BIOS User Guide

B760M-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

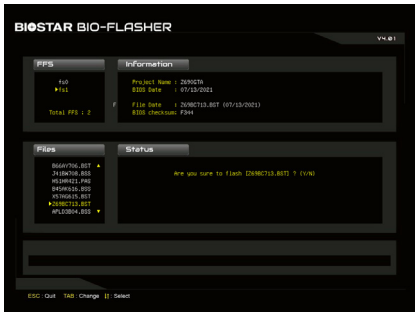
Note

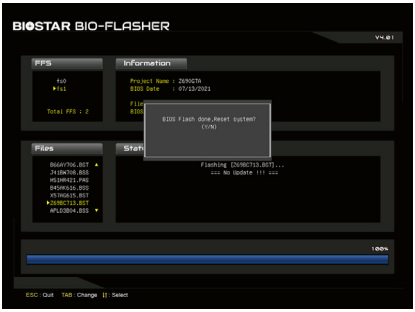
» *This utility only allows storage device with FAT32/16 format and single partition.*
» *Shutting down or resetting the system while updating the BIOS will lead to system boot failure.*

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.

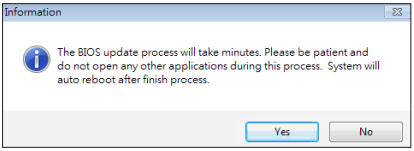
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes and Reset> to restart the computer. Then the BIOS Update is completed.

BIOS Update Utility (through the Internet)

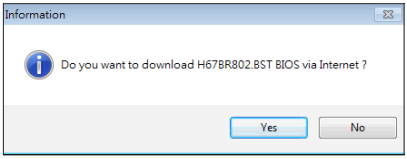
1. Installing BIOS Update Utility from the DVD Driver.
2. Please make sure the system is connected to the internet before using this function.

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

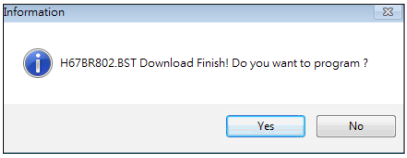
4. An open dialog will show up to request your agreement to start the BIOS update. Click “Yes” to start the online update procedure.



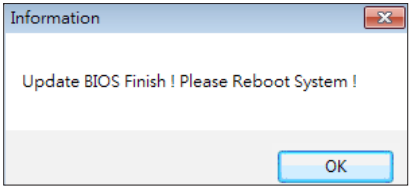
5. If there is a new BIOS version, the utility will ask you to download it. Click “Yes” to proceed.



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.

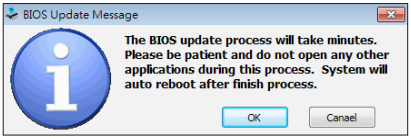
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes> and <Reset> to restart the computer. Then, the BIOS Update is completed.

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/

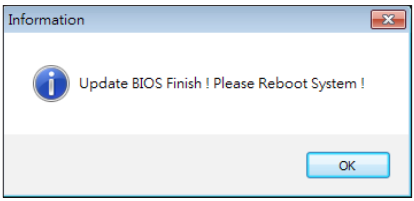
3. Launch BIOS Update Utility and click the “Update BIOS” button on the main screen.

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.

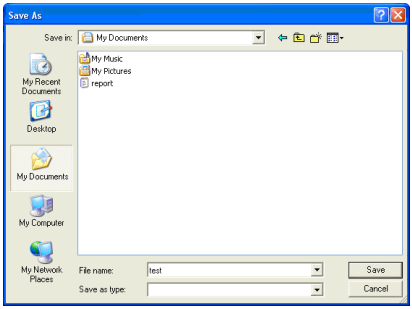


7. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.

