VANTAGEO Server

BIOS User Guide (Intel Whitley and Cedar Island)

Version: R1.2

VANTAGEO PRIVATE LIMITED
Corporate Address: 617, Lodha Supremus II,
Road No. 22, Wagle Estate,
Thane - 400604
URL: https://vantageo.com
E-mail: support@vantageo.com
Helpdesk - +91 18002669898

LEGAL INFORMATION

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of VANTAGEO, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. VANTAGEO will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.2	2023-05-25	Added 2.19 Setting C-State and P-State Parameters.
R1.1	2022-11-18	Full-text update.
R1.0	2022-06-02	First edition.

Serial Number: VT20230311

Publishing Date: 2023-05-25 (R1.2)

Contents

About This Manual

Purpose

This manual describes how to modify server BIOS settings.

Intended Audience

This manual is intended for:

- Planning engineers
- Network management and monitoring engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters:

Chapter 1, BIOS Overview	Describes basic BIOS concepts, the precautions for BIOS setup, and the server models that this manual applies to.
Chapter 2, Common Operations	Describes the common operations on the BIOS.
Chapter 3, Front Page Parameter Descriptions	Describes parameters on the Front Page screen and its sub-screens.
Chapter 4, Setup Utility Parameter Descriptions	Describes parameters on the Setup Utility screens.
Chapter 5, Reference: Control Keys for BIOS Setup	Describes common control keys used for BIOS setup.

Conventions

This manual uses the following conventions.

	Notice: indicates equipment or environment safety information. Failure to comply can result in equipment damage, data loss, equipment performance degradation, environmental contamination, or other unpredictable results. Failure to comply will not result in personal injury.
	Note: provides additional information about a topic.

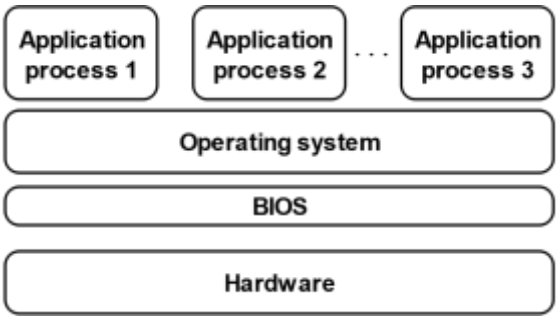
Chapter 1
BIOS Overview

Table of Contents

1.1 Basic Concepts

As a server's most basic program, the BIOS is pre-loaded on a ROM chip on the motherboard. Figure 1-1 shows the BIOS in a system, which bridges server hardware and an operating system. It initializes server hardware before booting an operating system.

Figure 1-1 BIOS in a System



The main functions of the BIOS include:

- Performing POST.
- Initializing CPUs and memory.
- Checking I/O devices and boot devices.
- Booting an operating system.

1.2 Precautions

Before modifying the BIOS setting of a server, you must record the corresponding initial settings so that the original settings can be restored if the modification results in improper operation of the server.

Notice

In general, the factory default settings are the optimal settings. Do not modify any parameter unless you are clear about it. Any improper modification may result in hardware resource conflicts or reduce the system performance.

1.3 Applicable Server Models

This document is applicable to VANTAGEO rack servers based on the **Whitley and Cedar Island** platform, including:

- 2230-RE

Chapter 2
Common Operations

Table of Contents

2.1 Entering the BIOS Setup Utility

Abstract

This procedure describes how to enter the BIOS Setup Utility so that you can view and modify BIOS information.

Steps

1. Connect to the server through either of the following ways:
   - Connect a display, mouse, and keyboard to the server.

- Start the KVM on the Web portal of the BMC.

  For details, refer to "3.8 Remotely Controlling the Server" in the *VANTAGEO Server BMC User Guide (BMC V3)*.

2. Power on and start the server. The POST is started. The system enters the screen displaying the logo and the hot keys for starting the BIOS, see Figure 2-1.

Figure 2-1 Entering the Screen Displaying the Logo and Hot Keys

For a description of the hot keys, refer to Table 2-1.

Table 2-1 Hot Keys for Starting the BIOS

Hot Key	Description
F12	Enters the PXE network environment.
ESC	Enters the Front Page screen of BIOS.
F2/DEL	Enters the BIOS Setup Utility.
F11	Enters the Boot Manager screen.

3. Perform the following operations as required.

To...	Do...
Enter the Front Page screen	Press **Esc**. The Front Page screen is displayed.

To...	Do...
	For a detailed description of the Front Page screen, refer to 3 Front Page Parameter Descriptions.
Enter the Setup Utility screen	Press **F2** or **DEL**. The Setup Utility screen is displayed. For a detailed description of the Setup Utility screen, refer to 4 Setup Utility Parameter Descriptions.

Note

- On the Front Page screen, you can configure boot parameters and devices.
- On the Setup Utility screens, you can configure each parameter.

2.2 Setting the BIOS Language

Abstract

This procedure describes how to set the BIOS language that the BIOS information is displayed in.

Steps

1. On the top-level Setup Utility screen, select the **Main** menu. The **Main** screen is displayed.
2. Select **Language**. The **Language** dialog box is displayed, see Figure 2-2.

Figure 2-2 Language Dialog Box

3. Select English or **Simplified Chinese** as required.
4. Press **F10**. In the displayed dialog box, select **Yes**.

2.3 Setting the BIOS Date and Time

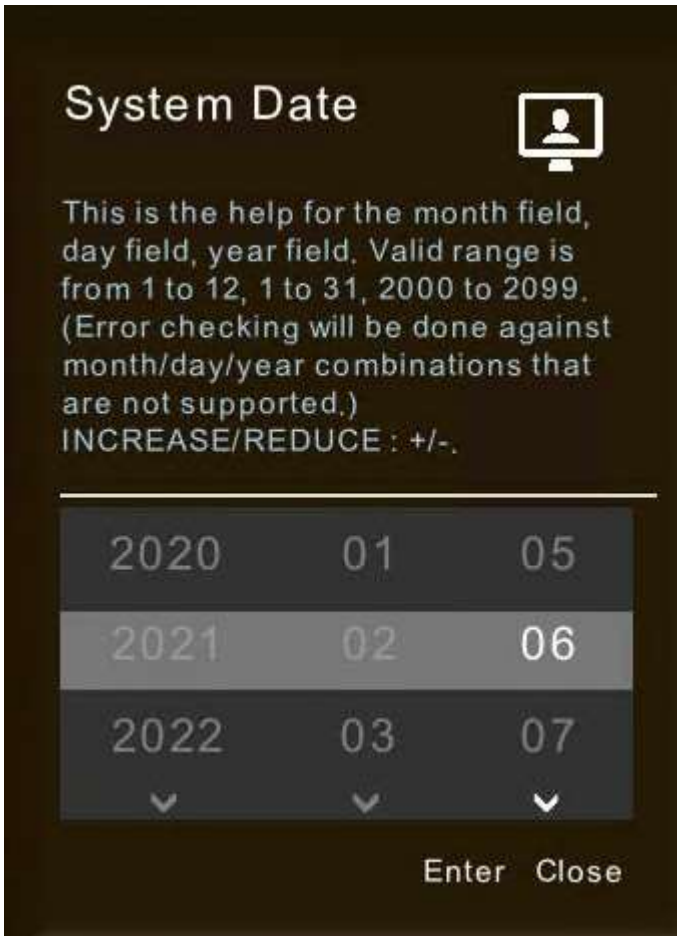
Abstract

This procedure describes how to set the BIOS date and time to the local date and time.

Steps

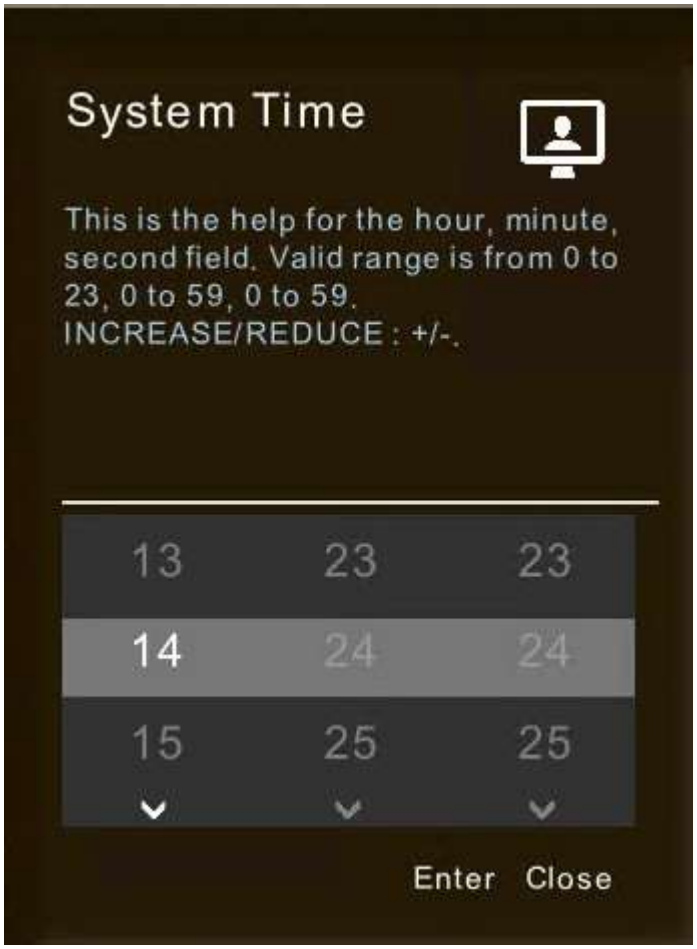
1. On the top-level Setup Utility screen, select the **Main** menu. The **Main** screen is displayed.
2. Select **System Date**. The **System Date** dialog box is displayed, see Figure 2-3.

Figure 2-3 System Date Dialog Box



3. Set the date and click **Enter** to return to the **Main** screen.
4. Select **System Time**. The **System Time** dialog box is displayed, see Figure 2-4.

Figure 2-4 System Time Dialog Box



5. Set the time and click **Enter** to return to the **Main** screen.
6. Press **F10**. In the displayed dialog box, select **Yes**.

2.4 Setting the Boot Mode

Abstract

The server boot modes include:

- Legacy mode: a relatively old boot mode with certain limitations.
- UEFI mode: a relatively new boot mode that supports PXE over IPv6 or IPv4 and provides the UEFI Shell environment.

Note

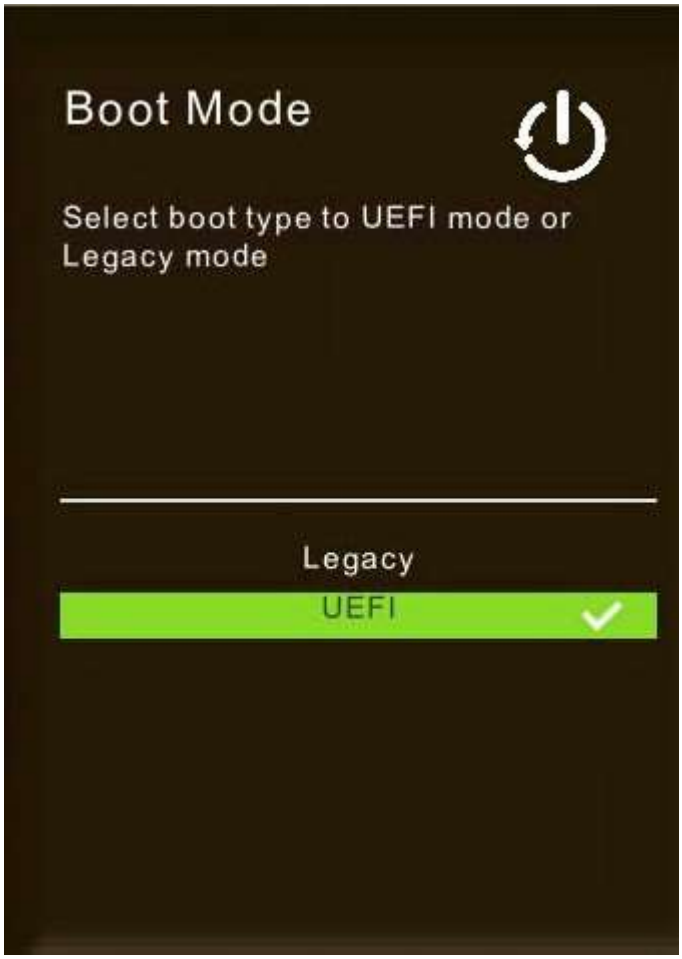
The UEFI mode is recommended.

Steps

1. On the top-level Setup Utility screen, click the **Boot** icon. The **Boot** screen is displayed.

2. Select **Boot Mode**. The **Boot Mode** dialog box is displayed, see Figure 2-5.

Figure 2-5 Boot Mode Dialog Box



3. Select **Legacy** or **UEFI** as required.

Note

After the boot mode is changed, some BIOS parameters are changed.

4. Press **F10**. In the displayed dialog box, select **Yes**.

2.5 Setting the Boot Order

Abstract

Generally, a server is configured with multiple boot devices such as the hard disk and the CD or DVD.

This procedure describes how to set the boot order by adjusting the priorities of these devices from which the server is booted.

Context

By default, the boot order of the server is as follows:

1. Hard disk
2. Network
3. USB device
4. CD/DVD device
5. Other devices

Steps

1. On the top-level Setup Utility screen, select the **Boot** menu. The **Boot** screen is displayed.
2. Select **Boot Device Type Order**. The **Boot Device Type Order** screen is displayed, see Figure 2-6.

Figure 2-6 Boot Device Type Order Screen

For a description of the boot devices, refer to Table 2-2.

Table 2-2 Boot Device Descriptions

Boot Device	Description
Hard Disk Drive	Boots the server from the hard disk.

Boot Device	Description
Network	Boots the server from the network device.
USB	Boots the server from the USB device.
CD/DVD-ROM Drive	Boots the server from the CD/DVD device.
Others	Boots the server from other devices.

3. Press **F5** or **F6** to adjust the priority of the device from which the server is booted.

Note

- The **F5** key is used to lower the device priority by one level.
- The **F6** key is used to raise the device priority by one level.

4. Press **F10**. In the displayed dialog box, select **Yes**.

2.6 Setting the BIOS Password

Abstract

This procedure describes how to set the BIOS password for security purposes when you log in to the server for the first time.

Note

The BIOS password must be kept safely.

Steps

1. On the top-level Setup Utility screen, select the **Security** menu. The **Security** screen is displayed.
2. Select **Set Administrator Password**. The **Set Administrator Password** dialog box is displayed, see Figure 2-7.

Figure 2-7 Set Administrator Password Dialog Box

3. Set the password and click **Yes** to return to the **Security** screen.

Note

The password consists of 8 to 32 characters, including uppercase and lowercase letters, digits, and special characters.

4. Press **F10**. In the displayed dialog box, select **Yes**.

Related Tasks

To change a BIOS password, perform the following operations:

1. On the **Security** screen, select **Set Administrator Password**. The **Set Administrator Password** dialog box is displayed, see Figure 2-8.

Figure 2-8 Set Administrator Password Dialog Box

2. Change the password and click **Yes** to return to the **Security** screen.

Note

The new password cannot be the same as the last three passwords used on the account.

2.7 Clearing the BIOS Password

Abstract

This procedure describes how to clear the BIOS password by entering only the old BIOS password during administrator password setting.

Note

The old BIOS password is just the password that you set before and want to clear now. Therefore, you must properly keep the password that you set.

Steps

1. On the top-level Setup Utility screen, select the **Security** menu. The **Security** screen is displayed.
2. Select **Set Administrator Password**. The **Set Administrator Password** dialog box is displayed, see Figure 2-9.

Figure 2-9 Set Administrator Password Dialog Box

3. In the **Enter Old Password** text box, enter the BIOS password that you want to clear. Leave the other two text boxes blank.
4. Click **Yes** to return to the **Security** screen.
5. Press **F10**. In the displayed dialog box, select **Yes**.

2.8 Restoring the Default BIOS Settings

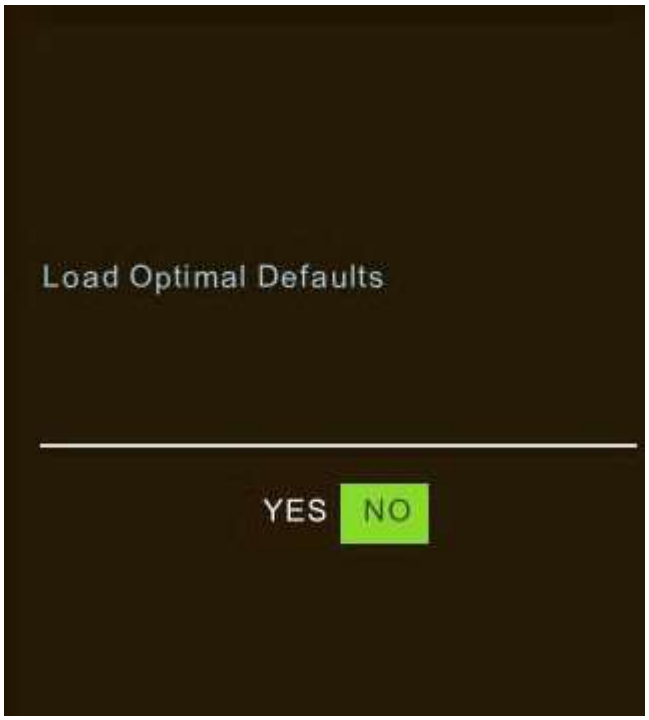
Abstract

This procedure describes how to restore the default BIOS settings when a system error occurs because of unknown changes to the BIOS.

Steps

1. On the top-level Setup Utility screen, perform either of the following operations, then the **Load Optimal Defaults** dialog box is displayed, see Figure 2-10.
   - Press **F9**.
   - Select the **Exit** menu. The **Exit** screen is displayed. Select **Load Defaults**.

Figure 2-10 Load Optimal Defaults Dialog Box



2. Click **Yes**.
3. Press **F10**. In the displayed dialog box, select **Yes**.

2.9 Querying CPU Information

Abstract

This procedure describes how to query CPU information including CPU parameter settings.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Socket Configuration > Processor Configuration > Per-Socket Information**. The **Per-Socket Information** screen is displayed, see Figure 2-11.

Figure 2-11 Per-Socket Information Screen

2.10 Querying Memory Information

Abstract

This procedure describes how to query memory parameter settings.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Memory Topology**. The **Memory Topology** screen is displayed, see Figure 2-12.

Figure 2-12 Memory Topology Screen

2.11 Querying SATA Hard Disk Information

Abstract

This procedure describes how to query parameter settings of SATA hard disks.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **PCH Configuration > PCH SATA Configuration**. The **PCH SATA Configuration** screen is displayed, see Figure 2-13.

Figure 2-13 PCH SATA Configuration Screen

3. Select **PCH Configuration > PCH sSATA Configuration**. The **PCH sSATA Configuration** screen is displayed, see Figure 2-14.

Figure 2-14 PCH sSATA Configuration Screen

2.12 Querying Server Configurations

Abstract

This procedure describes how to query server configurations including the BIOS version number and product name.

Steps

1. On the top-level Setup Utility screen, select the **Main** menu. The **Main** screen is displayed, see Figure 2-15 to Figure 2-16.

Figure 2-15 Main Screen 1

Figure 2-16 Main Screen 2

2.13 Setting the PCIe Function for a Port

Abstract

After the PCIe function of a port is enabled, the port adapts to different PCIe cards to maximize port resource utilization.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Socket Configuration > IIO Configuration > Socketx Configuration**. The **Socketx Configuration** screen is displayed, see Figure 2-17.

Figure 2-17 Socketx Configuration Screen

3. Click the port to be configured. The screen for configuring the port is displayed, see Figure 2-18.

Figure 2-18 Configuring a Port

4. Click **PCI-E Port**. The **PCI-E Port** dialog box is displayed, see Figure 2-19.

Figure 2-19 PCI-E Port Dialog Box

5. Configures the PCIe function as required.
   - **Auto**: Automatic mode.
   - **Disabled**: disables the PCIe function.
   - **Enabled**: enables the PCIe function.
6. Press **F10**. In the displayed dialog box, select **Yes**.

2.14 Setting the Console Redirection Function

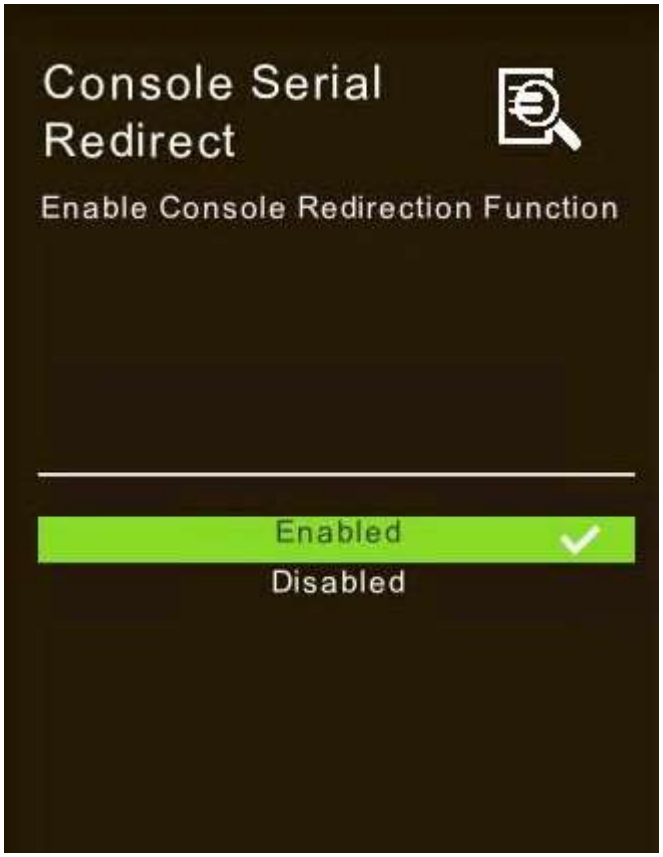
Abstract

This procedure describes how to set the console redirection function. After the function is enabled, the console can be redirected to a serial port.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Console Redirection**. The **Console Redirection** screen is displayed.
3. Select **Console Serial Redirect**. The **Console Serial Redirect** dialog box is displayed, see Figure 2-20.

