled ● 16GT/s Only ● 32GT/s Only	Enabled
./Advanced/Socket Configuration/IIO Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
PCI 64-Bit Resource Allocation	Pci64BitResourceAllocation	Enables or disables the PCI 64-bit resource allocation function. This option is automatically enabled when the server restarts when some PCIe devices that require more than 4 GB memory resources are used.	• Disabled • Enabled	Enabled
PCIe Completion Timeout	PcieCtoGlobal	Sets whether the completion timeout is controlled by each port independently or globally.	• Per-Port • Global	Per-Port
PCIe Completion Timeout Value	PcieCtoGlobalValue	Sets the timeout period of PCIe transfer completion.	• 50us to 50ms • 50us to 100us • 1ms to 10ms • 16ms to 55ms • 65ms to 210ms • 260ms to 900ms • 1s to 3.5s • Disabled	260ms to 900ms
./Advanced/Socket Configuration/Advanced Power Management Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Performance Profile	BenchMarkSelection	Select an energy efficiency test scenario.	• Custom • Efficiency • Performance • Load Balance • High RAS • HPC • General Computing • Low Latency • Server Side Java • Memory Throughput • I/O Throughput • Energy Saving • NFV	Custom
Static Turbo	StaticTurbo	Sets the static turbo policy to be applied by the BIOS.	• Disabled • Manual • Auto	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
CPU Frequency Select	FreqSelect	You need to select the frequency value between the fundamental frequency and the turbo frequency, in 100 MHz. When the input value is less than the fundamental frequency, set the value based on the fundamental frequency. When the input value is greater than the supported maximum turbo frequency, set the value based on the maximum turbo frequency.	12 to 50	50
PSS Table Turbo Frequency	PSSTableTurboFrequency	Select the ACPI _PSS table turbo frequency. The default is the maximum non-turbo frequency plus 1MHz.	• Max Non-Turbo Frequency Plus One • Max Turbo Frequency	Max Non-Turbo Frequency Plus One
DEMT	PowerSaving	Enables or disables the Dynamic Energy Management Technology (DEMT) mode.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SYS_USAGE Threshold	SystemCpuUsage	Sets the **SYS_USAGE** threshold.	50 to 99	95
SMI Interval	TcoTimeout	Sets the SMI interval in 0.6s.	2 to 10	6
Low Occupy Control	LowOccupyControl	Enables or disables the low usage control function.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU P-State Control				
AVX P1	AvxP1Level	Sets the AVX P1 level.	• Nominal • Level 1 • Level 2	Nominal
Intel SST-PP	IssTdpLevel	Sets the Intel speed select technology (SST).	• Auto • Level 0 • Level 1 • Level 2 • Level 3 • Level 4	Auto
Dynamic SST-PP	DynamicIss	Enables or disables the dynamic SST-PP.	• Disabled • Enabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Activate SST-BF	ProcessorActivePbf	Allows SST-BF to be enabled. **NOTE** This parameter is not displayed in the following cases: ● SST-BF is not supported by all CPU models. ● **Hardware P-State** is set to **Disabled** or **Out of Band Mode**. ● **AVX P1** is not set to **Nominal**.	● Enabled ● Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Configure SST-BF	ProcessorConfigurePbf	Allows BIOS to configure SST-BF high priority cores so that SW does not need to be configured. **NOTE** This parameter is not displayed in the following cases: ● SST-BF is not supported by all CPU models. ● **Hardware P-State** is set to **Disabled** or **Out of Band Mode**. ● **AVX P1** is not set to **Nominal**. This parameter can be edited in the following cases: **Activate SST-BF** is set to **Enabled** and **Hardware P-State** is set to **Native Mode with No Legacy Support**.	● Enabled ● Disabled	Enabled
SpeedStep (Pstates)	ProcessorEistEnable	Enables or disables EIST (P state).	● Disabled ● Enabled	Enabled
EIST PSD Function	ProcessorEistPsdFunc	Sets the PSD function.	● HW_ALL ● SW_ALL	HW_ALL