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.*

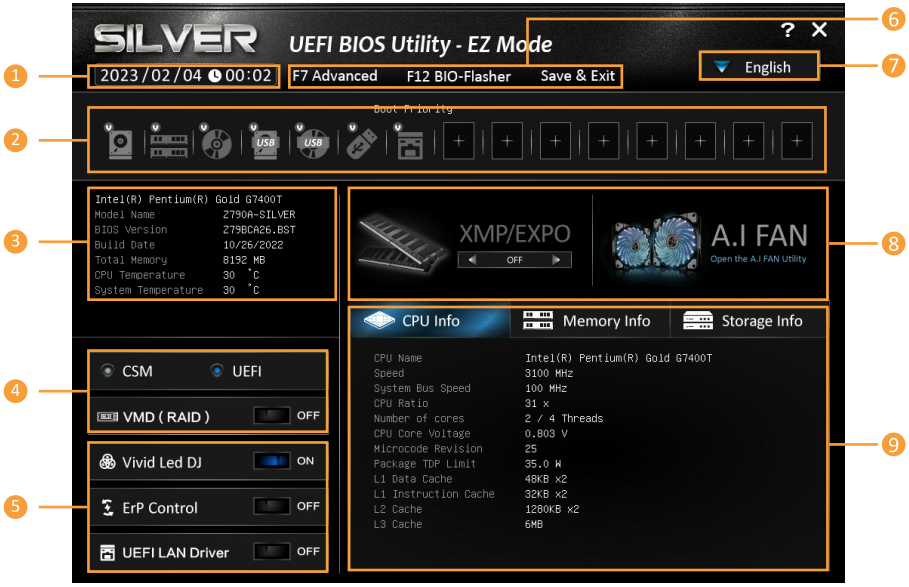
EZ Mode

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. **Boot Priority Bar:** you can move the device icons to change the boot priority.
3. **Hardware Information:** Shows the CPU/ MB temperature, memory size, BIOS version and build date.
4. **AHCI/ RAID/ CSM/ UEFI Function Settings Buttons:** Click on this button to sets the AHCI/ RAID, CSM/ UEFI.
5. **Vivid Led DJ/ Erp Control/ UEFI LAN Driver Switch:** This item enable or disable the UEFI LAN Driver, ErP Control, Vivid Led DJ.
6. **Setup Function Keys:** This item allows you to sets Save & Exit. Press F7/ F12 key to switch between Advanced mode and BIO-Flasher.
7. **Language Settings:** This item allows you to change language.
8. **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.
9. **CPU/ Memory/ Storage Information:** This item display CPU/ Memory/ Storage information.

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/ System3/ MOS FAN:** Click button to set the status value of CPU FAN, SYSTEM FAN and MOS FAN.
2. **PWM/ Temperature Panel:** According to the fan PWM value corresponding to CPU and system temperature to adjust the fan speed.

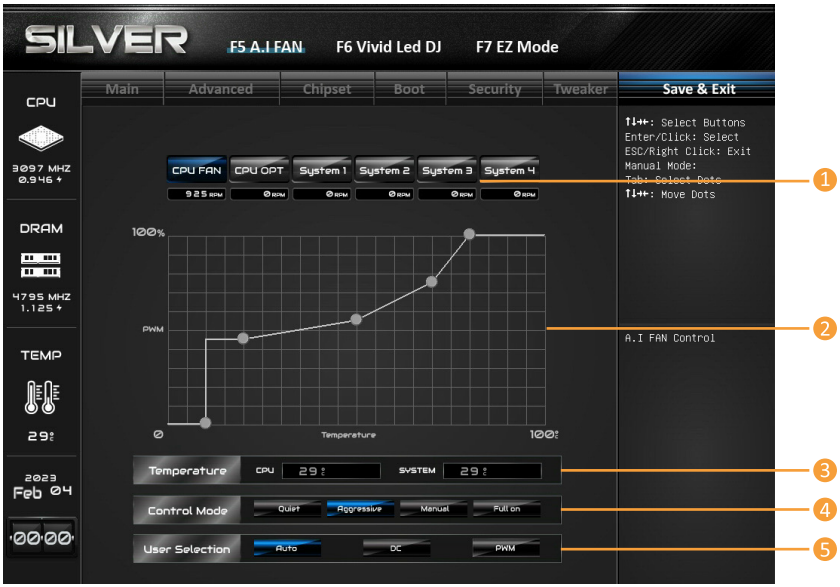
» *Allows you to adjust according to your preferences.*

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 COLOR:**
   - **Auto: LEDs will Automatically change the Color Palette and LED Brightness.**

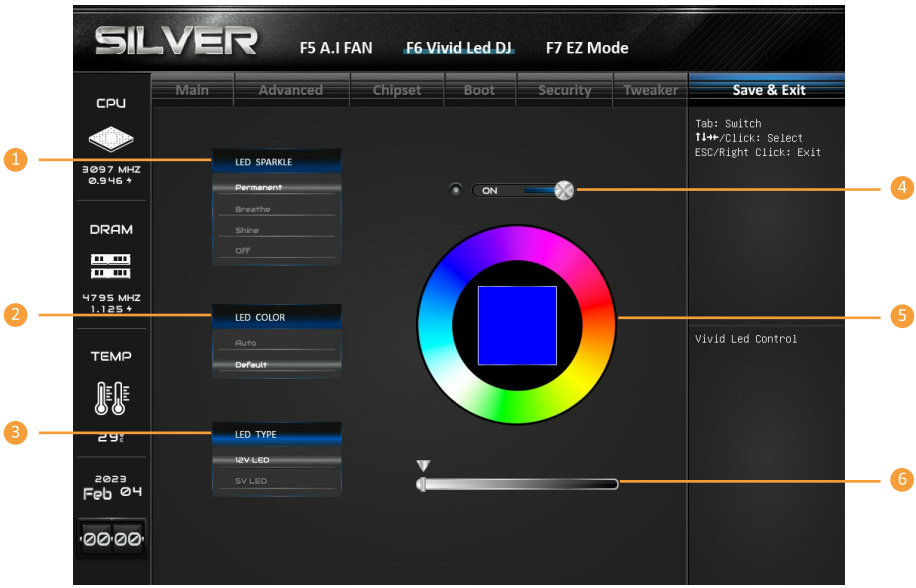
» *If you select Auto mode, the Color Pallette and LED Brightness Bar will disabled.*