Figure 2-20 Console Serial Redirect Dialog Box



4. Configure the console redirection function as required.
   - **Enabled**: enables the function.
   - **Disabled**: disables the function.
5. Press **F10**. In the displayed dialog box, select **Yes**.

2.15 Querying BMC Network Parameter Settings

Abstract

This procedure describes how to query BMC network parameter settings.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **iSAC > BMC Configuration**. The **BMC Configuration** screen is displayed, see Figure 2-21.

Figure 2-21 BMC Configuration Screen

2.16 Setting BMC Network Parameters

Abstract

This procedure describes how to set the BMC network parameters for connecting a local PC to the BMC.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **iSAC > BMC Configuration**. The **BMC Configuration** screen is displayed, see Figure 2-22.

Figure 2-22 BMC Configuration Screen

3. Click the parameter to be configured. The screen for setting the parameter is displayed. For a description of the BMC network parameters, refer to Table 2-3.

Table 2-3 BMC Network Parameter Descriptions

Parameter	Description	Setting
BMC Share Link	Configures BMC NIC (shared) link work mode.	Select whether to enable BMC NIC (shared) link work mode as required.

Parameter	Description	Setting
		● Auto: Automatic mode. ● Enabled: enables this mode. ● Disabled: disables this mode.
LAN Channel	Provides BMC channel options.	Select a BMC channel as required. ● iSAC (Dedicated): BMC-dedicated management network port. ● NIC (Shared): BMC shared network port.
IPv4 Mode	Enables or disables IPv4 mode.	Select whether to enable IPv4 mode as required. ● Enabled: enables IPv4 mode. If IPv4 mode is enabled, the IPv4 related parameters need to be configured. ● Disabled: disables IPv4 mode. If IPv4 mode is disabled, there is no need to configure the IPv4 related parameters.
IPv6 Mode	Enables or disables IPv6 mode.	Select whether to enable IPv6 mode as required. ● Enabled: enables IPv6 mode. If IPv6 mode is enabled, the IPv6 related parameters need to be configured. ● Disabled: disables IPv6 mode. If IPv6 mode is disabled, there is no need to configure the IPv6 related parameters.

4. Press **F10**. In the displayed dialog box, select **Yes**.

2.17 Creating an NVMe RAID

Abstract

This procedure describes how to create a RAID containing multiple NVMe SSDs to meet service requirements.

Note

- An NVMe RAID must be configured in UEFI mode.
- The NVMe SSDs must support RAID mode.
- A high-level RAID (except RAID 0) can be created only after a RAID key is installed.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Socket Configuration > IIO Configuration > Intel VMD technology**. The **Intel VMD technology** screen is displayed.

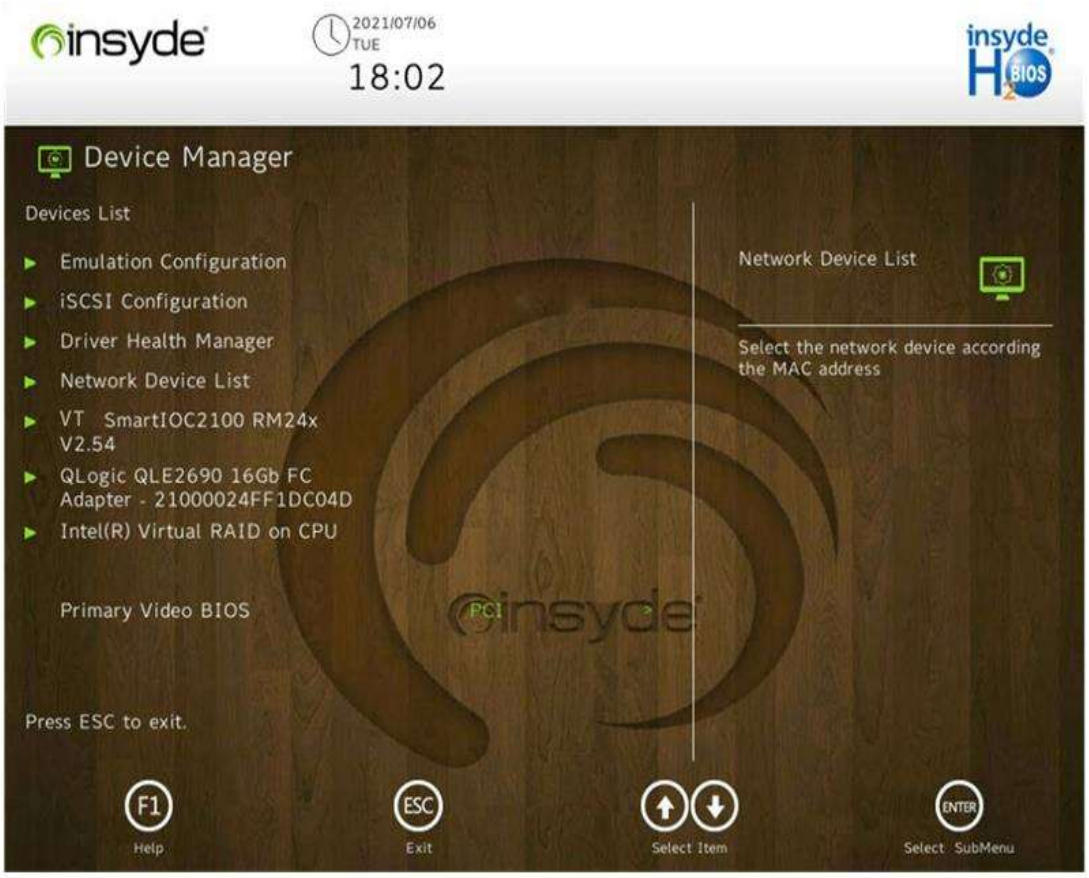
3. Click **Intel VMD Support**. In the displayed dialog box, modify the value of the **Intel VMD Support** parameter from **Disabled** (default value) to **Enabled**.
4. Press **F10**. In the displayed dialog box, select **Yes**.
5. During server rebooting, enter the Front Page screen.

Note

For how to enter the Front Page screen, refer to "2.1 Entering the BIOS Setup Utility".

6. Click **Device Management**. The **Device Manager** screen is displayed, see Figure 2-23.

Figure 2-23 Device Manager Screen

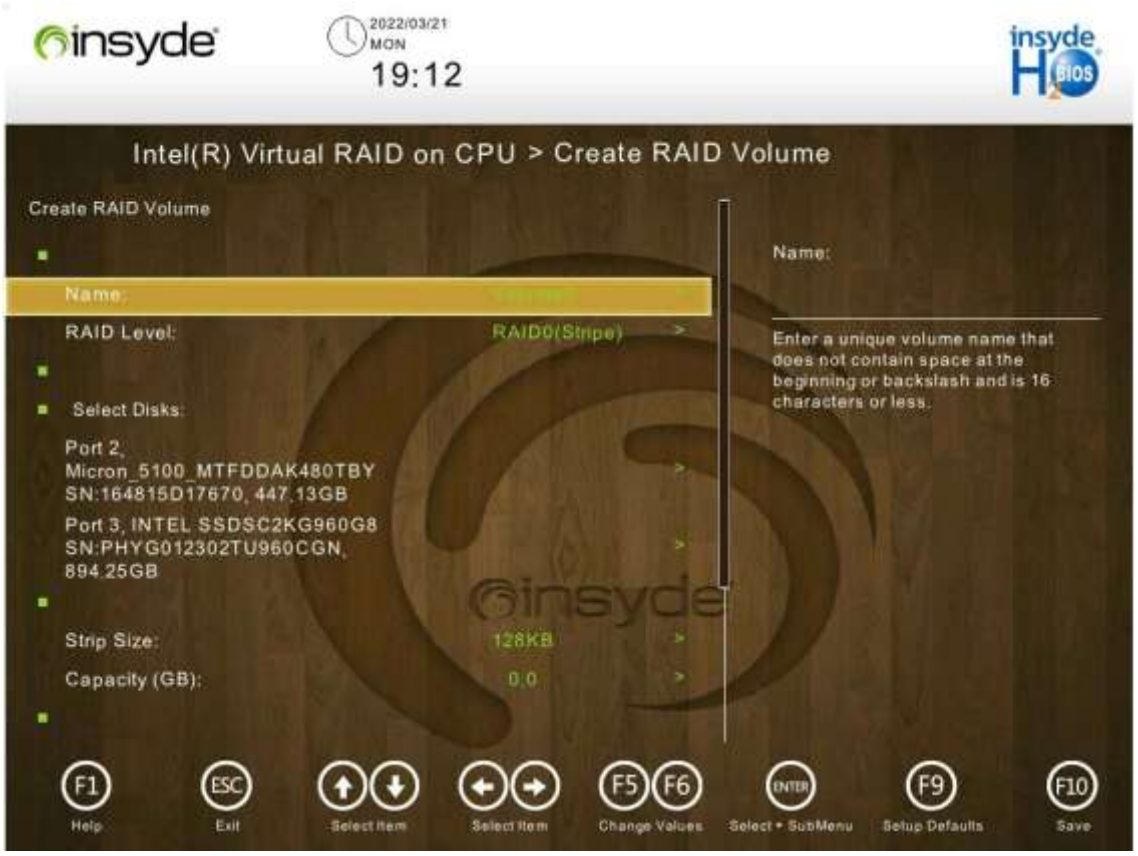


7. Select **Intel(R) Virtual RAID on CPU > All Intel VMD Controllers**. The **Intel VROC Managed VMD** screen is displayed, see Figure 2-24.

Figure 2-24 Intel VROC Managed VMD Screen

8. Click **Create RAID Volume**. The **Create RAID Volume** screen is displayed, see Figure 2-25.

Figure 2-25 Create RAID Volume Screen



9. Click the parameter to be configured. The screen for setting the parameter is displayed. For a description of the parameters that need to be configured, refer to Table 2-4.

Table 2-4 RAID Volume Parameter Descriptions

Parameter	Description	Setting
Name	Name of the RAID volume.	Enter a unique RAID volume name that contains not more than 16 characters. The name cannot be started or ended with a space.
RAID Level	RAID level.	Select a RAID level.
Select Disks	Member NVMe SSDs of the RAID volume.	Select the member NVMe SSDs of the RAID volume.
Strip Size	Stripe size of the RAID.	Select the stripe size.
Capacity (GB)	RAID capacity, unit: GB.	Enter the capacity of the RAID volume.

10. Click **Create Volume**. In the displayed dialog box, select **Yes**.
    When the RAID volume is displayed under **RAID Volumes** on the **Intel VROC Managed VMD** screen (see Figure 2-26), it indicates that the RAID volume is created successfully.

Figure 2-26 Example of Successfully Creating a RAID Volume

11. Press **F10**. In the displayed dialog box, select **Yes**.

2.18 Creating a RAID for SATA Hard Disks

Abstract

This procedure describes how to create a RAID for SATA hard disks to meet service requirements.

Steps

1. On the top-level Setup Utility screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **PCH Configuration > PCH sSATA Configuration**. The **PCH sSATA Configuration** screen is displayed, see Figure 2-27.

Figure 2-27 PCH sSATA Configuration Screen

3. Click **Configure sSATA as**. In the displayed dialog box, modify the value of the **Configure sSATA as** parameter from **AHCI** (default value) to **RAID**.
4. Press **F10**. In the displayed dialog box, select **Yes**.
5. During server rebooting, enter the Front Page screen.

Note

For how to enter the Front Page screen, refer to "2.1 Entering the BIOS Setup Utility".

6. Click **Device Management**. The **Device Management** screen is displayed, see Figure 2-28.

Figure 2-28 Device Manager Screen

7. Click **Intel(R) VROC sSATA Controller**. The **Intel(R) VROC sSATA Controller** screen is displayed, see Figure 2-29.

Figure 2-29 Intel(R) VROC sSATA Controller Screen

8. Click **Create RAID Volume**. The **Create RAID Volume** screen is displayed, see Figure 2-30.

Figure 2-30 Create RAID Volume Screen

9. Click the parameter to be configured. The screen for setting the parameter is displayed. For a description of the RAID volume parameters, refer to Table 2-5.

Table 2-5 RAID Volume Parameter Descriptions

Parameter	Description	Setting
name	Name of the RAID volume.	Enter a unique RAID volume name that contains not more than 16 characters. The name cannot be started or ended with a space.
RAID Level	RAID level.	Select a RAID level.
Select Disks	Member disks of the RAID volume.	Select the member disks of the RAID volume.
Strip Size	Stripe size of the RAID.	Select the stripe size.
Capacity (GB)	RAID capacity, unit: GB.	Enter the capacity of the RAID volume.

10. Click **Create Volume**. In the displayed dialog box, select **Yes**.
    When the RAID volume is displayed under **RAID Volumes** on the **Intel(R) VROC sSATA Controller** screen (see Figure 2-31), it indicates that the RAID volume is created successfully.

Figure 2-31 Example of Successfully Creating a RAID Volume

11. Press **F10**. In the displayed dialog box, select **Yes**.

2.19 Setting C-State and P-State Parameters

Abstract

This procedure describes how to set C-State and P-State parameters.

C-State refers to the power state of a CPU. It is mainly used to reduce the power consumption of the CPU to different levels through various power management policies for the idle states of a server. Lower power consumption means that more time is required to get the CPU active again and has a greater impact on CPU performance.

P-State, also known as EIST, is used to automatically adjust the voltage and frequency of a CPU, thus reducing both the electric energy consumption and the heat generated in accordance with the workload of a server.

Context

For details about the C-State and P-State parameters, refer to Table 2-6.

Table 2-6 C-State and P-State Parameter Descriptions

Parameter	Description	Setting
C-State Parameters		
Enhanced Halt State (C1E)	Determines whether to enable the C1E function.	● To enable C-State, set this parameter to **Enabled**. ● To disable C-State, set this parameter to **Disabled**.
CPU C6 report	Determines whether to report the C6 state to the OS.	● To enable C-State, set this parameter to **Enabled**. ● To disable C-State, set this parameter to **Disabled**.
Package C State	Sets package C-State limit. Options: ● C0/C1 state ● C2 state ● C6 (non-retention) state ● Auto The C0 state indicates that the CPU is actively running. Other C-States indicate idle states of different levels. From C0 to C6, the idle level is getting deeper. The deeper level saves more power but requires more time to get the CPU active again.	● To enable C-State, set this parameter to **Auto**. ● To disable C-State, set this parameter to **C0/C1 state**.
Enable Monitor MWAIT	Determines whether to enable the Monitor/Mwait instruction. Enabling the Monitor/Mwait instruction optimizes the instruction operation of a CPU. ● If C-State needs to be disabled, this parameter needs to be set to **Disabled** to disable the Monitor/Mwait instruction in some OSs as required. ● If an Enhanced VMotion Compatibility (EVC) error is reported when a VM is added to a cluster or a VM is migrated, this parameter needs to be set to **Enabled** .	● To enable C-State, set this parameter to **Enabled**. ● To disable C-State, set this parameter to **Disabled**.
P-State Parameters		
SpeedStep (Pstates)	Determines whether to enable the EIST function. EIST is used to automatically adjust the voltage and frequency of a CPU and	● To enable P-State, set this parameter to **Enabled**. ● To disable P-State, set this parameter to **Disabled**.

Parameter	Description	Setting
	reduce both the power consumption and the heat generated in accordance with the workload of a server.	

Steps

Configuring C-State Parameters

1. On the **Setup Utility** screen, select **Advanced** from the navigation tree on the left. The **Advanced** screen is displayed.
2. Select **Socket Configuration > Advanced Power Management Configuration > CPU C State Control**. The **CPU C State Control** screen is displayed, see Figure 2-32.

Figure 2-32 CPU C State Control Screen

3. Select the following parameters in turn, and select **Enabled** or **Disabled** in the dialog box displayed.

Note

To enable C-State, you need to set the parameters to **Enabled**; otherwise, set them to **Disabled**.

- **Enable Monitor MWAIT**
- **CPU C6 report**
- **Enhanced Halt State (C1E)**

4. Press the **Esc** key.

   The **Advanced Power Management Configuration** screen is displayed.

5. Select **Package C State Control**. The **Package C State Control** screen is displayed, see Figure 2-33.

Figure 2-33 Package C State Control Screen

6. Select **Package C State Control**, and select **Auto** or **C0/C1 state** in the dialog box displayed.

Note

To enable C-State, you need to set the parameter to **Auto**; otherwise, set it to **C0/C1 state**.

7. Press the **Esc** key.

   The **Advanced Power Management Configuration** screen is displayed.

Configuring P-State Parameters

8. Select **CPU P State Control**. The **CPU P State Control** screen is displayed, see Figure 2-33.

Figure 2-34 CPU P State Control Screen

9. Select **SpeedStep (Pstates)**, and select **Enabled** or **Disabled** in the dialog box displayed.

Note

To enable P-State, you need to set the parameter to **Enabled**; otherwise, set it to **Disabled**.

Chapter 3
Front Page Parameter Descriptions

Table of Contents

Figure 3-1 shows the Front Page screen.

Figure 3-1 Front Page Screen

For a description of the parameters on the Front Page screen, refer to Table 3-1.

Table 3-1 Front Page Parameter Descriptions

Parameter	Description
Continue	Continues the boot process.
Boot Manager	Enters the **Boot Manager** screen. For a description of the **Boot Manager** screen, refer to 3.1 Boot Manager.
Device Management	Enters the **Device Manager** screen. For a description of the **Device Manager** screen, refer to 3.2 Device Manager.
Boot From File	Enters a boot option through a file.
Administer Secure Boot	Enters the **Administer Secure Boot** screen. For a detailed description of the **Administer Secure Boot** screen, refer to 3.3 Administer Secure Boot.
Setup Utility	Enters the BIOS Setup Utility. For a detailed description of the Setup Utility screens, refer to 4 Setup Utility Parameter Descriptions. After entering the Setup Utility, you can press the **ESC** key to return to the Front Page screen.

3.1 Boot Manager

The **Boot Manager** screen provides the boot options, see Figure 3-2.

Figure 3-2 Boot Manager Screen

For a description of the parameters on the **Boot Manager** screen, refer to Table 3-2.

Table 3-2 Boot Manager Parameter Descriptions

Parameter	Description
Hard Disk Drive	Boots from a hard disk.
Network	Boots from a network device.
USB	Boots from a USB device.
CD/DVD-ROM Drive	Boots from a CD/DVD-ROM device.
Others	Boots from another device.

Note

On the **Boot Manager** screen, boot devices are displayed in top down order based on the boot priority. For example, the hard disk drive has the highest boot priority.

3.2 Device Manager

The **Device Manager** screen provides the configuration items for device management, see Figure 3-3.

Figure 3-3 Device Manager Screen

For a description of the parameters on the **Device Manager** screen, refer to Table 3-3.

Table 3-3 Device Manager Parameter Descriptions

Parameter	Description
Emulation Configuration	Enters the Emulation Configuration screen.
iSCSI Configuration	Enters the iSCSI Configuration screen.
Driver Health Manager	Enters the Driver Health Manager screen.
Network Device List	Enters the NIC configuration screen. You can select the corresponding NIC in accordance with the MAC address to check information such as the firmware version.
VT SmartIOC2100 RM24x V2.54	Enters the RAID card configuration screen. The RAID card configuration screen varies from card to card. Information such as the firmware version is listed under **Controller Information**.
QLogic QLE2690 16Gb FC Adapter - 21000024FF1DC04D	Enters the FC card configuration screen. The FC card configuration screen varies from card to card. Information such as the firmware version is listed under **Adapter Information**.

Parameter	Description
Inter(R) Virtual RAID on CPU	Enters the virtual RAID function.

Note

Inter(R) Virtual RAID on CPU is associated with the specified BIOS menus. Therefore, changes to the server configurations will result in changes to **Devices List** on the **Device Manager** screen.

3.3 Administer Secure Boot

The **Administer Secure Boot** screen provides the secure boot options, see Figure 3-4.

Figure 3-4 Administer Secure Boot Screen

For a description of the parameters on the **Administer Secure Boot** screen, refer to Table 3-4.