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Boot performance mode	BootPState	Sets the boot performance mode.	• Max Performance • Max Efficient • Set by Intel Node Manager	Max Performance
Energy Efficient Turbo	EETurboDisable	Enables or disables the energy saving turbo mode.	• Disabled • Enabled	Enabled
Turbo Mode	TurboMode	Enables or disables the processor acceleration mode.	• Disabled • Enabled	Enabled
CPU Flex Ratio Override	ProcessorFlexibleRatioOverrideEnable	Enables or disables the CPU frequency reset function in non-Turbo mode.	• Disabled • Enabled	Disabled
CPU Core Flex Ratio	ProcessorFlexibleRatio	Sets the processor core frequency in non-Turbo mode	0 to 100	23
./Advanced/Socket Configuration/Advanced Power Management Configuration/Hardware PM State Control				
Hardware P-State	ProcessorHWPMEnable	Sets the Hardware P-State function control switch.	• Disabled • Native Mode • Out of Band Mode • Native Mode with No Legacy Support	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
EPP Enable	ProcessorEPPEnable	Enables or disables the energy performance preference (EPP) control switch.	• Disabled • Enabled	Enabled
EPP Profile	ProcessorEppProfile	Sets the energy preference policy.	• Performance • Balanced Performance • Balanced Power • Power	Balanced Performance
Intel(R) Turbo Boost Max Technology 3.0	EnableItbm	Enables or disables the Intel turbo boost max technology 3.0 support. **NOTE** This parameter is available when the system supports the Intel turbo boost max technology 3.0.	• Enabled • Disabled	Enabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Frequency Prioritization				
SST-CP	ProcessorSstCpSetting	Enables or disables the SST-CP function, which will activate the per-core power budget when enabled.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU C-State Control				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Enable Monitor MWAIT	MonitorMWait	Enables, disables, or automatically sets the MONITOR MWAIT instruction.	• Disabled • Enabled • Auto	Disabled
CPU C6 report	C6Enable	Sets the feature of reporting CPU C6 (ACPI C3) information to the OS.	• Disabled • Enabled • Auto	Disabled
Enhanced Halt State (C1E)	ProcessorC1e Enable	Enables or disables the enhanced halt state (C1E) function.	• Disabled • Enabled	Disabled
C1E OS Indicator	CSOSIndicator	Enables or disables the CPU global C1E-state indicator of the OS.	• Disabled • Enabled	Disabled
C6 OS Indicator	C6OSIndicator	Enables or disables the CPU C6 status indicator of the OS.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Package C-State Control				
Package C-State	PackageCState	Sets the deep energy saving.	• C0/C1 State • C2 State • C6(Non-Retention State) • C6(Retention State) • No Limit • Auto	C0/C1 State

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU Advanced PM Tuning				
Uncore Freq Scaling	UncoreFreqScaling	Sets the non-core frequency scaling function.	• Disabled • Enabled • Manual	Enabled
Optimized Power Mode	OptimizedPowerMode	Enables or disables the optimized power mode.	• Enabled • Disabled	Disabled
Uncore Freq	InputUncoreFreq	Uncore frequency input by the user.	0 to 127	127
Input Min Uncore Freq	InputMinUncoreFreq	Minimum input uncore frequency.	0 to 127	0
Input Max Uncore Freq	InputMaxUncoreFreq	Maximum input uncore frequency.	0 to 127	127
./Advanced/Socket Configuration/Advanced Power Management Configuration/CPU Advanced PM Tuning/Energy Perf BIAS				
Power Performance Tuning	PwrPerfTuning	Sets the power performance tuning function.	• OS Controls EPB • BIOS Controls EPB • PECI Controls EPB	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	AltEngPerfBIAS	Sets the ENERGY_PERF_BIAS_CFG mode.	• Performance • Balanced Performance • Balanced Power • Power	Balanced Performance
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Thermal				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Throttling Mode	thermalthrottlingsupport	Sets the thermal energy throttling mode.	• Disabled • CLTT	CLTT
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options				
CKE Power Down	CkeProgramming	Enables or disables the CKE power-down function.	• Disabled • Enabled	Disabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options/CKE Feature				
CKE Idle Timer	CkeIdleTimer	Sets the CKE idle timer, in nanoseconds.	0 to 255	20
PPD	PpdEn	Enables or disables the pre-charge power down (PPD) function.	• Disabled • Enabled	Enabled
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options				
SREF Feature	SrefProgramming	Sets the self-refresh mode, which is used to retain data in sleep mode in low-power mode.	• Auto • Manual	Manual
./Advanced/Socket Configuration/Advanced Power Management Configuration/Memory Power & Thermal Configuration/Memory Power Savings Advanced Options/Self Refresh Feature				
CK in SR	CkMode	Sets the clock behavior during self-refresh.	• Driven • Pulled Low	Pulled Low

