BIOS User Guide

H310MHD PRO2

BIOSTAR®

WWW.BIOSTAR.COM.TW

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 BIOS 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.*

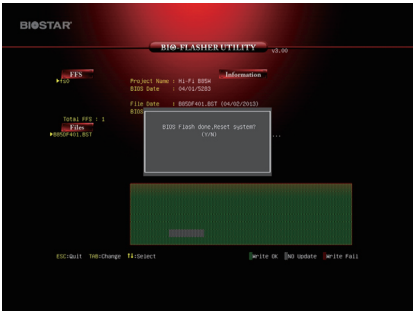
Updating BIOS with BIOSTAR BIOS Flasher

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 BIOS-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.



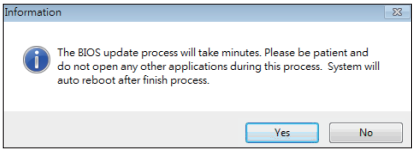
8. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes and Reset> to restart the computer. Then the BIOS Update is completed.

BIOS Update Utility (through the Internet)

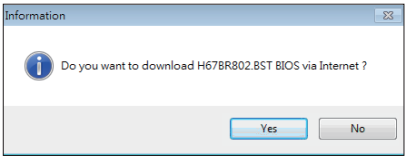
1. Installing BIOS Update Utility from the DVD Driver.
2. Please make sure the system is connected to the internet before using this function.

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

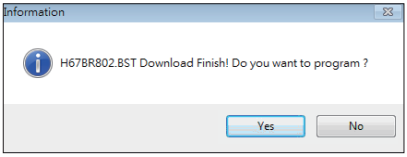
4. An open dialog will show up to request your agreement to start the BIOS update. Click "Yes" to start the online update procedure.



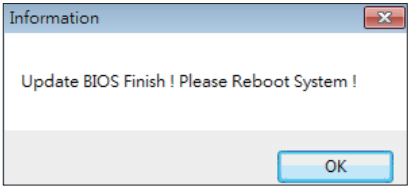
5. If there is a new BIOS version, the utility will ask you to download it. Click "Yes" to proceed.



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.



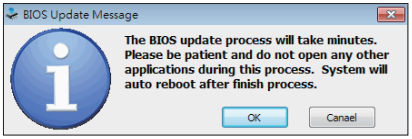
8. While the system boots up and the full screen logo shows up, press <DEL> key to enter BIOS setup.
After entering the BIOS setup, please go to the <Save & Exit>, using the <Restore Defaults> function to load Optimized Defaults, and select <Save Changes> and <Reset> to restart the computer. Then, the BIOS Update is completed.

BIOS Update Utility (through a BIOS file)

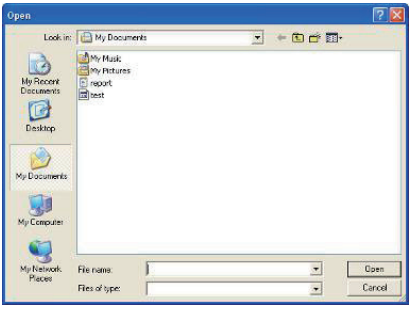
1. Installing BIOS Update Utility from the DVD Driver.
2. Download the proper BIOS from http://www.biostar.com.tw/

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

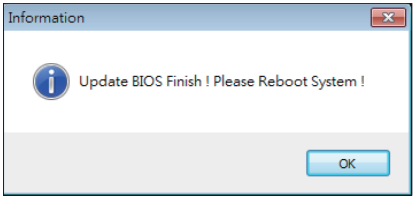
4. A warning message will show up to request your agreement to start the BIOS update. Click “OK” to start the update procedure.



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.



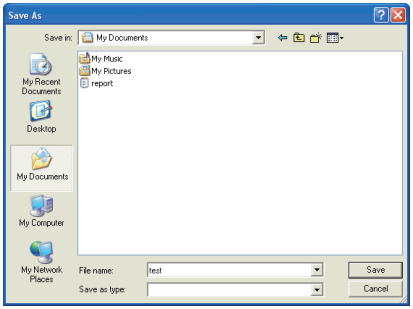
6. After the BIOS Update process is finished, click on “OK” to reboot the system.



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.

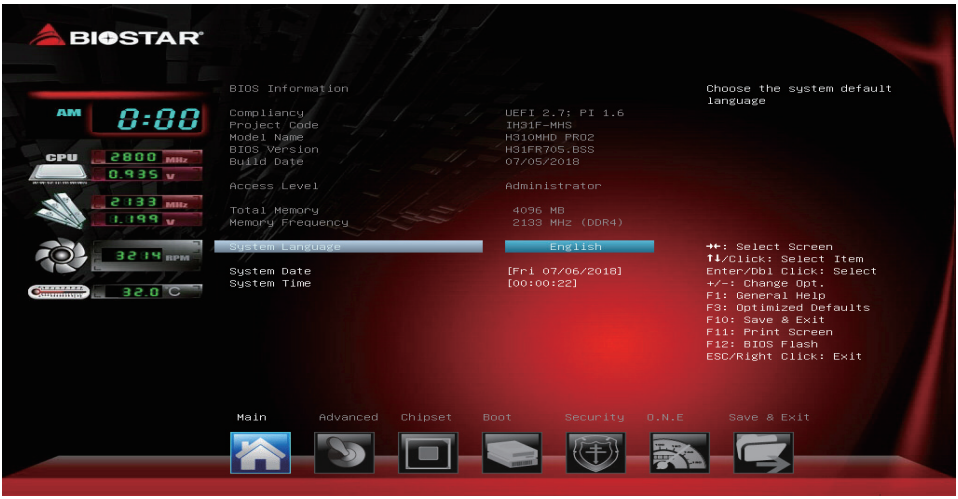
In the UEFI BIOS setup utility, you will see **General Help** description at the top right corner, and this is providing a brief description of the selected item. **Navigation Keys** for that particular menu are at the bottom right corner, and you can use these keys to select item and change the settings.

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.*

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.



BIOS Information

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

Total Memory

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

Memory Frequency

Shows the system memory frequency.

System Language

Choose the system default language.

System Date

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

System Time

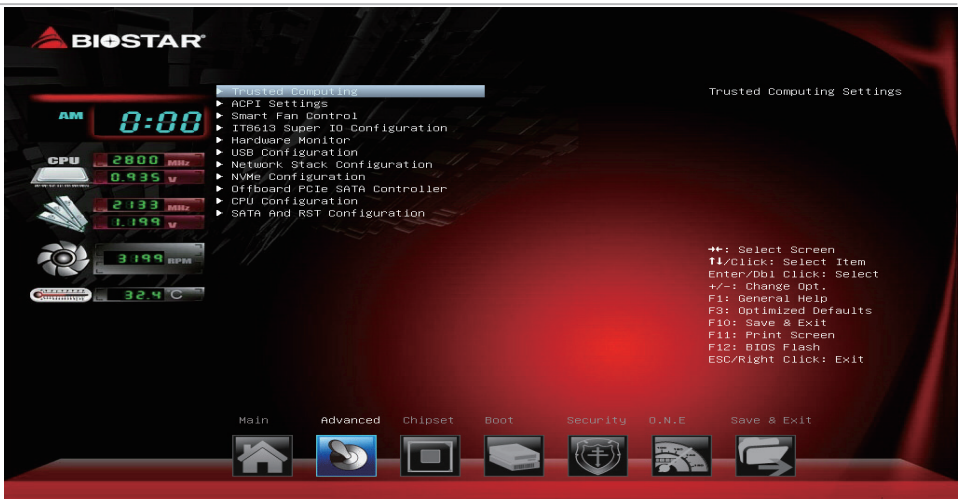
Set the system internal clock.

