BIOS User Guide

B860M-SILVER

Table of Contents

BIOS Update

The BIOS can be updated using either of the following utilities:

- BIOSTAR BIOS-FLASHER: Using this utility, the BIOS can be updated from a file on a hard disk, a USB drive (a flash drive or a USB hard drive), or a CD-ROM.
- BIOSTAR BIOS Update Utility: It enables automated updating while in the Windows environment. Using this utility, the BIOS can be updated from a file on a hard disk, a USB drive (a flash drive or a USB hard drive), or a CD-ROM, or from the file location on the Web.

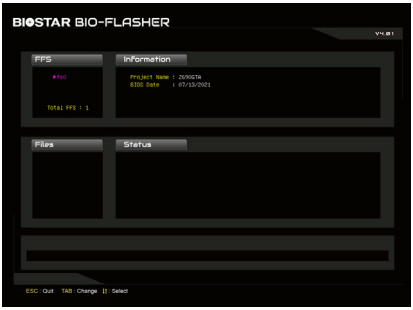
BIOSTAR BIO-FLASHER

Note

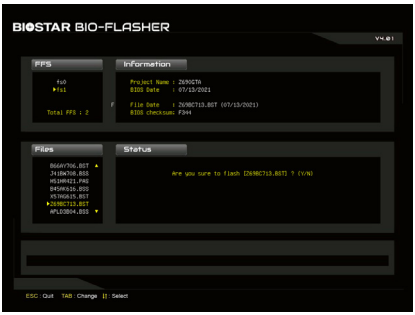
» *This utility only allows storage device with FAT32/16 format and single partition.*
» *Shutting down or resetting the system while updating the BIOS will lead to system boot failure.*

Updating BIOS with BIOSTAR BIO-FLASHER

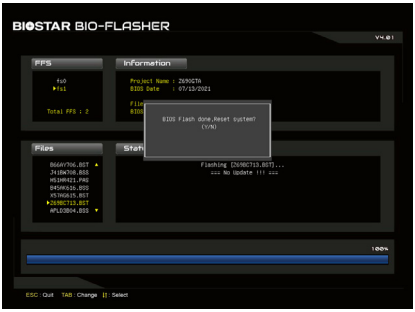
1. Go to the website to download the latest BIOS file for the motherboard.
2. Then, copy and save the BIOS file into a USB flash (pen) drive.(Only supported FAT/FAT32 format)
3. Insert the USB pen drive that contains the BIOS file to the USB port.
4. Power on or reset the computer and then press <F12> during the POST process.
5. After entering the POST screen, the BIO-FLASHER utility pops out. Choose <fs0> to search for the BIOS file.



6. Select the proper BIOS file, and a message asking if you are sure to flash the BIOS file. Click “Yes” to start updating BIOS.



7. A dialog pops out after BIOS flash is completed, asking you to restart the system. Press the <Y> key to restart system.



8. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.

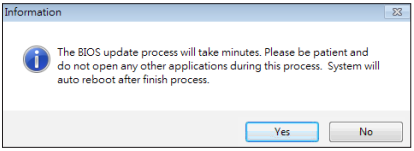
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes and Reset> to restart the computer. Then the BIOS Update is completed.

BIOS Update Utility (through the Internet)

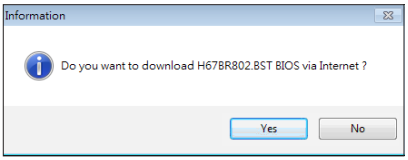
1. Installing BIOS Update Utility from the DVD Driver.
2. Please make sure the system is connected to the internet before using this function.

3. Launch BIOS Update Utility and click the "Online Update" button on the main screen.

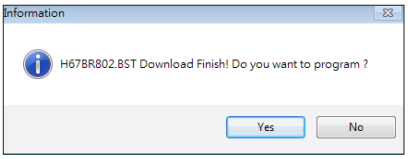
4. An open dialog will show up to request your agreement to start the BIOS update. Click "Yes" to start the online update procedure.



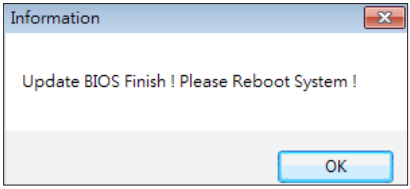
5. If there is a new BIOS version, the utility will ask you to download it. Click "Yes" to proceed.



6. After the download is completed, you will be asked to program (update) the BIOS or not. Click "Yes" to proceed.



7. After the updating process is finished, you will be asked you to reboot the system. Click “OK” to reboot.



8. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.

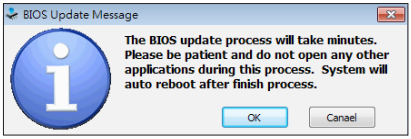
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes> and <Reset> to restart the computer. Then, the BIOS Update is completed.

BIOS Update Utility (through a BIOS file)

1. Installing BIOS Update Utility from the DVD Driver.
2. Download the proper BIOS from http://www.biostar.com.tw/

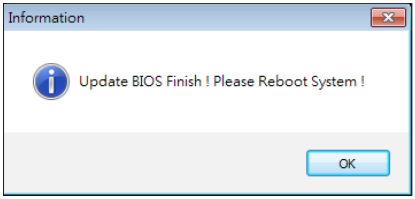
3. Launch BIOS Update Utility and click the “Update BIOS” button on the main screen.

4. A warning message will show up to request your agreement to start the BIOS update. Click “OK” to start the update procedure.



5. Choose the location for your BIOS file in the system. Please select the proper BIOS file, and then click on “Open”. It will take several minutes, please be patient.

6. After the BIOS Update process is finished, click on “OK” to reboot the system.

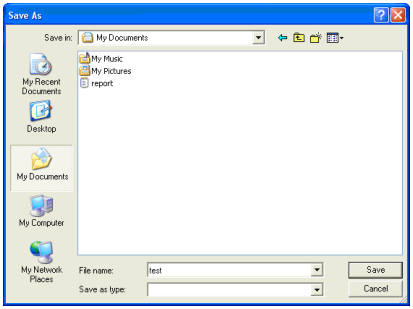


7. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.

After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes and Reset> to restart the computer. Then, the BIOS Update is completed.

Backup BIOS

Click the Backup BIOS button on the main screen for the backup of BIOS, and select a proper location for your backup BIOS file in the system, and click “Save”.



UEFI BIOS Setup

Introduction

The purpose of this manual is to describe the settings in the AMI UEFI BIOS Setup program on this motherboard. The Setup program allows users to modify the basic system configuration and save these settings to NVRAM.

UEFI BIOS determines what a computer can do without accessing programs from a disk. This system controls most of the input and output devices such as keyboard, mouse, serial ports and disk drives. BIOS activates at the first stage of the booting process, loading and executing the operating system. Some additional features, such as virus and password protection or chipset fine-tuning options are also included in UEFI BIOS.

The rest of this manual will to guide you through the options and settings in UEFI BIOS Setup.

Plug and Play Support

This AMI UEFI BIOS supports the Plug and Play Version 1.0A specification.

EPA Green PC Support

This AMI UEFI BIOS supports Version 1.03 of the EPA Green PC specification.

ACPI Support

AMI ACPI UEFI BIOS support Version 1.0/2.0 of Advanced Configuration and Power interface specification (ACPI). It provides ASL code for power management and device configuration capabilities as defined in the ACPI specification, developed by Microsoft, Intel and Toshiba.

PCI Bus Support

This AMI UEFI BIOS also supports Version 2.3 of the Intel PCI (Peripheral Component Interconnect) local bus specification.

Using Setup

When starting up the computer, press **<Del>** during the **Power-On Self-Test (POST)** to enter the UEFI BIOS setup utility.

In the UEFI BIOS setup utility, you will see **General Help** description at the top right corner, and this is providing a brief description of the selected item. **Navigation Keys** for that particular menu are at the bottom right corner, and you can use these keys to select item and change the settings.

Note

- *The default UEFI BIOS settings apply for most conditions to ensure optimum performance of the motherboard. If the system becomes unstable after changing any settings, please load the default settings to ensure system's compatibility and stability. Use Load Setup Default under the Exit Menu.*
- *For better system performance, the UEFI BIOS firmware is being continuously updated. The UEFI BIOS information described in this manual is for your reference only. The actual UEFI BIOS information and settings on board may be slightly different from this manual.*
- *The content of this manual is subject to be changed without notice. We will not be responsible for any mistakes found in this user's manual and any system damage that may be caused by wrong-settings.*

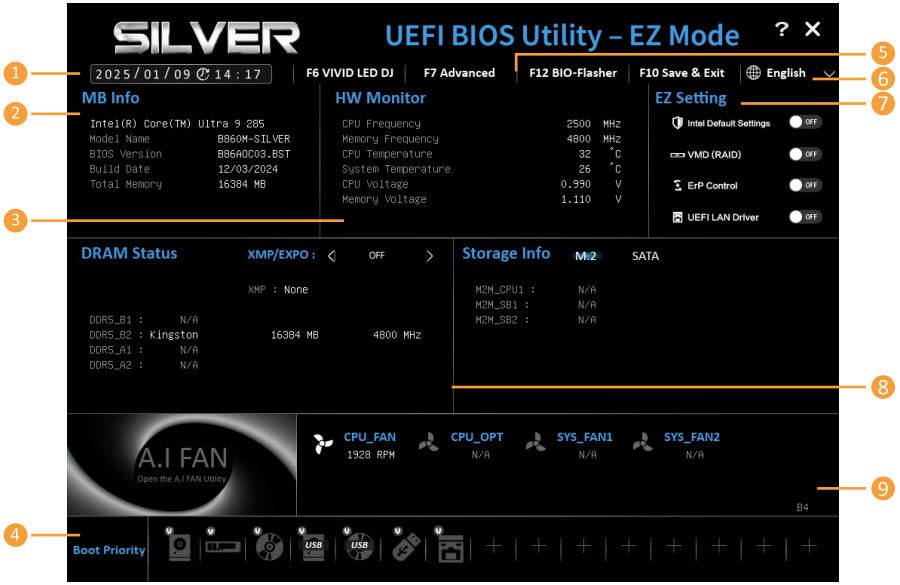
EZ Mode

In EZ mode, it allows you to quickly operate the basic system setting. Press <F7> to display the EZ Mode menu.

1. **System Time:** Display the system clock.
2. **MB Info:** Display the motherboard Information.
3. **Hardware Information:** Shows the CPU/ MB temperature, memory size, BIOS version and build date.
4. **Boot Priority Bar:** you can move the device icons to change the boot priority.
5. **Setup Function Keys:** This item allows you to sets Save & Exit. Press F6/ F7/ F12 key to switch between Vivid Led DJ, Advanced mode and BIO-Flasher.
6. **Language Settings:** This item allows you to change language.
7. **EZ Settings:** This item enable or disable the Intel Default Settings/ VMD(RAID)/ Erp Control/ UEFI LAN Driver.
8. **CPU/ Memory/ Storage Information:** This item display CPU/ Memory/ Storage information.
9. **XMP Settings & AI FAN Palette Interface:** Enables or disables the XMP menu. It also allows you to click or press the A.I FAN button to enter the fan setting interface.

Note

» *Menu contents will be different slightly, depending on different motherboard of users' computers.*



A.I FAN Control

Press <F5> to display the A.I FAN Control menu.