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Advanced/PCH-IO Configuration/PCI Express Configuration/PCI Express Root Port *X*				
ACS	PcieRootPort ACS[0]	Enable or disable Access Control Services Extended Capability. **NOTE** ● Only BIOS 01.02.08.09 and later versions support this parameter.	● Disabled ● Enabled	The default value of this parameter varies depending on the server model: ● G8600 V7 and G5500 V7 Disabled ● 2288 V7, 2488H V7, and 5885H V7 Enabled
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 1 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** cannot be modified.				
SATA Configuration	PchSata[0]	Enables or disables the SATA controller.	● Disabled ● Enabled	Enabled
SATA Mode Selection	SataInterface Mode[0]	Sets the working mode of the SATA controller.	● AHCI ● RAID	AHCI
RAID Device ID	RaidDeviceId[0]	Sets the device ID in RAID mode.	● Client ● Alternate ● Server	Server
SATA Port 0	SataPortController0[0]	Enables or disables the SATA port.	● Disabled ● Enabled	Enabled
SATA Port 1	SataPortController0[1]	Enables or disables the SATA port.	● Disabled ● Enabled	Enabled
SATA Port 2	SataPortController0[2]	Enables or disables the SATA port.	● Disabled ● Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController0[3]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController0[4]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController0[5]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController0[6]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController0[7]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 2 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** cannot be modified.				
SATA Configuration	PchSata[1]	Enables or disables the SATA controller.	• Disabled • Enabled	Enabled
SATA Mode Selection	SataInterfaceMode[1]	Sets the working mode of the SATA controller.	• AHCI • RAID	AHCI
RAID Device ID	RaidDeviceId[1]	Sets the device ID in RAID mode.	• Client • Alternate • Server	Server
SATA Port 0	SataPortController1[0]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 1	SataPortController1[1]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 2	SataPortController1[2]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController1[3]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController1[4]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController1[5]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController1[6]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController1[7]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/PCH-IO Configuration/SATA And RST Configuration/Controller 3 SATA And RST Configuration **NOTE** If **SATA Port***x* is not displayed on the BIOS screen, the corresponding **SataPortController** cannot be modified.				
SATA Configuration	PchSata[2]	Enables or disables the SATA controller.	• Disabled • Enabled	Enabled
SATA Mode Selection	SataInterfaceMode[2]	Sets the working mode of the SATA controller.	• AHCI • RAID	AHCI
RAID Device ID	RaidDeviceId[2]	Sets the device ID in RAID mode.	• Client • Alternate • Server	Server
SATA Port 0	SataPortController2[0]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 1	SataPortController2[1]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 2	SataPortController2[2]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
SATA Port 3	SataPortController2[3]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 4	SataPortController2[4]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 5	SataPortController2[5]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 6	SataPortController2[6]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
SATA Port 7	SataPortController2[7]	Enables or disables the SATA port.	• Disabled • Enabled	Enabled
./Advanced/PCH-IO Configuration/PCH-IO Configuration/USB Configuration				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Front USB Control/Rear USB Control ● USB Port 1	FsUsbPort[2]	Specifies the USB ports on the front panel/rear USB Control. Enables or disables this USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the front panel of the server.	● Enabled ● Disabled	Enabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Front USB Control/Rear USB Control ● USB Port 2	FsUsbPort[3]	Specifies the USB ports on the front panel/rear USB Control. Enables or disables this USB physical port. The menu options are as follows: ● Enabled ● Disabled **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports 1 and 2 correspond to USB 3.0 ports on the front panel of the server.	● Enabled ● Disabled	Enabled

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Built-in USB Control ● USB Port	FsUsbPort[4]	Specifies the built-in USB port. Enables or disables this USB physical port. **NOTE** ● USB devices connected to physical ports set to **Disabled** cannot be detected by the BIOS or OS. ● Mapping between ports and physical ports: Ports correspond to the built-in USB 3.0 ports of the server.	● Enabled ● Disabled	Enabled
USB3.0 Port	FsUsb3Port	Enable or disable this USB3.0 Physical Connector (physical port). Once disabled, any USB3.0 devices plug into the connector will not be detected by BIOS or OS. **NOTE** Only G8600 V7 supports this parameter.	● Enabled ● Disabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Legacy USB Support	UsbLegacySupport	Legacy USB support function. **NOTE** Only BIOS 01.02.08.05 and later versions support this parameter.	• Enabled • Disabled • Auto	Enabled
./Advanced/BMC Configuration/BMC Configuration				
BMC WDT Support For POST	SvrMngmntFrb2Enable	Enables or disables the BMC watchdog timer at the start of POST.	• Disabled • Enabled	Disabled
BMC WDT Time Out For POST	POSTBootWDTimerTimeout	Sets the maximum time allowed for the system to start the BIOS. If timeout occurs, the watchdog is triggered.	18 to 25	20
BMC WDT Action For POST	POSTBootWDTimerPolicy	Sets the action to be taken after the watchdog timer times out.	• NoAction • HardReset • PowerDown • PowerCycle	HardReset
BMC WDT Support For OS	OSBootWDTimer	Enables or disables the watchdog timer on the OS.	• Disabled • Enabled	Disabled
BMC WDT Time Out For OS	OSBootWDTimerTimeout	Sets the maximum time allowed for loading the OS completely, in minutes.	2 to 8	5