   - **Default: All the setting are back to default.**
3. **LED Type:** Select the LED lighting blocks.
   - **SYSTEM: System LED illuminations. (ARMOR GEAR LED)**
   - **12V LED: The 12V LED illumination. (12V_LED Device)**
   - **5V LED: The 5V LED illumination. (5V_LED Device)**
4. **ON/OFF:** To enable or disable VIVID LED function.
5. **Color Palette:** Allows to you choose specific color of the LEDs.
6. **LED Brightness Bar:** Allows you to adjust the LED brightness.

Note

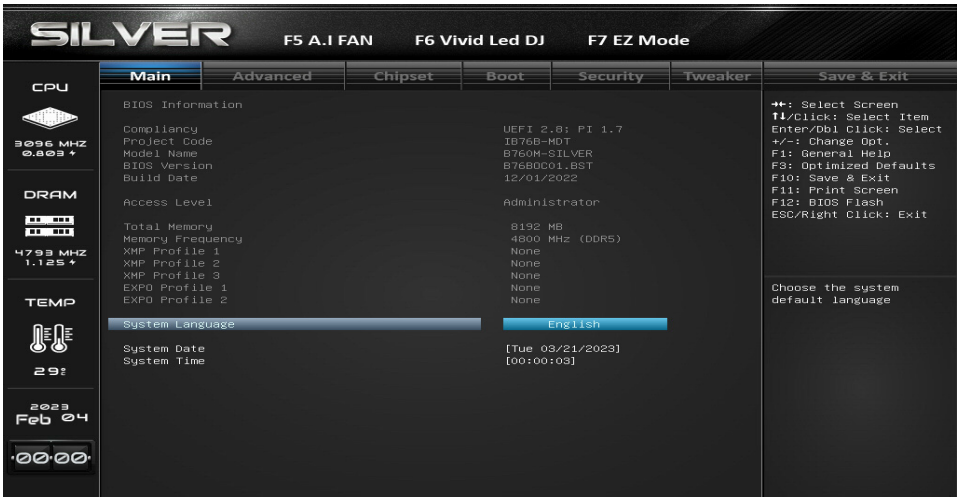
» *Menu contents will be different slightly, depending on different motherboard of users' computers.*

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



1. 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.



1-1 BIOS Information

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

1-2 Total Memory

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

1-3 Memory Frequency

Shows the system memory frequency.

1-4 System Language

Choose the system default language.

1-5 System Date

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

1-6 System Time

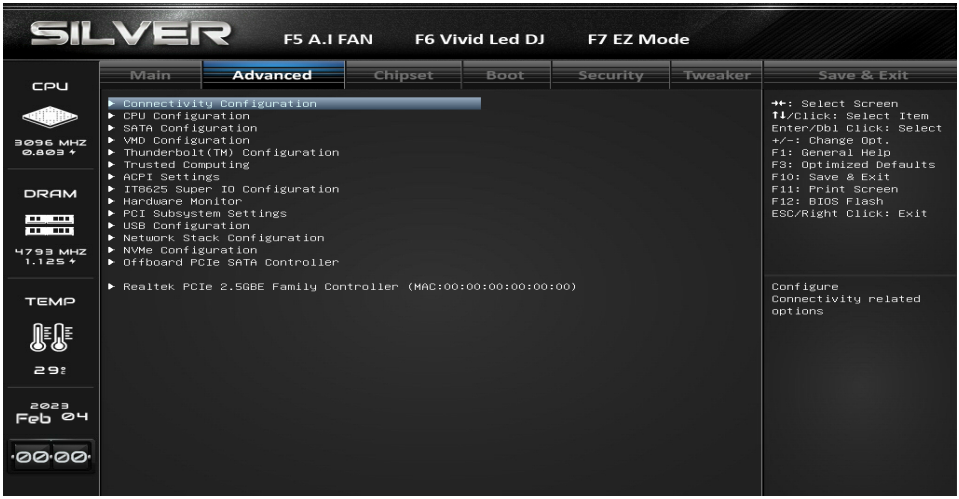
Set the system internal clock.