Table 3-4 Parameter Descriptions for Administer Secure Boot

Parameter	Description	Default
Secure Boot Database	Displays whether the Secure Boot certificate database is installed. ● Installed and lock: The Secure Boot certificate database is installed.	Unlocked

Parameter	Description	Default
	● Unlocked: The Secure Boot certificate database is not installed.	
Secure BootStatus	Displays whether Secure Boot is enabled or disabled. ● Enabled: Secure Boot is enabled. ● Disabled: Secure Boot is disabled.	Disabled
User CustomizedSecurity	Enables or disables user security configuration. ● Yes: enables user security configuration. ● No: disables user security configuration.	No
Select a UEFI file as trustedfor execution	Sets a UEFI file as a trusted file.	-
Enforce SecureBoot	Enables or disables Secure Boot. ● Enabled: enables Secure Boot. ● Disabled: disables Secure Boot.	Disabled
Erase all Secure Boot Settings	Enables or disables the function of erasing Secure Boot settings. ● Enabled: enables the function of erasing Secure Boot settings. ● Disabled: disables the function of erasing Secure Boot settings.	Disabled
Restore SecureBoot to FactorySettings	Configures whether to restore Secure Boot to factory default settings. ● Enabled: restores the security certificate database to factory default settings, and enables Secure Boot. ● Disabled: Disables the restoration of Secure Boot to factory default settings.	Disabled
PK Options	Enters the PK certificate setting screen.	-
KEK Options	Enters the KEK certificate setting screen.	-
DB Options	Enters the DB certificate setting screen to set the trusted whitelist.	-
DBX Options	Enters the DBX certificate setting screen to set the untrusted blacklist.	-

Chapter 4
Setup Utility Parameter Descriptions

Table of Contents

4.1 Main

The **Main** screen provides basic BIOS information including the BIOS version, memory capacity and system time. Figure 4-1 to Figure 4-2 show the **Main** screen.

Figure 4-1 Main Screen 1

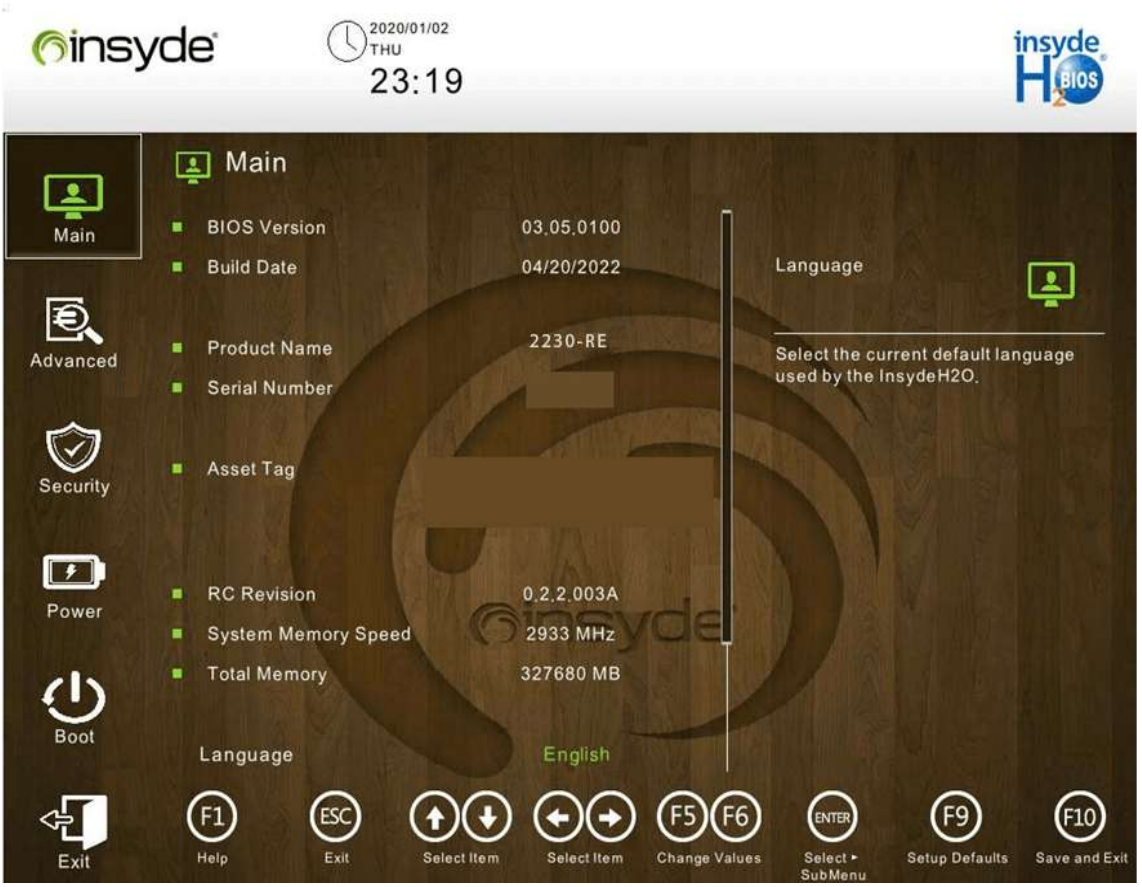


Figure 4-2 Main Screen 2

For a description of the parameters on the **Main** screen, refer to Table 4-1.

Table 4-1 Main Parameter Descriptions

Parameter	Description
BIOS Version	BIOS version.
Build Date	Compiling date (MM/DD/YYYY) of the BIOS.
Product Name	Product name.
Serial Number	Serial number of the product.
Asset Tag	Asset tag.
RC Revision	RC version.
System Memory Speed	Memory speed.
Total Memory	Total memory capacity.
Language	System language: ● English ● Simplified Chinese
System Time	Current system time.

Parameter	Description
	The system time is displayed in HH:MM:SS format based on a 24-hour clock system. You can press **Enter** to switch between the hour, minute, and second items and change the settings as follows: ● To increase the value by one, press **+**. ● To decrease the value by one, press **-**. ● To specify a value, press the corresponding number key.
System Date	Current system date. The system date is displayed in "day of week + month/date/year" format. You can press **Enter** to switch between the month, date, and year items and change the settings as follows: ● To increase the value by one, press **+**. ● To decrease the value by one, press **-**. ● To specify a value, press the corresponding number key.

4.2 Advanced

4.2.1 Advanced Screen

The **Advanced** screen provides advanced BIOS settings, such as peripheral configurations, mainboard information and console redirection. Figure 4-3 shows the **Advanced** screen.

Figure 4-3 Advanced Screen

For a description of the parameters on the **Advanced** screen, refer to Table 4-2.

Table 4-2 Advanced Parameter Descriptions

Parameter	Description
Mainboard Information	Mainboard information. For details, refer to 4.2.2 Mainboard Information.
Peripheral Configuration	Peripheral configurations. For details, refer to 4.2.3 Peripheral Information.
Video Configuration	Video configurations. For details, refer to 4.2.4 Video Configuration.
ACPI Table/Features Control	ACPI configurations. For details, refer to 4.2.5 ACPI Table/Features Control.
System Event Log	System event logs. For details, refer to 4.2.6 System Event Log.
Debug Configuration	Debug configurations. For details, refer to 4.2.7 Debug Configuration.
Socket Configuration	Socket configurations.

Parameter	Description
	For details, refer to 4.2.8 Socket Configuration.
ME Configuration	ME configurations. For details, refer to 4.2.9 ME Configuration.
PCH Configuration	PCH configurations. For details, refer to 4.2.10 PCH Configuration.
Server Mgmt	Server configurations. For details, refer to 4.2.11 Server Mgmt.
Console Redirection	Console redirection. For details, refer to 4.2.12 Console Redirection.
NVM Express Information	Detailed information about NVMe devices. For details, refer to 4.2.13 NVM Express Information.
Memory Topology	Memory topology. For details, refer to 4.2.14 Memory Topology.
PXE Configuration	NIC PXE configurations. For details, refer to 4.2.15 PXE Configuration.

4.2.2 Mainboard Information

The **Mainboard Information** screen provides such information as onboard interfaces and devices. Figure 4-4 to Figure 4-5 show the **Mainboard Information** screen.

Figure 4-4 Mainboard Information Screen 1

Figure 4-5 Mainboard Information Screen 2

For a description of the parameters on the **Mainboard Information** screen, refer to Table 4-3.

Table 4-3 Mainboard Information Parameter Descriptions

Parameter	Description	Default
Board Name	Name of the mainboard.	-
PCH Reversion	PCH version.	-
ME Version	ME version.	-
ME-BIOS Interface Ver	ME-BIOS interface version.	-
ME SKU	ME model.	Node Manager
ME Status	ME status.	Operational
USB2.0	Number of USB 2.0 interfaces and their physical locations.	2 (Front)
USB3.0	Number of USB 3.0 interfaces and their physical locations.	2 (Rear)
COM	Number of COM serial ports and their physical locations.	1 RJ45 (Rear)

Parameter	Description	Default
VGA	Number of VGA interfaces and their physical locations.	● 1 Connector (Front) ● 1 Connector (Rear)
OnBoard Device Information	Information about onboard devices. For details, refer to 4.2.2.1 OnBoard Device Information.	-
LAN MAC Information	Information about network port MAC addresses. For details, refer to 4.2.2.2 LAN MAC Information.	-
Graphics Card Information	Information about onboard graphics cards. For details, refer to 4.2.2.3 Graphics Card Information.	-
Slot Information	Information about PCIe card slots. For details, refer to 4.2.2.4 Slot Information.	-

4.2.2.1 OnBoard Device Information

Figure 4-6 shows the **OnBoard Device Information** screen.

Figure 4-6 OnBoard Device Information Screen

For a description of the parameters on the **OnBoard Device Information** screen, refer to Table 4-4.

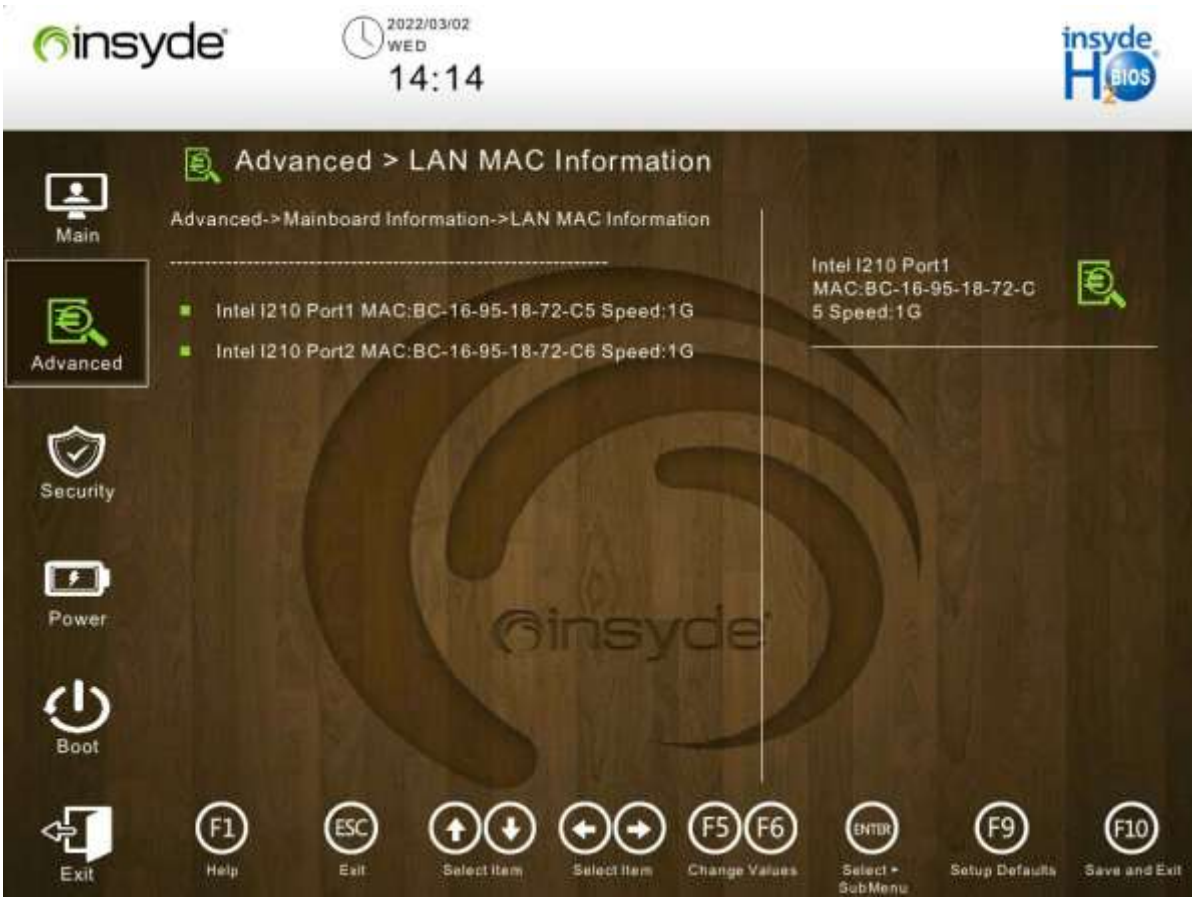
Table 4-4 Parameter Descriptions for OnBoard Device Information

Parameter	Description
VGA	Displays whether the VGA card on the mainboard is present. If the VGA card on the mainboard is not present, **Not Present** is displayed.
RAID Card	Displays whether the RAID card on the mainboard is present. If the RAID card on the mainboard is not present, Not Present is displayed.

4.2.2.2 LAN MAC Information

The **LAN MAC Information** screen displays port MAC addresses and speeds of external NICs. Figure 4-7 shows the **LAN MAC Information** screen.

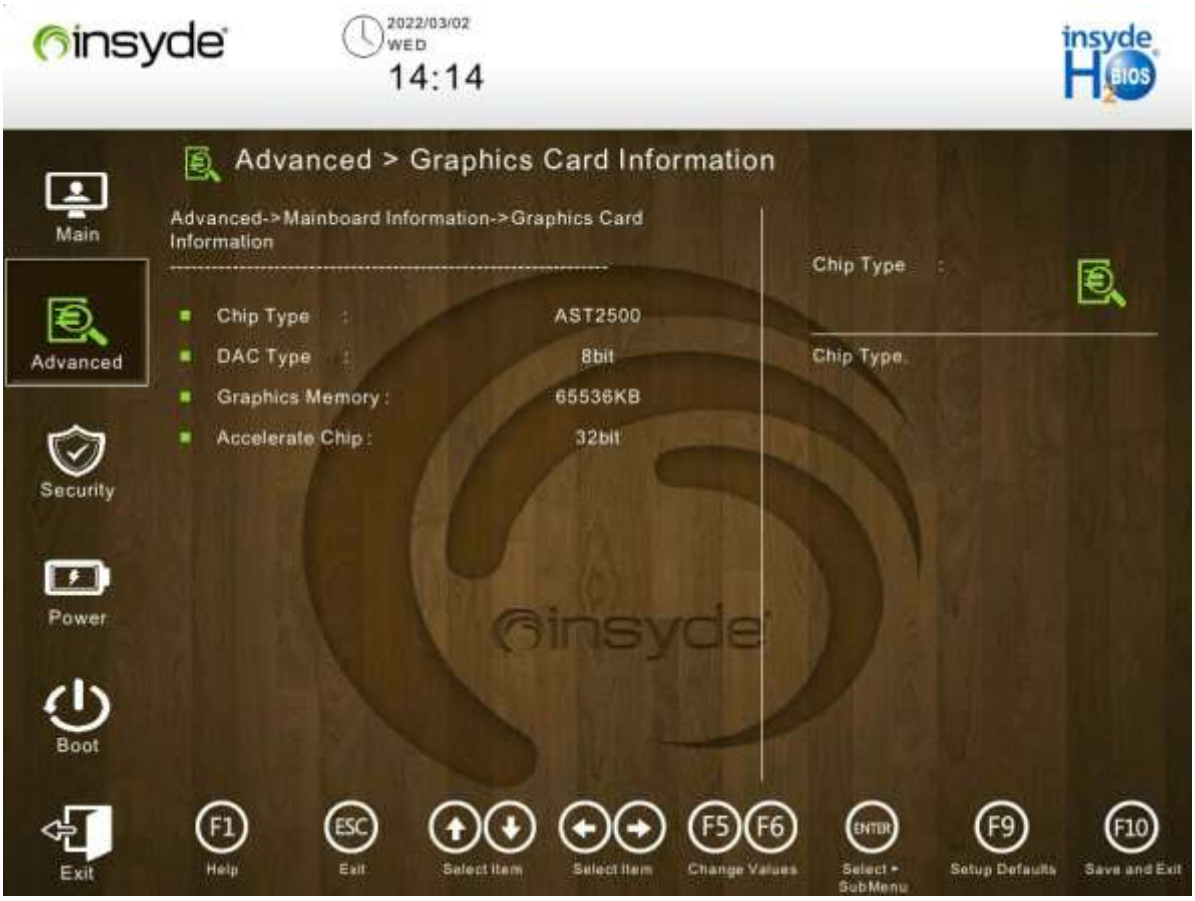
Figure 4-7 LAN MAC Information Screen



4.2.2.3 Graphics Card Information

Figure 4-8 shows the **Graphics Card Information** screen.

Figure 4-8 Graphics Card Information Screen



For a description of the parameters on the **Graphics Card** screen, refer to Table 4-5.

Table 4-5 Parameter Descriptions for Graphics Card Information

Parameter	Description
Chip Type	Chip type of the graphics card.
DAC Type	DAC type.
Graphics Memory	Graphics memory.
Accelerate Chip	Type of the graphics accelerator.

4.2.2.4 Slot Information

Figure 4-9 shows the **Slot Information** screen.

Figure 4-9 Slot Information Screen

For a description of the parameters on the **Slot Information** screen, refer to Table 4-6.

Table 4-6 Slot Information Parameter Descriptions

Parameter	Description
Total 3 Slots, Available 2 Slots	Total number of PCIe standard card slots and the number of available PCIe standard card slots on the mainboard.

4.2.3 Peripheral Information

Figure 4-10 shows the **Peripheral Information** screen.

Figure 4-10 Peripheral Information Screen

For a description of the parameters on the **Peripheral Information** screen, refer to Table 4-7.

Table 4-7 Peripheral Information Parameter Descriptions

Parameter	Description	Default
PCIe SR-IOV	Enables or disables the SR-IOV function. ● Enabled: enables the SR-IOV function. ● Disabled: disables the SR-IOV function.	Enabled
PCIe ARI	Enables or disables the ARI function. ● Enabled: enables the ARI function. ● Disabled: disables the ARI function.	Disabled
ARI Forward	Enables or disables the ARI forwarding function. ● Enabled: enables the ARI forwarding function. ● Disabled: disables the ARI forwarding function.	Disabled
Use 1G Page Table	Enables or disables the function of using 1 GB page table. ● Enabled: enables the function of using 1 GB page table. ● Disabled: disables the function of using 1 GB page table.	Enabled

4.2.4 Video Configuration

Figure 4-11 shows the **Video Configuration** screen.

Figure 4-11 Video Configuration Screen

For a description of the parameters on the **Video Configuration** screen, refer to Table 4-8.

Table 4-8 Video Configuration Parameter Descriptions

Parameter	Description	Default
Video Card Selected	Selects a VGA card type. ● Offboard Device: selects an offboard VGA card. ● Onboard Device: selects an onboard VGA card.	Offboard Device

4.2.5 ACPI Table/Features Control

On the **ACPI Table/Features Control** screen, you can configure the functions related to advanced power management. Figure 4-12 shows the **ACPI Table/Features Control** screen.

Figure 4-12 ACPI Table/Features Control Screen

For a description of the parameters on the **ACPI Table/Features Control** screen, refer to Table 4-9.

Table 4-9 Parameter Descriptions for ACPI Table/Features Control

Parameter	Description	Default
APIC-IO APIC Mode	Enables or disables the APIC-IO APIC mode. ● Enabled: enables the APIC-IO APIC mode. ● Disabled: disables the APIC-IO APIC mode.	Enabled

4.2.6 System Event Log

Figure 4-13 shows the **System Event Log** screen.

Figure 4-13 System Event Log Screen

For a description of the parameters on the **System Event Log** screen, refer to Table 4-10.

Table 4-10 Parameter Descriptions for System Event Logs

Parameter	Description	Default
System Errors	Enables or disables the function of collecting system errors. ● Enabled: enables the function of collecting system errors. ● Disabled: disables the function of collecting system errors.	Enabled
System Memory Poison	Enables or disables memory poisoning. ● Enabled: enables memory poisoning. ● Disabled: disables memory poisoning.	Enabled
eMCA Settings	Enters eMCA settings. For details, refer to 4.2.6.1 eMCA Settings.	-
WHEA Settings	Enters WHEA settings. For details, refer to 4.2.6.2 WHEA Settings.	-
Memory Error Enabling	Enters the screen concerning memory error handling.	-

Parameter	Description	Default
	For details, refer to 4.2.6.3 Memory Error Enabling.	
IIO Error Enabling	Enters the screen concerning IIO error handling. For details, refer to 4.2.6.4 IIO Error Enabling.	-
PCIe Error Enabling	Enters the screen concerning PCIe device error handling. For details, refer to 4.2.6.5 PCIe Error Enabling.	-

4.2.6.1 eMCA Settings

Figure 4-14 shows the **eMCA Settings** screen.

Figure 4-14 eMCA Settings Screen

For a description of the parameters on the **eMCA Settings** screen, refer to Table 4-11.

Table 4-11 Parameter Descriptions for eMCA Settings

Parameter	Description	Default
EMCA Logging Support	Enables or disables eMCA logging support. ● Enabled: enables eMCA logging support. ● Disabled: disables eMCA logging support.	Enabled

Parameter	Description	Default
LMCE Support	Enables or disables LMCE support. ● Enabled: enables LMCE support. ● Disabled: disables LMCE support.	Enabled
EMCA CMCI-SMI Morphing	Enables or disables eMCA CMCI-SMI morphing. ● Enabled: enables eMCA CMCI-SMI morphing. ● Disabled: disables eMCA CMCI-SMI morphing.	Disabled

4.2.6.2 WHEA Settings

Figure 4-15 shows the **WHEA Settings** screen.