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
BMC WDT Action For OS	OSBootWDTimerPolicy	Sets the action to be taken after the watchdog timer times out.	• NoAction • HardReset • PowerDown • PowerCycle	HardReset
./Advanced/Console Redirection Configuration				
Console Redirection	ConsoleRedirection	Enables or disables the serial port redirection.	• Disabled • Enabled	Enabled
Terminal Type	TerminalType	Sets the simulation type. The BIOS simulation type must match the mode selected in the terminal program.	• VT_100 • VT_100+ • VT_UTF8 • PC_ANSI • LOG_TERM	VT_100
Baud Rate	BaudRate	Sets the baud rate for serial port redirection.	• 115200 • 57600 • 38400 • 19200 • 9600 • 4800 • 2400 • 1200	115200
Data Bits	DataBits	Sets the data length of serial port redirection.	• 7 Bits • 8 Bits	8 Bits
Parity	Parity	Sets serial port redirection verification.	• None • Even • Odd	None

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Stop Bits	StopBits	Sets the stop bit of the serial port redirection function.	• 1 Bit • 2 Bit	1 Bit
Flow Control	FlowControl	Sets the control flow of the serial port redirection.	• None • RTS/CTS	None
./Advanced/PXE Configuration				
Slot PXE Control	SlotPxeEnable	Enables or disables the PXE function of all external PCIe NICs.	• Disabled • Enabled	Enabled
./Advanced/PXE Configuration/FLEXIO 1 PXE Configuration--FLEXIO 3 PXE Configuration				
Port 1 PXE Enabled	PXE1Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
Port 2 PXE Enabled	PXE2Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
Port 3 PXE Enabled	PXE3Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
Port 4 PXE Enabled	PXE4Setting	Enables or disables the PXE function of port of OCP NIC.	• Disabled • Enabled	Enabled
./Advanced/System Event Log				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
RAS Log Level	RasLogLevel	Sets the RAS log level.	• None • MIN (BASIC_FLOW) • MID (BASIC_FLOW, FUNC_FLOW) • MAX (BASIC_FLOW, FUNC_FLOW, REG)	MIN (BASIC_FLOW)
Viral Status	ViralEn	Enables or disables the virus status. **NOTE** This parameter is available only when **System Errors** is set to **Enabled**.	• Enabled • Disabled	Disabled
./Advanced/System Event Log/eMCA Settings				
LMCE Support	LmceEn	Enable or disable local MCE firmware support.	• Enabled • Disabled	Enabled
Opportunistic Spare Core	OscEn	Enables or disables the opportunity spare core. **NOTE** This parameter is unavailable when **eMCA Logging Support** is set to **Disabled**.	• Enabled • Disabled	Disabled
./Advanced/System Event Log/Error Control Setting				

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Patrol Scrub Error Reporting	PatrolScrubErrorReporting	Allows you to select the patrol scrub error type. **NOTE** This parameter is available when **System Memory Poisoning** is set to **Enabled**.	• UCNA • SRAO	UCNA
./Advanced/System Event Log/DWR Configuration				
Dirty Warm Reset	DwrEnable	Enables or disables DWR. The function promotes regular resets of DWR under internal error conditions.	• Enabled • Disabled	Enabled
Ierr Global Reset	IerrResetEnabled	Enables or disables the IERR global reset.	• Enabled • Disabled	Enabled
DWR/IERR Error harvesting stall	DwrStall	Enables or disables the DWR/IERR error harvesting stall. After this function is enabled, if a DWR/IERR error is captured, the system automatically processes the error. After this function is disabled, the system logs the error but does not process it.	• Enabled • Disabled	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
./Security				
TPM State	TpmState	TPM Status.	• Disabled • Enabled	Enabled
Simple Password	Authority	Enables or disables the simple password function.	• Disabled • Enabled	Disabled
Password Expiration Date	PasswordExpiration	Sets the validity period of the password.	• 0 day • 30 days • 60 days • 90 days • 180 days • 360 days	180 days
./Boot				
Boot Type	UefiOptimizedBootToggle	Sets the system boot type.	• UEFIBoot • LegacyBoot	UEFIBoot
OEM Fast Boot	OemFastBoot	Enables or disables the BIOS fast boot function.	• Disabled • Enabled	Disabled
Network Stack	PxeBootToLan	Enables or disables the network stack function.	• Disabled • Enabled	Enabled
PXE Boot Capability	NetworkProtocol	Sets the PXE boot network.	• Disabled • UEFI:IPv4 • UEFI:IPv6 • UEFI:IPv4/IPv6	UEFI:IPv4
IPv4 PXE	Ipv4Pxe	Enables or disables the IPv4 PXE function.	• Disabled • Enabled	Enabled
IPv6 PXE	Ipv6Pxe	Enables or disables the IPv6 PXE function.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
HTTPS Boot Capability	NetworkHttpsProtocol	Sets the HTTPS boot function.	• Disabled • HTTPS:IPv4 • HTTPS:IPv6 • HTTPS:IPv4/IPv6	HTTPS:IPv4
Boot Fail Policy	BootFailPolicy	Sets the operation to be performed after the boot fails.	• None • Boot Retry • Cold Boot	Boot Retry
PXE Retry Count	PxeRetrylimites	Sets the times of repeated boots from the PXE.	1 to 99	1
PXE Timeout Control	PxeTimeoutRetryCtrl	Sets the number of DHCP connection retries due to timeout occurring when each enabled port is booted from the PXE.	• Disabled • 1 • 2 • 3 • 4	Disabled
SP Boot	SPBoot	Enables or disables the boot function of Smart Provisioning (SP).	• Disabled • Enabled	Enabled
USB Boot	UsbBoot	Enables or disables the boot function of the external USB device.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Parameter	Attribute	Attribute Description	Redfish Option	Default Value
Boot Override	BootOverride	Sets the first priority boot device.	• Disabled • PCIe SSD First • iSCSI First • FC First • FCOE First • PCH Direct First • RAID First • USB First • Local Disk Boot Only	Disabled
OEM Secure Boot	OemSecureBoot	Enables or disables the OEM Secure Boot. **NOTE** This function is only supported in UEFI mode. The Redfish interface can only be used to enable this function.	• Disabled • Enabled	Disabled
./Boot/Boot Sequence				
Hard Disk Drive	HDDSupport	Change Hard Disk Drive boot order.	• Disabled • Enabled	Enabled
DVD-ROM Drive	CDROMSupport	Change DVD-ROM Drive boot order.	• Disabled • Enabled	Enabled
PXE	PXESupport	Change PXE boot order.	• Disabled • Enabled	Enabled
Others	OTHERSupport	Change Other Device boot order.	• Disabled • Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