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.*



Trusted Computing

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.
Options: Enabled (Default) / Disabled

SHA-1 PCR Bank

This item enables or disables SHA-1 PCR Bank.
Options: Enabled (Default) / Disabled

SHA256 PCR Bank

This item enables or disables SHA256 PCR Bank.
Options: Enabled (Default) / Disabled

Pending operation

This item schedule an operation for the security device.
Options: None (Default) / TPM Clear

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

Platform Hierarchy

This item enables or disables Platform Hierarchy.
Options: Enabled (Default) / Disabled

Storage Hierarchy

This item enables or disables Storage Hierarchy.
Options: Enabled (Default) / Disabled

Endorsement Hierarchy

This item enables or disables Endorsement Hierarchy.
Options: Enabled (Default) / Disabled

TPM2.0 UEFI Spec Version

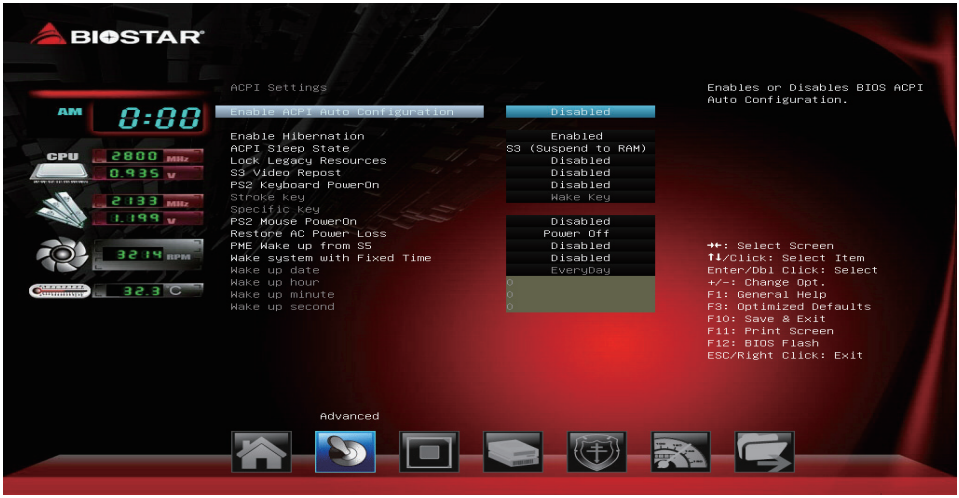
This item allows you to select the TCG2 Spec Version Support. TCG_1_2: the compatible mode for Win8/ Win10; TCG_2: Support new TCG2 protocol and event format for Win10 or later.
Options: TCG_2 (Default) / TCG_1_2

Physical Presence Spec Version

This item select to tell O.S. to support PPI Spec Version 1.2 or 1.3.
Options: 1.3 (Default) / 1.2

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

ACPI Settings



Enable ACPI Auto Configuration

This item enables or disables BIOS ACPI auto configuration function.
Options: Disabled (Default) / Enabled

Enable Hibernation

This item enables or disables system ability to hibernate (0S/S4 sleep state). This option may not be effective with some OSs.
Options: Enabled (Default) / Disabled

ACPI Sleep State

This item allows you to select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.
Options: S3 (Suspend to RAM) (Default) / Suspend Disabled

Lock Legacy Resources

The item enables or disables Lock of Legacy Resources.
Options: Disabled (Default) / Enabled

S3 Video Repost

The item enables or disables S3 Video Repost. On enabling, Video option ROM will be dispatched during S3 resume.
Options: Disabled (Default) / Enabled

PS2 Keyboard PowerOn

This item allows you to control the keyboard power on function.
Options: Disabled (Default) / Any Key / Stroke Key / Specific Key

Stroke Keys

This item will show only when Keyboard PowerOn is set “Stroke Key.”
Options: Wake Key (Default) / Power Key / Ctrl+F1 / Ctrl+F2 / Ctrl+F3 / Ctrl +F4 / Ctrl+F5 / Ctrl+F6

Specific Key

This item will show only when Keyboard PowerOn is set “Specific Key.” Press Enter to set Specific key.

PS2 Mouse PowerOn

This item allows you to control the mouse power on function.
Options: Disabled (Default) / Enabled

Restore AC Power Loss

Specify what state to go to when power is re-applied after a power failure.
Options: Power Off (Default) / Power On / Last State

PME Wake up from S5

The item enables the system to wake from S5 using PME event.
Options: Disabled (Default) / Enabled

Wake system with Fixed Time

This item enables or disables the system to wake on by alarm event. When this item is enabled, the system will wake on the hr::min::sec specified.
Options: Disabled (Default) / Enabled

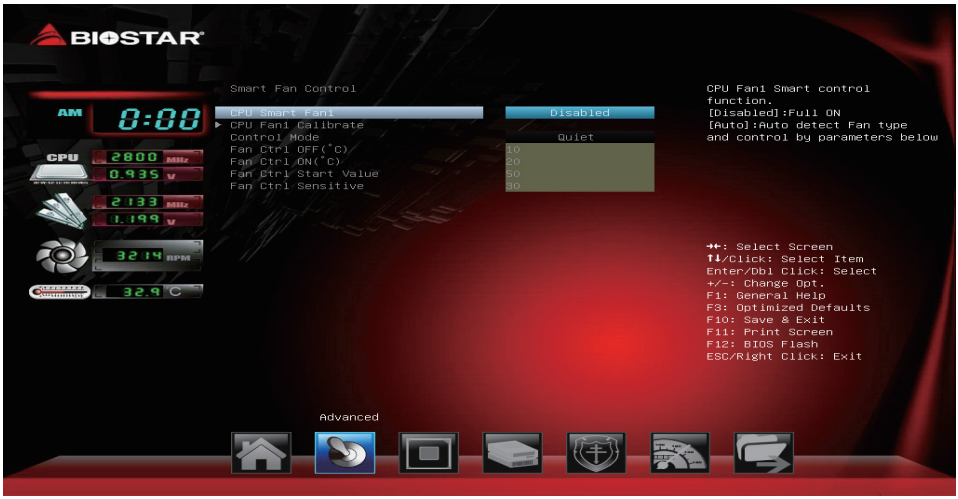
Wake up date

You can choose which date the system will boot up.

Wake up hour / Wake up minute / Wake up second

You can choose the system boot up time, input hour, minute and second to specify.

SMART FAN Control



CPU Smart Fan1

This item allows you to control the CPU Smart Fan function.
Options: Disabled (Default) / Auto

CPU Fan1 Calibrate

Press [ENTER] to calibrate CPU Fan1 speed.