2. 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.*



2-1 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.

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

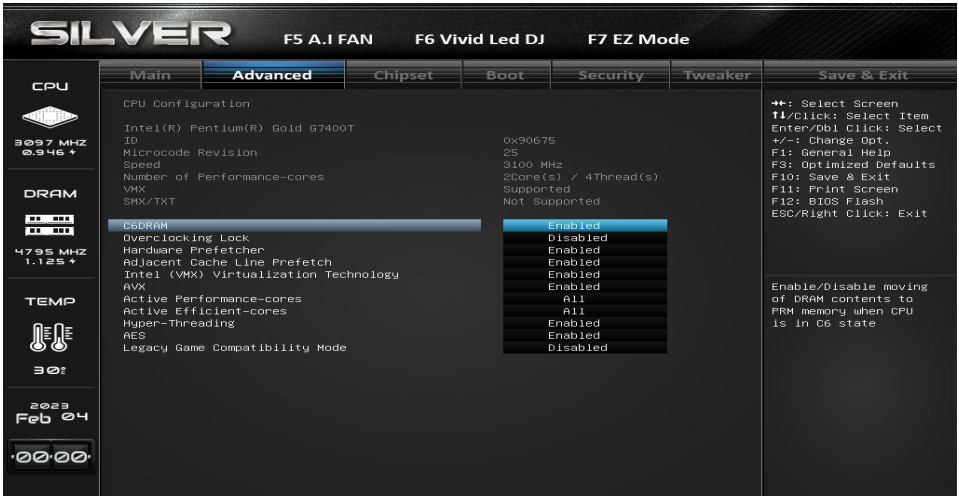
WWAN OEM Sub-Vendor ID

WA - WWAN SVID Detect Timeout

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

2-2 CPU Configuration

This item shows CPU Information



Overclocking Lock

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

Hardware Prefetcher

To turn on/off the MLC streamer prefetcher.

Adjacent Cache Line Prefetch

To turn on/off prefetching of adjacent cache lines.

Intel (VMX) Virtualization Technology

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

Hyper-Threading

Enable or Disable Hyper-Threading Technology.

AES

Enable/Disable AES (Advanced Encryption Standard).

2-3 SATA Configuration

The BIOS will automatically detect the presence of SATA devices. There is a sub-menu for each SATA device. Select a device and press <Enter> to enter the sub-menu for detailed options.

SATA Controller(s)

Enable/Disable SATA Device

SMART Self Test

Run SMART Self Test on all HDDs during POST.

SATA Hot Plug

Designates SATA port as Hot Pluggable.

SATA Test Mode

Test Mode Enable/Disable (Loop Back)

Aggressive LPM Support

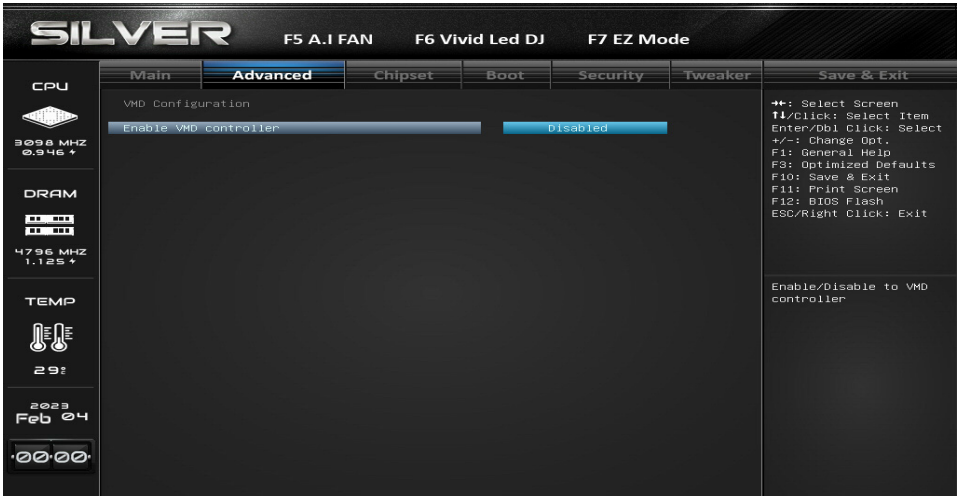
Enable PCH to aggressively enter link power state.

Hybrid Storage Detection and Configuration Mode

Select Hybrid Storage Detection and Configuration Mode.