1. **CPU FAN/ CPU OPT/ System1/ System2:** Click button to set the status value of CPU FAN, SYSTEM FAN.
2. **PWM/ Temperature Panel:** According to the fan PWM value corresponding to CPU and system temperature to adjust the fan speed.

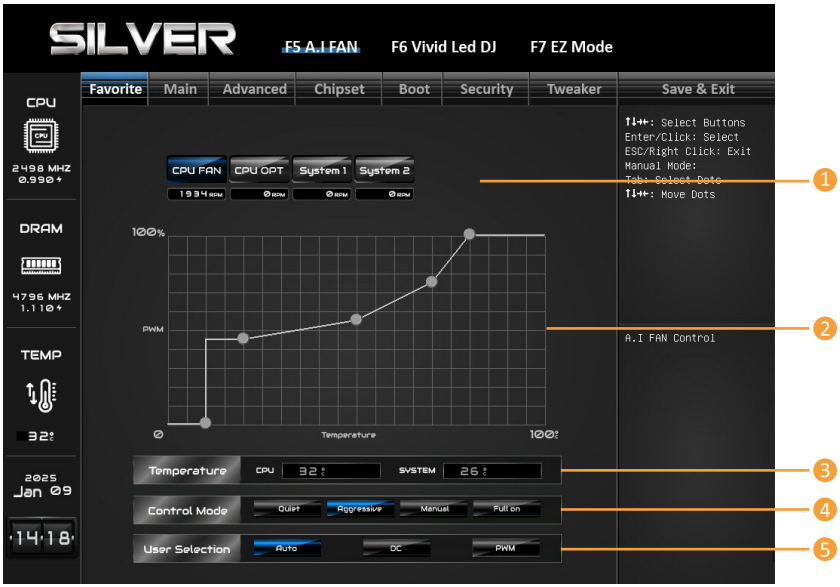
» *Allows you to adjust according to your preferences.*

3. **Temperature:** Shows the current CPU and system temperature.
4. **Control Mode:** Allows you to control mode of the fans.
   - **Quiet: Enable Quiet mode.**
   - **Aggressive: Enable Aggressive mode.**
   - **Manual: Enable Manual mode.**
   - **Full on: Enable Full On mode.**
5. **User Selection:** Sets the fan property controls the actual selection operation.
   - **Auto: Allows you to adjust the Automatic detection Mode.**
   - **DC: Allows you to adjust the Direct Current (DC) Mode.**
   - **PWM: Allows you to adjust the Pulse Width Modulation (PWM) Mode.**

Note

» *Menu contents will be different slightly, depending on different motherboard of users' computers.*

» *Once you are finished making your selections, choose the <Save & Exit> menu to save.*



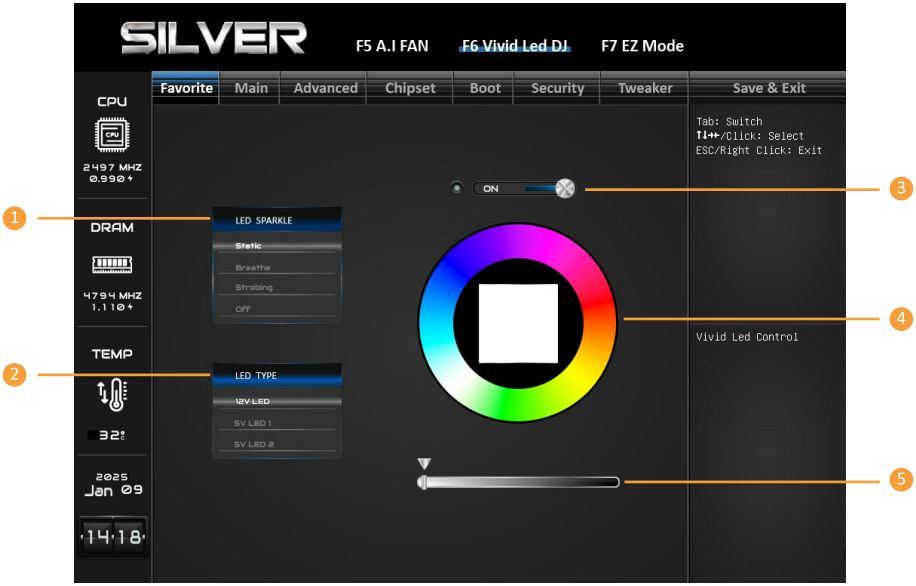
VIVID LED Control

Press <F6> to display the VIVID LED DJ Control menu.

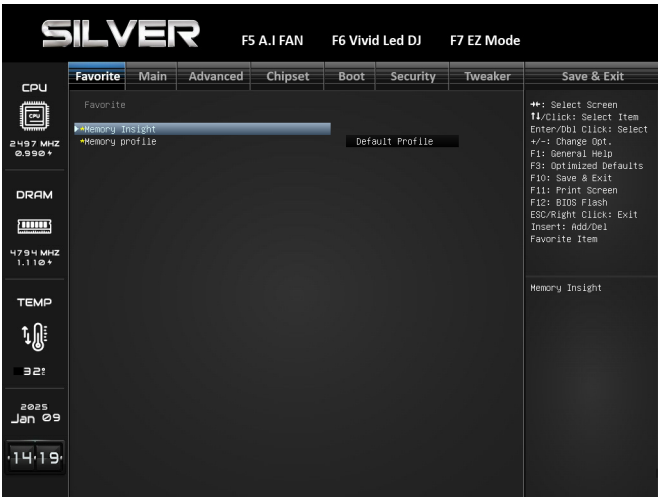
1. **LED SPARKLE:** Allows to you choose sparkle of the LEDs.
   - **Permanent: LEDs are constantly lit.**
   - **Breath: LEDs gradually flash on and off.**
   - **Shine: LEDs flash at a specific frequency.**
   - **OFF: Allows you to enable or disable VIVID LED of a single item.**
2. **LED Type:** Select the LED lighting blocks.
   - **12V LED: The 12V LED illumination. (12V_LED Device)**
   - **5V LED1: The 5V LED illumination. (5V_LED Device)**
   - **5V LED2: The 5V LED illumination. (5V_LED Device)**
3. **ON/OFF:** To enable or disable VIVID LED function.
4. **Color Palette:** Allows to you choose specific color of the LEDs.
5. **LED Brightness Bar:** Allows you to adjust the LED brightness.

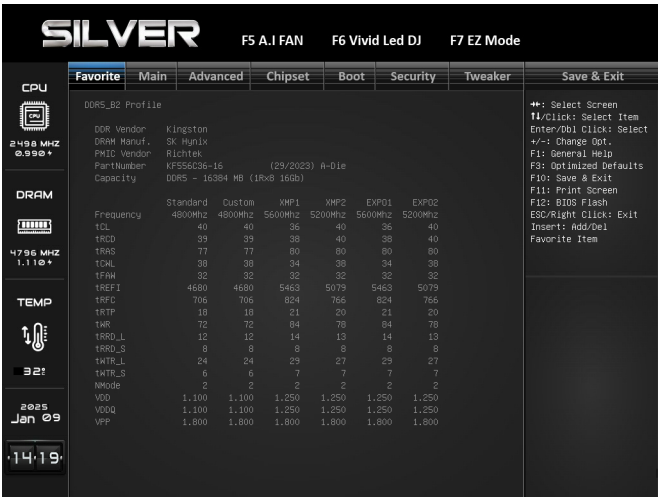
Note

» *Menu contents will be different slightly, depending on different motherboard of users' computers.*
» *Once you are finished making your selections, choose the <Save & Exit> menu to save.*



1. Favorite





Memory Insight

These items display memory information.

DDR5_B1 Profile

DDR5_B2 Profile

DDR5_A1 Profile

DDR5_A2 Profile

DDR Vender

DRAM Manuf.

PMIC Vender

DataCode

Capacity

Frequency | Standard | Custom | XMP1 | EXPO1
tCL
tRCD
tRAS
tCWL
tFAW
tREFI
tRFC
tRTP
tWR
tRRD_L
tRRD_S
tWTR_L
tWTR_S
NMode
VDD
VDDQ
VPP

Memory profile

Select DIMM timing profile. The below values start with the currently running values and don't auto populate.

Default Profile

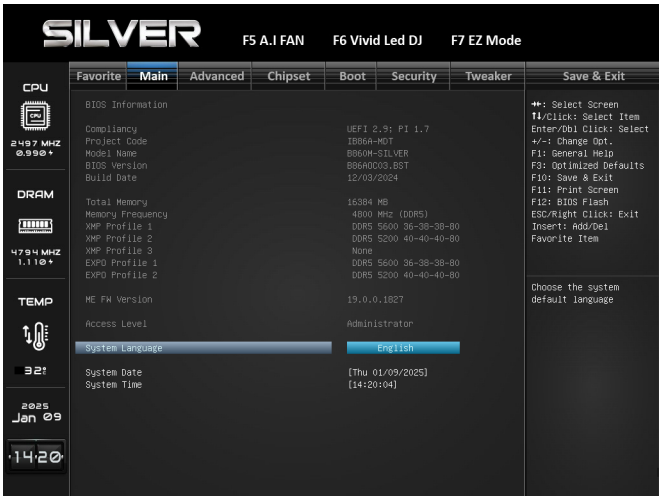
Custom Profile

XMP Profile 1

EXPO Profile 1

2. Main Menu

Once you enter AMI UEFI BIOS Setup Utility, the Main Menu will appear on the screen providing an overview of the basic system information.



2-1 BIOS Information

It shows system information including UEFI BIOS version, Project Code, Model Name, Build Date and etc.

2-2 Total Memory

Shows system memory size, VGA shard memory will be excluded.

2-3 Memory Frequency

Shows the system memory frequency.

2-4 System Language

Choose the system default language.

2-5 System Date

Set the system date. Note that the 'Day' automatically changes when you set the date.

2-6 System Time

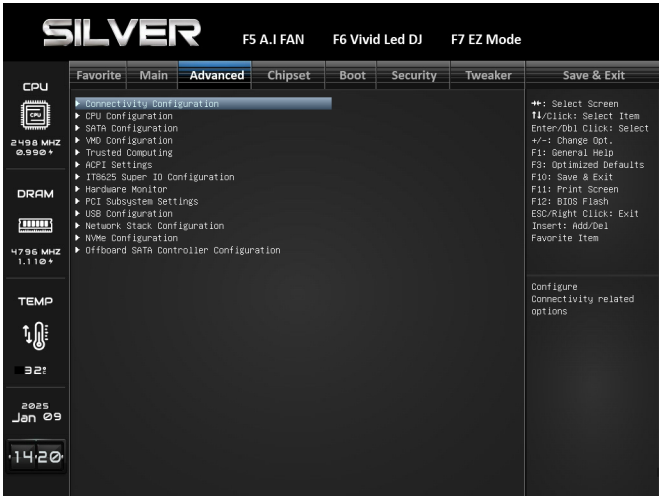
Set the system internal clock.