Control Mode

This item provides several operation modes of the fan.
Options: Quiet (Default) / Aggressive / Manual

Note

» *The following items appear only when you set the Control Mode function to [Manual].*

Fan Ctrl OFF(°C)

When CPU temperature is lower than this value, the CPU fan will keep lowest RPM.
Options: 10 (°C) (default)

Fan Ctrl On(°C)

When CPU temperature is higher than this value, the CPU fan controller will turn on.
Options: 20 (°C) (Default)

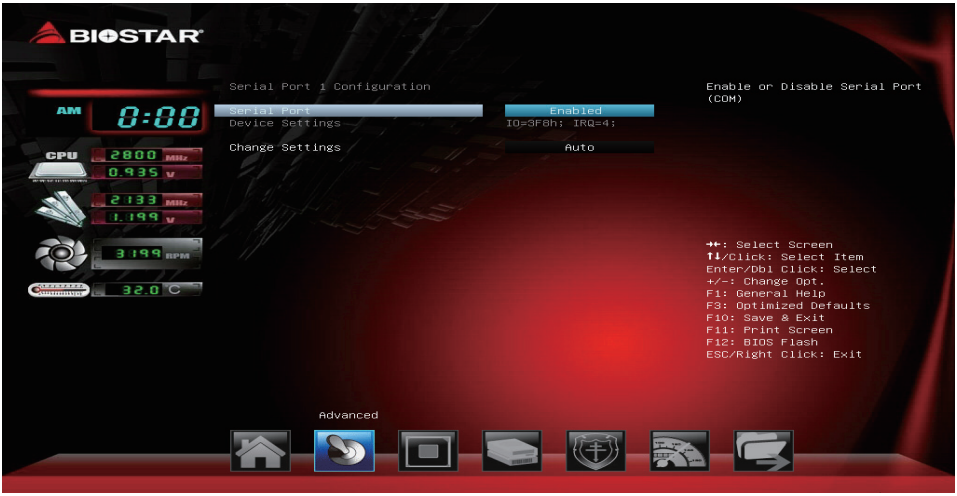
Fan Ctrl Start Value

This item sets CPU FAN Start Speed Value.
Options: 50 (Default)

Fan Ctrl Sensitive

The bigger the numeral is, the higher the FAN speed is.
Options: 30 (Default)

IT8613 Super IO Configuration



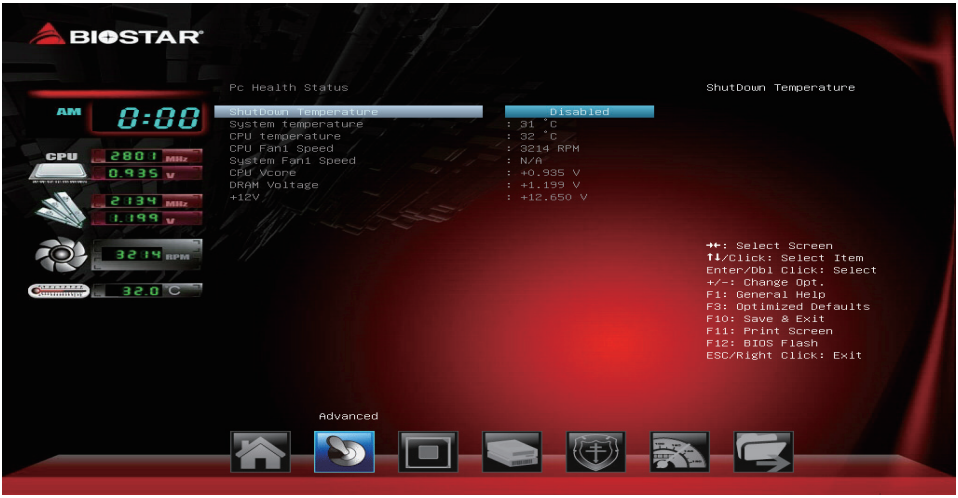
Serial Port

This item enables or disables Serial Port (COM).
Options: Enabled (Default) / Disabled

Change Settings

This item Select an optimal settings for Super IO Device.
Options: Auto (Default) / IO=3F8h; IRQ=4 / IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12 / IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12 / IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12 / IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12

H/W Monitor



Shutdown Temperature

This item allows you to set up the CPU shutdown Temperature.
Options: Disabled (Default) / 70°C/158°F / 75°C/167°F / 80°C/176°F / 85°C/185°F / 90°C/194°F

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.
Options: Enabled (Default) / Disabled / Auto

XHCI Hand-off

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
Options: Disabled (Default) / Enabled

USB Mass Storage Driver Support

The item allows you to enable or disable USB Mass Storage Driver Support.
Options: Enabled (Default) / Disabled

Port 60/64 Emulation

The item enable or disable Port 60/64 Emulation. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
Options: Enabled (Default) / Disabled

USB transfer time-out

The time-out value for Control, Bulk, and Interrupt transfers.
Options: 20 sec (Default) / 1 sec / 5 sec / 10 sec

Device reset time-out

The item sets USB mass storage device Start Unit command time-out.
Options: 20 sec (Default) / 10 sec / 30 sec / 40 sec

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.
Options: Auto (Default) / Manual

Note

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

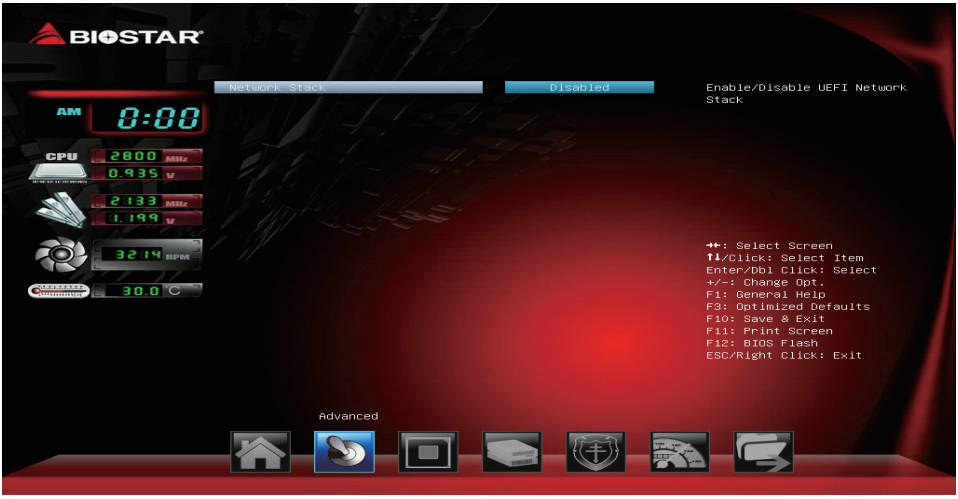
Device power-up delay in seconds

Delay range is 1 ~ 40 seconds, in one second increments.
Options: 5 (Default)

USB FLASH DRIVE PMAP

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.
Options: Auto (Default) / Floppy / Forced FDD / Hard Disk / CD-ROM

Network Stack Configuration



Network Stack

This item enables or disables UEFI network stack
Options: Disabled (Default) / Enabled

Note

» *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.
Options: Disabled (Default) / Enabled

IPv4 HTTP Support
This item enables or disables IPv4 HTTP Boot Support. If disabled IPv4 HTTP boot support will not be available.
Options: Disabled (Default) / Enabled

IPv6 PXE Support
This item enables or disables IPv6 PXE Boot Support. If disabled IPv6 PXE boot support will not be available.
Options: Disabled (Default) / Enabled

IPv6 HTTP Support
This item enables or disables IPv6 HTTP Boot Support. If disabled IPv6 HTTP boot support will not be available.
Options: Disabled (Default) / Enabled

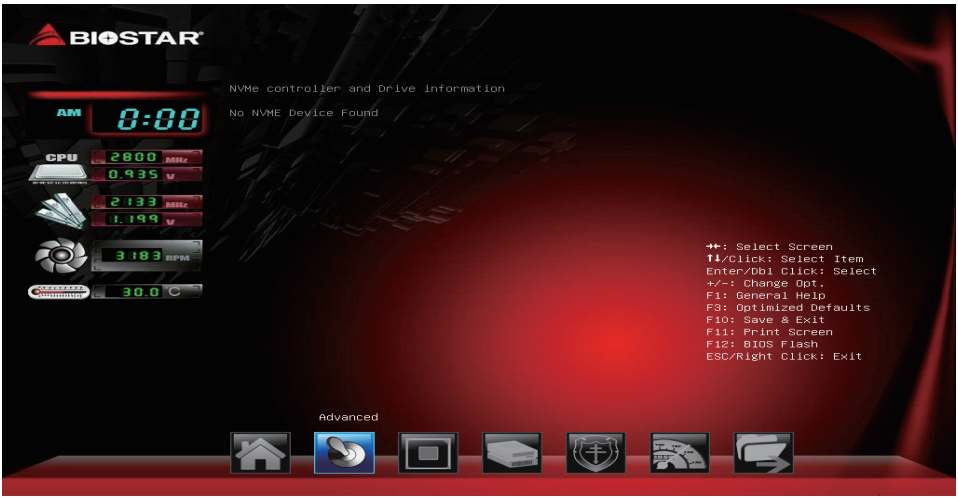
IPSEC Certificate
This item enables or disables IPSEC certificate for Ikev.
Options: Enabled (Default) / Disabled

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

Media detect count
Wait time in sec to detect media.