D Linkage Options in Energy Efficiency Test Scenarios (Only for 1288H V7/2288H V7/5288 V7/5298 V7/G5200 V7)

Table D-1 Linkage options in energy efficiency test scenarios 1

Linkage Option in Energy Efficiency Test Scenarios	Custom	Efficiency	Performance	Load Balance
Hardware Prefetcher	Enabled	Disabled	Enabled	Enabled
Adjacent Cache Prefetch	Enabled	Disabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	Enabled
LLC Prefetch	Enabled	Enabled	Enabled	Enabled
Enable LP [Global]	ALL LPs	ALL LPs	ALL LPs	ALL LPs
DCU Streamer Prefetcher	Enabled	Disabled	Enabled	Enabled
CPU Flex Ratio Override	Disabled	Disabled	Disabled	Disabled
Isoc Mode	Auto	Auto	Auto	Auto
NUMA	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Custom	Efficiency	Performance	Load Balance
Link L1 Enable	Enabled	Enabled	Disabled	Enabled
LLC dead line alloc	Enabled	Enabled	Enabled	Enabled
KTI Prefetch	Enabled	Enabled	Enabled	Enabled
Link Frequency Select	Auto	Auto	Auto	Auto
Enable Monitor MWAIT	Disabled	Enabled	Disabled	Enabled
Uncore Freq Scaling	Enabled	Enabled	Enabled	Enabled
DEMT	Disabled	Enabled	Disabled	Disabled
EIST PSD Function	HW_ALL	HW_ALL	HW_ALL	HW_ALL
Boot performance mode	Max Performance	Max Performance	Max Performance	Max Performance
Energy Efficient Turbo	Enabled	Enabled	Enabled	Enabled
Power Performance Tuning	OS Controls EPB	OS Controls EPB	PECI Controls EPB	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Balanced Performance	Balanced Performance	Balanced Performance	Balanced Performance
SpeedStep (Pstates)	Enabled	Enabled	Enabled	Enabled
Turbo Mode	Enabled	Enabled	Enabled	Enabled
EPP Enable	Enabled	Enabled	Enabled	Enabled
EPP profile	Balanced Performance	Balanced Performance	Performance	Balanced Performance
Static Turbo	Disabled	Disabled	Manual	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Custom	Efficiency	Performance	Load Balance
CPU Frequency Select	50	50	50	50
Enhanced Halt State (C1E)	Disabled	Enabled	Disabled	Enabled
CPU C6 report(29)	Disabled	Enabled	Disabled	Enabled
Hardware P-State	Disabled	Disabled	Out of Band Mode	Disabled
Package C-State	C0/C1 state	Auto	C0/C1 state	Auto
Extreme Edition	Enabled	Enabled	Enabled	Enabled
System Errors	Enabled	Enabled	Enabled	Enabled
FDM	Enabled	Enabled	Enabled	Enabled
System Memory Poisoning	Enabled	Enabled	Enabled	Enabled
CKE Power Down	Disabled	Enabled	Disabled	Disabled
Refresh Options	Dynamic Mode	Dynamic Mode	Dynamic Mode	Dynamic Mode
Page Policy	Disabled	Disabled	Disabled	Disabled
ADDDC Sparing	Enabled	Enabled	Disabled	Enabled
Custom Refresh	Disabled	Disabled	Disabled	Disabled
Custom Refresh Rate	20	20	20	20
Attempt Fast Cold Boot	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Custom	Efficiency	Performance	Load Balance
Patrol Scrubbing	Enabled/ Enable at End of POST	Enabled	Enabled	Enabled
Partial Cache Line Sparing PCLS	Enabled	Enabled	Enabled	Enabled
DDR PPR Type	Soft PPR	Soft PPR	Soft PPR	Soft PPR