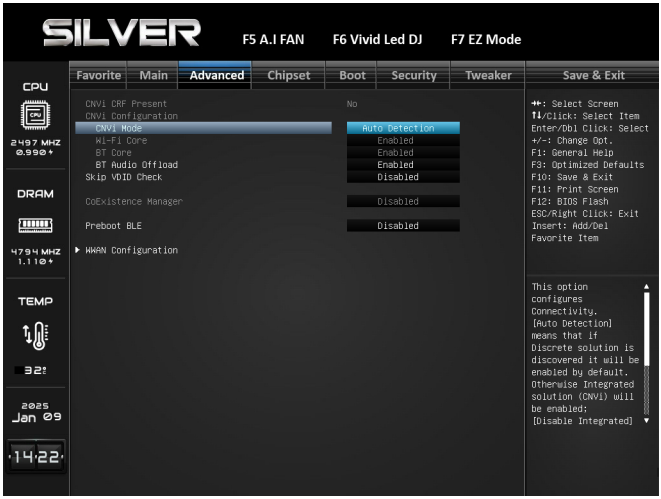
3. Advanced Menu

The Advanced Menu allows you to configure the settings of CPU, Super I/O, Power Management, and other system devices.

Note

» *Beware of that setting inappropriate values in items of this menu may cause system to malfunction.*





3-1 Connectivity Configuration

This item shows Configure Connectivity related options.

CNVi Mode

This option configures Connectivity. [Auto Detection] means that if Discrete solution is discovered it will be enabled by default. Otherwise Inegrated solution (CNVi) will be enabled; [Disable

Integrated] disables Integrated Solution.

» *Note: When CNVi is present, the GPIO pins that are used for ratio.*

Wi-Fi Core

This is an option intended to Enable/Disable Wi-Fi Core in CNVi.

BT Core

This is an option intended to Enable/Disable BT Core in CNVi.

BT Audio Offload

This is an option to Enable/Disable BT Audio Offload which enables audio input from BT device in HFP format to the audio DSP and enables power efficient audio output to BT device via A2DP format. This feature only support with Intel(R) Wireless-AX 22560.

Skip VDID Check

This is an option to Enable/Disable skip VDID Check for CNVd.

Preboot BLE

This item enables or disables Preboot Bluetooth function.

WWAN Configuration

Configure WWAN related options.

WWAN Device

Select the M.2 WWAN Device options to enable 4G - 7360/7560 (Intel), 5G - M80 (Media Tek) Modems.

Firmware Flash Device

Enable or Disable WWAN Fireware Flash Device.

Wireless CNV Config Device

Enable or Disable WCCD ACPI device node.

WWAN Reset Workaround

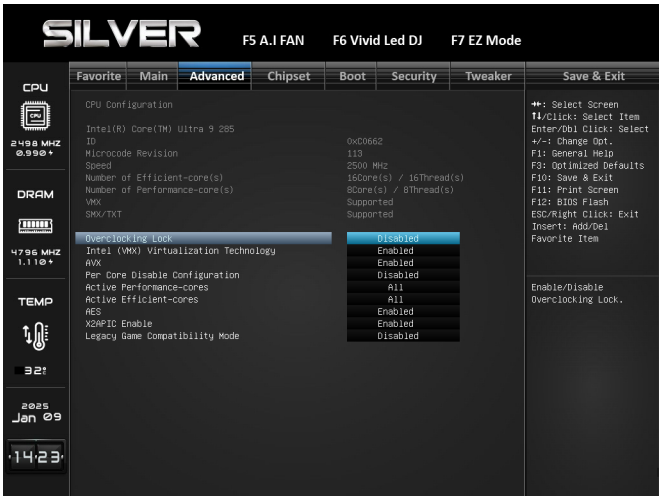
Enabling this workardound will result in BIOS asserting FULL_CARD_POWER_OFF#, PERST# and RESET#WWAN signals before the WWAN device Power-On Sequence is ececuted. Disabling it has no impact.

WA - WWAN OEM SVID

WWAN OEM Sub-Vendor ID

WA - WWAN SVID Detect Timeout

The timeout value (ms) for detecting WWAN OEM SVID. Please notice it’s workaround for OEM only.



3-2 CPU Configuration

This item shows CPU Information

Overclocking Lock

Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO (194) MSR.

Intel (VMX) Virtualization Technology

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

AVX

This item enables or disables the AVX 2/3 Instructions. This is applicable for big core only.

Per Core Disable Configuration

Enable/Disable Per Core Disable. When Per Core Disable Configuration is enabled, selection of Active Cores and Active. Efficient-cores will be disabled.

Active Performance-cores

Number of P-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.

Active Efficient-cores

Number of E-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.

AES

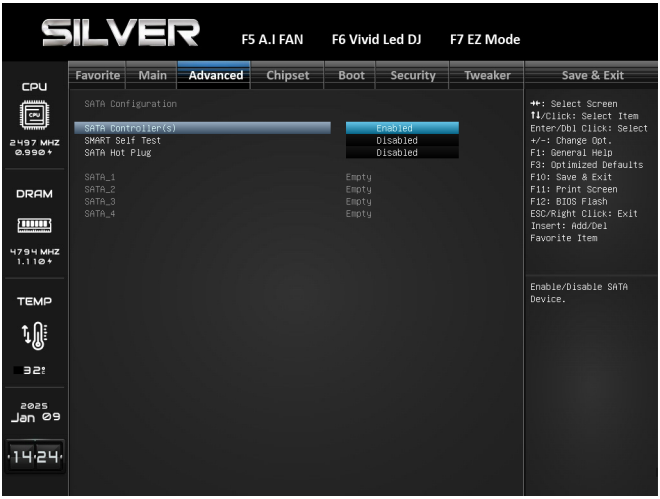
Enable/Disable AES (Advanced Encryption Standard).

X2APIC Enable

Enable/Disable X2APIC Operating Mode. When this option is configured as ‘Enabled’, ‘VT-d’ option must be ‘Enabled’ and ‘X2APIC Opt Out’ option must be ‘Disabled’ as well. This option will be grayed out when ‘VT-d’ option is configured as ‘Disabled’.

Legacy Game Compatibility Mode

When enabled, Pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when LED is off.



3-3 SATA Configuration

SATA Device Options Settings

SATA Controller(s)

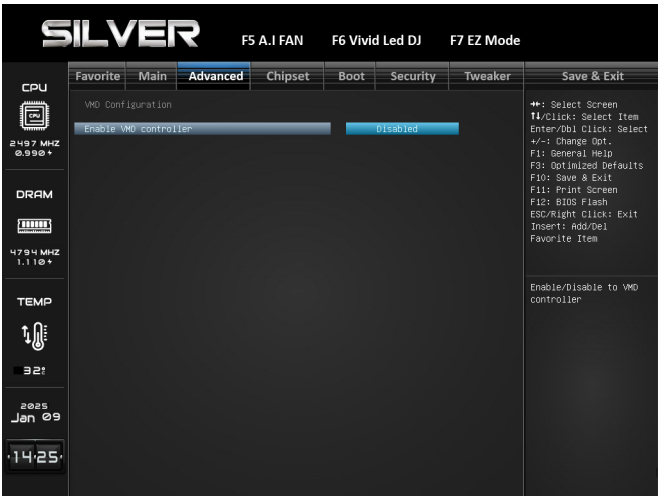
This item enables or disables Serial ATA Device.

SMART Self Test

This item runs SMART Self Test on all HDDs during POST.

SATA Hot Plug

This item Designates SATA port as Hot Pluggable.



3-4 VMD Configuration

VMD Options Settings.

Enable VMD controller

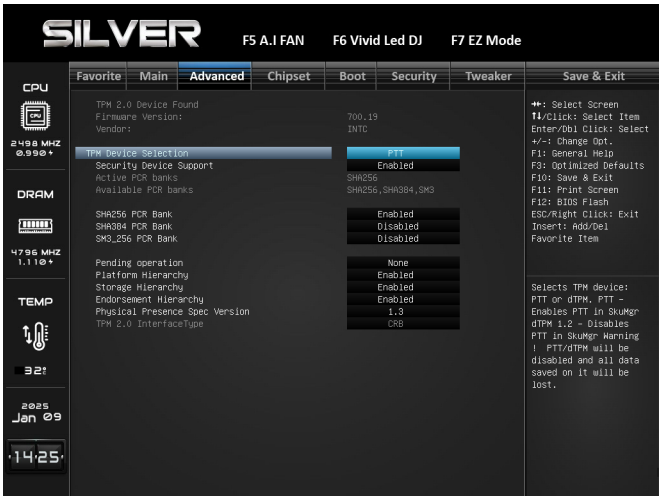
Enable/Disable to VMD controller

SATA Mode Selection

Detetmines how SATA controller(s) operate.

PCIE Storage Mode Selection

Determines how PCIE Storage operate.



3-5 Trusted Computing

Trusted Computing Settings

TPM Device Selection

This item allows you to selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT/ dTPM will be disabled and all data saved on it will be lost.

Security Device Support

This item enables or disables BIOS support for security device. O.S will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

SHA256 PCR Bank

This item enables or disables SHA256 PCR Bank.

SHA384 PCR Bank

This item enables or disables SHA384 PCR Bank.

SM3_256 PCR Bank

This item enables or disables SM3_256 PCR Bank.

Pending operation

This item schedule an operation for the security device.

» *Note: Your comuter will reboot during restart in order to change state of security device.*

Platform Hierarchy

This item enables or disables Platform Hierarchy.

Storage Hierarchy

This item enables or disables Storage Hierarchy.

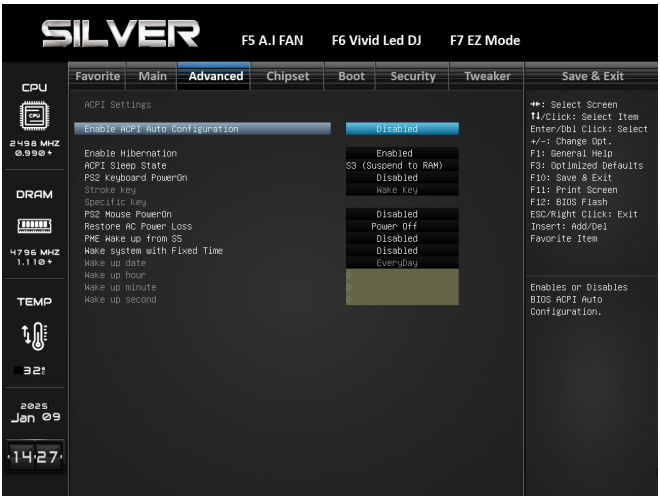
Endorsement Hierarchy

This item enables or disables Endorsement Hierarchy.

Physical Presence Spec Version

This item select to tell O.S. to support PPI Spec Version 1.2 or 1.3.

» *Note some HCK tests might not support 1.3.*



3-6 ACPI Settings

System ACPI Parameters

Enable ACPI Auto Configuration

This item enables or disables BIOS ACPI auto configuration function.

Enable Hibernation

This item enables or disables system ability to Hibernate (0S/S4 sleep state). This option may not be effective with some 0Ss.

ACPI Sleep State

This item selects the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

Restore AC Power Loss

Specify what state to go to when power is re-applied after a power failure.

PME Wake up from S5

Enables or Disables BIOS ACPI Auto Configuration.

Wake system with Fixed Time

Enable or disable System wake on alarm event. When enabled, System will wake on the hr::min::sec specified.