Figure 4-15 WHEA Settings Screen

For a description of the parameters on the **WHEA Settings** screen, refer to Table 4-12.

Table 4-12 Parameter Descriptions for WHEA Settings

Parameter	Description	Default
WHEA Support	Enables or disables the support for WHEA ● Enabled: enables the support for WHEA. ● Disabled: disables the support for WHEA.	Enabled

Parameter	Description	Default
WHEA Log Memory Error	Enables or disables the support for WHEA in logging memory errors. ● Enabled: enables the support for WHEA in logging memory errors. ● Disabled: disables the support for WHEA in logging memory errors.	Disabled

4.2.6.3 Memory Error Enabling

Figure 4-16 shows the **Memory Error Enabling** screen.

Figure 4-16 Memory Error Enabling Screen

For a description of the parameters on the **Memory Error Enabling** screen, refer to Table 4-13.

Table 4-13 Parameter Descriptions for Memory Error Enabling

Parameter	Description	Default
Memory Error	Enables or disables the memory error reporting function. ● Enabled: enables the memory error reporting function.	Enabled

Parameter	Description	Default
	● Disabled: disables the memory error reporting function.	
Memory Corrected Error	Enables or disables the reporting of correctable memory errors. ● Enabled: enables the reporting of correctable memory errors. ● Disabled: disables the reporting of correctable memory errors.	Enabled

4.2.6.4 IIO Error Enabling

Figure 4-17 shows the **IIO Error Enabling** screen.

Figure 4-17 IIO Error Enabling Screen

For a description of the parameters on the **IIO Error Enabling** screen, refer to Table 4-14.

Table 4-14 Parameter Descriptions for IIO Error Enabling

Parameter	Description	Default
IIO/PCH Global Error Support	Enables or disables the IIO/PCH global error logging function.	Enabled

Parameter	Description	Default
	● Enabled: enables the IIO/PCH global error logging function. ● Disabled: disables the IIO/PCH global error logging function.	
OS Native AER Support	Enables or disables the OS Native to control AER error handling. ● Enabled: enables the OS Native to control AER error handling. ● Disabled: disables OS Native to control AER error handling.	Disabled
IIO OOB Mode	Enables or disables IIO OOB mode. ● Enabled: enables IIO OOB mode. ● Disabled: disables IIO OOB mode.	Enabled
IIO eDPC Support	Enables or disables the IIO eDPC function. ● Enabled: enables the IIO eDPC function. ● Disabled: disables the IIO eDPC function.	Disabled

4.2.6.5 PCIe Error Enabling

Figure 4-18 shows the **PCIe Error Enabling** screen.

Figure 4-18 PCIe Error Enabling Screen

For a description of the parameters on the **PCIe Error Enabling** screen, refer to Table 4-15.

Table 4-15 Parameter Descriptions for PCIe Error Enabling

Parameter	Description	Default
PCIE Unsupported Request Error	Enables or disables the reporting of PCIE Unsupported Request errors. ● Enabled: enables the reporting of PCIe Unsupported Request errors. ● Disabled: disables the reporting of PCIe Unsupported Request errors	Disabled
PCIE Surprise Link Down Error	Enables or disables the reporting of PCIe Surprise Link Down errors. ● Enabled: enables the reporting of PCIe Surprise Link Down errors. ● Disabled: disables the reporting of PCIe Surprise Link Down errors.	Disabled

4.2.7 Debug Configuration

Figure 4-19 shows the **Debug Configuration** screen.

Figure 4-19 Debug Configuration Screen

For a description of the parameters on the **Debug Configuration** screen, refer to Table 4-16.

Table 4-16 Debug Configuration Parameter Descriptions

Parameter	Description	Default
Serial Debug Message Level	Level of debugging messages output by the serial port. ● Disabled: No system debugging message is output. ● Minimum: Only key debugging messages are output. ● Normal: Key debugging messages and common debugging messages are output. ● Minimum: All debugging messages are output.	Disabled
Trace Messages	Configures the display of trace messages. ● Enabled: The access messages of each I/O port are displayed. ● Disabled: The access messages of no I/O port are displayed.	Disabled

Parameter	Description	Default
	● Enabled for registry writes only: Only the messages written into the registry are displayed.	
Training Messages	Enables or disables the display of training messages. ● Enabled: enables the display of training messages. ● Disabled: disables the display of training messages. If **Serial Debug Message Level** is set to **Maximum**, training messages are displayed even if **Training Messages** is set to **Disabled**.	Disabled

4.2.8 Socket Configuration

Figure 4-20 shows the **Socket Configuration** screen.

Figure 4-20 Socket Configuration Screen

For a description of the parameters on the **Socket Configuration** screen, refer to Table 4-17.

Table 4-17 Socket Configuration Parameter Descriptions

Parameter	Description
Processor Configuration	Processor configuration function.

Parameter	Description
	For details, refer to 4.2.8.1 Processor Configuration.
Common RefCode Configuration	Common RefCode configuration function. For details, refer to 4.2.8.2 Common RefCode Configuration.
UPI Configuration	UPI configuration function. For details, refer to 4.2.8.3 UPI Configuration.
Memory Configuration	Memory configuration function. For details, refer to 4.2.8.4 Memory Configuration.
IIO Configuration	IIO configuration function. For details, refer to 4.2.8.5 IIO Configuration.
Advanced Power Management Configuration	Advanced power management configuration function. For details, refer to 4.2.8.6 Advanced Power Management Configuration.

4.2.8.1 Processor Configuration

Figure 4-21 to Figure 4-22 show the **Processor Configuration** screen.

Figure 4-21 Processor Configuration Screen 1

Figure 4-22 Processor Configuration Screen 2

For a description of the parameters on the **Processor Configuration** screen, refer to Table 4-18.

Table 4-18 Processor Configuration Parameter Descriptions

Parameter	Description	Default
Per-Socket Information	Displays information about each socket. For details, refer to "4.2.8.1.1 Per-Socket Information".	-
Core Disable Number	Number of disabled CPU cores. The value 0 indicates that no core of the CPU is disabled.	0
Hyper- Threading [ALL]	Enables or disables hyper-threading. ● Enabled: enables hyper-threading. ● Disabled: disables hyper-threading. In other BIOS platforms, this parameter is presented as: ● Purley platform: Hyper-Threading ● AMD platform: SMT Mode ● HG platform: AMD CPU SMT Support	Enabled
Check CPU BIST Result	Checks the CPU BIST result.	Enabled

Parameter	Description	Default
	● Enabled: disables the core whose BIST fails. ● Disabled: ignores the BIST result.	
Hardware Prefetcher	Before a CPU processes data or instructions, the hardware prefetcher will prefetch streams of the data and instructions from the main memory to the L2 cache to reduce time required by the CPU for reading data from the memory, thus improving CPU performance. Enables or disables the hardware prefetch function. ● Enabled: enables the hardware prefetch function. ● Disabled: disables the hardware prefetch function.	Enabled
L2 RFO Prefetch Disable	Enables or disables the L2 RFO prefetch function. ● Enabled: enables the L2 RFO prefetch function. ● Disabled: disables the L2 RFO prefetch function.	Disabled
Adjacent Cache Prefetch	After the adjacent cache prefetch function is enabled, the server reads the adjacent data in advance when reading data, accelerating the read speed. Enables or disables the adjacent cache prefetch function. ● Enabled: enables the adjacent cache prefetch function. ● Disabled: disables the adjacent cache prefetch function.	Enabled
DCU Streamer Prefetcher	Enables or disables the DCU stream prefetch function. ● Enabled: enables the DCU stream prefetch function. ● Disabled: disables the DCU stream prefetch function.	Enabled
DCU IP Prefetcher	Enables or disables the DCU IP prefetch function. ● Enabled: enables the DCU IP prefetch function. ● Disabled: disables the DCU IP prefetch function.	Enabled
LLC Prefetcher	Enables or disables the L3 cache prefetch function. ● Enabled: enables the L3 cache prefetch function. ● Disabled: disables the L3 cache prefetch function.	Enabled
DCU Mode	Displays DCU mode. ● Normal: normal mode. ● Mirror-Mode: mirror mode.	Normal
Extended APIC	Enables or disables extended APIC support.	Disabled

Parameter	Description	Default
	● Enabled: enables extended APIC support. ● Disabled: disables extended APIC support.	
APIC Physical Mode	Enables or disables APIC physical mode. ● Enabled: enables APIC physical mode. ● Disabled: disables APIC physical mode.	Disabled
Intel (R) TXT	Enables or disables Intel TXT support. ● Enabled: enables Intel TXT support. ● Disabled: disables Intel TXT support. If this parameter is set to **Enabled**, **VMX** is greyed out.	Disabled
VMX	Enables or disables Vanderpool. ● Enabled: enables Vanderpool. ● Disabled: disables Vanderpool. In other BIOS platforms, this parameter is presented as: ● Purley platform: VT-x ● AMD platform: SVM mode ● HG platform: SVM support	Enabled
Enable SMX	Enables or disables SMX. ● Enabled: enables SMX. ● Disabled: disables SMX.	Disabled
Lock Chipset	Enables or disables the chipset lock. ● Enabled: enables the chipset lock. ● Disabled: disables the chipset lock.	Enabled
AES-NI	Enables or disables AES-NI. ● Enable: enables AES-NI. ● Disable: disables AES-NI.	Enabled

4.2.8.1.1 Per-Socket Information

Figure 4-23 And Figure 4-24 show the **Per-Socket Information** screen.

Figure 4-23 Per-Socket Information Screen—1

Figure 4-24 Per-Socket Information Screen—2

For a description of the parameters on the **Per-Socket Information** screen, refer to Table 4-19.

Table 4-19 Per-Socket Information Parameter Descriptions

Parameter	Description
Processor BSP Rev	CPU ID and stepping.
Processor Socket	Processor socket number.
Processor ID	Processor ID.
Processor Frequency	Nominal frequency of a processor.
Processor Max Ratio	Maximum multiplier of a processor.
Processor Min Ratio	Minimum multiplier of a processor.
Microcode Revision	Microcode version of a processor.
L1 Cache RAM (Per Core)	L1 cache capacity.
L2 Cache RAM (Per Core)	L2 cache capacity.
L3 Cache RAM	L3 cache capacity.
CPU Voltage	CPU voltage.

Parameter	Description
Active Cores/Total Cores	Active cores/total cores.
Active Threads	Number of active threads.
TDP	Heat release of a processor under the maximum load.
Processor 0 Version	Version of processor 0.
Processor 1 Version	Version of processor 1.

4.2.8.2 Common RefCode Configuration

Figure 4-25 shows the **Common RefCode Configuration** screen.

Figure 4-25 Common RefCode Configuration Screen

For a description of the parameters on the **Common RefCode Configuration** screen, refer to Table 4-20.

Table 4-20 Parameter Descriptions for Common RefCode Configuration

Parameter	Description	Default
MMCFG Size	MMCFG size.	Auto
MMIO High Base	Starting address of the MMIO high base.	32T

Parameter	Description	Default
MMIO High Granularity Size	MMIO high granularity size per stack.	64G
Isoc Mode	Enables or disables isochronous transmission. If this mode is enabled, the data transmission quality is improved and the memory bandwidth and performance are reduced. ● Enabled: enables isochronous mode. ● Disabled: disables isochronous mode.	Auto
Numa	Enables or disables (NUMA) Non-Uniform Memory Access support. ● Enabled: enables NUMA support. ● Disabled: disables NUMA support.	Enabled
Virtual Numa	Enables or disables virtual NUMA support. ● Enabled: enables virtual NUMA support. ● Disabled: disables virtual NUMA support.	Disabled
UMA-Based Clustering	Enables or disables UMA-Based Clustering (UBC) mode ● Hemisphere (2-clusters): enables Hemisphere mode (also called UBC mode). ● Disabled (All2All): disables UBC mode.	Hemisphere (2-clusters)

4.2.8.3 UPI Configuration

Figure 4-26 shows the **UPI Configuration** screen.

Figure 4-26 UPI Configuration Screen

For a description of the parameters on the **UPI Configuration** screen, refer to Table 4-21.

Table 4-21 UPI Configuration Parameter Descriptions

Parameter	Description
UPI General Configuration	UPI general configuration. For details, refer to "4.2.8.3.1 UPI General Configuration".
Uncore Dfx Configuration	Uncore DFX configuration. For details, refer to "4.2.8.3.2 Uncore Dfx Configuration".

4.2.8.3.1 UPI General Configuration

Figure 4-27 and Figure 4-28 show the **UPI General Configuration** screen.

Figure 4-27 UPI General Configuration Screen—1

Figure 4-28 UPI General Configuration Screen—2

For a description of the parameters on the **UPI General Configuration** screen, refer to Table 4-22.

Table 4-22 Parameter Descriptions for UPI General Configuration

Parameter	Description	Default
UPI Status	UPI status. Press **Enter** to unfold the detailed information about UPI status: ● Number of CPU: number of CPUs. ● Number of IIO: number of IIOs. ● Current UPI Link Speed: current UPI link speed. ● Current UPI Link Frequency: current UPI link frequency.	-
Link Speed Mode	Link speed mode. ● Fast ● Slow	Fast
Link Speed	Link speed. ● 9.6 GT/s ● 10.4 GT/s	Auto

Parameter	Description	Default
	● 11.2 GT/s ● Auto ● Use Per Link Setting	
Link L0p	Enables or disables link L0p. ● Enabled ● Disabled ● Auto	Auto
Link L1	Enables or disables link L1. ● Enabled ● Disabled ● Auto	Auto
Directory Mode Enable	Enables or disables directory mode. ● Enabled ● Disabled ● Auto	Auto
XPT Remote Prefetch	Enables or disables XPT remote prefetch. ● Enabled ● Disabled ● Auto	Auto
KTI Prefetch	Enables or disables KTI prefetch. ● Enabled ● Disabled ● Auto	Auto
RdCur for XPT Prefetch	Enables or disables RdCur for XPT prefetch. ● Enabled ● Disabled ● Auto	Auto
Local/Remote Threshold	Sets the local/remote threshold. ● Low ● Medium ● High ● Disabled ● Auto	Auto
IO Directory Cache(IODC)	Enables or disables IODC. ● Disabled ● Auto ● Enabled for Remote InvItoM Hybrid Push ● Enabled for Remote InvItoM AllocFlow ● Enabled for Remote InvItoM Hybrid AllocNonAlloc	Auto

Parameter	Description	Default
	● Enabled for Remote InvItoM and Remote WCiLF	
SNC(Sub NUMA)	● Disabled ● Enable SNC2(2-clusters)	Disabled
XPT Prefetch	Enables or disables XPT prefetch. ● Enabled ● Disabled ● Auto	Auto
State AtoS	Enables or disables switchover between the SnoopAll (A) and Shared (S) states of memory. ● Enabled ● Disabled ● Auto	Auto
LLC dead line alloc	Enables or disables LLC dead line allocation. ● Enabled ● Disabled ● Auto	Enabled

4.2.8.3.2 Uncore Dfx Configuration

Figure 4-29 shows the **Uncore Dfx Configuration** screen.

Figure 4-29 Uncore Dfx Configuration Screen

For a description of the parameters on the **Uncore Dfx Configuration** screen, refer to Table 4-23.

Table 4-23 Parameter Descriptions for Uncore DFX Configuration

Parameter	Description	Default
OSB Enabled	Enables or disables the OSB function. ● Enabled ● Disabled ● Auto	Auto
OSB Local Rd Enabled	Enables or disables the local OSB Rd function. ● Enabled ● Disabled ● Auto	Auto
OSB Local RdCur Enabled	Enables or disables the local OSB RdCur function. ● Enabled ● Disabled ● Auto	Auto
OSB Remote Rd Enabled	Enables or disables the remote OSB Rd function. ● Enabled	Auto

Parameter	Description	Default
	● Disabled ● Auto	

4.2.8.4 Memory Configuration

Figure 4-30 to Figure 4-31 show the **Memory Configuration** screen.

Figure 4-30 Memory Configuration Screen 1

Figure 4-31 Memory Configuration Screen 2

For a description of the parameters on the **Memory Configuration** screen, refer to Table 4-24.

Table 4-24 Memory Configuration Parameter Descriptions

Parameter	Description	Default
Enforce Population POR	Enables or disables the enforcement of POR. After POR enforcement, memory modules must be installed in accordance with the POR. ● Disable Enforcement: disables the enforcement of POR. ● Enforce Supported Populations: enables the enforcement of POR. ● Enforce Validated Populations: enables the enforcement of validated POR. Generally, both validated POR and invalidated POR are supported.	Disable Enforcement
PPR Type	Configures the type of PPR. ● Hard PPR: hardware PPR. ● Soft PPR: software PPR. ● PPR Disabled: disables PPR.	Soft PPR

Parameter	Description	Default
Memory Frequency	Configures the memory frequency. ● Auto ● 2666 ● 2933 ● 3200	Auto
Halt on Memory Fault	Enables or disables halt on memory faults. ● Enabled: enables halt on memory faults. ● Disabled: disables halt on memory faults.	Disabled
Adv MemTest Options	Provides advanced memory test options.	0x0
Adv MemTest Retry After Repair	Configures whether to retry the memory test after a memory fault is resolved. ● Enabled: enables the memory test retry function. ● Disabled: disables the memory test retry function.	Enabled
Attempt Fast Boot	Enables or disables the function of attempting to fast boot the server. ● Enabled: enables the function of attempting to fast boot the server. ● Disabled: disables the function of attempting to fast boot the server.	Disabled
Attempt Fast Cold Boot	Enables or disables fast cold boot attempts. ● Enabled: enables fast cold boot attempts. ● Disabled: disables fast cold boot attempts.	Disabled
MemTest On Clod Fast Boot	Enables or disables the memory test during fast cold boot. ● Enabled: enables the memory test during fast cold boot. ● Disabled: disables the memory test during fast cold boot.	Disabled
RMT On Cold Fast Boot	Enables or disables the RMT during fast cold boot. ● Enabled: enables the RTM during fast cold boot. ● Disabled: disables the RTM during fast cold boot.	Disabled
Rank Margin Tool	Enables or disables the rank margin tool that determines whether to conduct a margin test on the memory timings and voltage signals. ● Enabled: enables the rank margin tool. After being enabled, the rank margin tool runs after memory training. ● Disabled: disables the rank margin tool.	Disabled

Parameter	Description	Default
Enable ADR	Enables or disables ADR, that is saving memory information upon power failure. ● Enabled: enables ADR. ● Disabled: disables ADR.	Enabled
Legacy ADR Mode	Enables or disables legacy ADR, that is saving memory information in a traditional way upon power failure. ● Enabled: enables legacy ADR. ● Disabled: disables legacy ADR.	Disabled
Custom Refresh	Enables or disables the function for customizing the memory refresh rate. ● Enabled: enables the function for customizing the memory refresh rate. ● Disabled: disables the function for customizing the memory refresh rate.	Disabled
2x Refresh Enable	Enables or disables the function for doubling the memory refresh rate. ● Enabled: enables the function for doubling the memory refresh rate. ● Disabled: disables the function for doubling the memory refresh rate. ● Auto: automatic mode.	Auto
Page Policy	Page policy. For details, refer to "4.2.8.4.1 Page Policy".	-
Memory Map	Memory mapping. For details, refer to "4.2.8.4.2 Memory Map".	-
Memory RASConfiguration	Memory RAS configuration. For details, refer to "4.2.8.4.3 Memory RAS Configuration".	-
BSSA Configuration Menu	BSSA configuration. For details, refer to "4.2.8.4.4 BSSA Configuration Menu".	-

4.2.8.4.1 Page Policy

Figure 4-32 shows the **Page Policy** screen.

Figure 4-32 Page Policy Screen

For a description of the parameters on the **Page Policy** screen, refer to Table 4-25.