2-4 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.

2-5 Trusted Computing

Trusted Computing Settings.

TPM Device Selection

Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning! PTT/dTPM will be disabled and all data saved on it will be lost.

Security Device Support

Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Active PCR banks

Available PCR banks

SHA256 PCR Bank

Enable or Disable SHA256 PCR Bank

SHA384 PCR Bank

Enable or Disable SHA384 PCR Bank

SM3_256 PCR Bank

Enable or Disable SM3_256 PCR Bank

Pending operation

Schedule an Operation for the Security Device.

» *Note: Your Computer will reboot during restart in order to change State of the Device.*

Platform Hierarchy

Enable or Disable Platform Hierarchy

Storage Hierarchy

Enable or Disable Storage Hierarchy

Endorsement Hierarchy

Enable or Disable Endorsement Hierarchy

TPM 2.0 UEFI Spec Version

Select the TCG2 Spec Version Support, TCG_1_2: the Compatible mode for Win8/Win10. TCG_2: Support new TCG2 protocol and event format for Win10 or later.

Physical Presence Spec Version

Sekect to Tell O.S. to support PPI Spec Version 1.2 or 1.3.

» *Note: Some HCK tests might not support 1.3.*

TPM 2.0 InterfaceType

Select the Communication Interface to TPM 20 Device.

Pending operation

Schedule an Operation for the Security Device.

» *Note: Your Computer will reboot during restart in order to change State of the Device.*

Security Device Support

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.

TCM State

Enable/Disable Security Device.

» *Note: Your Computer will reboot during restart in order to change State of the Device.*

2-6 ACPI Settings

System ACPI Parameters.

Enable ACPI Auto Configuration

Enables or Disables BIOS ACPI Auto Configuration.

Enable Hibernation

Enables or Disables System ability to Hibernate (OS/S4 Sleep State). THis option may not be effective with some OSs.

ACPI Sleep State

Select the hightest 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

Enable system to wake from S5 using PME event.

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

2-7 IT8625 Super IO Configuration

System Super IO Parameters.

Super IO Chip

System Super IO Chip Parameters.

Serial Port 1 Configuration

Set Parameters of Serial Port 1 (COMA)

Serial Port

Enable or Disable Serial Port (COM)

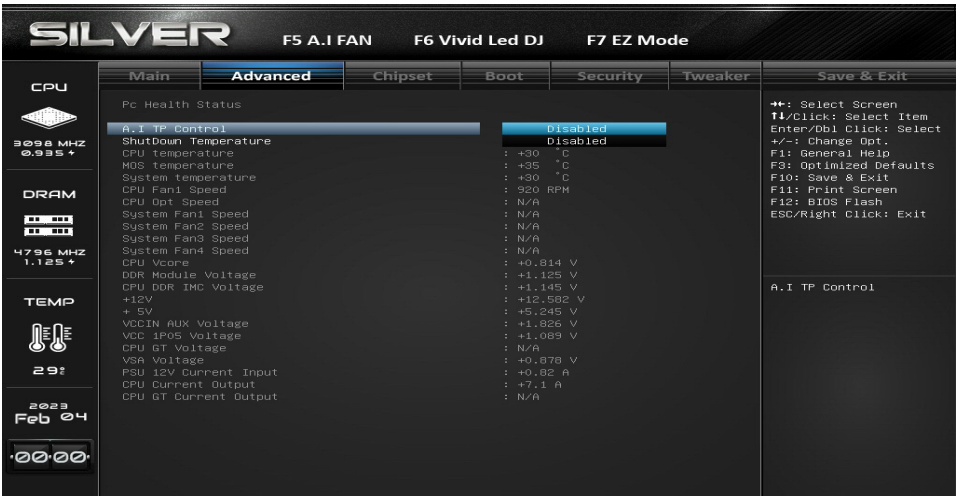
Device Settings

Set Parameters of Serial Port 1 (COMA)

Change Settings

Select an optional settings for Super IO Device.

2-8 Hardware Monitor



A.I TP Control

This item enables or disables A.I TP Control.