Wake up date

Select Wakeup date

Wake up hour

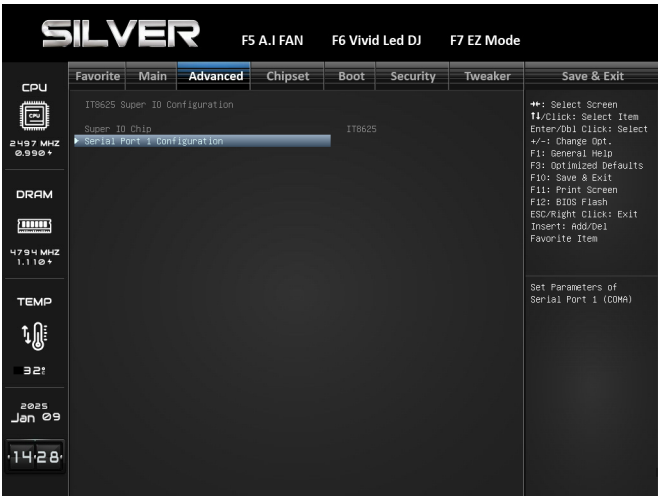
Select 0-23 For example enter 3 for 3am and 15 for 3pm.

Wake up minute

0-59

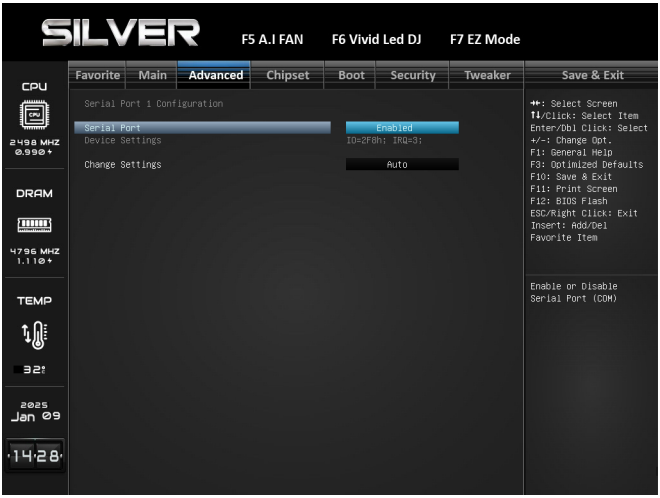
Wake up second

0-59



3-7 IT8625 Super IO Configuration

System Super IO Chip Parameters



Serial Port 1 Configuration

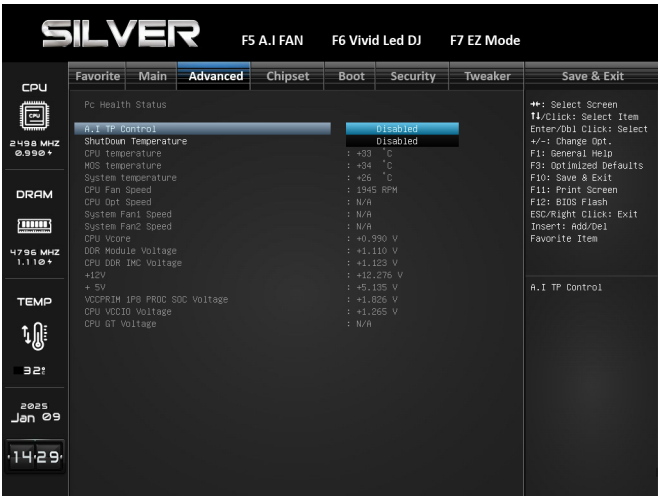
Set Parameters of Serail Port 1 (COMA).

Serial Port

This item enables or disables serial Port.

Change Settings

This item allows you to select an optimal settings for Super IO Device.



3-8 Hardware Monitor

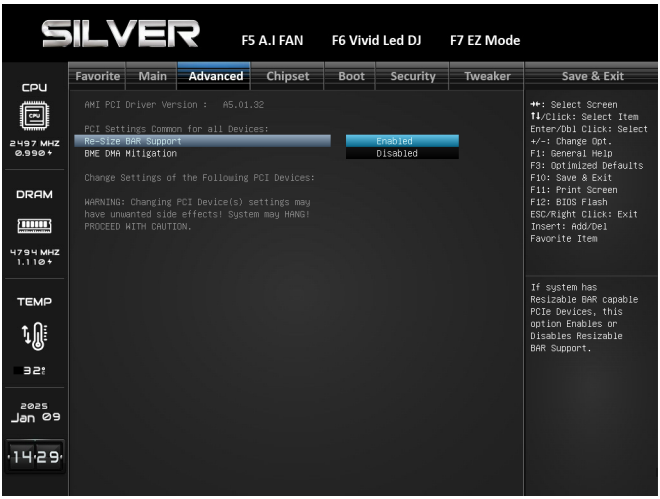
Hardware Monitor Status

A.I TP Control

This item enables or disables A.I TP Control.

Shutdown Temperature

This item allows you to set up the CPU shutdown Temperature.



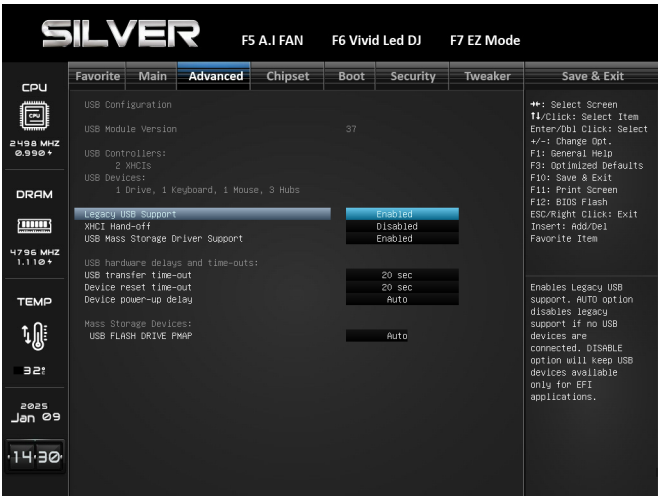
3-9 PCI Subsystem Settings

Re-Size BAR Support

If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support (Only if system supports 64 bit PCI Decoding).

BME DMA Mitigation

This item enables or disables BME DMA Mitigation. Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked.



3-10 USB Configuration

Legacy USB Support

The item allows you to enable Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.

XHCI Hand-off

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

USB Mass Storage Driver Support

The item enables or disables USB Mass Storage Driver Support.

USB transfer time-out

The time-out value for Control, Bulk, and Interrupt transfers.

Device reset time-out

The item sets USB mass storage device Start Unit command time-out.

Device power-up delay

Maximum time the device will take before it properly reports itself to the Host Controller. “Auto” uses default value: for a Root port it is 100ms, for a Hub port the delay is taken from Hub descriptor.

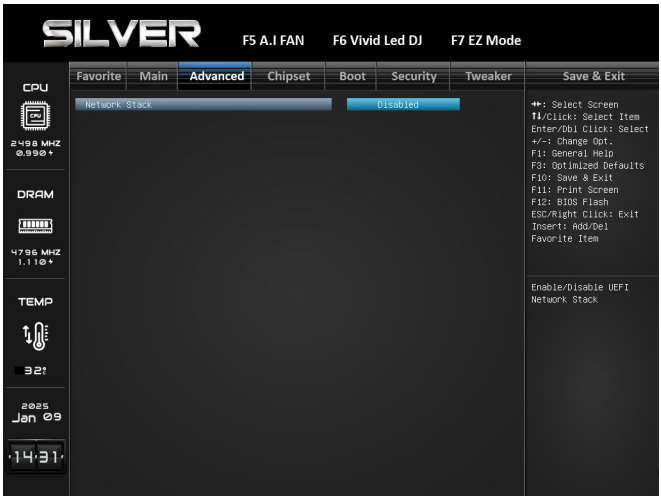
» *The following items appear only when you set the Device power-up delay function to [Manual].*

Device power-up delay in seconds

Delay range is 1 ~ 40 seconds, in one second increments.

USB FLASH DRIVE PMAP

This item Mass storage device emulation type. ‘AUTO‘ enumerates devices according to their media format. Optical drives are emulated as ‘CDROM’ , drives with no media will be emulated according to a drive type.



3-11 Network Stack Configuration

Network Stack Settings

Network Stack

This item enables or disables UEFI network stack.

» *The following items appear only when you set the Network Stack function to [Enabled]*

IPv4 PXE Support

This item enables or disables IPv4 PXE Boot Support. If disabled IPv4 PXE boot support will not be available.

IPv4 HTTP Support

This item enables or disables IPv4 HTTP Boot Support. If disabled IPV4 HTTP boot support will not be available.

IPv6 PXE Support

This item enables or disables IPv6 PXE Boot Support. If disabled IPv6 PXE boot support will not be available.

IPv6 HTTP Support

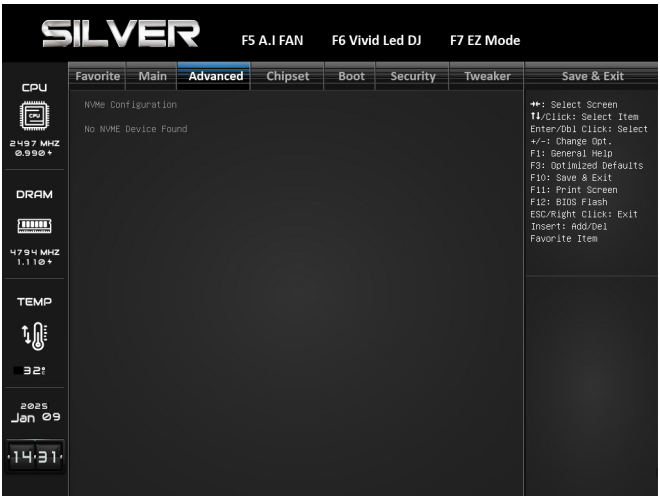
This item enables or disables IPv6 HTTP Boot Support. If disabled IPv6 HTTP boot support will not be available.

PXE boot wait time

Wait time to press ESC key to abort the PXE boot.

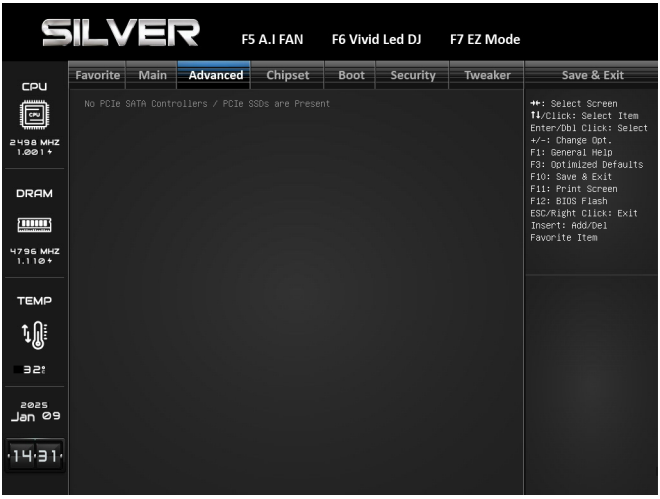
Media detect count

Number of times presence of media will be checked.



3-12 NVMe Configuration

The item shows NVMe controller and driver information.