NVMe Configuration

The item shows NVMe controller and driver information.



Offboard PCIe SATA Controller

CPU Configuration

This item shows CPU Information

Software Guard Extensions (SGX)

This item enables or disableds Software Guard Extensions (SGX).
Options: Software Controlled (Default) / Enabled / Disabled

PRMRR Size

This item allows you to setting the PRMRR Size.
Options: INVALID PRMRR (Default) / 32MB / 64MB / 128MB

Overclocking Lock

This item enables or disableds Overclocking Lock.
Options: Disabled (Default) / Enabled

Hardware Prefetcher

This item to turn on/off the MLC streamer prefetcher.
Options: Enabled (Default) / Disabled

Adjacent Cache Line Prefetch

This item to turn on/off prefetching of adjacent cache lines.
Options: Enabled (Default) / Disabled

Intel (VMX) Virtualization Technology

This item enableds or disableds Intel Virtualization Technology. When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Options: Enabled (Default) / Disabled

Active Processor Cores

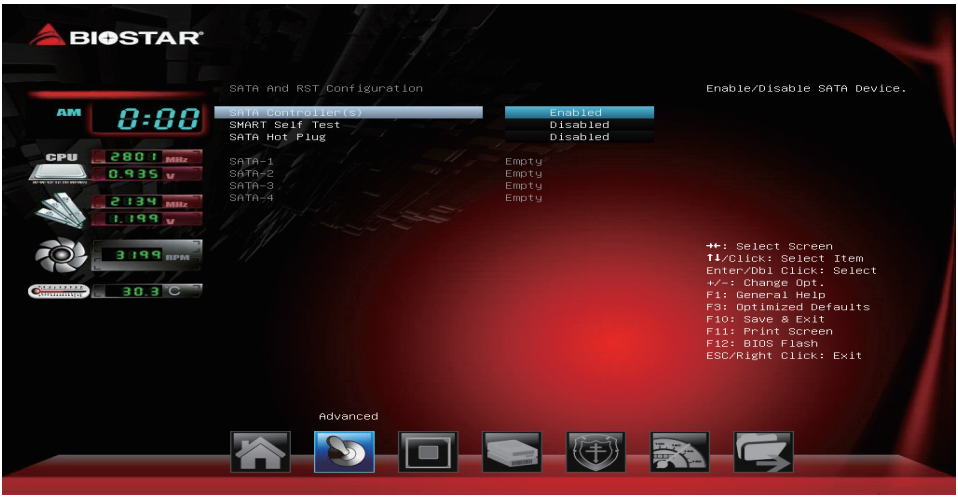
This item sets number of cores to enable in each processor package.
Options: All (Default) / 1 / 2 / 3 / 4 / 5

AES

This item sets CPU Advanced Encryption Standard instructions.
Options: Enabled (Default) / Disabled

SATA and RST 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)

This item enables or disables Serial ATA Device.
Options: Enabled (Default) / Disabled

SMART Self Test

This item runs SMART Self Test on all HDDs during POST.
Options: Disabled (Default) / Enabled

SATA Hot Plug

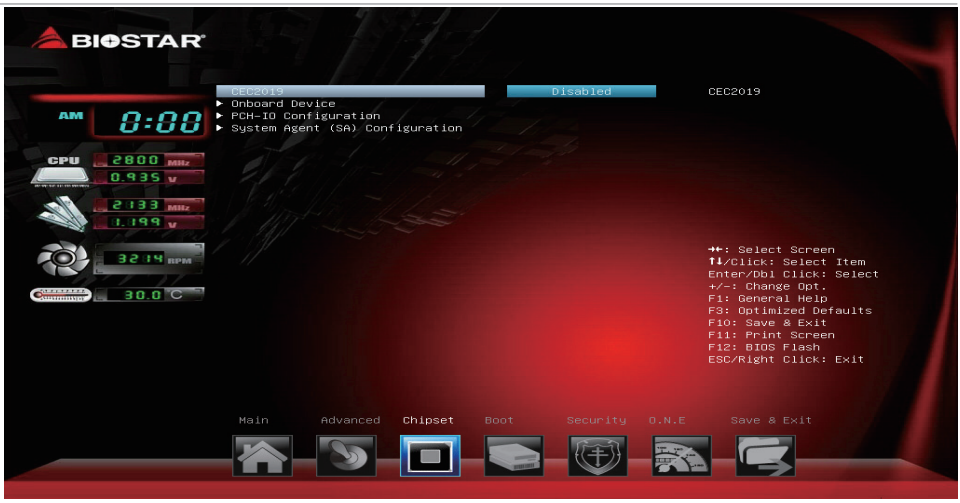
This item enables or disables designates SATA port as Hot Pluggable.
Options: Disabled (Default) / Enabled

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

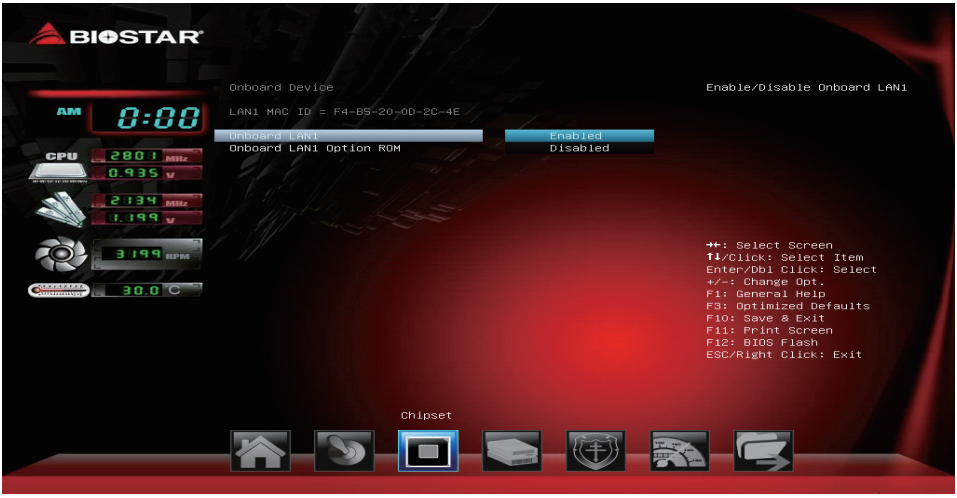
» *Beware of that setting inappropriate values in items of this menu may cause system to malfunction.*



CEC2019

This item CEC2019.
Options: Disabled (Default) / Enabled

Onboard Device



Onboard LAN1

This item enables or disables Onbaord LAN1.