High Limit Temperature

High Limit Temperature Range: 50-127

Base Limit Temperature

Base Limit Temperature Range: 50-127

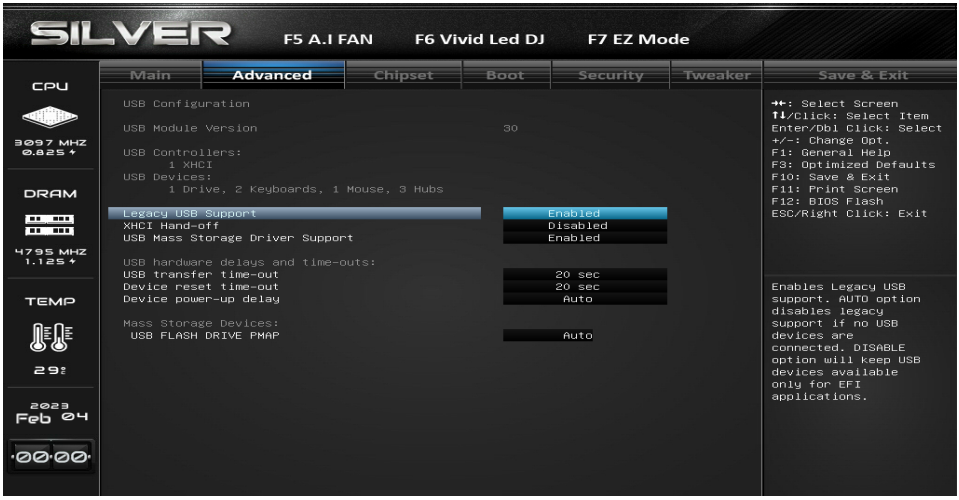
Shutdown Temperature

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

2-9 PCI Subsystem Settings

2-10 USB Configuration

USB Configuration Parameters.



Legacy USB Support

Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.

XHCI Hand-off

THis is a workaround for OSes without XHCI hand-off support. THe CHCI ownership change should be claimed by XHCI driver.

USB Mass Storage Driver Support

Enable/Disable USB Mas Storage Driver Support.

USB transfer time-out

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

Device reset time-out

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.

Device power-up delay in seconds

Delay range is 1..40 secinds, 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.

2-11 Network Stack Configuration

Network Stack Settings.

IPv4 PXE Support

Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

IPv4 HTTP Support

Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.

IPv6 PXE Support

Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.

IPv6 HTTP Support

Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.

PXE boot wait time

Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.

Media detect count

Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

2-12 NVMe Configuration

The item shows NVMe controller and driver information.

2-13 Offboard PCIe SATA Controller

3. 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.*

3-1 System Agent (SA) Configuration

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.

GTT Size

This item select the GTT Size.

Aperture Size

This item selects Aperature Size.

» *Note : Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.*

DVMT Pre-Allocated

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

DVMT Total Gfx Mem

This item selects DVMT5.0 Total Graphic 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.

VT-d

This item enables or disables VT-d capability.

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.

3-2 PCH-IO Configuration

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 Enable feature. Required to be enabled to ensure SMM protection of flash.

3-3 Onboard Device

Onboard LAN1

This item enables or disables Onbaord LAN1.

4. Boot Menu

This menu allows you to setup the system boot options.

4-1 Setup Prompt Timeout

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

4-2 Bootup NumLock State

This item selects the keyboard NumLock state.

4-3 Full Screen Logo Display

This item enables or disables Full Screen Logo Show function.

4-4 Boot Success Beep

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

4-5 BIOS Flash protection

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

4-6 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.

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.

VGA Support

If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. EFI driver will still installed with EFI OS.

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.

PS2 Devices Support

If Disabled, PS2 devices will be skipped.

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.

4-7 CSM Support

This option enables or disables CSM support.

Network

This option controls the execution of UEFI and Legacy PXE OpROM.

Storage

This option controls the execution of UEFI and Legacy Storage OpROM.

Video

This option controls the execution of UEFI and Legacy Video OpROM.

Other PCI device

Determines OpROM execution policy for devices other than Network, Storage, or Video.

4-8 Fixed Boot order Priorities

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. Security Menu

5-1 Administrator Password

This item sets Administrator Password.

5-2 User Password

This item sets User Password.

5-3 Secure Boot Menu

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.

Restore To Setup Mode

Delete NVRAM content of all UEFI Secure Boot Key databases.

Key Management

Factory Key Provision
Install factory default Keys on next re-boot only when system in setup mode.

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

Restore To Setup Mode
Delete NVRAM content of all UEFI Secure Boot Key databases.

Export Secure Boot variables
Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.

Enroll Efi Image
Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).