Table D-2 Linkage options in energy efficiency test scenarios 2

Linkage Option in Energy Efficiency Test Scenarios	High RAS	HPC	General Computing	Low Latency
Hardware Prefetcher	Enabled	Enabled	Enabled	Enabled
Adjacent Cache Prefetch	Enabled	Enabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	Enabled
LLC Prefetch	Enabled	Enabled	Disabled	Enabled
Enable LP [Global]	ALL LPs	ALL LPs	ALL LPs	ALL LPs
DCU Streamer Prefetcher	Enabled	Enabled	Enabled	Enabled
CPU Flex Ratio Override	Disabled	Disabled	Disabled	Disabled
Isoc Mode	Auto	Auto	Auto	Auto
NUMA	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	High RAS	HPC	General Computing	Low Latency
Link L1 Enable	Disabled	Enabled	Enabled	Enabled
LLC dead line alloc	Enabled	Enabled	Enabled	Enabled
KTI Prefetch	Enabled	Enabled	Enabled	Enabled
Link Frequency Select	Auto	Auto	Auto	Auto
Enable Monitor MWAIT	Disabled	Disabled	Disabled	Disabled
Uncore Freq Scaling	Enabled	Enabled	Enabled	Enabled
DEMT	Disabled	Disabled	Disabled	Disabled
EIST PSD Function	HW_ALL	HW_ALL	HW_ALL	HW_ALL
Boot performance mode	Max Performance	Max Performance	Max Performance	Max Performance
Energy Efficient Turbo	Enabled	Enabled	Enabled	Enabled
Power Performance Tuning	OS Controls EPB	OS Controls EPB	OS Controls EPB	PECI Controls EPB
ENERGY_PERF_BIAS_CFG mode	Balanced Performance	Balanced Performance	Balanced Performance	Balanced Performance
SpeedStep (Pstates)	Enabled	Enabled	Enabled	Enabled
Turbo Mode	Enabled	Enabled	Enabled	Enabled
EPP Enable	Enabled	Enabled	Enabled	Enabled
EPP profile	Balanced Performance	Balanced Performance	Balanced Performance	Performance
Static Turbo	Disabled	Disabled	Disabled	Manual

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	High RAS	HPC	General Computing	Low Latency
CPU Frequency Select	50	50	50	50
Enhanced Halt State (C1E)	Disabled	Disabled	Disabled	Disabled
CPU C6 report(29)	Disabled	Disabled	Disabled	Disabled
Hardware P-State	Disabled	Disabled	Disabled	Out of Band Mode
Package C-State	Auto	C0/C1 state	Auto	C0/C1 state
Extreme Edition	Disabled	Enabled	Enabled	Enabled
System Errors	Enabled	Enabled	Enabled	Enabled
FDM	Enabled	Enabled	Enabled	Enabled
System Memory Poisoning	Enabled	Enabled	Enabled	Enabled
CKE Power Down	Disabled	Disabled	Disabled	Disabled
Refresh Options	Dynamic Mode	Dynamic Mode	Dynamic Mode	Dynamic Mode
Page Policy	Disabled	Disabled	Disabled	Disabled
ADDDC Sparing	Enabled	Enabled	Disabled	Enabled
Custom Refresh	Enabled	Disabled	Disabled	Disabled
Custom Refresh Rate	20	20	20	20
Attempt Fast Cold Boot	Disabled	Enabled	Enabled	Enabled
Patrol Scrubbing	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	High RAS	HPC	General Computing	Low Latency
Partial Cache Line Sparing PCLS	Enabled	Enabled	Enabled	Enabled
DDR PPR Type	Soft PPR	Soft PPR	Soft PPR	Soft PPR