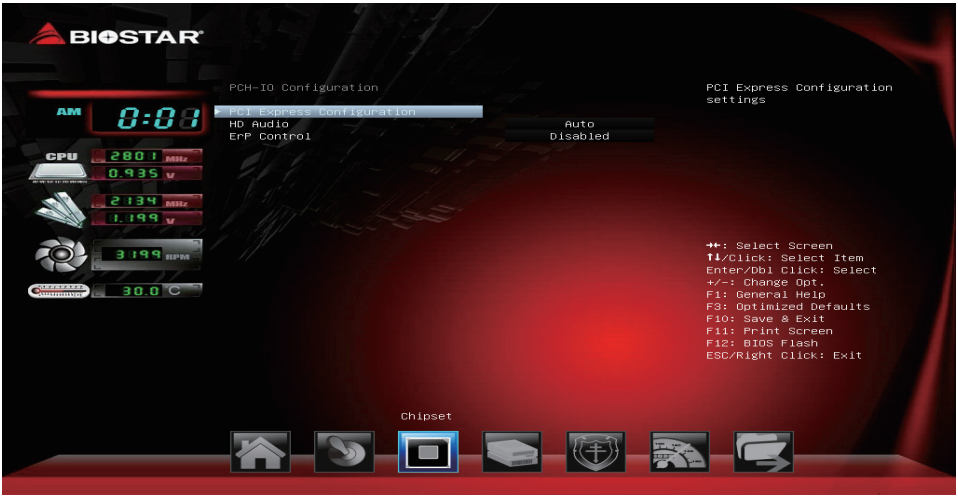
Options: Enabled (Default) / Disabled

Onboard LAN1 Option ROM

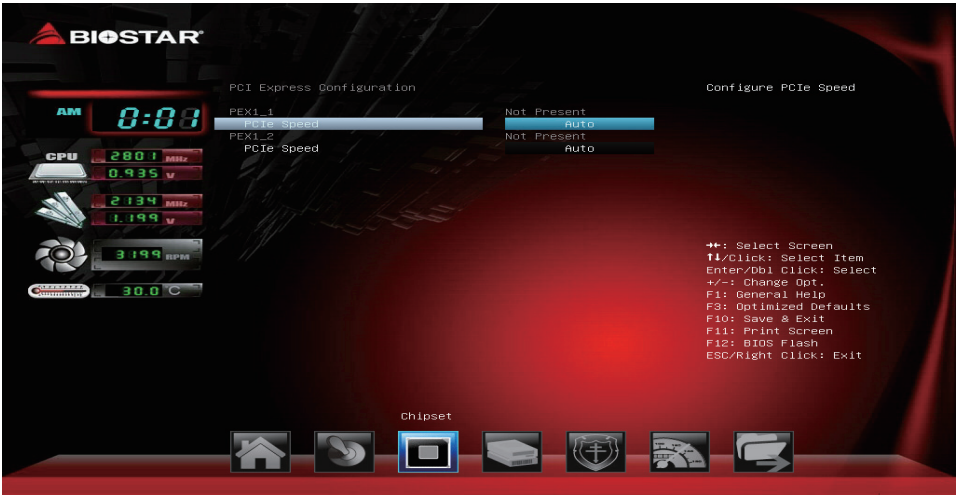
This item enables or disables Onboard LAN1 Option ROM.

Options: Disabled (Default) / Enabled

PCH-IO Configuration



PCI Express Configuration



PEX1_1/ PEX1_2 PCIe Speed

This item Configure PCIe Speed.

Options: Auto(Default) / Gen1 / Gen2 / Gen3

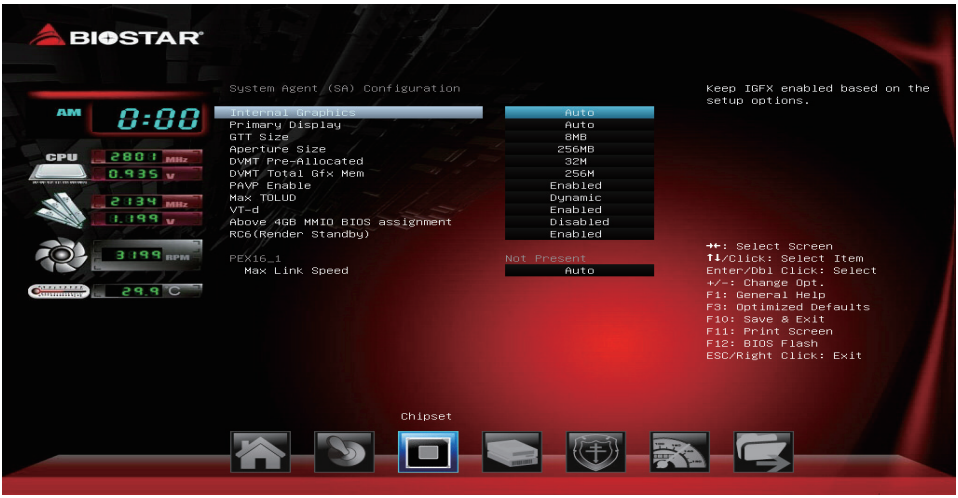
HD Audio

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.
Options: Auto (Default) / Disabled / Enabled

ErP Control

When ErP is enabled, the system will meet ErP requirement.
Options: Disabled (Default) / Enabled in S4-S5

System Agent (SA) Configuration



Internal Graphics

This item keeps IGFX enabled based on the setup options.
Options: Auto (Default) / Disabled / Enabled

Primary Display

This item selects which of IGFX/PEG/PCI Graphics device should be Primary Display or select SG for Switchable Gfx.
Options: Auto (Default) / IGFX / PEG / PCI / SG

GTT Size

This item selects GTT Size.
Options: 8MB (Default) / 4MB / 2MB

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.
Options: 256MB (Default) / 128MB / 512MB / 1024MB / 2048MB

DVMT Pre-Allocated

This item selects DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
Options: 32M (Default) / 0M / 64M / 4M / 8M / 12M / 16M / 20M / 24M / 28M / 32M/F7 / 36M / 40M / 44M / 48M / 52M / 56M / 60M

DVMT Total Gfx Mem

This item selects DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Options: 256MB (Default) / 128MB / MAX

PAVP Enable

This item enables or disables PAVP.
Options: Enabled (Default) / Disabled

Max TOLUD

Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.
Options: Dynamic (Default) / 1 GB / 1.25 GB / 1.5 GB / 1.75 GB / 2 GB / 2.25 GB / 2.5 GB / 2.75 GB / 3 GB / 3.25 GB / 3.5GB

VT-d

This item enables or disables VT-d capability.
Options: Enabled (Default) / Disabled

Above 4GB MMIO BIOS assignment

This item enables or disables above 4GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.
Options: Disabled (Default) / Enabled

RC6 (Render Standby)

This item enables or disables render standby support.
Options: Enabled (Default) / Disabled

PEX16_1

MAX Link Speed

Configure PEX16_1 Max Speed.
Options: Auto (Default) / Gen1 / Gen2 / Gen3

4. Boot Menu

This menu allows you to setup the system boot options.