Platform Key (PK)

Key Exchange Keys

Authorized Signatures

Forbidden Signatures

Authorized Timestamps

OsRecovery Signatures

6. 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*

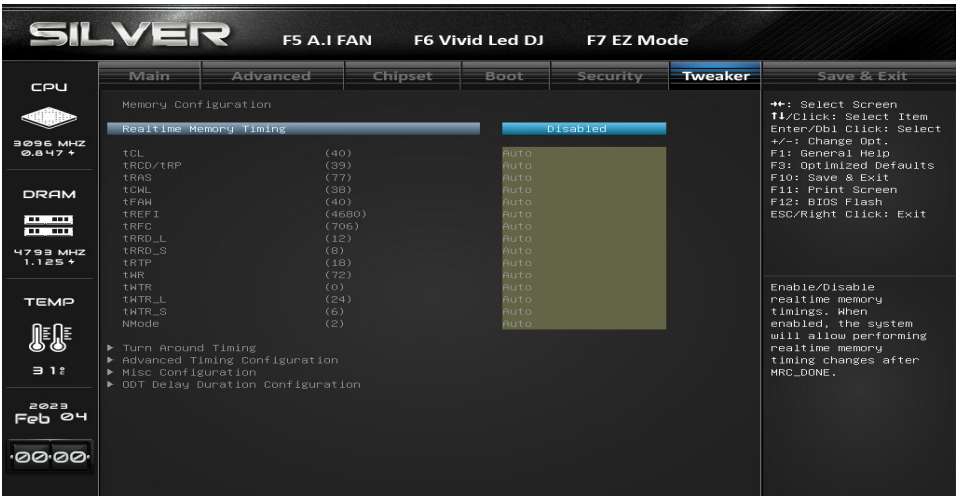
6-1 Start Page

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

6-2 Memory Profile

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

6-3 Memory Configuration



Realtime Memory Timing

This item enables or disables realtime memory timings. When enabled, the system will allow performing realtime memory timing changes after MRC_DONE.

tCL

This item allows you to select CAS Latency.

tRCD/tRP

This item allows you to select RAS to CAS delay time and Row Prechrge delay time.

tRAS

This item allows you to select RAS Active Time.

tCWL

This item allows you to select Min CAS Write Latency Delay Time.

tFAW

This item allows you to select Min Four Activate Window Delay Time.

tREFI

This item allows you to select Refresh Interval.

tRFC

This item allows you to select Min Refresh Recovery Delay Time.

tRTP

This item allows you to select Min Internal Read to Precharge Delay Time. Shall be set to half of tWR value.

tWR

This item allows you to select Min Write Recovery Time.

tRRD_L
This item allows you to select Min Row Active to Row Active Delay Time.

tRRD_S
This item allows you to select Min Row Active to Row Active Delay Time.

tWTR_L
This item allows you to select Min Internal Write to Read Command Delay Time, Same Bank Group.

tWTR_S
This item allows you to select Min Internal Write to Read Command Delay Time, Differnet Bank Group.

NMode
This item allows you to select System command tate.

6-4 Voltage Configuration

BCLK Aware Adaptive Voltage

This item enables or disables BCLK Aware Adaptive Voltage. When enabled, pcode will be aware of the BCLK frequency when calculating the CPU V/F curves. This is ideal for BCLK OC to avoid high voltage overrides.

CPU Load-Line Calibration

This item adjust CPU Load Line Calibration function.

CPU GT Voltage

This item allows you to configure the CPU GT voltage fixed or offset value

» *The following items appear only when you set the CPU GT Voltage to [Override]*

CPU GT Adjust Voltage

» *The following items appear only when you set the CPU GT Voltage to [Adaptive]*

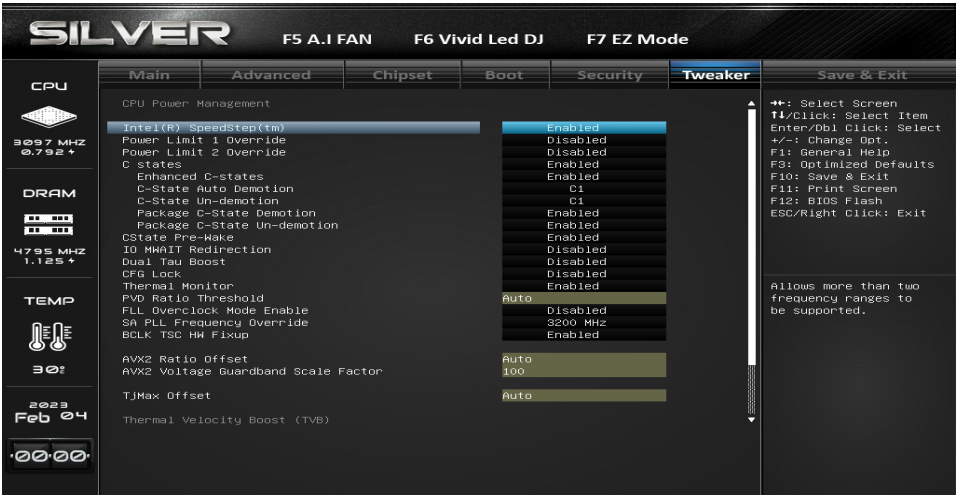
CPU GT Offset Prefix

CPU GT Offset Voltage

DRAM Voltage

This item sets DRAM Voltage.