3-13 Offboard PCIe SATA Controller

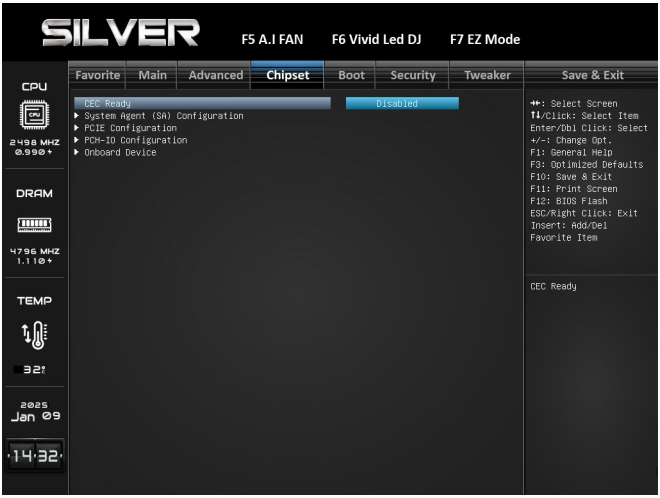
Offboard PCIe SATA Controller

4. Chipset Menu

This section describes configuring the PCI bus system. PCI, or Personal Computer Interconnect, is a system which allows I/O devices to operate at speeds nearing the speed of the CPU itself uses when communicating with its own special components.

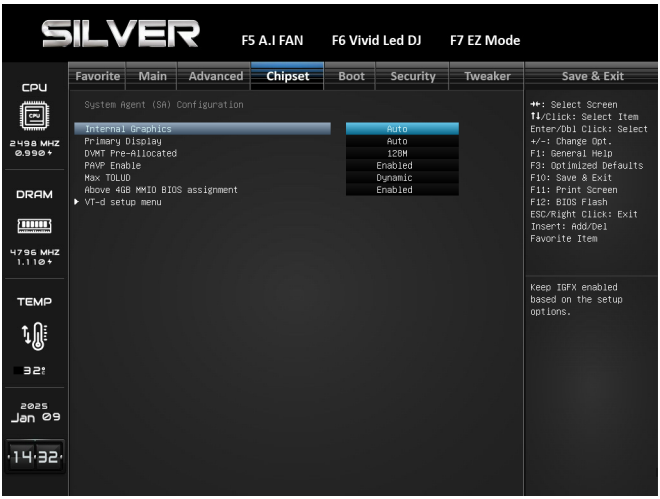
Note

» *Beware of that setting inappropriate values in items of this menu may cause system to malfunction.*



4-1 CEC Ready

CEC Ready



4-2 System Agent (SA) Configuration

System Agent (SA) Parameters

Internal Graphics

This item keeps IGFX enabled based on the setup options.

Primary Display

This item selects which of IGFX/ PEG/ PCI Graphics device should be Primary Display or select SG for Switchable Gfx.

DVMT Pre-Allocated

This item selects DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

PAVP Enable

This item enables or disables PAVP.

Max TOLUD

Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.

Above 4GB MMIO BIOS assignment

This item enables or disables above 4GB Memory Mapped IO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.

VT-d setup menu

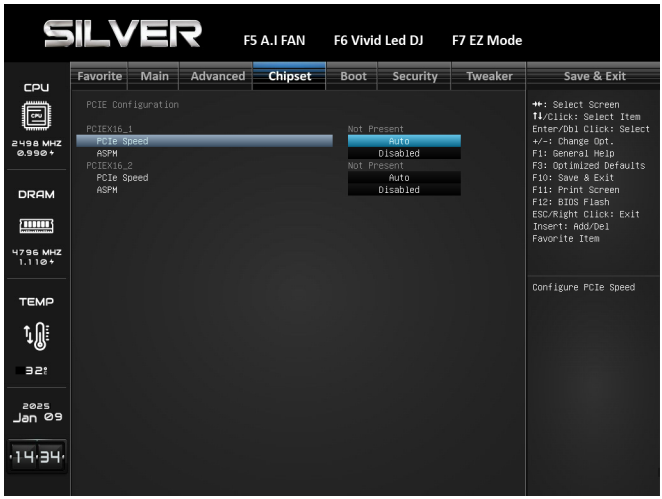
VT-d Configuration settings.

Pre-boot DMA Protection

Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

DMA Control Guarantee

Enable/Disable DMA_CONTROL_GUARANTEE bit.



4-3 PCIE Configuration

PCIE Parameters

PCIe Speed

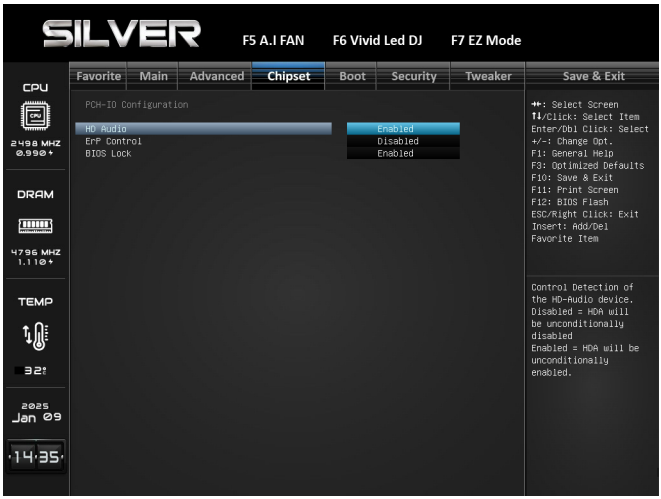
Configure PCIe Speed

ASPM

Set the ASPM Level:
Force L0s - Force all links to L0s State.
AUTO - BIOS auto configure.
DISABLE - Disables ASPM.

PCIE Bifurcation Support

Configure PCIEG4X16 Slot PCIe Lanes.



4-4 PCH-IO Configuration

PCH Parameters

PCI Express Configuration

PCI Express Configuration Settings

HD Audio

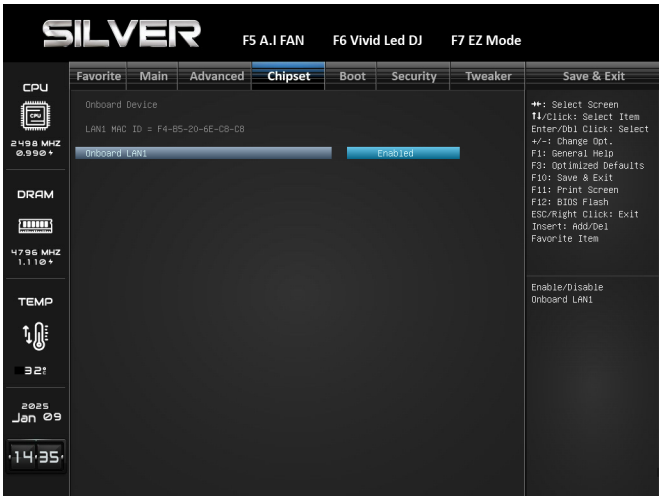
Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled. Enabled = HDA will be unconditionally enabled. Auto = HDA will be enabled if present, disabled otherwise.

ErP Control

When ErP is enabled, the system will meet ErP requirement.

BIOS Lock

This item enables or disables the PCH BIOS Lock. Required to be enabled to ensure SMM protection of flash.



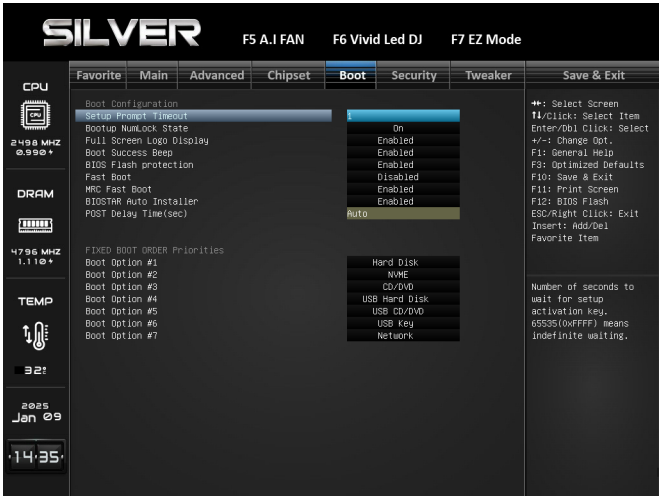
4-5 Onboard Device

Onboard LAN1

This item enables or disables Onbaord LAN1.

5. Boot Menu

This menu allows you to setup the system boot options.



5-1 Setup Prompt Timeout

This item sets number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.

5-2 Bootup NumLock State

This item selects the keyboard NumLock state.

5-3 Full Screen Logo Display

This item enables or disables Full Screen Logo Show function.

5-4 Boot Success Beep

When this item is set to Enabled, BIOS will let user know boot success with beep.

5-5 BIOS Flash protection

While enabled, it can’t flash write and flash erase by SMI.

5-6 Fast Boot

This item allows you to enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.

» *The following items appear only when you set the Fast Boot function to [Enabled]*

SATA Support

If Last Boot HDD Only, Only last boot HDD device will be available in Post. If All Sata Devices, all SATA devices, all SATA devices will be available in OS and Post.

USB Support

If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.

Network Stack Driver Support

If Disabled, Network Stack Drivers will be skipped.

Redirection Support

If Disabled, Redirection function will be disabled.

GateA20 Active

Upon Request – GA20 can be disabled using BIOS services. Always – do not allow disabling GA20; this option is useful when any RT code is executed above 1MB

Option ROM Messages

This item sets the display mode for Option ROM.

5-7 MRC Fast Boot

Enable/Disable fast path thru the MRC.

5-8 BIOSTAR Auto Installer

BIOSTAR windows Platform Auto Install.

5-9 POST Delay Time (sec)

POST Delay Time.

5-10 Fixed Boot order Priorities

Sets the system boot order.

Boot Option #1/ #2/ #3/ #4/ #5/ #6/ #7/ #8/ #9/ #10/ #11/ #12/ #13/ #14/ #15

It controls the placement of newly detected UEFI boot options.
#1 Options: UEFI Hard Disk (Default)
#2 Options: UEFI NVME (Default)
#3 Options: UEFI CD/DVD (Default)
#4 Options: UEFI USB Hard Disk (Default)
#5 Options: UEFI USB CD/DVD (Default)
#6 Options: UEFI USB Key (Default)
#7 Options: UEFI Network (Default)

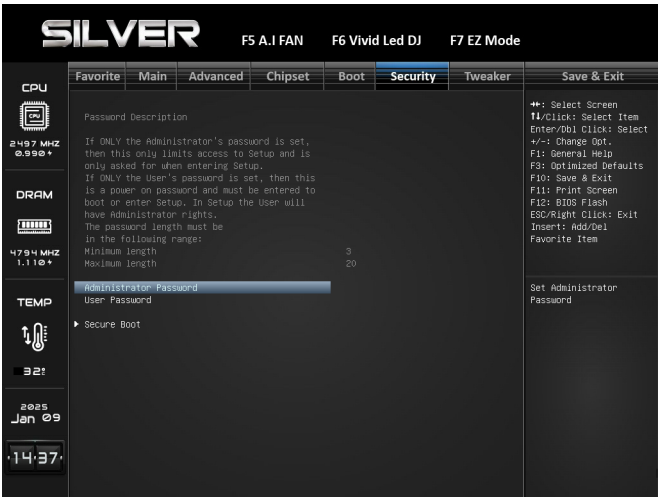
5-11 UEFI USB Key Driver BBS Priorities

Specifies the Boot Device Priority sequence from available UEFI USB Key Drives.

Boot Option #1

Sets the system boot order.

6. Security Menu



6-1 Administrator Password

This item sets Administrator Password.

6-2 User Password

This item sets User Password.