Setup Prompt Timeout

This item sets number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Options: 1 (Default)

Bootup NumLock State

This item selects the keyboard NumLock state.
Options: On (Default) / Off

Full Screen Logo Display

This item enable or disable Full Screen Logo Show function.
Options: Enabled (Default) / Disabled

Boot Success Beep

When this item is set to Enabled, BIOS will let user know boot success with beep.
Options: Enabled (Default) / Disabled

BIOS Flash protection

While enabled, it can't flash write and flash erase by SMI.
Options: Enabled (Default) / Disabled

Fast Boot

This item 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.
Options: Disabled (Default) / Enabled

Note

» *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 will be available in OS and post.
Options: All Sata Devices (Default) / Last Boot HDD Only

VGA Support
If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. EFI driver will still be installed with EFI OS.
Options: EFI Driver (Default) / Auto

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.
Options: Disabled (Default) / Full Initial / Partial Initial

PS2 Devices Support
If Disabled, PS2 devices will be skipped.
Options: Enabled (Default) / Disabled

Network Stack Driver Support
If Disabled, Network Stack Drivers will be skipped.
Options: Disabled (Default) / Enabled

Redirection Support

If disable, Redirection function will be disabled.
Options: Disabled (Default) / Enabled

CSM Support

This option enables or disables CSM support.
Options: Disabled (Default) / Enabled

Note

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

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.
Options: Upon Request (Default) / Always

Option ROM Messages

This item sets the display mode for Option ROM.
Options: Force BIOS (Default) / Keep Current

Boot option filter

This option controls Legacy/UEFI ROMs priority.
Options: UEFI and Legacy (Default) / Legacy only / UEFI only

Network

This option controls the execution of UEFI and Legacy Network OpROM
Options: Legacy (Default) / UEFI / Do not launch

Storage

This option controls the execution of UEFI and Legacy Storage OpROM
Options: Legacy (Default) / UEFI / Do not launch

Video

This option controls the execution of UEFI and Legacy Video OpROM
Options: Legacy (Default) / UEFI / Do not launch

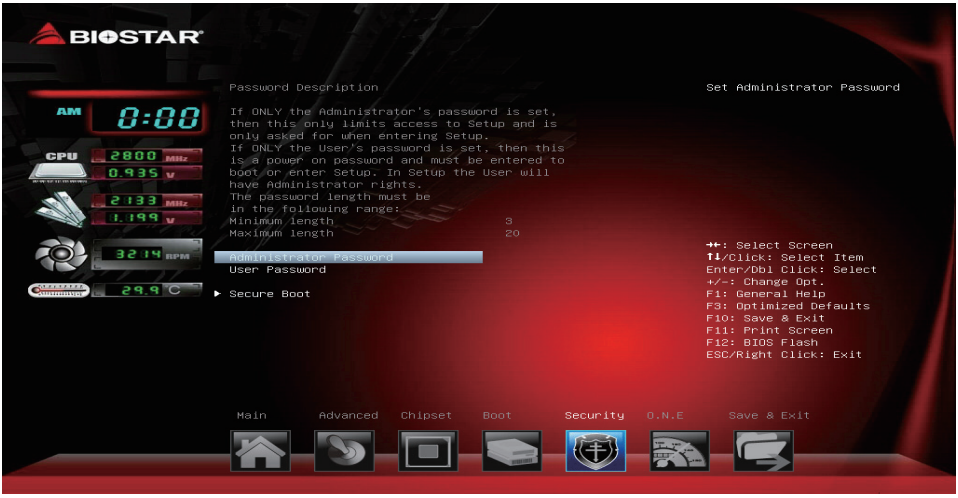
Other PCI devices

This item determines OpROM execution policy for devices other than Network, Storage, or Video.
Options: UEFI (Default) / Legacy / Do not launch

New Boot Option Policy

This item allows you to controls the placement of newly detected UEFI boot options.
Options: Default (Default) / Place First / Place Last

5. Security Menu



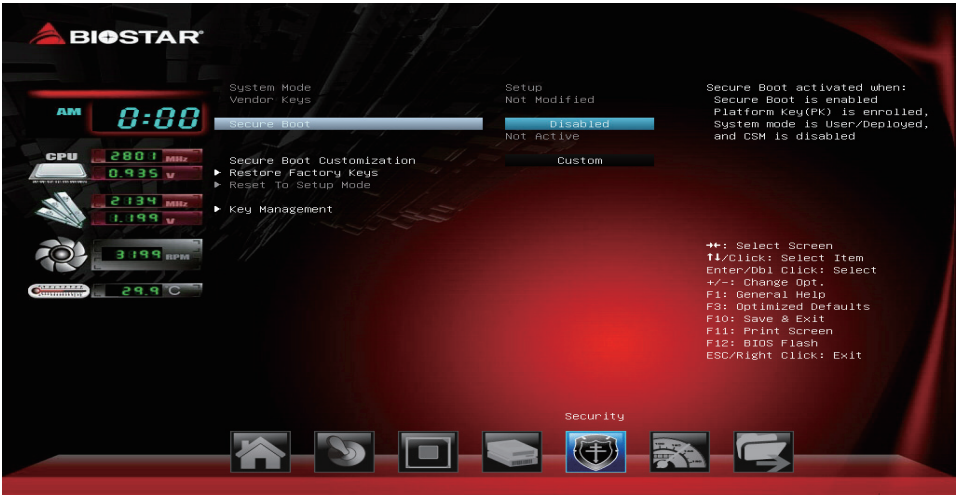
Administrator Password

This item sets Administrator Password.

User Password

This item sets User Password.

Secure Boot Menu



Secure Boot

Secure Boot feature is active if Secure Boot is enabled, Platform Key(PK) is enrolled and the system is in user mode. The mode change requires platform reset.
Options: Disabled (Default) / Enabled

Secure Boot Customization

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

Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot Key databases.

Restore To Setup Mode

Delete all Secure Boot Key databases from NVRAM.

Key Management

Factory Key Provision
This item install factory default Secure Boot Keys after the platform reset and while the system is in setup mode.
Options: Disabled (Default) / Enabled

Install Factory Default Keys
Force System to User Mode - install all Factory Default Keys(PK, KEK, , dbt, dbx). Change takes effect after reboot.

Reset To Setup Mode
This item delete all Secure Boot key databases from NVRAM.

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
This item allows the image to run in Secure Boot mode. Enroll SHA256 hash certificate of a PE image into Authorized Signature Database(db).

Remove 'UEFI CA' from DB
Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database(db).

Restore DB defaults
Restore DB variable to factory defaults.

Platform Key (PK)
Options: Details / Export / Update / Delete

Key Exchange Keys
Options: Details / Export / Update / Append / Delete

Authorized Signatures
Options: Details / Export / Update / Append / Delete

Forbidden Signatures
Options: Details / Export / Update / Append / Delete

Authorized Timestamps
Options: Update / Append

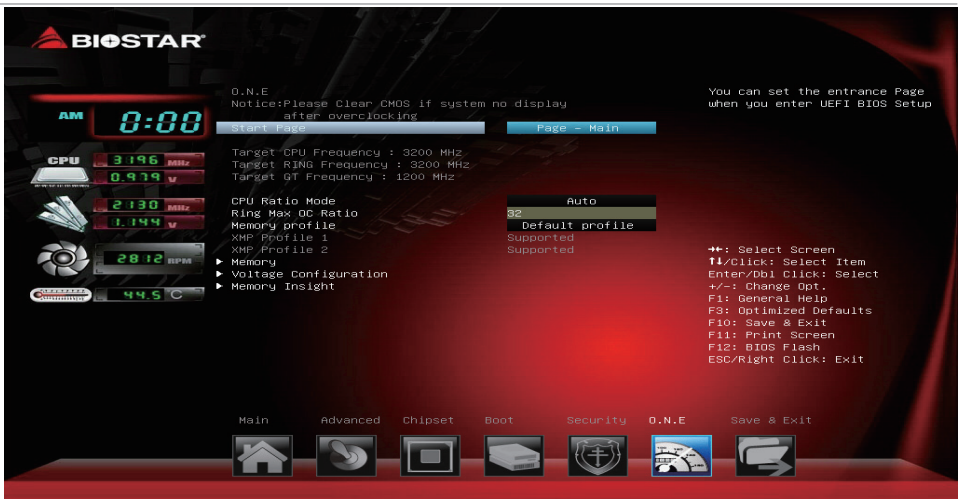
OsRecovery Signatures
Options: Update / Append

6. O.N.E 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*



Start Page

You can set the entrance page when you enter UEFI BIOS Setup.
Options: Page – Main (Default) / Page – Advanced / Page – Chipset / Page – Boot / Page – Security / Page –O.N.E / Page – Save & Exit

CPU Ratio Mode

This item sets CPU Ratio Mode.
Options: Auto (Default) / ALL Cores / Per Core / Fixed

Note

» *The following items appear only when you set the CPU Ratio Mode function to [All Cores] & [Fixed]*

Max OC Ratio

This item sets the maximum OC Ratio for the CPU Core.