Table D-3 Linkage options in energy efficiency test scenarios 3

Linkage Option in Energy Efficiency Test Scenarios	Server Side Java	Memory Throughput	I/O Throughput	Energy Saving
Hardware Prefetcher	Enabled	Enabled	Enabled	Enabled
Adjacent Cache Prefetch	Enabled	Enabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	Enabled
LLC Prefetch	Disabled	Enabled	Enabled	Enabled
Enable LP [Global]	ALL LPs	Single LP	ALL LPs	Single LP
DCU Streamer Prefetcher	Disabled	Enabled	Enabled	Enabled
CPU Flex Ratio Override	Disabled	Disabled	Disabled	Disabled
Isoc Mode	Auto	Disabled	Auto	Auto
NUMA	Enabled	Enabled	Enabled	Enabled
Link L1 Enable	Enabled	Enabled	Enabled	Auto
LLC dead line alloc	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Server Side Java	Memory Throughput	I/O Throughput	Energy Saving
KTI Prefetch	Enabled	Enabled	Enabled	Enabled
Link Frequency Select	Auto	Auto	Auto	Auto
Enable Monitor MWAIT	Disabled	Disabled	Disabled	Enabled
Uncore Freq Scaling	Enabled	Enabled	Enabled	Enabled
DEMT	Disabled	Disabled	Disabled	Disabled
EIST PSD Function	HW_ALL	HW_ALL	HW_ALL	HW_ALL
Boot performance mode	Max Performance	Max Performance	Max Performance	Max Performance
Energy Efficient Turbo	Enabled	Enabled	Enabled	Enabled
Power Performance Tuning	PECI Controls EPB	OS Controls EPB	PECI Controls EPB	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Balanced Performance	Balanced Performance	Balanced Performance	Balanced Performance
SpeedStep (Pstates)	Enabled	Enabled	Enabled	Enabled
Turbo Mode	Enabled	Enabled	Enabled	Enabled
EPP Enable	Enabled	Enabled	Enabled	Enabled
EPP profile	Performance	Balanced Performance	Balanced Performance	Balanced Performance
Static Turbo	Manual	Disabled	Auto	Disabled
CPU Frequency Select	50	50	50	50

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Server Side Java	Memory Throughput	I/O Throughput	Energy Saving
Enhanced Halt State (C1E)	Disabled	Disabled	Disabled	Enabled
CPU C6 report(29)	Disabled	Disabled	Disabled	Enabled
Hardware P-State	Out of Band Mode	Disabled	Disabled	Out of Band Mode
Package C-State	C0/C1 state	Auto	C0/C1 state	(non Retention) state
Extreme Edition	Enabled	Enabled	Enabled	Enabled
System Errors	Enabled	Enabled	Enabled	Enabled
FDM	Enabled	Enabled	Enabled	Enabled
System Memory Poisoning	Enabled	Enabled	Enabled	Enabled
CKE Power Down	Disabled	Disabled	Disabled	Enabled
Refresh Options	Dynamic Mode	Dynamic Mode	Dynamic Mode	Dynamic Mode
Page Policy	Disabled	Disabled	Disabled	Disabled
ADDDC Sparing	Enabled	Enabled	Enabled	Enabled
Custom Refresh	Disabled	Disabled	Disabled	Disabled
Custom Refresh Rate	20	20	20	20
Attempt Fast Cold Boot	Enabled	Enabled	Enabled	Enabled
Patrol Scrubbing	Enabled	Enabled	Enabled	Enabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	Server Side Java	Memory Throughput	I/O Throughput	Energy Saving
Partial Cache Line Sparing PCLS	Enabled	Enabled	Enabled	Enabled
DDR PPR Type	Soft PPR	Soft PPR	Soft PPR	Soft PPR

Table D-4 Linkage options in energy efficiency test scenarios 4

Linkage Option in Energy Efficiency Test Scenarios	NFV
Hardware Prefetcher	Enabled
Adjacent Cache Prefetch	Enabled
DCU IP Prefetcher	Enabled
LLC Prefetch	Enabled
Enable LP [Global]	ALL LPs
DCU Streamer Prefetcher	Enabled
CPU Flex Ratio Override	Disabled
Isoc Mode	Auto
NUMA	Enabled
Link L1 Enable	Disabled
LLC dead line alloc	Enabled
KTI Prefetch	Enabled
Link Frequency Select	Auto
Enable Monitor MWAIT	Disabled
Uncore Freq Scaling	Enabled
DEMT	Disabled
EIST PSD Function	HW_ALL
Boot performance mode	Max Performance
Energy Efficient Turbo	Disabled

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Linkage Option in Energy Efficiency Test Scenarios	NFV
Power Performance Tuning	BIOS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Performance
SpeedStep (Pstates)	Enabled
Turbo Mode	Enabled
EPP Enable	Enabled
EPP profile	Balanced Performance
Static Turbo	Disabled
CPU Frequency Select	50
Enhanced Halt State (C1E)	Disabled
CPU C6 report(29)	Disabled
Hardware P-State	Disabled
Package C-State	C0/C1 state
Extreme Edition	Enabled
System Errors	Enabled
FDM	Enabled
System Memory Poisoning	Enabled
CKE Power Down	Disabled
Refresh Options	Dynamic Mode
Page Policy	Disabled
ADDDC Sparing	Enabled
Custom Refresh	Disabled
Custom Refresh Rate	20
Attempt Fast Cold Boot	Enabled
Patrol Scrubbing	Enabled
Partial Cache Line Sparing PCLS	Enabled
DDR PPR Type	Soft PPR