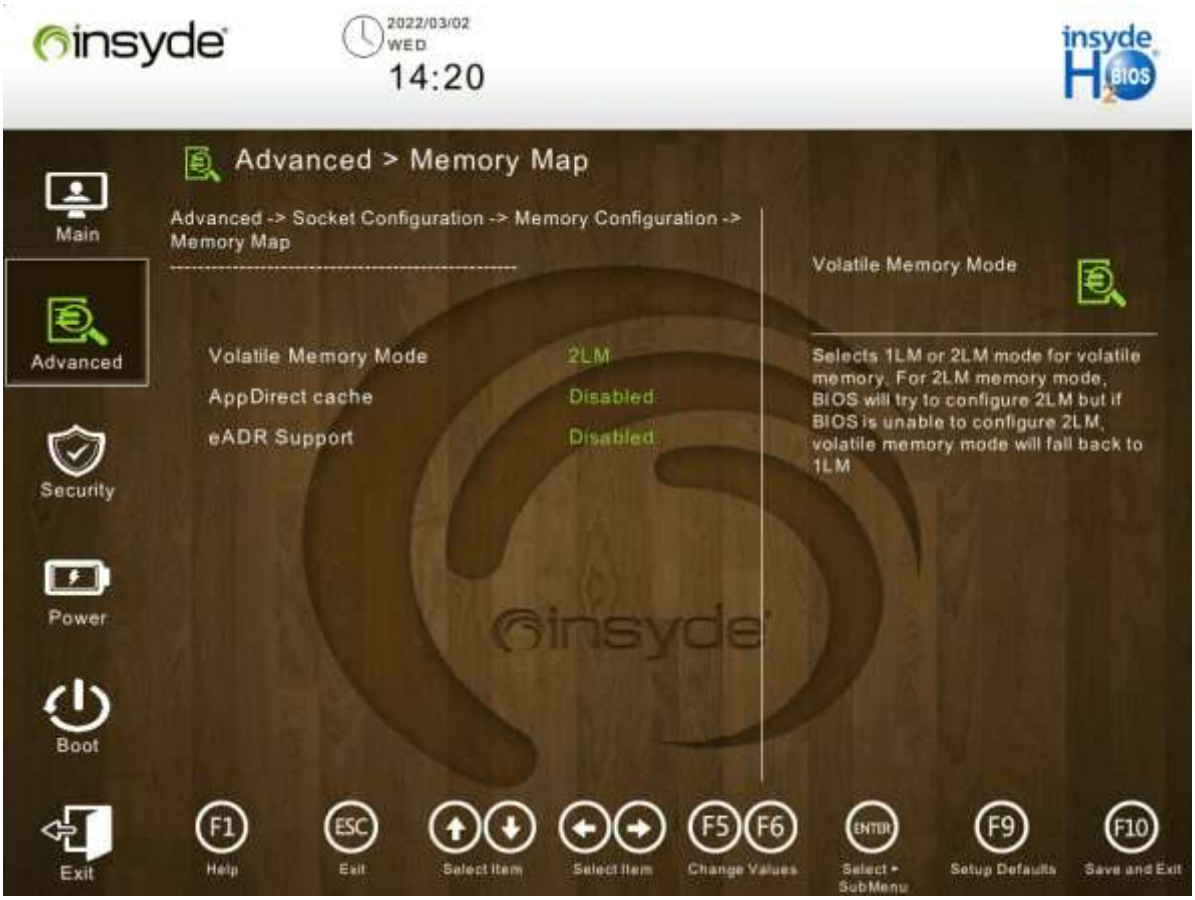
Table 4-25 Page Policy Parameter Descriptions

Parameter	Description	Default
Page Policy	Sets the page management policy. ● Closed: disables the page management policy. ● Adaptive: adaptive.	Adaptive

4.2.8.4.2 Memory Map

Figure 4-33 shows the **Memory Map** screen.

Figure 4-33 Memory Map Screen



For a description of the parameters on the **Memory Map** screen, refer to Table 4-26.

Table 4-26 Memory Mapping Parameter Descriptions

Parameter	Description	Default
Volatile Memory Mode	Sets the volatile memory mode. ● 1LM ● 2LM	2LM
App Direct cache	Enables or disables cache in app direct mode. ● Enabled ● Disabled	Disabled
eADR Support	Enables or disables eADR. ● Enabled ● Disabled ● Auto	Disabled

4.2.8.4.3 Memory RAS Configuration

Figure 4-34 to Figure 4-36 show the **Memory RAS Configuration** screen.

Figure 4-34 Memory RAS Configuration Screen—1

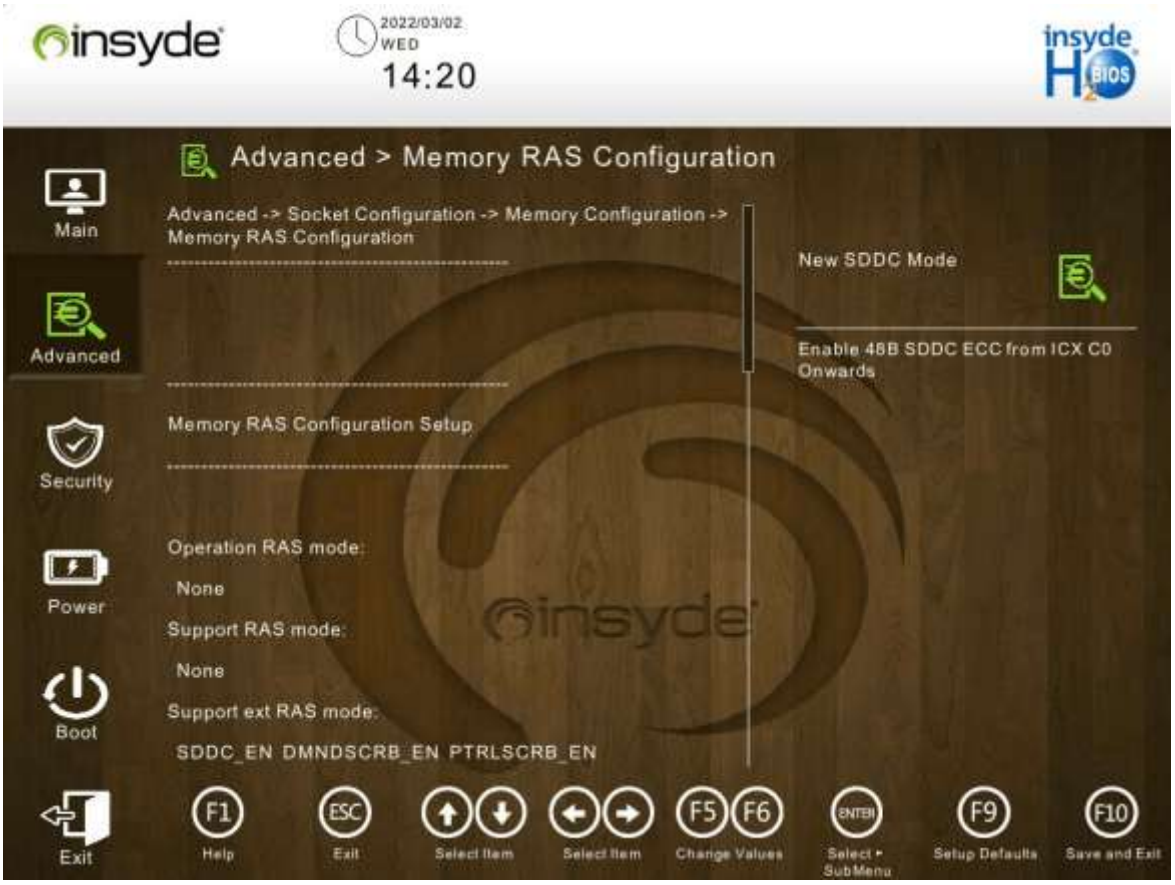


Figure 4-35 Memory RAS Configuration Screen—2

Figure 4-36 Memory RAS Configuration Screen—3

For a description of the parameters on the **Memory RAS Configuration** screen, refer to Table 4-27.

Table 4-27 Parameter Descriptions for Memory RAS Configuration

Parameter	Description	Default
New SDDC Mode	Enables or disables SDDC mode. ● Enabled ● Disabled	Enabled
Mirror Mode	Sets the memory mirroring mode. ● Full Mirror Mode ● Partial Mirror Mode ● Disabled	Disabled
Mirror TAD0	Enables or disables mirroring of all memory for TAD0. ● Enabled ● Disabled	Disabled
UEFI ARM Mirror	Enables or disables UEFI ARM mirroring. ● Enabled ● Disabled	Disabled

Parameter	Description	Default
Memory Correctable Error Flood Policy	Sets the flooding policy of correctable memory errors. ● Disabled ● Once ● Frequency	Frequency
Correctable Error Threshold	Sets the threshold for the number of correctable memory errors. Range: 1–32767.	32767
Trigger SW Error Threshold	Enables or disables the trigger SW error threshold. ● Enabled ● Disabled	Disabled
Sparing SW Error Match Threshold	Sets the sparing SW error match threshold. Range: 1–32767.	0x04
Correctable Error Time Window	Sets the correctable error time window. Range: 1–24.	0x0
Leaky bucket time window based interface	Enables or disables the interface that is based on the leaky bucket time window. ● Enabled ● Disabled	Disabled
Leaky bucket low bit	Sets the leaky bucket low bit. Range: 1–63.	22
Leaky bucket high bit	Sets the leaky bucket high bit. Range: 1–41.	23
Partial Cache Line Sparing PCLS	Enables or disables PCLS. ● Enabled ● Disabled	Disabled
ADDDC Sparing	Enables or disables ADDDC sparing. ● Enabled ● Disabled	Disabled
Column Correction Disable	Enables or disables column correction. ● Enabled ● Disabled	Disabled
Set PMem Die Sparing	Enables or disables PMem die sparing. ● Enabled ● Disabled	Enabled
Patrol Scrub	Enables or disables memory patrol scrubbing. ● Enabled ● Disabled ● Enable at End of POST	Enable at End of POST
Patrol Scrub Interval	Sets the interval (in hours) at which patrol scrubbing is performed. Range: 1–24.	24

4.2.8.4.4 BSSA Configuration Menu

Figure 4-37 shows the **BSSA Configuration Menu** screen.

Figure 4-37 BSSA Configuration Menu Screen

For a description of the parameters on the **BSSA Configuration Menu** screen, refer to Table 4-28.

Table 4-28 BSSA Configuration Parameter Descriptions

Parameter	Description	Default
BSSA Rank Margin Tool	Enables or disables the BSSA RMT tool. ● Enabled ● Disabled	Disabled
BSSA RMT on Fast Cold Boot	Enables or disables the BSSA RMT tool for fast cold boot. ● Enabled ● Disabled	Disabled

4.2.8.5 IIO Configuration

Figure 4-38 to Figure 4-39 show the **IIO Configuration** screen.

Figure 4-38 IIO Configuration Screen 1

Figure 4-39 IIO Configuration Screen 2

For a description of the parameters on the **IIO Configuration** screen, refer to Table 4-29.

Table 4-29 IIO Configuration Parameter Descriptions

Parameter	Description	Default
Socket0 Configuration	Configures socket 0. For details, refer to "4.2.8.5.1 Socket0 Configuration".	-
Socket1 Configuration	Configures socket 1. The parameters of socket 1 are the same as those of socket 0. For details, refer to "4.2.8.5.1 Socket0 Configuration".	-
Intel VT for Directed I/O(VT-d)	Configures the I/O virtualization feature of the Intel chipset. For details, refer to "4.2.8.5.2 Intel VT for Directed I/O(VT-d)".	-
Intel VMD technology	Configures the Intel VMD technology. For details, refer to "4.2.8.5.3 Intel VMD technology".	-
IIO DFX Configuration	Configures the DFX feature. For details, refer to "4.2.8.5.4 IIO DFX Configuration".	-

Parameter	Description	Default
IIO Global Performance Tuning	Configures IIO global performance tuning. For details, refer to "4.2.8.5.5 IIO Global Performance Tuning".	-
Above 4G Decoding	Enables or disables memory mapped I/O for a 64-bit PCIe device to 4GB or greater address space. ● Enabled: enables the above-4G decoding function. ● Disabled: disables the above-4G decoding function.	Enabled
PCIe Hot Plug	Enables or disables the PCIe hot plugging function. ● Enabled: enables the PCIe hot plugging function. ● Disabled: disables the PCIe hot plugging function.	Enabled
PCI-E Completion Timeout(Global)	Enables or disables PCIe completion timeout globally. ● Enabled: enables PCIe completion timeout. ● Disabled: disables PCIe completion timeout.	Enabled
PCI-E Completion Timeout	Sets the time range allowed for PCIe completion.	260 ms to 900 ms
PCI-E ASPM Support (Global)	Configures PCIe active state power management (ASPM) support. ● Per-Port: Each port is configured with a state. ● L1 Only: enters L1 state only. ● No: disables the PCIe ASPM support.	Disabled
PCI-E Port MPSS(Global)	Sets the maximum payload size supported by all PCIe ports. ● 128B ● 256B ● 512B ● Auto	Auto

4.2.8.5.1 Socket0 Configuration

Figure 4-40 shows the **Socket0 Configuration** screen.

Figure 4-40 Socket0 Configuration Screen

For a description of the parameters on the **Socket0 Configuration** screen, refer to Table 4-30.

Table 4-30 Socket0 Configuration Parameter Descriptions

Parameter	Description	Default
Enable PCI-E Completion Timeout(Per- Port)	Enables or disables PCIe completion timeout for each port. ● Yes ● No	No
PCI-E Completion Timeout Value	Sets the maximum time allowed for PCIe completion. Options: ● 50 us to 50 ms ● 50 us to 100 us ● 1 ms to 10 ms ● 16 ms to 55 ms ● 65 ms to 210 ms ● 260 ms to 900 ms ● 1 s to 3.5 s	260 ms to 900 ms
Port 0/DMI	Provides access to port 0/DMI configurations, see Figure 4-41.	-

Parameter	Description	Default
Port 1A	Provides access to port 1A configurations, see Figure 4-42.	-
Port 2A	Provides access to port 2A configurations. Port 2A configurations are similar to port 1A configurations.	-
Port 2C	Provides access to port 2C configurations. Port 2C configurations are similar to port 1A configurations.	-
Port 4A	Provides access to port 4A configurations. Port 4A configurations are similar to port 1A configurations.	-
Port 4C	Provides access to port 4C configurations. Port 4C configurations are similar to port 1A configurations.	-
Port 5A	Provides access to port 5A configurations. Port 5A configurations are similar to port 1A configurations.	-
Port 5B	Provides access to port 5B configurations. Port 5B configurations are similar to port 1A configurations.	-
Port 5C	Provides access to port 5C configurations. Port 5C configurations are similar to port 1A configurations.	-
Port 5D	Provides access to port 5D configurations. Port 5D configurations are similar to port 1A configurations.	-

Figure 4-41 Port 0/DMI Screen

For a description of the parameters on the **Port 0/DMI** screen, refer to Table 4-31.

Table 4-31 Port 0/DMI Parameter Descriptions

Parameter	Description	Default
Link Speed	Sets the link speed. Options: ● Auto ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s)	Auto
PCI-E Port DeEmphasis	Sets the PCIe port de-emphasis level. Options: ● –6.0 dB ● –3.5 dB	-6.0 dB
PCI-E Port Link Status	Displays the current PCIe port link status.	-
PCI-E Port Link Max	Displays the maximum bandwidth of the PCIe port link.	-
PCI-E Port Link Speed	Displays the PCIe port link speed.	-
DMI Port MPSS	Sets the maximum payload size supported by the DMI port.	Auto

Parameter	Description	Default
	● 128B ● 256B ● Auto	
MCTP	Enables or disables the MCTP function. ● Yes ● No	Yes

Figure 4-42 Port 1A Screen

For a description of the parameters on the **Port 1A** screen, refer to Table 4-32.

Table 4-32 Port 1A Parameter Descriptions

Parameter	Description	Default
PCI-E Port	Enables or disables the PCIe port function. ● Enabled ● Disabled ● Auto	Auto
PCI-E Port Link Disable	Enables or disables the PCIe port link. ● Yes ● No	No

Parameter	Description	Default
Link Speed	Sets the link speed. Options: ● Auto ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s)	Auto
PCI-E Port DeEmphasis	Sets the PCIe port de-emphasis level. Options: ● –6.0 dB ● –3.5 dB	-3.5 dB
PCI-E Port Link Status	Displays the current PCIe port link status.	-
PCI-E Port Link Max	Displays the maximum bandwidth of the PCIe port link.	-
PCI-E Port Link Speed	Displays the current PCIe port link speed.	-
PCI-E Port MPSS	Sets the maximum payload size supported by the PCIe port. ● 128B ● 256B ● 512B ● Auto	Auto
MCTP	Enables or disables the MCTP function. ● Yes ● No	Yes

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

Figure 4-43 shows the **Intel VT for Directed I/O (VT-d)** screen.

Figure 4-43 Intel VT for Directed I/O (VT-d) Screen

For a description of the parameters on the **Intel VT for Directed I/O (VT-d)** screen, refer to Table 4-33.

Table 4-33 Parameter Descriptions for Intel VT for Directed I/O (VT-d)

Parameter	Description	Default
Intel VT for Directed I/O	Enables or disables Intel VT for Directed I/O (VT-d). ● Enabled ● Disabled In other BIOS platforms, this parameter is presented as: ● Purley platform: VT-d ● AMD platform: IOMMU ● HG platform: IOMMU	Enabled
DMA Control Opt-In Flag	Enables or disables DMA opt-in. ● Enabled ● Disabled	Disabled
Interrupt Remapping	Enables or disables VT-d interrupt remapping. After this function is enabled, the management programs and operating systems that support this	Auto

Parameter	Description	Default
	function can use the Intel VT to provide interrupt remapping for the directed I/O device. ● Enabled ● Disabled ● Auto	
X2APIC Opt Out	Enables or disables x2APIC opt-out. ● Enabled ● Disabled	Disabled
Pre-boot DMA Protection	Enables or disables pre-boot DMA protection. ● Enabled ● Disabled	Disabled

4.2.8.5.3 Intel VMD technology

Figure 4-44 shows the **Intel VMD technology** screen.

Figure 4-44 Intel VMD Technology Screen

For a description of the parameters on the **Intel VMD technology** screen, refer to Table 4-34.

Table 4-34 Parameter Descriptions for Intel VMD Technology

Parameter	Description	Default
Intel VMD Support	Enables or disables the Intel VMD function. ● Enabled ● Disabled	Disabled
Intel VMD for Volume Management Device on Socket 0	Provides access to VMD configurations on socket 0, see Figure 4-45.	-
Intel VMD for Volume Management Device on Socket 1	Provides access to VMD configurations on socket 1, which are similar to those on socket 0.	-

Figure 4-45 Intel VMD Configurations on Socket 0

4.2.8.5.4 IIO DFX Configuration

Figure 4-46 shows the **IIO DFX Configuration** screen.

Figure 4-46 IIO DFX Configuration Screen

For a description of the parameters on the **IIO DFX Configuration** screen, refer to Table 4-35.

Table 4-35 Parameter Descriptions for IIO DFX Configuration

Parameter	Description	Default
EV DFX Features	Enables or disables EV DFX features. ● Enabled ● Disabled	Disabled

4.2.8.5.5 IIO Global Performance Tuning

Figure 4-47 shows the **IIO Global Performance Tuning** screen.

Figure 4-47 IIO Global Performance Tuning Screen

For a description of the parameters on the **IIO Global Performance Tuning** screen, refer to Table 4-36.

Table 4-36 Parameter Descriptions for IIO Global Performance Tuning

Parameter	Description	Default
Performance Tuning Mode	Sets the IIO performance tuning mode. Options: ● Safe Mode: safe mode. ● Performance Enable Mode: In this mode, recommended performance values are given.	Performance Enable Mode

4.2.8.6 Advanced Power Management Configuration

Figure 4-48 to Figure 4-49 show the **Advanced Power Management Configuration** screen.

Figure 4-48 Advanced Power Management Configuration Screen 1

Figure 4-49 Advanced Power Management Configuration Screen 2

For a description of the parameters on the **Advanced Power Management Configuration** screen, refer to Table 4-37.

Table 4-37 Parameter Descriptions for Advanced Power Management Configuration

Parameter	Description	Default
Power Policy Select	Selects the power policy. ● Max Performance: maximum performance mode. In this mode, the CPU remains stable at the Max Turbo frequency. ● Performance: performance mode. This mode is applicable to high-performance scenarios characterized by high load, multiple threads and low latency. In this mode, the CPU usage and memory usage are high and power saving is automatically disabled, therefore the overall power consumption is increased. ● Efficient: efficiency mode. This mode is applicable to most common scenarios.	Custom

Parameter	Description	Default
	In this mode, the server enables power saving with minimal performance compromise and parks some CPU cores at a low load, to increase power savings while delivering good performance. ● Custom: user-defined mode. This mode is applicable to the scenarios where you need to customize the power management policy as required. ● Latency-Performance: low latency and stable frequency mode. This mode is applicable to the scenarios with strict requirements for latency and jitter, for example, the real-time operating system. In this mode, the server disables power saving and other management functions that may cause latency, and keeps idle CPUs at their highest frequency for faster response. ● IEM Power: IEM power saving mode. This mode is developed by VANTAGEO and is applicable to the scenarios where the overall power consumption of the server needs to be controlled. In this mode, the server enables power saving, and dynamically adjusts the load of non-core areas in accordance with the core load to reduce the overall power consumption of non-core areas. ● IEM Balance Performance: IEM balance mode. This mode is developed by VANTAGEO and is applicable to the scenarios where power consumption and performance need to be balanced. In this mode, the server enables power saving to reduce power consumption, and dynamically adjusts the load of non-core areas in accordance with the core load, to balance power consumption and performance and maximize the performance per unit power consumption.	
IEMA	Sets IEM adjustment coefficient A, range: 0–24.	8
IEMB	Sets IEM adjustment coefficient B, range: 0–10.	0
CPU P State Control	CPU P state controlling function. Enables or disables Turbo mode and Enhanced Intel SpeedStep Technology mode. For details, refer to "4.2.8.6.1 CPU P State Control".	-

Parameter	Description	Default
	In other BIOS platforms, this parameter is presented as: ● Purley platform: CPU P State Control ● AMD platform: AMD CPU P-state Control ● HG platform: AMD CPU P-state Control	
Hardware PM State Control	Hardware PM state controlling function. For details, refer to "4.2.8.6.2 Hardware PM State Control".	-
Frequency Prioritization	Frequency prioritization function. For details, refer to "4.2.8.6.3 Frequency Prioritization".	-
CPU C State Control	CPU C state controlling function. Controls power consumption of CPUs in idle state. For details, refer to "4.2.8.6.4 CPU C State Control". In other BIOS platforms, this parameter is presented as: ● Purley platform: CPU C State Control ● AMD platform: Global C-state Control ● HG platform: Global C-state Control	-
Package C State Control	Package C state controlling function. For details, refer to "4.2.8.6.5 Package C State Control".	-
CPU Thermal Management	CPU thermal management function. For details, refer to "4.2.8.6.6 CPU Thermal Management".	-
CPU-Advanced PM Tuning	CPU-advanced PM tuning function. For details, refer to "4.2.8.6.7 CPU-Advanced PM Tuning".	-
SOCKET RAPL Config	Socket RAPL configuration function. For details, refer to "4.2.8.6.8 SOCKET RAPL Config".	-
ACPI Sx State Control	ACPI Sx state controlling function. For details, refer to "4.2.8.6.9 ACPI Sx State Control".	-
Memory Power & Thermal Configuration	Memory power and thermal configuration function. For details, refer to "4.2.8.6.10 Memory Power/ Thermal Configuration".	-

4.2.8.6.1 CPU P State Control

Figure 4-50 and Figure 4-51 show the **CPU P State Control** screen.