Note

» *The following items appear only when you set the CPU Ratio Mode function to [Per Core]*

1/2/3/4/5/6-Core Ratio Limit Override

This item 1/2/3/4/5/6-Core Ratio Limit with range 0 to 83.

Ring Max Ratio

This sets the maximum overclocking ratio for the CPU Ring.

Memory Profile

Select DIMM timing profile. The below values start with the currently running values and don't auto populate.
Options: Default profile (Default) / Custom profile

Note

» *The following items appear only when you set the Memory Profiles function to [Custom profile]*

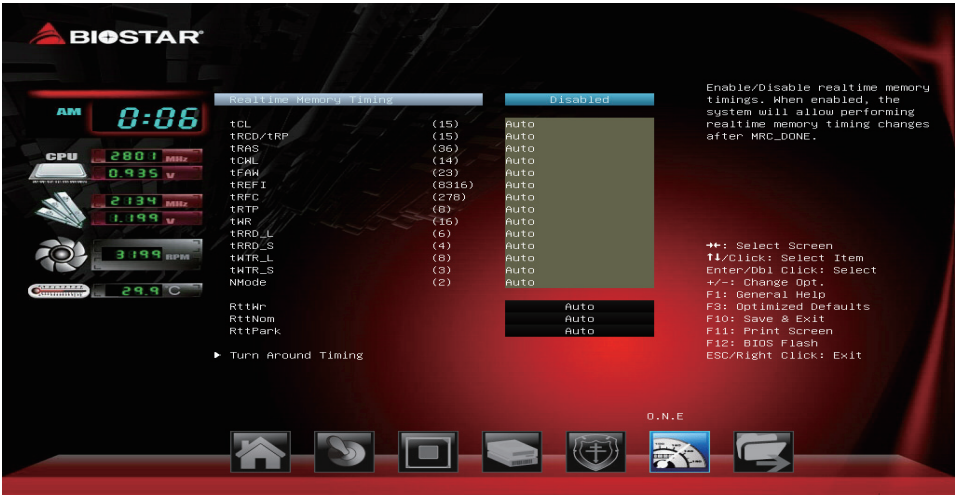
Memory Ratio

Automatic or the frequency will equal ratio times reference clock. Set to Auto to recalculate memory timings listed below.
Options: Auto (Default) / DDR4 800MHz / DDR4 1066MHz / DDR4 1333MHz / DDR4 1600MHz / DDR4 1866MHz / DDR4 2133MHz / DDR4 2400MHz / DDR4 2666MHz

QCLK Odd Ratio

Adds 133 or 100 MHz to QCLK frequency, depending on RefClk.
Options: Disabled (Default) / Enabled

Memory Timing 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.
Options: Disabled (Default) / Enabled

tCL

This item allows you to select CAS Latency, 0: AUTO, max: 31
Options: Auto (Default)

tRCD/tRP

This item allows you to select RAS to CAS delay time and Row Prechrge delay time, 0: AUTO, max: 63
Options: Auto (Default)

tRAS
This item allows you to select Row Active Time, 0: AUTO, max: 64
Options: Auto (Default)

tCWL
This item allows you to select Minimum CAS Write Latency Delay, 0: AUTO, max: 20
Options: Auto (Default)

tFAW
This item allows you to select Four Activate Window Delay Time, 0: AUTO, max: 63
Options: Auto (Default)

tREFI
This item allows you to select Refresh Interval, 0: AUTO, max: 65535
Options: Auto (Default)

tRFC
This item allows you to select Min Refresh Recovery Delay Time, 0: AUTO, max: 1023
Options: Auto (Default)

tRTP
This item allows you to select Min Internal Read to Precharge Command Delay Time. 0: AUTO, max: 15. DDR4 legal values: 5, 6, 7, 8, 9, 10, 12
Options: Auto (Default)

tWR
This item allows you to select Min Write Recovery Time, 0: AUTO, legal values: 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 24, 30, 34, 40
Options: Auto (Default)

tRRD_L
This item allows you to select Min Row Active to Row Active Delay Time for Same Bank Group, 0: AUTO, max: 31
Options: Auto (Default)

tRRD_S
This item allows you to select Min Row Active to Row Active Delay Time for Different Bank Group, 0: AUTO, max: 31
Options: Auto (Default)

tWTR_L
This item allows you to select Min Internal Write to Read Command Delay Time for Same Bank Group, 0: AUTO, max: 60
Options: Auto (Default)

tWTR_S
This item allows you to select Min Internal Write to Read Command Delay Time for Different Bank Group, 0: AUTO, max: 28
Options: Auto (Default)

NMode
This item allows you to select System command rate, range 0-2, 0 means auto, 1 = 1N, 2 = 2N
Options: Auto (Default)

RttWr

Options: Auto (Default) / Disabled / RZQ/1 / RZQ/2 / RZQ/3 / Hi-Z

RttNom

Options: Auto (Default) / Disabled / RZQ/1 / RZQ/2 / RZQ/3 / RZQ/4 / RZQ/5 / RZQ/6 / RZQ/7

RttPark

Options: Auto (Default) / Disabled / RZQ/1 / RZQ/2 / RZQ/3 / RZQ/4 / RZQ/5 / RZQ/6 / RZQ/7

Turn Around Timing

tRD2RD_SG

This item delay between Read-to-Read commands in the same Bank Group, Range 4-54.

Options: Auto (Default)

tRD2RD_DG

This item delay between Read-to-Read commands in different Bank Group for DDR4. All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Options: Auto (Default)

tRD2RD_DR

This item delay between Read-to-Read commands in different Ranks. 0-Auto, Range 4-54.

Options: Auto (Default)

tRD2RD_DD

This item delay between Read-to-Read commands in different DIMMs. 0-Auto, Range 4-54.

Options: Auto (Default)

tRD2WR_SG

This item delay between Read-to-Write commands in the same Bank Group. 0-Auto, Range 4-54.

Options: Auto (Default)

tRD2WR_DG

This item delay between Read-to-Write commands in different Bank Group for DDR4. All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Options: Auto (Default)

tRD2WR_DR
This item delay between Read-to-Write commands in different Ranks. 0-Auto, Range 4-54.
Options: Auto (Default)

tRD2WR_dd
This item delay between Read-to-Write commands in different DIMMs. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2RD_SG
This item delay between Write-to-Read commands in the same Bank Group. 0-Auto, Range 4-86.
Options: Auto (Default)

tWR2RD_DG
This item delay between Write-to-Read commands in different Bank Group for DDR4. All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2RD_DR
This item delay between Write-to-Read commands in different Ranks. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2RD_DD
This item delay between Write-to-Read commands in different DIMMs. 0-Auto, Range 4-54.
Options: Auto (Default)