6-3 Disable Sanitize Freeze Lock

If this option is enabled, then sending Sanitize Freeze Lock command to HDDs will be skipped in next boot.

6-4 Secure Boot

Secure Boot

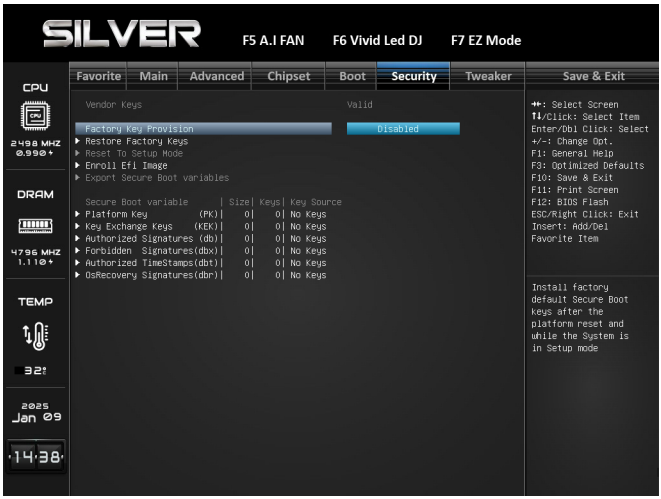
Secure Boot feature is active if secure boot is Enabled, when Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset.

Secure Boot Mode

Secure Boot mode options: Standard or Custom mode. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.

Restore Factory Keys

Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot Keys.



Expert Key Management

Enables expert users to modify Secure Boot Policy variables without variable authentication.

Factory Key Provision

Restore Factory Keys

Reset To Setup Mode

Enroll Efi Image

Export Secure Boot variables

Secure Boot variable | Size | Keys | Key Source

Platform Key (PK)

Key Exchange Keys (KEK)

Authorized Signatures (db)

Forbidden Signatures (dbx)

Authorized TimeStamps (dbt)

OsRecovery Signatures (dbr)

7. Tweaker Menu

This submenu allows you to change voltage and clock of various devices.

Note

» *We suggest you use the default setting. Changing the voltage and clock improperly may damage the device.*

» *The options and default settings might be different by RAM or CPU models.*

» *Beware of that setting inappropriate values in items of this menu may cause system to malfunction.*

- *Values in Red: Danger*
- *Values in Yellow: Warning*
- *Values in White: Normal*

7-1 Start Page

You can set the entrance page when you enter UEFI BIOS Setup.

7-2 CPU Base Clock

This item CPU Base Clock.

7-3 Spread Spectrum

This item Spread Spectrum can help reduce nosie and interference. (EMI)

7-4 CPU Ratio Mode

Setting CPU Ratio Mode.

7-5 Ring Ratio Mode

Setting Ring Ratio Mode.

7-6 NGU Ratio Mode

Setting NGU Ratio Mode.

7-7 CPU D2D Ratio

Set CPU D2D Ratio from Range 15 to 40. 0 indicates no setting.

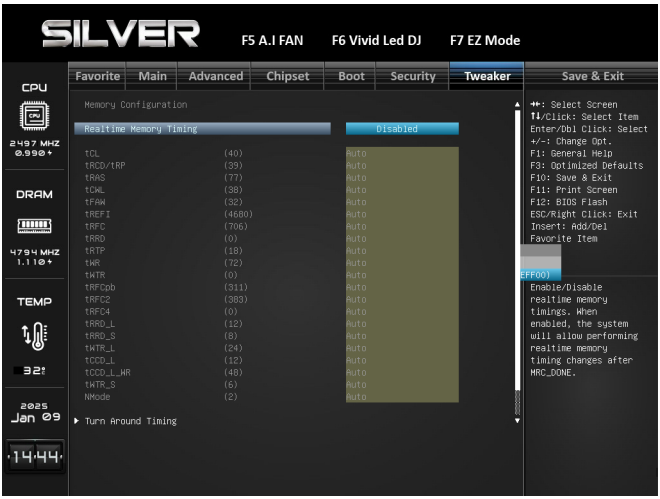
7-8 Memory Profile

Select DIMM timing profile. The below values start with the currently running values and don't auto populate.

7-9 Memory Clock : Memory Controller (Gear4)

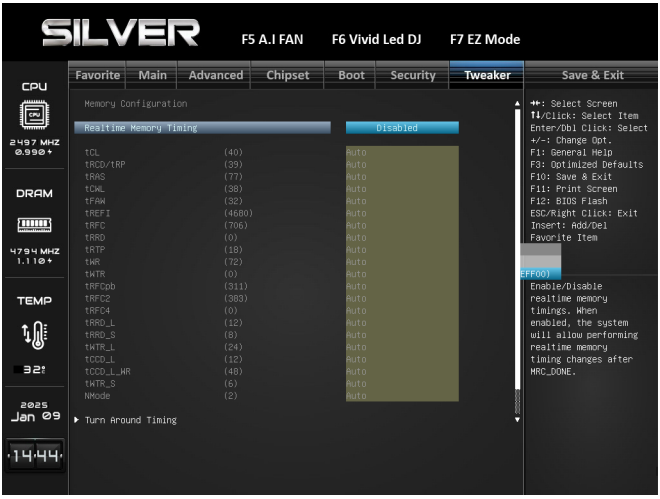
7-10 Enhanced Memory Latency

Enhanced Memory Latency.



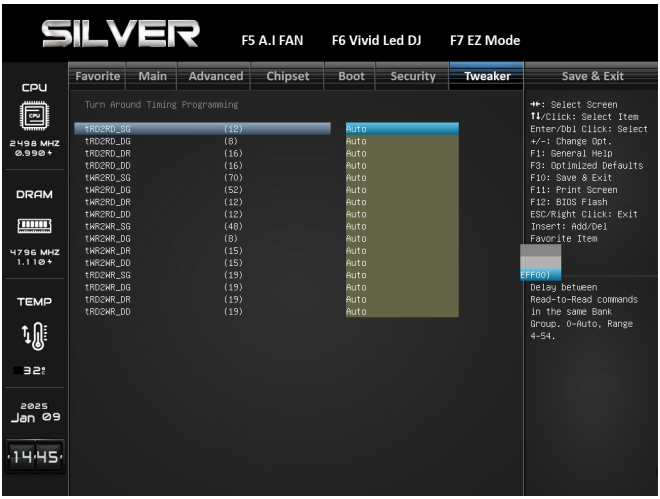
7-11 Memory Timing

Memory Timing Settings.



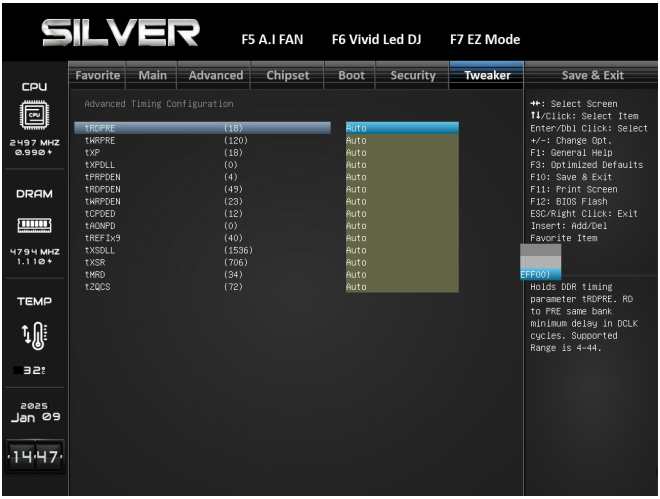
Realtime Memory Timing

Enable.Disable realtime memory timings. When enabled, the system will allow performing realtime memory timing memory timing changes after MRC_DONE.



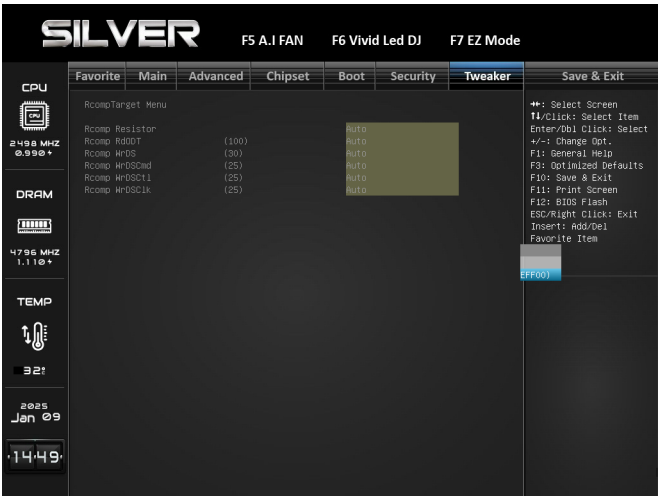
Turn Around Timing

Knobs to override default timings. 0 is no override.
Delay between Real-to-Read commands in the same Bank Group. 0-Auto, Range 4-54.



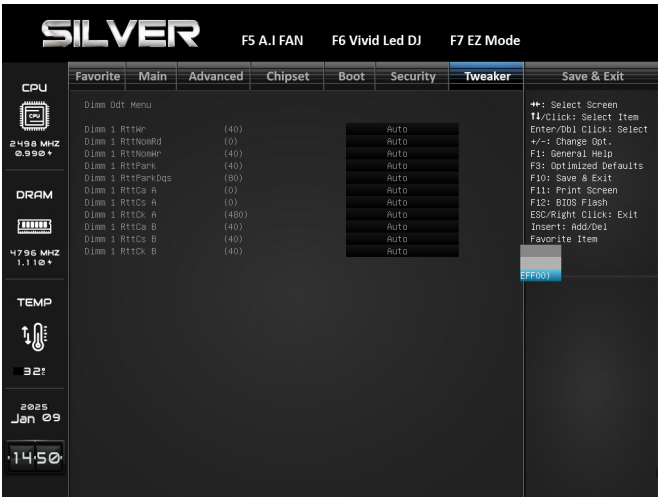
Advanced Timing Configuration

Holds DDR timing parameter tRDPRE. RD to PRE same bank minimum delay in DCLK cycles. Supported Range is 4-44.



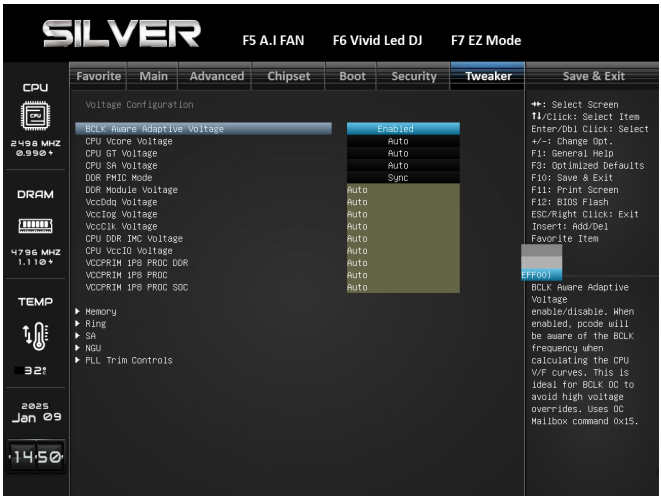
Romp Target

Romp Target Menu.



Dimm ODT

Dimm ODT Menu.



7-12 Voltage Configuration

Voltage Configuration.