Figure 4-50 CPU P State Control Screen—1

Figure 4-51 CPU P State Control Screen—2

For a description of the parameters on the **CPU P State Control** screen, refer to Table 4-38.

Table 4-38 Parameter Descriptions for CPU P-State Control

Parameter	Description	Default
AVX License Pre-Grant Override	Enables or disables AVX license pre-grant level override. ● Enabled ● Disabled	Diabled
Uncore CLR Freq OVRD	Sets the configuration mode of maximum/minimum CPU uncore frequency. ● Auto: The default maximum/minimum CPU uncore frequency is used. ● Manual: The maximum/minimum CPU uncore frequency is configured manually.	Auto
SpeedStep(Pstates)	Enables or disables EIST. ● Enabled ● Disabled If it is disabled, the **Turbo Mode** parameter is hidden.	Enabled

Parameter	Description	Default
	In other BIOS platforms, this parameter is presented as: ● Purley platform: EIST (P-states) ● AMD platform: no corresponding parameter ● HG platform: no corresponding parameter	
Config TDP Lock	Enables or disables the TDP lock. ● Enabled ● Disabled	Enabled
Active SST-BF	Enables or disables SST-BF. ● Enabled ● Disabled	Disabled
Configure SST-BF	Enables or disables SST-BF configuration. ● Enabled ● Disabled	Enabled
EIST PSD Function	Sets the EIST PSD function. ● HW_ALL ● SW_ALL	HW_ALL
Boot Performance Mode	Sets the boot performance mode. Options: ● Max Performance: ensures the maximum boot performance. ● Max Efficient: ensures the maximum boot efficiency. ● Set by Intel Node Manager: The management engine (ME) controls the boot performance. If **EIST(P-states)** is set to **Disabled**, this parameter is unavailable.	Max Performance
Energy Efficient Turbo	Enables or disables the Energy Efficient Turbo feature. ● Enabled ● Disabled	Enabled
Turbo Mode	Enables or disables Turbo mode. ● Enabled ● Disabled In other BIOS platforms, this parameter is presented as: ● Purley platform: Turbo Mode ● AMD platform: Core Performance Boost ● HG platform: Core Performance Boost	Enabled

Parameter	Description	Default
CPU Flex Ratio Override	Enables or disables the function of setting the maximum frequency for non-Turbo mode. ● Enabled ● Disabled	Disabled
CPU Core Flex Ratio	Maximum frequency for non-Turbo mode.	23

4.2.8.6.2 Hardware PM State Control

Figure 4-52 shows the **Hardware PM State Control** screen.

Figure 4-52 Hardware PM State Control Screen

For a description of the parameters on the **Hardware PM State Control** screen, refer to Table 4-39.

Table 4-39 Parameter Descriptions for Hardware PM State Control

Parameter	Description	Default
Hardware P-States	Enables or disables hardware P-states (HWP) adjustment. ● Native Mode: The hardware chooses a P-state in accordance with OS guidance.	Native Mode

Parameter	Description	Default
	● Out of Band Mode: The hardware autonomously chooses a P-state without OS guidance. ● Disabled: The hardware chooses a traditional P-state in accordance with the OS request.	
Hardware PM Interrupt	Enables or disables hardware PM interrupts. ● Enabled ● Disabled	Disabled
EPP Enable	Enables or disables EPP. ● Enabled ● Disabled	Enabled
APS rocketing	Enables or disables APS switching. ● Enabled ● Disabled	Disabled
Scalability	Enables or disables scalability. ● Enabled ● Disabled	Disabled

4.2.8.6.3 Frequency Prioritization

Figure 4-53 shows the **Frequency Prioritization** screen.

Figure 4-53 Frequency Prioritization Screen

For a description of the parameters on the **Frequency Prioritization** screen, refer to Table 4-40.

Table 4-40 Frequency Prioritization Parameter Descriptions

Parameter	Description	Default
RAPL Prioritization	Enables or disables the RAPL priority function. ● Enabled ● Disabled	Disabled

4.2.8.6.4 CPU C State Control

Figure 4-54 shows the **CPU C State Control** screen.

Figure 4-54 CPU C State Control Screen

For a description of the parameters on the **CPU C State Control** screen, refer to Table 4-41.

Table 4-41 Parameter Descriptions for CPU C-State Control

Parameter	Description	Default
Enable Monitor MWAIT	Enables or disables MONITOR/MWAIT instructions. ● Enabled ● Disabled For some OSs, you must disable both **Monitor/Mwait** and **C State** to disable **C State**. In other BIOS platforms, this parameter is presented as: ● Purley platform: Monitor/Mwait ● AMD platform: no corresponding parameter ● HG platform: no corresponding parameter	Enabled
CPU C6 report	Enables or disables the reporting of CPU C6 state to the OS. ● Enabled ● Disabled ● Auto	Disabled

Parameter	Description	Default
	In other BIOS platforms, this parameter is presented as: ● Purley platform: CPU C6 report ● AMD platform: no corresponding parameter ● HG platform: no corresponding parameter	
Enhanced Halt State(C1E)	Enables or disables enhanced halt state (C1E). After it is enabled, the OS can change C-states. ● Enabled ● Disabled In other BIOS platforms, this parameter is presented as: ● Purley platform: Enhanced Halt State(C1E) ● AMD platform: no corresponding parameter ● HG platform: no corresponding parameter	Disabled
OS ACPI Cx	Sets the mapping relationship between CPU C-states and ACPI C-states. ● ACPI C2: ACPI C2 mode. ● ACPI C3: ACPI C3 mode.	ACPI C2

4.2.8.6.5 Package C State Control

Figure 4-55 shows the **Package C State Control** screen.

Figure 4-55 Package C State Control Screen

For a description of the parameters on the **Package C State Control** screen, refer to Table 4-42.

Table 4-42 Parameter Descriptions for Package C-State Control

Parameter	Description	Default
Package C State	Sets the package C-state. Options: ● C0/C1state ● C2state ● C6(non Retention) state ● Auto	C0/C1state

4.2.8.6.6 CPU Thermal Management

Figure 4-56 shows the screen.

Figure 4-56 CPU Thermal Management Screen

For a description of the parameters on the **CPU Thermal Management** screen, refer to Table 4-43.

Table 4-43 Parameter Descriptions for CPU Thermal Management

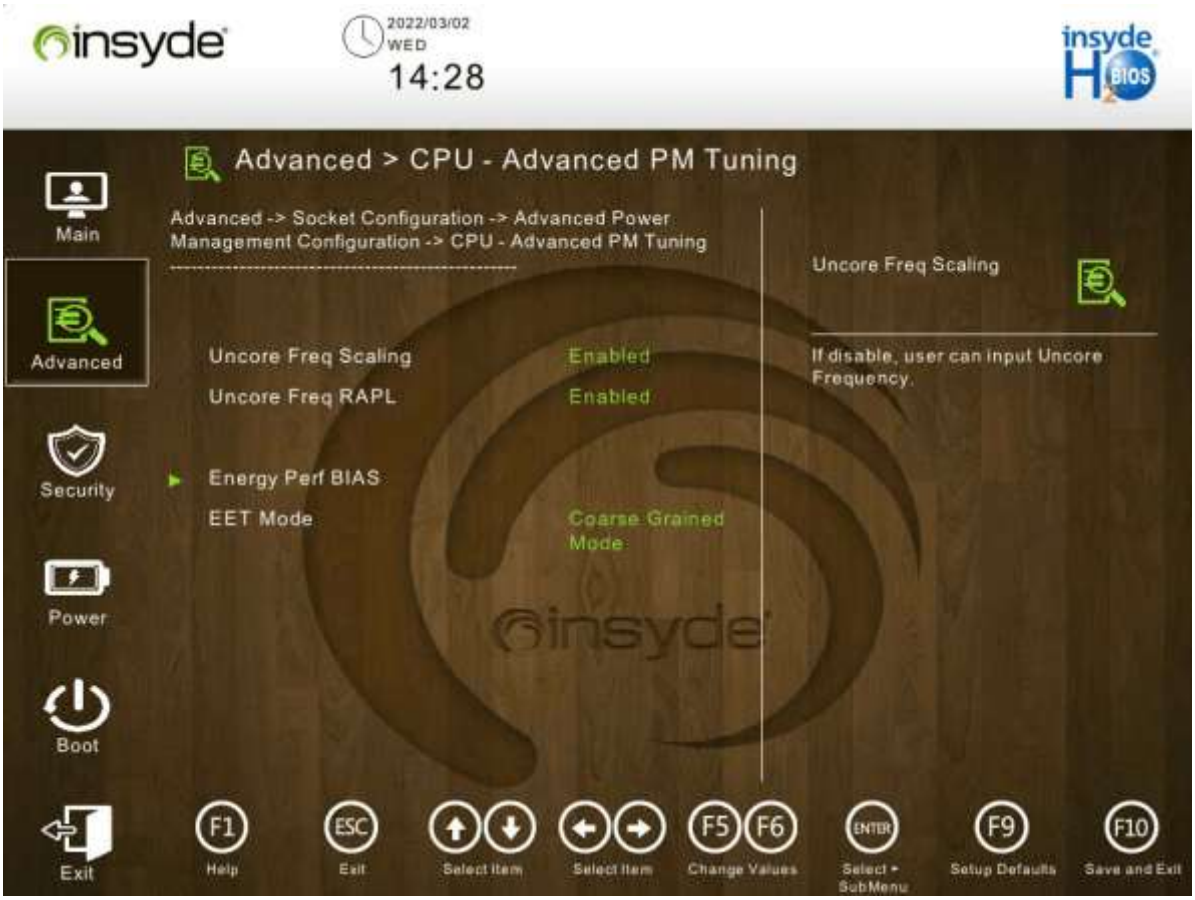
Parameter	Description
CPU T State Control	Provides access to CPU T-state control, see Figure 4-57.

Figure 4-57 CPU T State Control Screen

4.2.8.6.7 CPU-Advanced PM Tuning

Figure 4-58 shows the **CPU-Advanced PM Tuning** screen.

Figure 4-58 CPU-Advanced PM Tuning Screen



For a description of the parameters on the **CPU-Advanced PM Tuning** screen, refer to Table 4-44.

Table 4-44 Parameter Descriptions for CPU-Advanced PM Tuning

Parameter	Description	Default
Uncore Freq Scaling	Enables or disables uncore frequency scaling. ● Enabled ● Disabled	Enabled
Uncore Freq RAPL	Enables or disables uncore frequency RAPL. ● Enabled ● Disabled	Enabled
Energy Perf BIAS	Provides access to energy/ performance bias settings, see Figure 4-59.	-
EET Mode	Sets the EET mode. Options: ● Coarse Grained Mode	Coarse Grained Mode

Parameter	Description	Default
	● Fine Grained Mode	

Figure 4-59 Energy Perf BIAS Screen

4.2.8.6.8 SOCKET RAPL Config

Figure 4-60 shows the **SOCKET RAPL Config** screen.

Figure 4-60 SOCKET RAPL Config Screen

For a description of the parameters on the **SOCKET RAPL Config** screen, refer to Table 4-45.

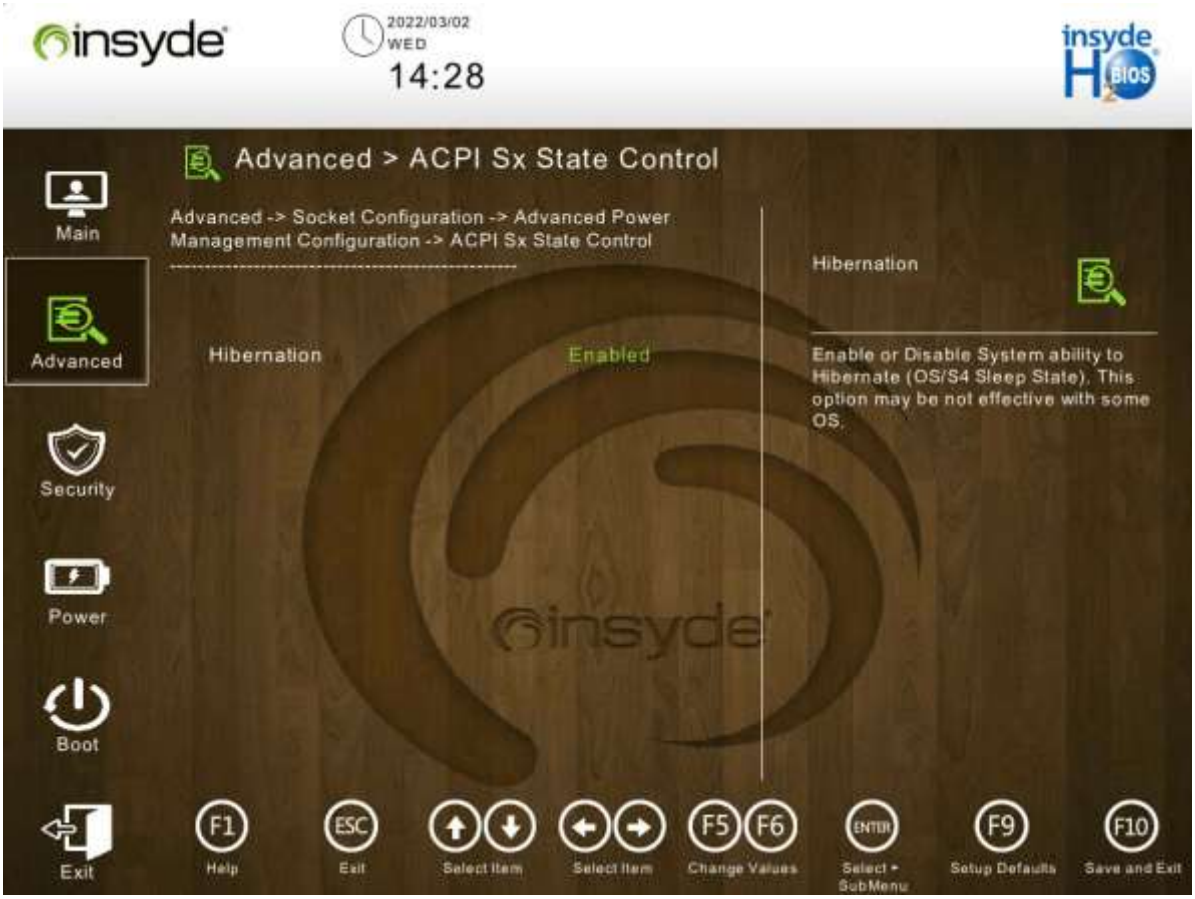
Table 4-45 Parameter Description for Socket RAPL Configuration

Parameter	Description	Default
PL1 Power Limit	Sets the PL1 power limit. Range: 0 to fused value. If the PL1 power limit is set to 0, it indicates that the fused value is used.	0
PL2 Power Limit	Sets the PL2 power limit. Range: 0 to fused value. If the PL2 power limit is set to 0, it indicates that the fused value is used.	0

4.2.8.6.9 ACPI Sx State Control

Figure 4-61 shows the **ACPI Sx State Control** screen.

Figure 4-61 ACPI Sx State Control Screen



For a description of the parameters on the **ACPI Sx State Control** screen, refer to Table 4-46.

Table 4-46 Parameter Descriptions for ACPI Sx State Control

Parameter	Description	Default
Hibernation	Enables or disables OS hibernation. ● Enabled ● Disabled	Enabled

4.2.8.6.10 Memory Power/Thermal Configuration

Figure 4-62 shows the **Memory Power/Thermal/Configuration** screen.

Figure 4-62 Memory Power/Thermal/Configuration Screen

For a description of the parameters on the **Memory Power/Thermal/Configuration** screen, refer to Table 4-47.

Table 4-47 Parameter Descriptions for Memory Power/Thermal/Configuration

Parameter	Description
DRAM RAPL Configuration	Provides access to DRAM RAPL configuration, see Figure 4-63.
Memory Thermal	Provides access to memory thermal configuration, see Figure 4-64.
Memory Power Savings Advanced Options	Provides access to memory power saving configuration, see Figure 4-65.

Figure 4-63 DRAM RAPL Configuration Screen

For a description of the parameters on the **DRAM RAPL Configuration** screen, refer to Table 4-48.

Table 4-48 Parameter Descriptions for DRAM RAPL Configuration

Parameter	Description	Default
DRAM RAPL	Enables or disables the DRAM RAPL function. ● Enabled ● Disabled	Enabled

Figure 4-64 Memory Thermal Screen

For a description of the parameters on the **Memory Thermal** screen, refer to Table 4-49.

Table 4-49 Parameter Descriptions for Memory Thermal Configuration

Parameter	Description	Default
Throttling Mode	Sets the memory throttling mode. ● CLTT ● OLTT ● CLTT with PECI ● Disabled	CLTT

Figure 4-65 Memory Power Savings Advanced Options Screen

For a description of the parameters on the **Memory Power Savings Advanced Options** screen, refer to Table 4-50.

Table 4-50 Parameter Descriptions for Memory Power Savings Advanced Options

Parameter	Description	Default
CKE Throttling	Sets the CKE throttling mode. ● Auto ● Manual If **CKE Throttling** is set to **Manual**, **CKE Feature** is displayed below **CKE Throttling**. Select **CKE Feature** and press **Enter**. The **CKE Feature** screen is displayed, see Figure 4-66.	Auto
SREF Feature	Sets the SREF feature. ● Auto ● Manual If **SREF Feature** is set to **Manual**, **Self Refresh Feature** is displayed below **SREF Feature**. Select **Self Refresh Feature**, and press **Enter**. The **Self**	Auto

Parameter	Description	Default
	Refresh Feature screen is displayed, see Figure 4-67.	
PKGC SREF EN	Enables or disables the PKGC self-refresh function. ● Enabled ● Disabled	Enabled

Figure 4-66 CKE Feature Screen

For a description of the parameters on the **CKE Feature** screen, refer to Table 4-51.

Table 4-51 CKE Feature Parameter Descriptions

Parameter	Description	Default
CKE Idle Timer	Sets the CKE idle timer. Minimum value: 20. Unit: ns.	20
APD	Enables or disables the APD function. ● Enabled ● Disabled	Disabled
PPD	Enables or disables the PPD function. ● Enabled ● Disabled	Enabled

Figure 4-67 Self Refresh Feature Screen

For a description of the parameters on the **Self Refresh Feature** screen, refer to Table 4-52.

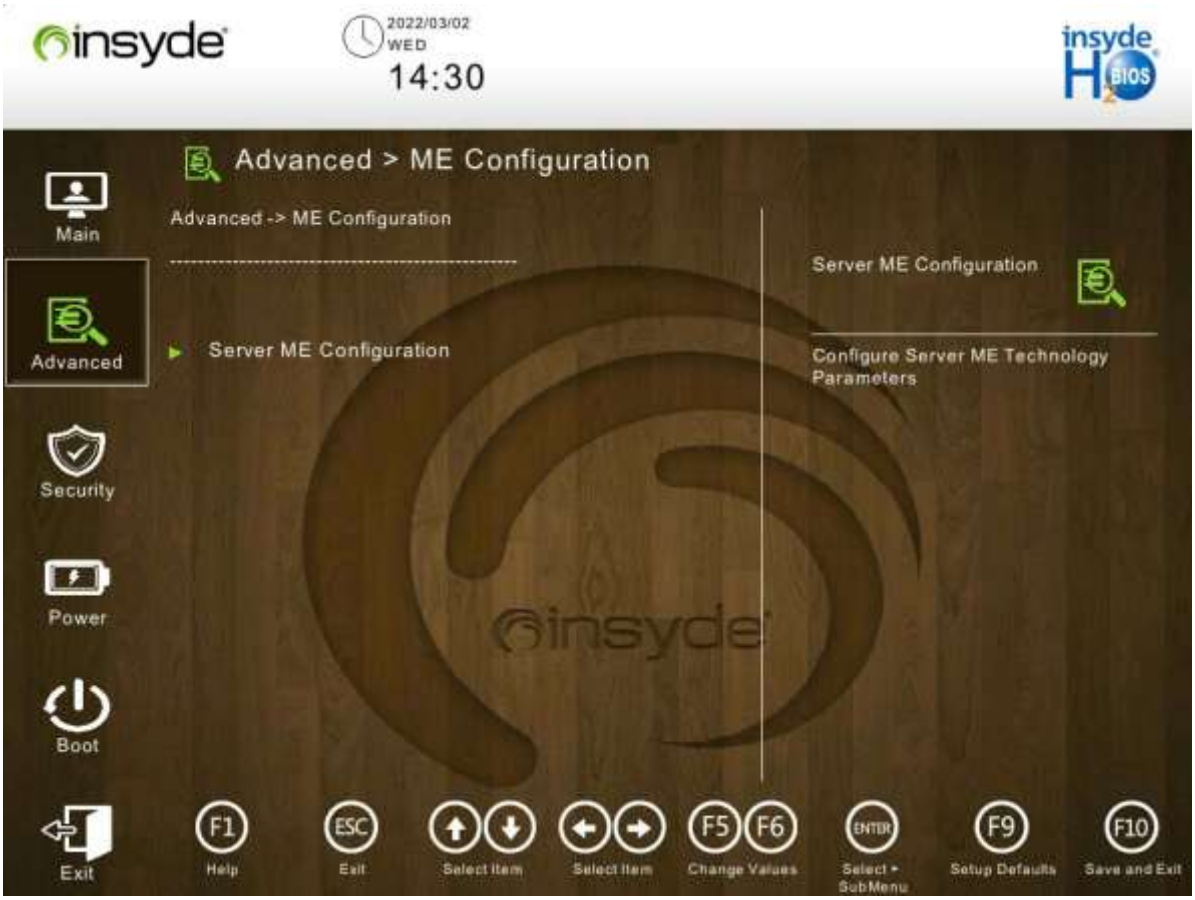
Table 4-52 Parameter Descriptions for the Self Refresh Feature

Parameter	Description	Default
Opportunistic SR	Enables or disables the self-refresh function. ● Enabled ● Disabled	Disabled
MDLL OFF	Enables or disables the MDLL OFF function. ● Enabled ● Disabled	Enabled
CK in SR	Sets clock behaviors during self-refresh. ● Driven ● Pulled Low	Pulled Low

4.2.9 ME Configuration

Figure 4-68 shows the **ME Configuration** screen.