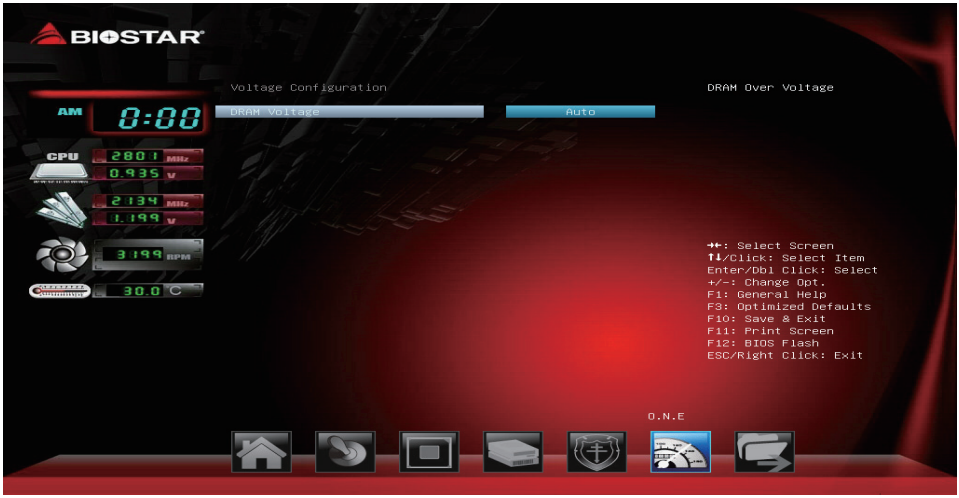
tWR2WR_SG
This item delay between Write-to-Write commands in the same Bank Group. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2WR_DG
This item delay between Write-to-Write commands in different Bank Group for DDR4. All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2WR_DR
This item delay between Write-to-Write commands in different Ranks. 0-Auto, Range 4-54.
Options: Auto (Default)

tWR2WR_DD
This item delay between Write-to-Write commands in different DIMMs. 0-Auto, Range 4-54.
Options: Auto (Default)

Voltage Configuration



DRAM Voltage

This item sets DRAM Over Voltage.
Options: Auto (Default) / 1.20V / 1.35V

CPU Power Management

Intel(R) SpeedStep(tm)

This item allows more than two frequency ranges to be supported.
Options: Enabled (Default) / Disabled

Race To Halt (RTH)

This item enables or disables Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Options: Enabled (Default) / Disabled

Intel(R) Speed Shift Technology

This item enables or disables Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Options: Enabled (Default) / Disabled

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.
Options: Enabled (Default) / Disabled

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.
Options: 95000 (Default)

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.
Options: Enabled (Default) / Disabled

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.
Options: 131000 (Default)

Energy Efficient P-state

This item enables or disables Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX [3] will read 0 indicating no support for Energy Efficient policy setting.
Options: Enabled (Default) / Disabled

Energy Efficient Turbo

This item enables or disables Energy Efficient Turbo feature. This feature will opportunistically lower the turbo frequency to increase efficiency.
Options: Enabled (Default) / Disabled

C states

This item enables or disables CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Options: Auto (Default) / Enabled / Disabled

Enhanced C-states

This item enables or disables C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
Options: Enabled (Default) / Disabled

C-States Auto Demotion

This item sets C-State Auto Demotion.
Options: C1 and C3 (Default) / C1 / C3/ Disabled

C-States Un-demotion

This item sets C-State Un-demotion.
Options: C1 and C3 (Default) / C1 / C3/ Disabled

Package C-State Demotion

This item sets Package C state Demotion.
Options: Disabled (Default) / Enabled

Package C-State Un-demotion

This item sets Package C-State Un-demotion.
Options: Disabled (Default) / Enabled

CState Pre-Wake

Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake.
Options: Enabled (Default) / Disabled

Package C State Limit

This item sets Package C State Limit.
Options: Auto (Default) / C0/C1 / C2 / C3 / C6 / C7 / C7S / C8 / C9 / C10 / CPU Default

Thermal Monitor

This item enables or disables Thermal Monitor.
Options: Enabled (Default) / Disabled

CFG Lock

This item confgire MSR 0xE2[15], CFG lock bit.
Options: Enabled (Default) / Disabled

RSR

This item enables or disables Reliability Stress Restrictor (RSR) feature.
Options: Enabled (Default) / Disabled

AC Loadline

AC Loadline defined in 1/100 m0hms. A value of 100=1.00 m0hm, and 1255 =12.55 m0hm. Range is 0-6249 (0-62.49 m0hms). 0=AUTO/HW default.
Options: 210 (Default)

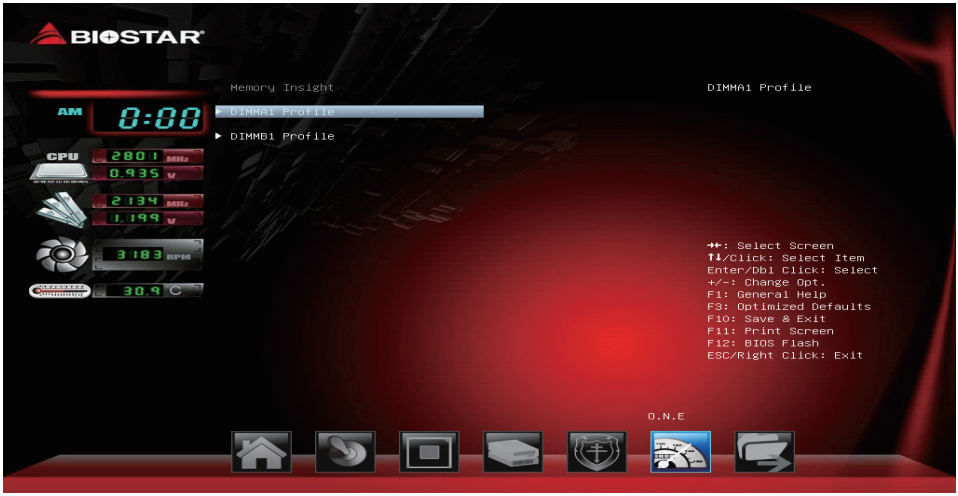
DC Loadline

DC Loadline defined in 1/100 m0hms. A value of 100=1.00 m0hm, and 1255 =12.55 m0hm. Range is 0-6249 (0-62.49 m0hms). 0=AUTO/HW default.
Options: 210 (Default)

FCLK Frequency for Early Power On

FCLK frequency can take values of 400MHz, 800MHz and 1GHz (1GHz not supported for ULT/ULX SKUs).
Options: 1GHz (Default) / Normal (800Mhz) / 400MHz

Memory Insight

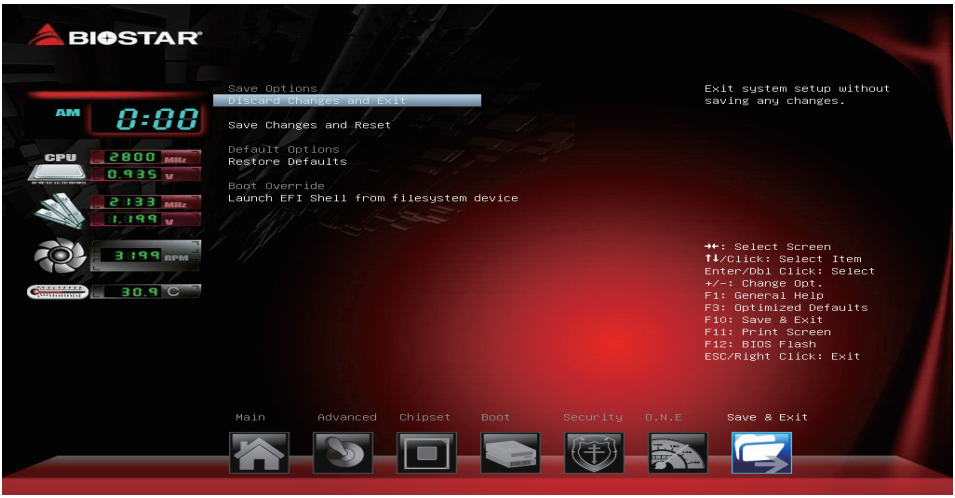


DIMM Profile

These items display memory information.

7. Exit Menu

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



Discard Changes and Exit

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

Save Changes and Reset

Reset the system after saving the changes.

Restore Defaults

This selection allows you to reload the BIOS when problem occurs during system booting sequence. These configurations are factory settings optimized for this system.