BCLK Aware Adaptive Voltage

BCLK Aware Adaptive Voltage enable/disable. When enabled, code will be aware of the BCLK frequency when calculating the CPU V/F curves. This is ideal for BCLK OC to avoid hight voltage overrides. Uses OC Mailbox command ox15.

CPU Load-Line Calibration

Adjust CPU LLC function.

CPU Vcore Voltage

CPU Vcore Voltage.

CPU GT Voltage

CPU GT Voltage.

VSA Voltage

VSA Voltage.

DDR PMIC Mode

DDR PMIC Mode.

DDR Module Voltage

Memory Voltage.

VccDdq Voltage

DDR transmitter FIVR Voltage rail per technology and per data rate.

Vcclog Voltage

Data Tx PreDriver. Data receive, and analog FIVR voltage rail.

VccClk Voltage

IO Clock and clock distribution FIVR voltage rail.

CPU DDR IMC Voltage

CPU DDR IMC Voltage (1.0V ~ 1.600V). default 1.100V

CPU VccIO Voltage

CPU VccIO Voltage (1.0V ~ 1.600V). default 1.250V

VCCPRIM 1P8 PROC DDR

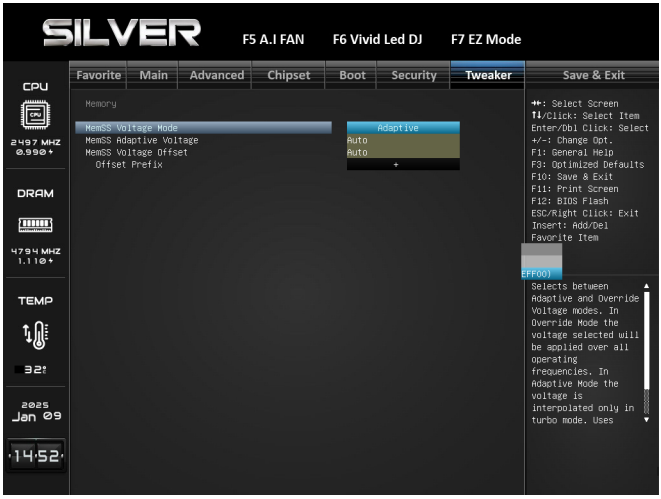
VCCPRIM 1P8 PROC DDR (1.750V ~ 2.500V) default 1.800V

VCCPRIM 1P8 PROC

VCCPRIM 1P8 PROC (1.750V ~ 2.500V) default 1.800V

VCCPRIM 1P8 PROC SOC

VCCPRIM 1P8 PROC SOC (1.750V ~ 2.500V) default 1.800V



Memory

Memory Ratio adn Voltage Settings.

MemSS Voltage Mode

Selects between Adaptive and Override Voltage modes. In Override Mode the voltage selected will be applied over all operating frequencies. In Adaptive Mode the voltage is interpolated only in turbo mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11.

MemSS Adaptive Voltage

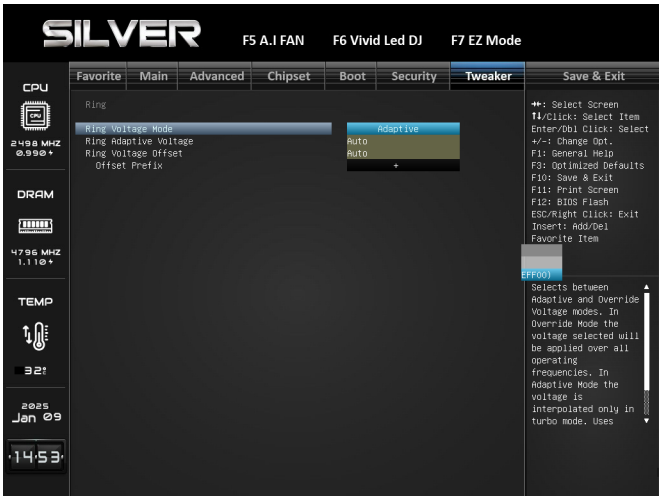
Specifies the adaptive voltage applied while memory subsystem is operating in adaptive mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11. Range 0-2000 mV.

MemSS Voltage Offset

Specifies the Offset Voltage applied to memory subsystem domain. This voltage is specified in millivolts. Range -500 to 500 mV.

Offset Prefix

Sets the offset value as positive or negative.



Ring

Ring Ratio and Voltage Settings.

Ring Voltage Mode

Selects between Adaptive and Override Voltage modes. In Override Mode the voltage selected will be applied over all operating frequencies. In Adaptive Mode the voltage is interpolated only in turbo mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11.

Ring Adaptive Voltage

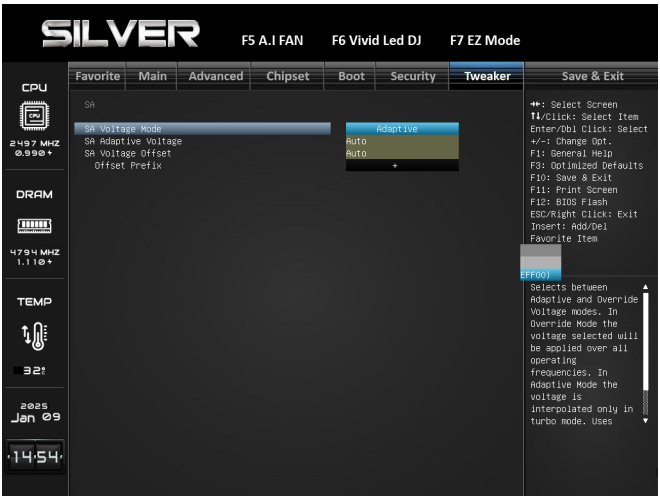
Specifies the adaptive voltage applied while memory subsystem is operating in adaptive mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11. Range 0-2000 mV.

Ring Voltage Offset

Specifies the Offset Voltage applied to memory subsystem domain. This voltage is specified in millivolts. Range -500 to 500 mV.

Offset Prefix

Sets the offset value as positive or negative.



SA

SA Overclocking Menu.

SA Voltage Mode

Selects between Adaptive and Override Voltage modes. In Override Mode the voltage selected will be applied over all operating frequencies. In Adaptive Mode the voltage is interpolated only in turbo mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11.

SA Adaptive Voltage

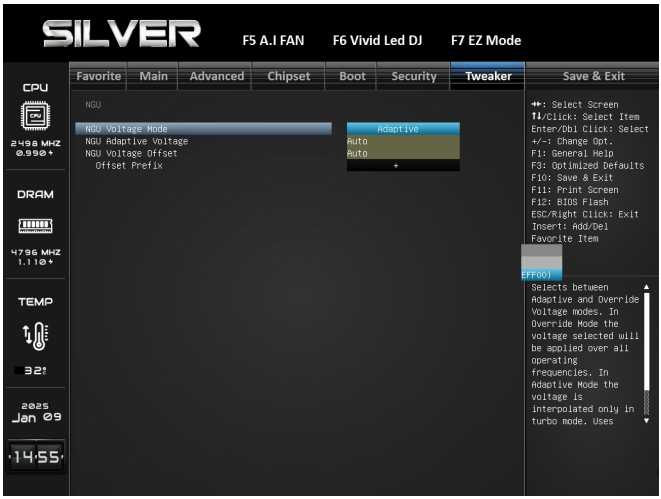
Specifies the adaptive voltage applied while memory subsystem is operating in adaptive mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11. Range 0-2000 mV.

SA Voltage Offset

Specifies the Offset Voltage applied to memory subsystem domain. This voltage is specified in millivolts. Range -500 to 500 mV.

Offset Prefix

Sets the offset value as positive or negative.



NGU

NGU Ratio and Voltage Settings.

NGU Voltage Mode

Selects between Adaptive and Override Voltage modes. In Override Mode the voltage selected will be applied over all operating frequencies. In Adaptive Mode the voltage is interpolated only in turbo mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11.

NGU Adaptive Voltage

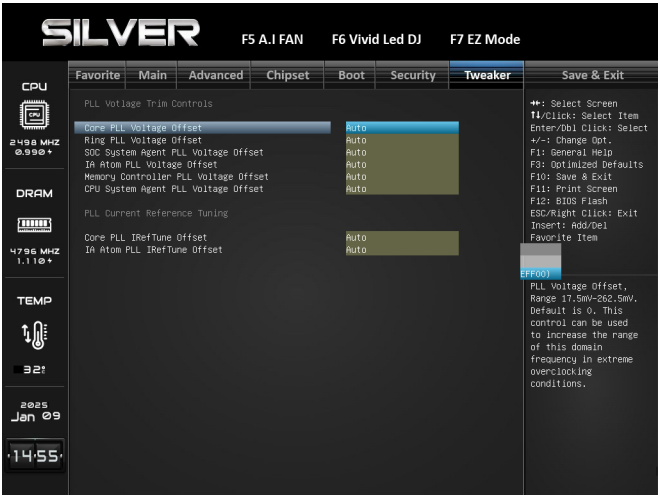
Specifies the adaptive voltage applied while memory subsystem is operating in adaptive mode. Uses Mailbox MSR 0x150, cmd 0x10, 0x11. Range 0-2000 mV.

NGU Voltage Offset

Specifies the Offset Voltage applied to memory subsystem domain. This voltage is specified in millivolts. Range -500 to 500 mV.

Offset Prefix

Sets the offset value as positive or negative.



PLL Trim Controls

PLL Trim Controls Menu.

Core PLL Voltage Offset

PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

Ring PLL Voltage Offset

PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

SOC System Agent PLL Voltage Offset

PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

IA Atom PLL Voltage Offset

PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

Memory COntroller PLL Voltage Offset

PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

CPU System Agent PLL Voltage Offset

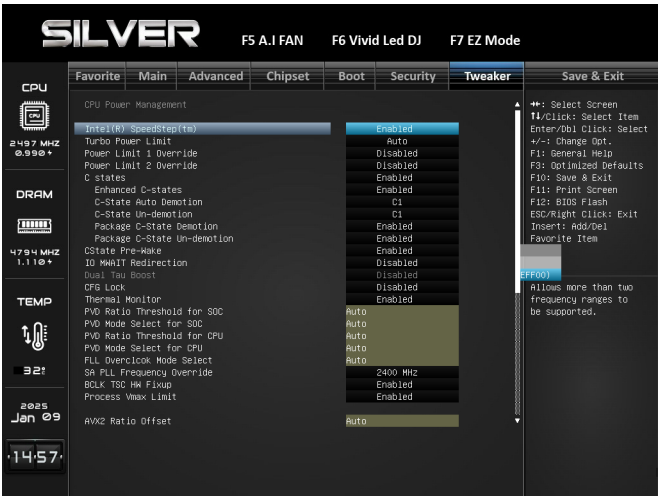
PLL Valtage offset, Range 17.5mV ~ 262.5mV. Default is 0. This control can be used to increase the range of this domain frequency in extreme overclocking conditions.

Core PLL IRef Tune Offset

PLL Current Reference Tuning Offset, Range 0-15. Default is 0. The value provided in this field is added to the PLL fuse. The value after adding offset cannot exceed 0xF, it is does, FW clips the vlaue to 0xF before writing back the value to fuse.

IA Atom PLL IRef Tune Offset

PLL Current Reference Tuning Offset, Range 0-15. Default is 0. The value provided in this field is added to the PLL fuse. The value after adding offset cannot exceed 0xF, it is does, FW clips the vlaue to 0xF before writing back the value to fuse.