6-5 CPU Power Management



Intel(R) SpeedStep(tm)

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

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.

Dual Tau Boost
This item allows you to set Dual Tau Boost. This is only applicable for CMLS 35W/ 65W/ 125W sku. When DPTF is enabled this feature is ignored.

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

Thermal Monitor
This item enables or disables Thermal Monitor.

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.

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

CEP Disable
CEP (Current Excursion Protecttion) Disable Menu

6-6 GT Power Management

RC6(Render Standby)

This item enables or disables Render Standby.

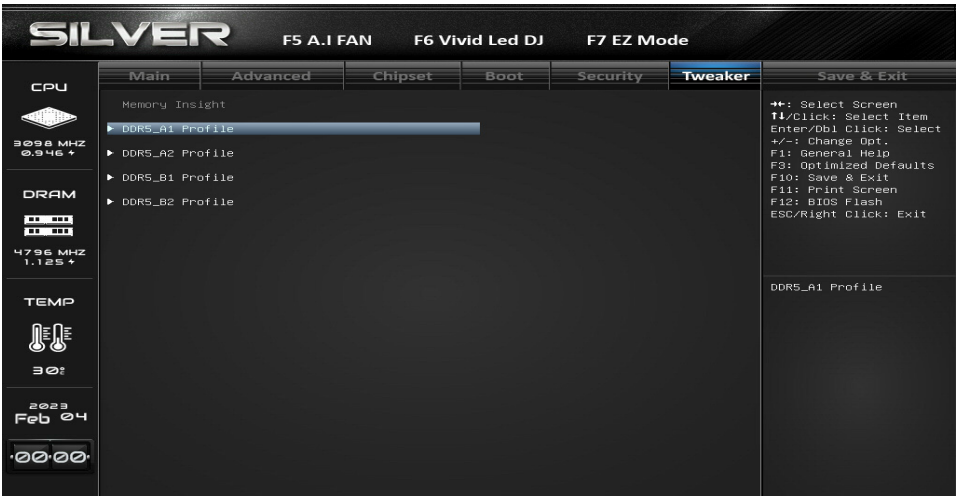
Maximum GT frequency

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

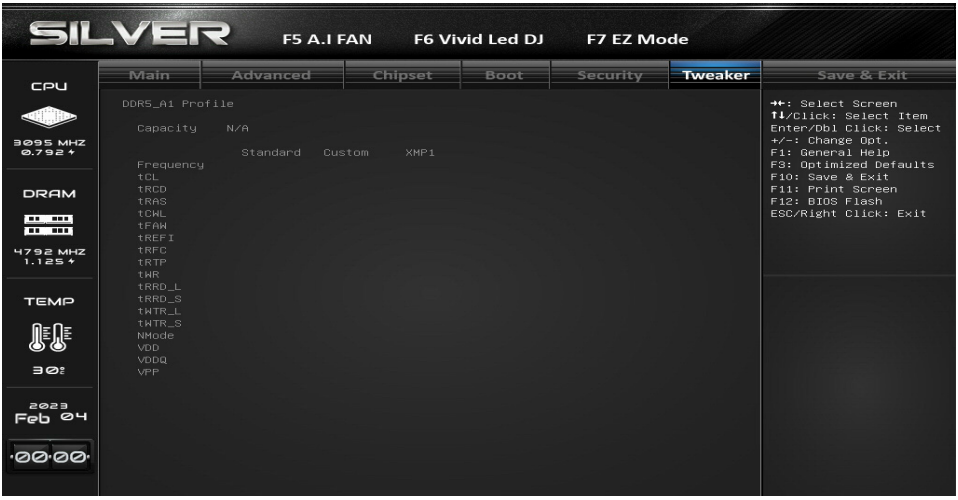
This item Disable Turbo GT frequency. Enabled: Disables Turbo GT frequency. Disabled: GT frequency is no limited.

6-7 Memory Insight



DIMM Profile

These items display memory information.



7. Save & Exit Menu

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

7-1 Discard Changes and Exit

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

7-2 Save Changes and Reset

Reset the system after saving the changes.

7-3 Restore Defaults

Restore/Load Default values for all the setup options.

7-4 Launch EFI Shell from filesystem device

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

7-5 Saving SetupData to Profile

Saving SetupData to Profile.

7-6 Restoring SetupData from Profile

Restoring SetupData from Profile.

7-7 Saving SetupData to Storage

Saving SetupData to Storage.

7-8 Restoring SetupData from Storage

Saving SetupData to Storage.