Figure 4-68 ME Configuration Screen



For a description of the parameters on the **ME Configuration** screen, refer to Table 4-53.

Table 4-53 ME Configuration Parameter Descriptions

Parameter	Description
Sever ME Configuration	General ME configuration information, see Figure 4-69.

Figure 4-69 Server ME Configuration Screen

For a description of the parameters on the **Sever ME Configuration** screen, refer to Table 4-54.

Table 4-54 Parameter Descriptions for Sever ME Configuration

Parameter	Description	Default
Oper. Firmware Version	Valid firmware version number.	0F:4.4.4.538
Backup Firmware Version	Backup firmware version number.	N/A
Recovery Firmware Version	Version number of the running firmware in recovery mode.	0F:4.4.4.58
ME Firmware Status #1	ME firmware status #1.	0x000F0245
ME Firmware Status #2	ME firmware status #2.	0x89114026
Current State	Current ME state.	Operational
Error Code	Error code information.	No Error
Recovery Cause	Recovery cause.	N/A
MCTP Bus Owner	Location of MCTP bus owner.	0x408

4.2.10 PCH Configuration

Figure 4-70 shows the **PCH Configuration** screen.

Figure 4-70 PCH Configuration Screen

For a description of the parameters on the **PCH Configuration** screen, refer to Table 4-55.

Table 4-55 PCH Configuration Function Descriptions

Parameter	Description
PCH Devices	PCH device configuration function. For details, refer to 4.2.10.1 PCH Devices.
PCIe Configuration	PCIe configuration function. For details, refer to 4.2.10.2 PCIe Configuration.
PCH SATA Configuration	PCH SATA configuration function. For details, refer to 4.2.10.3 PCH SATA Configuration.
PCH sSATA Configuration	PCH sSATA configuration function. For details, refer to 4.2.10.4 PCH sSATA Configuration.
USB Configuration	USB configuration function. For details, refer to 4.2.10.5 USB Configuration.
ADR Configuration	ADR configuration function.

Parameter	Description
	For details, refer to 4.2.10.6 ADR Configuration.

4.2.10.1 PCH Devices

Figure 4-71 shows the **PCH Devices** screen.

Figure 4-71 PCH Devices Screen

For a description of the parameters on the **PCH Devices** screen, refer to Table 4-56.

Table 4-56 PCH Device Parameter Descriptions

Parameter	Description	Default
External SSC Enable - CK420	Enables or disables external Spread Spectrum Clocking (SSC). ● Enabled: enables external SSC. ● Disabled: disables external SSC.	Enabled
Restore on AC Power Loss	Configures the system power-off policy. ● Always On: keeps the system powered on. ● Always Off: keeps the system powered off. ● Last Stat: keeps the last state.	Always Off
Pcie Pll SSC	Enables or disables PCIe PLL SSC.	Enabled

Parameter	Description	Default
	● Enabled: enables PCIe PLL SSC. ● Disabled: disables PCIe PLL SSC. ● Auto: automatic mode.	

4.2.10.2 PCIe Configuration

Figure 4-72 shows the **PCIe Configuration** screen.

Figure 4-72 PCIe Configuration Screen

For a description of the parameters on the **PCIe Configuration** screen, refer to Table 4-57.

Table 4-57 PCIe Configuration Parameter Descriptions

Parameter	Description	Default
OnBoard Lan	Enables or disables the onboard LAN. ● Enabled: enables the onboard LAN. ● Disabled: disables the onboard LAN.	Enabled

4.2.10.3 PCH SATA Configuration

Figure 4-73 shows the **PCH SATA Configuration** screen.

Figure 4-73 PCH SATA Configuration Screen

For a description of the parameters on the **PCH SATA Configuration** screen, refer to Table 4-58.

Table 4-58 Parameter Descriptions for PCH SATA Configuration

Parameter	Description	Default
SATA Controller	Enables or disables SATA controllers. ● Enabled: enables SATA controllers. ● Disabled: disables SATA controllers. If this parameter is set to **Disabled**, the **Configure SATA as** option is hidden.	Enabled
Configure SATA as	SATA controller mode. ● AHCI: AHCI mode. ● RAID: RAID mode.	AHCI
SATA Port0	Name of the device installed in SATA port 0. If the device is present, the device information is displayed. If not, "Not Installed" is displayed.	Not Installed
Software Preserve	Software preservation.	Unknown
port0	Enables or disables SATA port 0.	Enabled

Parameter	Description	Default
	● Enabled: enables SATA port 0. ● Disabled: disables SATA port 0.	
Hot Plug	Enables or disables the hot plugging function. ● Enabled: enables the hot plugging function. ● Disabled: disables the hot plugging function.	Disabled
Configuration as eSATA	Enables or disables the eSATA configuration function. ● Enabled: enables the eSATA configuration function. ● Disabled: disables the eSATA configuration function.	Disabled
SATA Device Type	SATA device type. ● Hard Disk Drive: supports the hard disk drive. ● Solid State Drive: supports the solid state drive.	Hard Disk Drive
SATA Topology	SATA topological structure. ● Unknown: unknown mode. ● ISATA: ISATA mode. ● Direct Connect: direct connection mode. ● Flex: flexible mode. ● M2: M2 mode.	Unknown

Note

The configuration parameters of other SATA ports are the same as those of SATA port 0. This section uses SATA port 0 as an example.

4.2.10.4 PCH sSATA Configuration

Figure 4-74 shows the **PCH sSATA Configuration** screen.

Figure 4-74 PCH sSATA Configuration Screen

For a description of the parameters on the **PCH sSATA Configuration** screen, refer to Table 4-59.

Table 4-59 Parameter Descriptions for PCH sSATA Configuration

Parameter	Description	Default
sSATA Controller	Enables or disables the sSATA controller. ● Enabled: enables the sSATA controller. ● Disabled: disables the sSATA controller. If this parameter is set to **Disabled**, the **Configure sSATA as** option is hidden.	Enabled
Configure sSATA as	sSATA controller mode. ● AHCI: AHCI mode. ● RAID: RAID mode.	AHCI
sSATA Port0	Name of the device installed in sSATA port 0. If the device is present, the device information is displayed. If not, "Not Installed" is displayed.	Not Installed
port0	Enables or disables sSATA port 0. ● Enabled: enables sSATA port 0.	Enabled

Parameter	Description	Default
	● Disabled: disables sSATA port 0.	
Hot Plug	Enables or disables the hot plugging function. ● Enabled: enables the hot plugging function. ● Disabled: disables the hot plugging function.	Disabled
Configuration as eSATA	Enables or disables the eSATA configuration function. ● Enabled: enables the eSATA configuration function. ● Disabled: disables the eSATA configuration function.	Disabled
sSATA Device Type	sSATA device type. ● Hard Disk Drive: supports the hard disk drive. ● Solid State Drive: supports the solid state drive.	Hard Disk Drive
SATA Topology	sSATA topological structure. ● Unknown: unknown mode. ● ISATA: ISATA mode. ● Direct Connect: direct connection mode. ● Flex: flexible mode. ● M2: M2 mode.	Unknown

Note

The configuration parameters of other sSATA ports are the same as those of sSATA port 0. This section uses sSATA port 0 as an example.

4.2.10.5 USB Configuration

Figure 4-75 shows the **USB Configuration** screen.

Figure 4-75 USB Configuration Screen

For a description of the parameters on the **USB Configuration** screen, refer to Table 4-60.

Table 4-60 USB Configuration Parameter Descriptions

Parameter	Description	Default
1 USB Mouse	Number of USB mice connected to the server.	-
1 USB Keyboard	Number of USB keyboards connected to the server.	-
2 USB MassStorage	Number of USB media devices connected to the server.	-
USB Port Connected BMC	Enables or disables the USB port connected to the BMC. ● Enable: enables the USB port connected to the BMC. ● Disable: disables the USB port connected to the BMC.	Enabled
USB XHCI MSI Disable WA	Enables or disables the xHCI MSI function. ● Enabled: enables the xHCI MSI function. ● Disabled: disables the xHCI MSI function.	Disabled
XHCI Over Current Pins	Enables or disables the xHCI Over Current function.	Enabled

Parameter	Description	Default
	● Enabled: enables the xHCI Over Current function. ● Disabled: disables the xHCI Over Current function.	
XHCI Wake On Usb Enable	Enables or disables the USB wake-up function. ● Enabled: enables the USB wake-up function. ● Disabled: disables the USB wake-up function.	Enabled

4.2.10.6 ADR Configuration

Figure 4-76 shows the **ADR Configuration** screen.

Figure 4-76 ADR Configuration Screen

For a description of the parameters on the **ADR Configuration** screen, refer to Table 4-61.

Table 4-61 ADR Configuration Parameter Descriptions

Parameter	Description	Default
Enable/Disable ADR	Enables or disables the ADR function. ● Platform-POR ● Enabled: enables the ADR function. ● Disabled: disables the ADR function.	Platform- POR

Parameter	Description	Default
	If the eADR function is enabled, this parameter cannot be configured.	
ADR GPIO	GPIO address. ● GPIO B ● GPIO C	GPIO B
Host Partition Reset ADR Enable	Enables or disables the function of resetting address for the host partition. ● Platform-POR ● Enabled: enables the function of resetting address for the host partition. ● Disabled: disables the function of resetting address for the host partition.	Platform- POR

4.2.11 Server Mgmt

Figure 4-77 shows the **Server Mgmt** screen

Figure 4-77 Server Mgmt Screen

For a description of the parameters on the **Server Mgmt** screen, refer to Table 4-62.

Table 4-62 Server Management Parameter Descriptions

Parameter	Description
IPMI Interface Configuration	IPMI configuration. For details, refer to "4.2.11.1 IPMI Interface Configuration".
BMC Firmware Version	BMC firmware version.
IPMI Specification Version	IPMI version.
BMC MAC Address	MAC address of the BMC.
BMC Configuration	BMC configuration. For details, refer to "4.2.11.2 BMC Configuration".

4.2.11.1 IPMI Interface Configuration

Figure 4-78 shows the **IPMI Interface Configuration** screen.

Figure 4-78 IPMI Interface Configuration Screen

For a description of the parameters on the **IPMI Interface Configuration** screen, refer to Table 4-63.

Table 4-63 Parameter Descriptions for IPMI Interface Configuration

Parameter	Description	Default
Interface Type	IPMI interface type.	KCS
Address	IPMI address.	0x0CA2/0x0CA3
Interface Status	IPMI interface status.	OK

4.2.11.2 BMC Configuration

Figure 4-79 to Figure 4-82 show the **BMC Configuration** screen.

Figure 4-79 BMC Configuration Screen 1

Figure 4-80 BMC Configuration Screen 2

Figure 4-81 BMC Configuration Screen 3

Figure 4-82 BMC Configuration Screen 4

BMC Configuration Table 4-64

Table 4-64 BMC Configuration Parameter Descriptions

Parameter	Description	Default
POST Timer	After the POST timer is enabled, the POST timer is started during the POST. ● Enabled: enables the POST timer. ● Disabled: disables the POST timer. When this parameter is set to **Disabled**, the **POST Timer Timeout** and **POST Timer Policy** parameters are greyed out.	Enabled
POST Timer timeout	Time of the POST timer, range: 10–60, unit: minutes.	15
POST Timer Policy	Power policy applied after a POST timer timeout. ● No Action: no operation. ● Hard Reset: resets the server. ● Power Down: powers off the server. ● Power Cycle: powers off the server and then powers it on.	Power Cycle

Parameter	Description	Default
OS Watchdog Timer	After the OS watchdog timer is enabled, the watchdog timer is started when the operating system is started. ● Enabled: enables the OS watchdog timer. ● Disabled: disables the OS watchdog timer. When this parameter is set to **Enabled**, the **OS Wtd Timer Timeout** and **OS Wtd Timer Policy** parameters are displayed.	Disabled
OS Wtd Timer Timeout	Time of the OS watchdog timer, range: 10–60, unit: minutes.	20
OS Wtd Timer Policy	Power policy applied after an OS watchdog timer timeout. ● No Action: No operation. ● Hard Reset: resets the server. ● Power Down: powers off the server. ● Power Cycle: powers off the server and then powers it on.	Power Cycle
SOL	Enables or disables the SOL function. ● Enabled: enables the SOL function. ● Disabled: disables the SOL function.	Enabled
Set BMC to default	Enables or disables the function of restoring the BMC to default settings. ● Enabled: enables the function of restoring the BMC to default settings. ● Disabled: disables the function of restoring the BMC to default settings.	Disabled
User Configuration	Sets the username and password.	-
BMC Share Link	Configures BMC NIC (shared) link work mode. ● Auto: automatic mode. ● Enabled: enables BMC NIC (shared) link work mode. ● Disabled: disables BMC NIC (shared) link work mode.	Enabled
Work Mode	Configures the work mode of the BMC. ● Auto: automatic mode. Both eth0 and eth1 are configured with the MAC address of the dedicated network port. ● Bonding: bonding mode. Both eth0 and eth1 are configured with the MAC address of the bonding interface.	Normal

Parameter	Description	Default
	● Normal: normal mode. eth0 and eth1 are configured with their respective MAC addresses.	
LAN Channel	NIC interface type. ● iSAC (Dedicated): dedicated BMC management network port. ● NIC (Shared): shared BMC network port.	iSAC
IPv4 Mode	Enables or disables IPv4 mode. ● Enabled: enables IPv4 mode. ● Disabled: disables IPv4 mode.	Enabled
IPv4 Source	IPv4 address mode. ● Static: static IP address. ● DHCP: IP address allocated by the DHCP server.	Static
IPv4 IP Address	Static IPv4 address.	192.168.5.9
IPv4 Subnet Mask	IPv4 subnet mask.	255.255.255.0
IPv4 Gateway Address	IPv4 gateway address.	192.168.5.255
IPv6 Mode	Enables or disables IPv6 mode. ● Enabled: enables IPv6 mode. ● Disabled: disables IPv6 mode.	Enabled
Enable IPv6 Static IP Address	Enables or disables static IPv6 address mode. ● Enabled: enables static IPv6 address mode. ● Disabled: disables static IPv6 address mode.	Enabled
IPv6 Prefix Length	IPv6 address prefix length.	64
IPv6 Static IP Address	Static IPv6 address.	-
IPv6 Router Address Control	Enables or disables the IPv6 routing function. ● All Disabled ● Enable static router address ● Enable dynamic router address ● All Enabled	Enable static router address
IPv6 Static Router 1 Address	IP address of IPv6 static router 1.	::
IPv6 Static Router 1 MAC Address	MAC address of IPv6 static router 1.	00:00:00:00:00:00
IPv6 Static Router 1 Prefix Length	Prefix length of the IP address of IPv6 static router 1.	0
IPv6 Dynamic IP	Dynamic IPv6 address.	::
IPv6 Dynamic IP PrefixLength	Prefix length of the dynamic IPv6 address.	0

Parameter	Description	Default
Vlan Id	VLAN ID, range: 0–4094. The value 0 indicates all VLANs are disabled.	0

Note

The configuration of IPv6 static router 2 is the same as that of IPv6 static router 1.

4.2.12 Console Redirection

Figure 4-83 shows the **Console Redirection** screen.

Figure 4-83 Console Redirection Screen

For a description of the parameters on the **Console Redirection** screen, refer to Table 4-65.

Table 4-65 Console Redirection Parameter Descriptions

Parameter	Description	Default
Console Serial Redirect	Enables or disables the serial port redirection function, which maps the data of a specified physical or virtual serial port to a specified system serial port.	Enabled

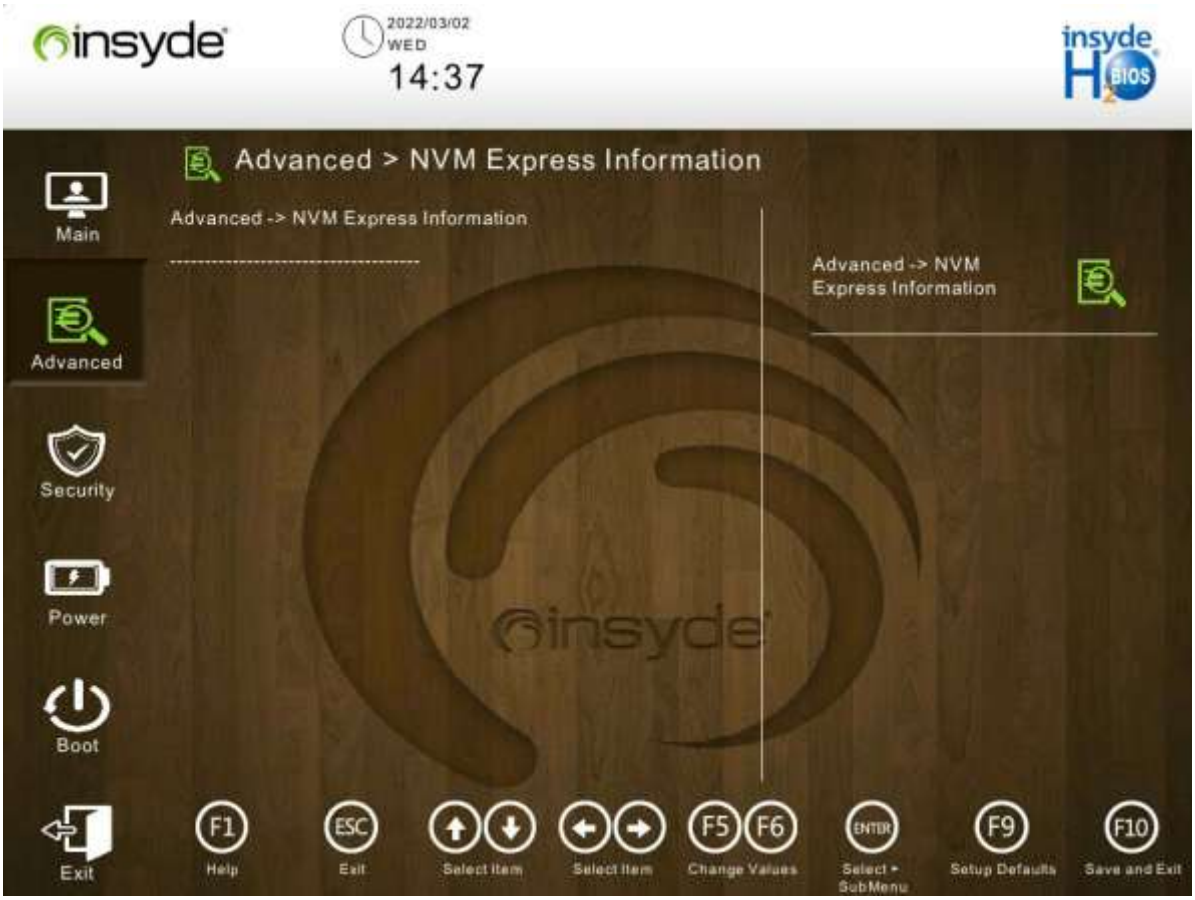
Parameter	Description	Default
	● Enabled: enables the serial port redirection function. ● Disabled: disables the serial port redirection function.	
Terminal Type	Configures the terminal type. ● VT_100 ● VT_100+ ● VT_UTF8 ● PC_ANSI ● LOG_TERM	VT_100
Baud Rate	Configures the number of bits transmitted per second. ● 1200: A total of 1200 bits are transmitted per second. ● 2400: A total of 2400 bits are transmitted per second. ● 4800: A total of 4800 bits are transmitted per second. ● 9600: A total of 9600 bits are transmitted per second. ● 19200: A total of 19200 bits are transmitted per second. ● 38400: A total of 38400 bits are transmitted per second. ● 57600: A total of 57600 bits are transmitted per second. ● 115200: A total of 115200 bits are transmitted per second.	115200
Data Bits	Configures the number of actual data bits in each byte. ● 7 Bits: The actual data occupies 7 bits in each byte. ● 8 Bits: The actual data occupies 8 bits in each byte.	8 Bits
Parity	Configures parity bits. ● None: no parity. ● Even: even parity. ● Odd: odd parity.	None
Stop Bits	Configures the stop bit (last bit of a single packet). ● 1 Bit: The stop bit is 1. ● 2 Bit: The stop bit is 2.	1 Bit

Parameter	Description	Default
Flow Control	Configures the flow control type. ● None ● RTS/CTS ● XON/XOFF	None
Information Wait Time	Configures the wait time. ● 0 Second ● 2 Seconds ● 5 Seconds ● 10 Seconds ● 30 Seconds	5 Seconds
C.R After POST	Configures whether to continue using console redirection after the POST is completed. ● Yes: After the POST is completed, console redirection is still used. ● No: After the POST is completed, console redirection is not used.	YES
Auto Refresh	Enables or disables the automatic refresh function. ● Enabled: enables the automatic refresh function. ● Disabled: disables the automatic refresh function.	Disabled

4.2.13 NVM Express Information

Figure 4-84 shows the **NVM Express Information** screen.