7-13 CPU Power Management

Intel(R) SpeedStep(tm)

This item allows more than two frequency ranges to be supported.

Turbo Power Limit

Turbo Power Limit

Power Limit 1 Override

This item enables or disables Power Limit 1 Override. If this option is disabled,BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.

» *The following items appear only when you set the Power Limit 1 Override function to [Enabled]*

Power Limit 1

This item Power Limit 1 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500.

Power Limit 2 Override

This item enables or disables Power Limit 2 Override. If this option is disabled, BIOS will program the default values for Power Limit 2.

» *The following items appear only when you set the Power Limit 2 Override function to [Enabled]*

Power Limit 2

This item Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.

C states

This item enables or disables CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.

Enhanced C-states

This item enables or disables C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.

C-States Auto Demotion
This item sets C-State Auto Demotion.

C-States Un-demotion
This item sets C-State Un-demotion.

Package C-State Demotion
This item sets Package C state Demotion.

Package C-State Un-demotion
This item sets Package C-State Un-demotion.

CState Pre-Wake

Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake.

IO MWAIT Redirection

This item allows you to set IO MWAIT Redirection. When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+0 ffset to MWAIT (offset)

CFG Lock

This item confgire MSR 0xE2[15], CFG lock bit.

Thermal Monitor

This item enables or disables Thermal Monitor.

PVD Ratio Threshold for SOC

Select PVD Ratio Threshold Value from Range 1 to 63. 0 - Static PVD ratio specified by PvdMode for SOC.

PVD Mode Select for SOC

Select PVD Mode Value from Range 1 to 3.
0x0 = div-1 (VCO = Output clock), 0x1 = div-2 (VCO = 2x Output clock), 0x2 = div-4 (VCO = 4x Output Clock), 0x3 = div-8 (VCO = 8x Output clock)

PVD Ratio Threshold for CPU

Select PVD Ratio Threshold Value from Range 1 to 63. 0 - Static PVD ratio sprcofoed by PvdMode for CPU.

PVD Mode Select for CPU

Select PVD Mode Value from Range 1 to 3.
0x0 = div-1 (VCO = Output clock), 0x1 = div-2 (VCO = 2x Output clock), 0x2 = div-4 (VCO = 4x Output Clock), 0x3 = div-8 (VCO = 8x Output clock)

FLL Overclock Mode Select

Select FLL Mode Value from Range 1 to 3. 0x0 = no overclocking, 0x1 = ratio overclocking with nominal (0.5-1x) reference clock frequency, 0x2 = BCLK overclocking with elevated (1-3x) reference clock frequency, 0x3 = BCLK overclocking with extreme elevated (3-5x) reference clock frequency and ratio limited to 63.

SA PLL Frequency Override

Configure Sa PLL Frequency.

BCLK TSC HW Fixup

BCLK TSC HW Fixup disable during TSC copy from PMA to APIC.

Process Vmax Limit

Disabling the Vmax limit Setting will allow user to set any voltage. But disabling the voltage limit

checks may cause permanent damage to processor. Disaling limit check will persist until next cold boot.

AVX2 Ratio Offset

This item AVX2 Ratio Offset. Specifies number of bins to decrease AVX ratio vs. Core Ratio. AVX is a more stressful workload, it is helpful to lower the AVX ratio to ensure maximum possible ratio for SSE workloads.

AVX2 Voltage Guardband Scale Factor

AVX2 Voltage Guardband Scale Factor. Controls the voltage guardband applied to AVX workloads. Range 0 - 200 in 1/100 units, where 125 = 1.25 scale factor. A default value of 100 applies the default voltage guardband scale factor of 1.0. A value > 100 will increase the votlage guardband, and < 100 will decrease the voltage guardband.

TjMax Offset

This item TjMax Offset. Specified value here is clipped by pCode to support TjMax in the range of 62 to 115 deg Celsius.

TVB Voltage Optimizations

This service controls thermal based voltage optimizations for processors that implement the Intel Thermal Velocity Boost (TVB) feature. Uses Overclocking Mailbox command 0x18/ 0x19

TVB Tatio Clipping

> his service controls Core frequency reduction caused by high package temperatures for processors that implement the Intel Thermal Velocity Boost (TVB) feature. Uses Overclocking Mailbox command 0x18/0x19.

OC TVB

> This control will allow user to modify and program new parameters for temperature thresholds T0, T1 and delta DownBins for temp thresholds T0 and T1

Core VR Fast Vmode

Core VR Fast Vmode. Use to control Core Fast Vmode Enable/Disable.

VR Fast Vmode ICC Limit

Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.

VR Fast Vmode Offset

Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep at the default setting.

GT VR Fast Vmod

GT VR Fast Vmode. Use to control GT Fast Vmode Enable/Disable.

VR Fast Vmode ICC Limit

Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.

VR Fast Vmode Offset

Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep

at the default setting.

SA VR Fast Vmode

SA VR Fast Vmode. Use to control SA Fast Vmode Enable/Disable.

VR Fast Vmode ICC Limit

Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.

VR Fast Vmode Offset

Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep at the default setting.

CEP Enable

Enable/Disable CEP (Current Excursion Protection) Support.

IA AC Loadine

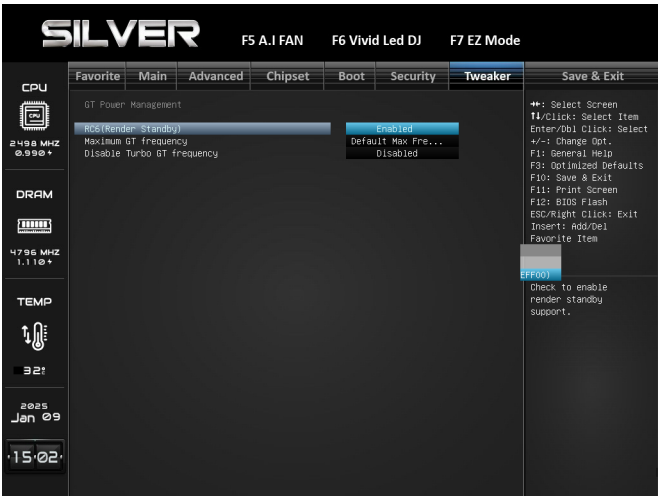
AC Loadline defined in mOhms.

IA DC Loadine

DC Loadline defined in mOhms.

VR IccMax

Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time.



7-14 GT Power Management

RC6 (Render Standby)

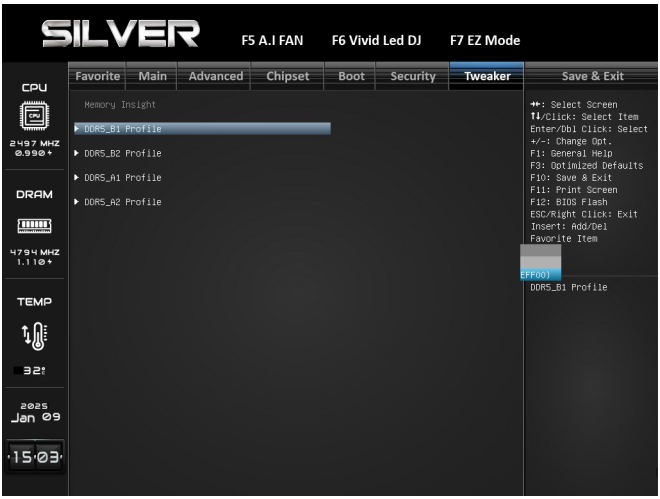
This item enables or disables Render Standby.

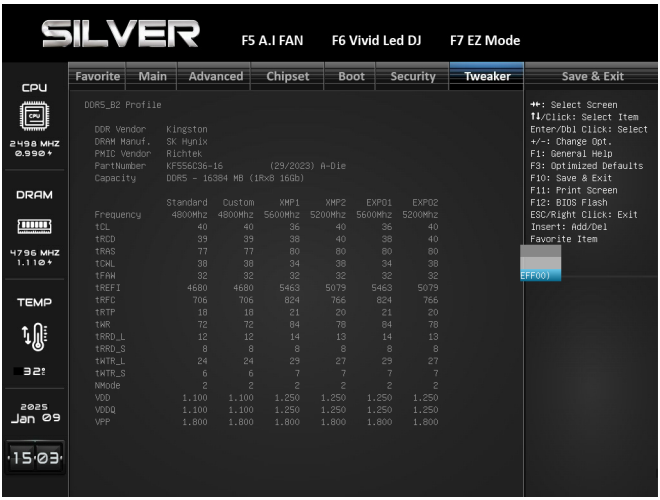
Maximum GT frequency

This item maximum GT frequency limited by te user. Value beyond the range will be clipped to min/max supported by SKU.

Disable Turbo GT frequency

This item Disable Turbo GT frequency. Enabled: Disables Turbo GT frequency. Disabled: GT frequency is no limited.





7-15 Memory Insight

Memory Insight

These items display memory information.
DDR5_B1 Profile
DDR5_B2 Profile
DDR5_A1 Profile
DDR5_A2 Profile

DDR Vender
DRAM Manuf.
PMIC Vender
DataCode

Capacity

Frequency | Standard | Custom | XMP1 | EXPO1
tCL
tRCD
tRAS
tCWL
tFAW
tREFI
tRFC
tRTP
tWR
tRRD_L
tRRD_S
tWTR_L
tWTR_S
NMode
VDD
VDDQ
VPP

Memory profile

Select DIMM timing profile. The below values start with the currently running values and don't auto populate.

Default Profile

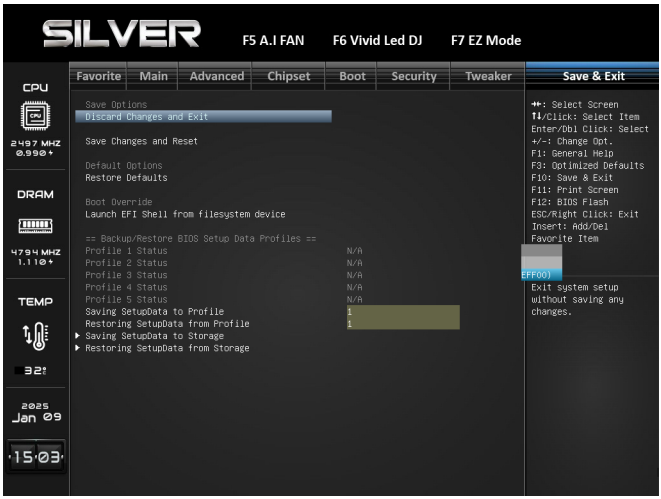
Custom Profile

XMP Profile 1

EXPO Profile 1

8. Save & Exit Menu

This menu allows you to load the optimal default settings, and save or discard the changes to the BIOS items.



8-1 Discard Changes and Exit

Abandon all changes made during the current session and exit setup.

8-2 Save Changes and Reset

Reset the system after saving the changes.

8-3 Restore Defaults

Restore/Load Default values for all the setup options.

8-4 UEFI: USB FLASH DRIVE PMAP, Partition 4 (USB FLASH DRIVE PMAP)

8-5 Launch EFI Shell from filesystem device

Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

8-6 Saving SetupData to Profile

Saving SetupData to Profile.

8-7 Restoring SetupData from Profile

Restoring SetupData from Profile.

8-8 Saving SetupData to Storage

Saving SetupData to Storage.

8-9 Restoring SetupData from Storage

Saving SetupData to Storage.