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

E Acronyms and Abbreviations

Term	Definition
A	
ACPI	Advanced Configuration and Power Interface
ADR	Asynchronous Dram Refresh
AER	Advanced Error Reporting
AHCI	Advanced Host Controller Interface
ARI	Alternative Routing-ID Interpretation
ARS	Address Range Scrub
ANSI	American National Standards Institute
API	Application Programming Interface
APIC	Advanced Programmable Interrupt Controller
ASPM	Active State Power Management
ADDDC	Adaptive Double Device Data Correction Sparing
B	
BBU	Battery Backup Unit
BMC	Baseboard Management Controller
BIOS	Basic Input/Output System
BIST	Built-In Self-Test
BSSA	BIOS Shared SW Architecture
C	
CE	Correctable Error
CFG	Config

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Term	Definition
CLTT	Closed Loop Thermal Throttling
CMCI	Corrected Machine Check Interrupt
CMOS	Complementary metal-oxide-semiconductor
D	
DCU	Data Cache Unit
DEMT	Dynamic Energy Management Technology
DHCP	Dynamic Host Configuration Protocol
DMA	Direct Memory Access
DMI	Direct Media Interface
DIMM	Dual In-line Memory Module
DRAM	Dynamic Random-Access Memory
DRHD	DMA Remapping Hardware Unit Definition
DXE	Driver Execution Environment
E	
ECC	Error Checking and Correcting
eDPC	Enhanced Downstream Port Containment
EEPROM	Electrically Erasable Programmable Read Only Memory
EFI	Extensible Firmware Interface
EIST	Enhanced Intel SpeedStep Technology
EMP	Emergency Management Port
eMCA	Enhanced Machine Check Architecture
F	
FDM	Fault Diagnose Management
G	
GUID	Globally Unique Identifier
I	
IIO	Integrated I/O Module
IMC	Integrated Memory Controller
iSCSI	Internet Small Computer System Interface

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Term	Definition
ISOC	Isochronous
IRQ	Interrupt Request
L	
LLC	Last Level Cache
LMCE	Local Machine Check Exception
LPASR	Low Power Auto Self Refresh
M	
MADT	Multiple APIC Descriptor Table
MCE	Machine Check Exception
MCTP	Management Component Transport Protocol
ME	Management Engine
MMIO	Memory Mapped I/O
MPSS	Max Payload size Supported
MRC	Memory Reference Code
MWAIT	Monitor Wait
N	
NCSI	Network Controller Sideband Interface
NFIT	NVM DIMM Firmware Interface Table
NUMA	Non-Uniform Memory Access
NIC	Network Interface Card
NVMCTLR	Non-Volatile Memory Controller
O	
OEM	Original Equipment Manufacturer
OLTT	Open Loop Thermal Throttling
OOB	Out Of Band
OS	Operating System
OSB	Opportunistic Snoop Broadcast
P	
PCH	Platform Controller Hub
PCLS	Partial Cache Line Sparing

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Term	Definition
PCU	Power Controller Unit
PEI	Pre EFI Initialization
PECI	Platform Environmental Control Interface
PK	Platform Key
PME	Power Management Event
POST	Power On Self-Test
PPIN	Protected Processor Inventory Number
PSD	P-State Dependency
PXE	Pre-execution Environment
R	
RAID	Redundant Array of Inexpensive Disks
RAPL	Running Average Power Limit
RAS	Reliability, Availability, Serviceability
RDIMM	Registered DIMM
RRQ	Remote Request Queue
ROM	Read-only memory
RTC	Real Time Clock
RTS/CTS	Request To Send/Clear To Send
S	
SATA	Serial Advanced Technology Attachment
SBIOS	System BIOS
SCSI	Small Computer System Interface
SAS	Serial Attached SCSI
SEC	Security
SEL	System Event Log
SPI	Serial Peripheral Interface
SMBIOS	System Management BIOS
SMI	System Management Interrupt
SMM	System Management Mode
SPD	Serial Presence Detect

 Copyright © XFUSION INTERNATIONAL PTE. LTD.

Term	Definition
SR-IOV	Single Root I/O virtualization
SREF	Self Refresh Entry with Frequency Change
SST-PP	Speed Select Technology-Performance Profile
T	
TCG	Trusted Computing Group
TCM	Trusted Cryptography Module
TDP	Thermal Design Power
TPM	Trusted Platform Module
TXT	Trusted Execution Technology
U	
UEFI	Unified Extensible Firmware Interface
UE or UCE	Uncorrectable Error
UFS	Uncore Freq Scaling
UFMT	Uncore Frequency Management Technology
UPI	Ultra Path Interconnect
V	
VBIOS	Video BIOS
VMD	Volume Management Device
VT-d	Intel Virtualization Technology For Directed I/O
W	
WHEA	Windows Hardware Error Architecture

 Copyright © XFUSION INTERNATIONAL PTE. LTD.