Figure 4-84 NVM Express Information Screen



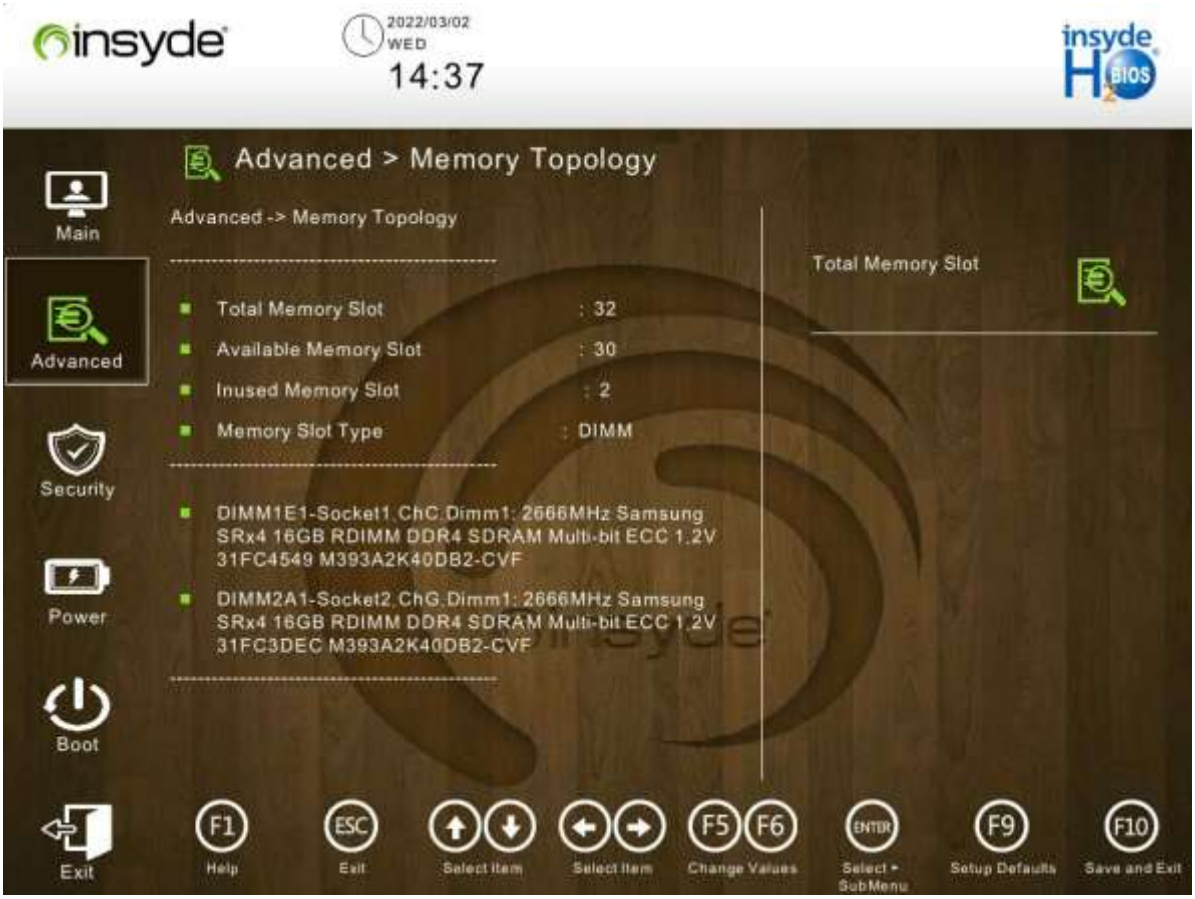
Note

If the mainboard is mounted with an NVMe hard disk, the NVMe hard disk information is displayed on the screen.

4.2.14 Memory Topology

Figure 4-85 shows the **Memory Topology** screen.

Figure 4-85 Memory Topology Screen



For a description of the parameters on the **Memory Topology** screen, refer to Table 4-66.

Table 4-66 Memory Topology Parameter Descriptions

Parameter	Description	Default
Total Memory Slot	Total number of memory slots.	32
Available Memory Slot	Number of available memory slots.	-
Inused Memory Slot	Number of used memory slots.	-
Memory Slot Type	Type of memory slots.	DIMM

4.2.15 PXE Configuration

Figure 4-86 the **PXE Configuration** screen.

Figure 4-86 PXE Configuration Screen

For a description of the parameters on the **PXE Configuration** screen, refer to Table 4-67.

Table 4-67 PXE Configuration Parameter Descriptions

Parameter	Description	Default
Embedded LOM Port1	Enables or disables the PXE function for network port 1 of the onboard NIC. ● Enabled: enables the PXE function. ● Disabled: disables the PXE function.	Enabled
MAC Address	MAC address of network port 1.	-
Embedded LOM Port2	Enables or disables the PXE function for network port 2 of the onboard NIC. ● Enabled: enables the PXE function. ● Disabled: disables the PXE function.	Disabled
MAC Address	MAC address of network port 2.	-
Slot 7 PXE	Enables or disables the PXE function for all network ports of the standard NIC in slot 7. ● Enabled: enables the PXE function for all network ports.	Enabled

Parameter	Description	Default
	● Disabled: disables the PXE function for all network ports.	
MAC Address	MAC address of each network port of the standard NIC in slot 7.	-

4.3 Security

The **Security** screen provides the administrator password settings, see Figure 4-87.

Figure 4-87 Security Screen

For a description of the parameters on the **Security** screen, refer to Table 4-68.

Table 4-68 Security Parameter Descriptions

Parameter	Description	Default
Current TPM Device	Dynamically shows the TPM device type. If the server is not installed with a TPM device, **Not Detected** is displayed. ● When the device of the TPM x.x type is selected, the parameters **TPM**, **TPM Active PCR Hash Algorithm**, **TPM Hardware Supported Hash**,	-

Parameter	Description	Default
	TPM Availability and **TPM Operation Clear TPMS** are displayed. ● When the TCM type of device is selected, the **Trusted Platform Support** parameter is displayed.	
TPM State	State of the TPM device. ● If there is a TPM device, the device state is displayed. ● If there is no TPM device, **Not Installed** is displayed.	-
Administrator Password	Displays whether the administrator password is set. ● If a password is set, **Installed** is displayed. ● If no password is set, **Not Installed** is displayed.	-
Set Administrator Password	Sets the administrator password. The password consists of 8 to 32 characters, including uppercase and lowercase letters, digits, and special characters. After the administrator password is set, **Installed** will be displayed next to **Administrator Password**. You need to enter this password when you enter the Setup Utility.	-
Power on Password	Enables or disables the power-on password setting. ● Enabled: enables the function. ● Disabled: disables the function. The **Power on Password** parameter is displayed only after the administrator password is set.	Disabled
Security Freeze Lock	Enables or disables Security Freeze Lock state. ● Enabled: enables the state. ● Disabled: disables the state.	Enabled

4.4 Power

Figure 4-88 shows the **Power** screen.

Figure 4-88 Power Screen

For a description of the parameters on the **Power** screen, refer to Table 4-69.

Table 4-69 Power Parameter Descriptions

Parameter	Description	Default
Wake On PME	Enables or disables the PME function. ● Enabled: enables the PME function. ● Disabled: disables the PME function.	Disabled

4.5 Boot

The **Boot** screen provides boot item settings, such as boot mode settings, boot order settings, and boot process settings. Figure 4-89 to Figure 4-90 show the **Boot** screen.

Figure 4-89 Boot Screen 1

Figure 4-90 Boot Screen 2

For a description of the parameters on the **Boot** screen, refer to Table 4-70.

Table 4-70 Boot Parameter Descriptions

Parameter	Description	Default
Boot Mode	Boot mode of the system. ● UEFI: UEFI mode. ● Legacy: Legacy mode.	UEFI
Quick Boot	Enables or disables quick boot. ● Enabled: If quick boot is enabled, the memory test is skipped so that the boot time is shorten. ● Disabled: If quick boot is disabled, a full-memory test is performed so that the boot time is longer.	Enabled
Quiet Boot	Enables or disables quiet boot. ● Enabled: If quiet boot is enabled, the product logo instead of POST information is displayed on the boot screen. ● Disabled: If quiet boot is disabled, POST information is displayed on the boot screen.	Disabled
Network Stack	Enables or disables the PXE boot function.	Enabled

Parameter	Description	Default
	● Enabled: enables the PXE boot function. ● Disabled: disables the PXE boot function. The **Network Stack** parameter can be configured only when **Boot Mode** is set to **UEFI**.	
IPv4 PXE Support	Enables or disables the IPv4 PXE boot function. ● Enabled: enables the IPv4 PXE boot function. ● Disabled: disables the IPv4 PXE boot function. The **IPv4 PXE Support** parameter can be configured only when **Network Stack** is set to **Enabled**.	Enabled
IPv4 HTTP Support	Enables or disables the IPv4 HTTP boot function. ● Enabled: enables the IPv4 HTTP boot function. ● Disabled: disables the IPv4 HTTP boot function. The **IPv4 HTTP Support** parameter can be configured only when **Network Stack** is set to **Enabled**.	Disabled
IPv6 PXE Support	Enables or disables the IPv6 PXE boot function. ● Enabled: enables the IPv6 PXE boot function. ● Disabled: disables the IPv6 PXE boot function. The **IPv6 PXE Support** parameter can be configured only when **Network Stack** is set to **Enabled**.	Enabled
IPv6 HTTP Support	Enables or disables the IPv6 HTTP boot function. ● Enabled: enables the IPv6 HTTP boot function. ● Disabled: disables the IPv6 HTTP boot function. The **IPv6 HTTP Support** parameter can be configured only when **Network Stack** is set to **Enabled**.	Disabled
Endless Boot Support	Sets the function of automatically rebooting the system when no boot device is available. ● Enabled: enables the boot retry function. ● Disabled: disables the boot retry function.	Enabled
Pxe Retry Count	Sets the number of PXE polling times. 99 indicates infinite polling.	3
USB Boot	Enables or disables boot from an external USB device (including the virtual CD-ROM drive, floppy drive, and physical USB CD-ROM drive). ● Enabled: enables boot from an external USB device. ● Disabled: disables boot from an external USB device.	Enabled
Embedded Shell Boot	Enables or disables embedded shell boot. ● Enabled: enables embedded shell boot. ● Disabled: disables embedded shell boot.	Disabled
Boot Device Type Order	Sets the boot order.	-

Parameter	Description	Default
	For details, refer to "4.5.1 Boot Device Type Order".	
UEFI App Boot	Sets Memtest boot. For details, refer to "4.5.2 UEFI App Boot".	-
Hard Disk Drive	Sets the priority at which the system is booted from a hard disk. For details, refer to "4.5.3 Hard Disk Drive".	-
Network	Sets the priority at which the system is booted from a network device. For details, refer to "4.5.4 Network".	-
Others	Enables or disables Shell boot. For details, refer to "4.5.5 Others".	-

4.5.1 Boot Device Type Order

Figure 4-91 shows the **Boot Device Type Order** screen.

Figure 4-91 Boot Device Type Order Screen

By default, the boot order of the server is as follows:

1. Hard Disk Drive
2. Network
3. USB
4. CD/DVD-Rom Drive
5. Others

4.5.2 UEFI App Boot

Figure 4-92 shows the **UEFI App Boot** screen.

Figure 4-92 UEFI App Boot Screen

Click **Launch Memtest Boot**. In the displayed screen, you can start the Test86 memory test.

Note

Once the Test86 memory test is started, you cannot go back to the BIOS setup screens.

4.5.3 Hard Disk Drive

Figure 4-93 shows the **Hard Disk Drive** screen.

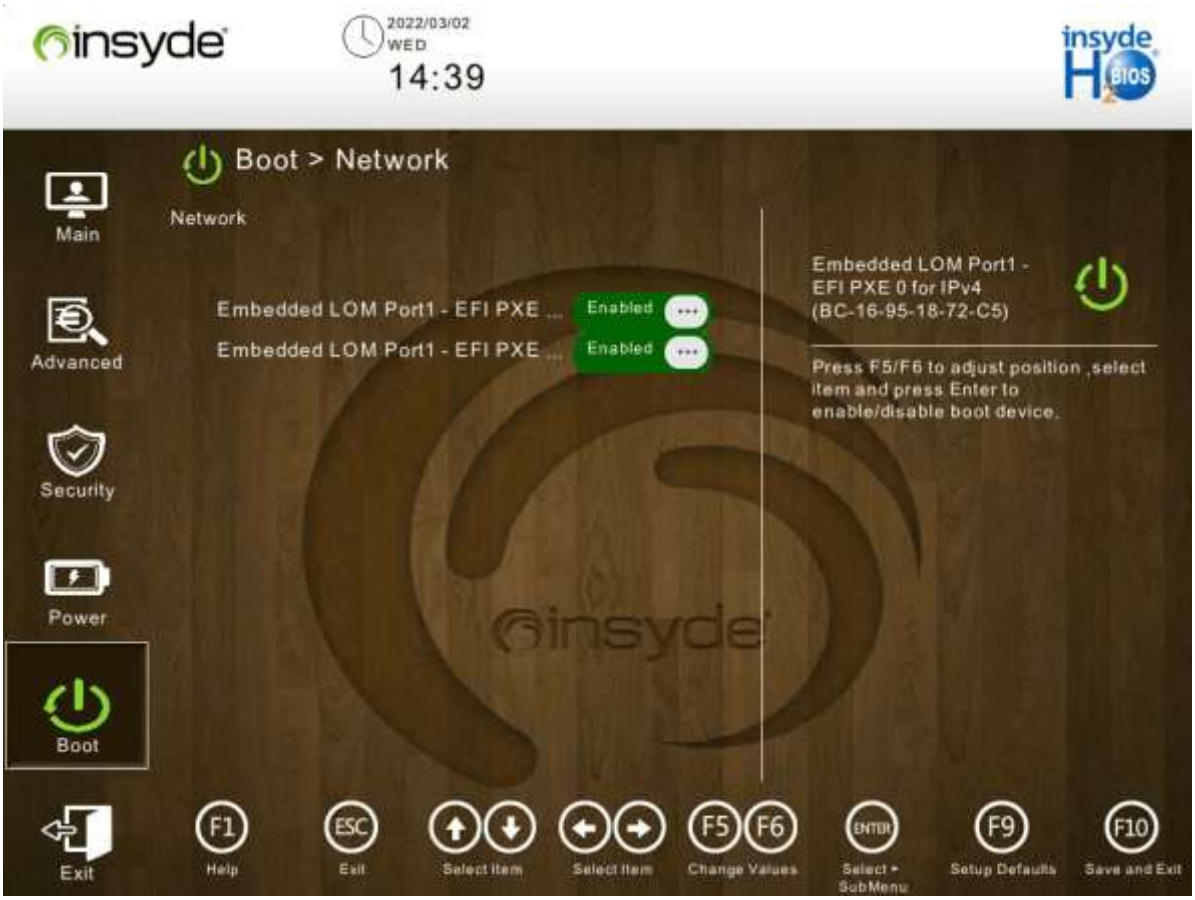
Figure 4-93 Hard Disk Drive Screen

On the **Hard Disk Drive** screen, you can set the sequence of booting from each hard disk.

4.5.4 Network

Figure 4-94 shows the **Network** screen.

Figure 4-94 Network Screen



On the **Network** screen, you can set the sequence of booting from each network device.

4.5.5 Others

Figure 4-95 shows the **Others** screen.

Figure 4-95 Others Screen

For a description of the parameters on the **Others** screen, refer to Table 4-71.

Table 4-71 Descriptions for the Parameter on the Others Screen

Parameter	Description	Default
Internal EFI Shell	Enables or disables Shell boot. The EFI shell is a built-in command line. After it is enabled, Shell boot options are displayed. ● Enabled ● Disabled	Disabled

4.6 Exit

The **Exit** screen enables you to save the BIOS settings and exit the BIOS Setup Utility, see Figure 4-96.

Figure 4-96 Exit Screen

For a description of the parameters on the **Exit** screen, refer to Table 4-72.

Table 4-72 Exit Screen Parameter Descriptions

Parameter	Description
Saving Changes & Exit	Saves the changes and exits the BIOS.
Save Change Without Exit	Saves the changes without exiting the BIOS.
Discard Changes & Exit	Discards the changes and exits the BIOS.
Load Defaults	Restores the default BIOS settings.
Load Custom Defaults	Loads the custom defaults.
Save Custom Defaults	Saves the custom defaults.
Discard Changes Without Exiting	Discards the changes without exiting the BIOS.

Chapter 5
Reference: Control Keys for BIOS Setup

The **Whitley & Cedar Island** platform provides GUI-based BIOS setup, so you can perform operations with either the mouse or keyboard. For a description of the available control keys, refer to Table 5-1.

Table 5-1 Control Keys

Control Key	Description
F1	Opens the **General Help** screen that displays the descriptions of the available keys.
Esc	Exits the current menu: ● If you press the **Esc** key when you are editing a field or selecting a menu, or when you are in any sub-menu, the system returns to the upper-layer menu. ● If you press the **Esc** key under any main menu, a dialog box is displayed to confirm whether you want to exit the menu.
←/→ direction key	Moves the cursor leftwards or rightwards to select a main menu.
↑/↓ direction key	Moves the cursor upwards or downwards.
F5/F6	Modifies the settings.
Enter	Executes a command or selects a sub-menu.
F9	Sets the default value.
F10	Saves the changes and exits the BIOS Setup Utility.

Glossary

AC

- Alternating Current

ACPI

- Advanced Configuration and Power Interface

ADR

- Automatic DIMM Refresh

AER

- Advanced Error Reporting

AES

- Advanced Encryption Standard

AHCI

- Advanced Host Controller Interface

APD

- AC Power Distribution Module

APIC

- Advanced Programmable Interrupt Controller

APS

- Automatic Phase Shifter

ARI

- Assist Request Instruction

ARM

- Asynchronous Response Mode

BIOS

- Basic Input/Output System

BIST

- Built-In Self-Test

BMC

- Baseboard Management Controller

BSSA

- BIOS Shared Software Architecture

CD

- Compact Disk

CMCI

- Corrected Machine Check Interrupt

COM

- Component Object Model

CPU

- Central Processing Unit

DAC

- Digital Analog Converter

DB

- Database

DCU

- Data Collection Unit

DFX

- Design for X

DHCP

- Dynamic Host Configuration Protocol

DIMM

- Dual Inline Memory Module

DRAM

- Dynamic Random Access Memory

DVD

- Digital Versatile Disc

EFI

- Extensible Firmware Interface

EIST

- Enhanced Intel Speed Step Technology

eMCA

- Enhanced Machine Check Architecture

EPP

- Energy Performance Preference

FC

- Fiber Channel

GPIO

- General Purpose Input Output

GUI

- Graphical User Interface

HTTP

- Hypertext Transfer Protocol

I/O

- Input/Output

ID

- Identification

IEM

- Interface ETH M

IIO

- Integrated I/O Module

IOMMU

- Input/Output Memory Management Unit

IPMI

- Intelligent Platform Management Interface

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

iSAC

- Integrated Server Administrator Controller

iSCSI

- Internet Small Computer System Interface

KEK

- Key Exchange Key

KVM

- Keyboard, Video and Mouse

LAN

- Local Area Network

LMCE

- Local Machine Check Exception

LOM

- LAN on Motherboard

MAC

- Media Access Control

MCTP

- Management Component Transport Protocol

ME

- Management Engine

MMCFG

- Memory Mapped Configuration

MMIO

- Memory-mapped I/O

MSI

- Mobile Storage Interface

NIC

- Network Interface Card

NUMA

- Non-Uniform Memory Access Architecture

NVMe

- Non-Volatile Memory Express

OOB

- Out of Band

OS

- Operating System

PC

- Personal Computer

PCH

- Platform Controller Hub

PCIe

- Peripheral Component Interconnect Express

PECI

- Platform Environment Control Interface

PK

- Platform Key

PM

- Power Module

PME

- Power Management Event

POST

- Power-On Self-Test

PPR

- Post-Package Repair

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RAS

- Reliability, Availability and Serviceability

RFO

- Read-For-Ownership

RMT

- Remote Maintenance Terminal

ROM

- Read-Only Memory

SATA

- Serial ATA

SDDC

- Single Device Data Correction

SMI

- System Management Interruption

SMT

- Simultaneous Multi-Threading

SMX

- Safer Mode Extension

SOL

- Serial Over LAN

SR-IOV

- Single-Root I/O Virtualization

SSC

- Spread Spectrum Clock

SSD

- Solid State Drive

SVM

- Secure Virtual Machine

TCM

- Trusted Cryptography Module

TDP

- Thermal Design Power

TPM

- Trusted Platform Module

TXT

- Trusted Execution Technology

UEFI

- Unified Extensible Firmware Interface

UPI

- Ultra Path Interconnect

USB

- Universal Serial Bus

VGA

- Video Graphic Adapter

VLAN

- Virtual Local Area Network

VM

- Virtual Machine

VMD

- Volume Management Device

VMX

- Virtual Machine Extension

WHEA

- Windows Hardware Error Architecture