intel.

Intel® NUC Laptop Kit
Aptio V BIOS Glossary
Revision 1.1 – May 2021

intel.

Disclaimer

Intel Corporation disclaims all warranties and liabilities for the use of this document and the information contained herein and assumes no responsibility for any errors which may appear in this document. Intel makes no commitment to update the information contained herein and may make changes at any time without notice. There are no express or implied licenses granted there under to any intellectual property rights of Intel Corporation or others to design or fabricate Intel integrated circuits or integrated circuits based on the information in this document. Contact your local sales office to obtain the latest specifications before placing your order.

Information in this document is provided in connection with Intel products. Intel assumes no liability whatsoever, including infringement of any patent or copyright, for sale and use of Intel products except as provided in Intel's Terms and Conditions of Sale for such products. Intel retains the right to make changes to these specifications at any time, without notice. Intel processors and chipsets may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

HDMI is a registered trademark of HDMI Licensing, LLC.

DisplayPort is a trademark of VESA.

Bluetooth is a registered trademark of Bluetooth SIG, Inc.

PCI, PCIe, and PCI Express are trademarks of PCI-SIG.

* Other names and brands may be claimed as the property of others.

Contents

intel.

Introduction

The BIOS Setup program can be used to view and change the BIOS settings for the Intel® NUC Laptop Kit. BIOS Setup is accessed by pressing **F2** after the Power-On Self-Test (POST) memory test begins and before the operating system boot begins.

The presence of menus and BIOS settings are dependent on your Intel NUC Laptop Kit model, hardware components installed, and the BIOS version.

If any problems occur (poor performance, intermittent issues) after making BIOS settings changes, reset the BIOS to default values:

1. Press **F2** during boot to enter the BIOS Setup.
2. Press **F9** to set defaults.
3. Press **F10** to save and exit.

If the system locks or won't boot after making BIOS settings changes, perform a BIOS Recovery.

How to Read this Glossary

Type	Indicates the type of BIOS setting.
	• **Action:** BIOS takes a specific action when this is selected. There may be a confirmation prompt before the action is taken.
	• **Checkbox:** BIOS displays a checkbox that can be set or cleared.
	• **Information:** BIOS displays non-selectable text.
	• **Numeric:** BIOS displays a number that can be incremented, decremented, manually entered, or set with a slider bar.
	• **One-of:** BIOS displays a list of options and allows one to be selected.
	• **Ordered List:** BIOS displays a list of options that can be reordered.
	• **Password:** BIOS displays a window for the user to enter text. Each character entered is displayed as an asterisk character (*). If an invalid character is entered, the BIOS will beep and will not display an additional asterisk.
Range	Minimum and Maximum values that can be set (for Numeric questions).
Help	Help text that appears in the standard Help section of the Setup screen.
Advanced Help	Help text that appears in the Advanced Help pop-up window.
Requires	Lists requirements for this question to appear in BIOS Setup.
Aptio V BIOS Page	Indicates the BIOS page or menu where the setting is found.

intel.

Setup Hotkeys

F1	Opens the Advanced Help pop-up window for the selected question.
F3	Resets any change made on a setting back to its previous value
F9	Invokes a confirmation dialog to load default settings.
F10	Invokes a confirmation dialog to Exit and Save Changes.
Ctrl + Alt + Del	Restarts the system.
Arrow Left Arrow Right Arrow Up Arrow Down Tab Shift + Tab	Moves the cursor left/right/up/down one question. Will wrap if already at first or last question on the page. When selecting an option from a drop-down list, moves the cursor up/down one option.
Esc	**When selecting an option for a One-Of/Ordered List question:** Close option selection box and cancel changes. **When selecting a value for a Numeric question:** Cancel changes. **When viewing a Setup sub-screen page**: Return to parent Setup page. **When viewing a top-level Setup page:** Invoke confirmation dialog box to Exit Discarding Changes. **When viewing a confirmation dialog box:** Close confirmation dialog box without taking action. **When entering text into a Password/Text Entry window**: Close window and cancel changes.

intel.

Main

System Information

Manufacturer	System Manufacturer string from SMBIOS Type 1 structure.
Product Name	System Product Name string from SMBIOS Type 1 structure.
Version	System Version string from SMBIOS Type 1 structure.
Serial Number	System Serial Number string from SMBIOS Type 1 structure.
UUID	System UUID/GUID from SMBIOS Type 1 structure.
SKU Number	System SKU Number string from SMBIOS Type 1 structure.
Family	System Family string from SMBIOS Type 1 structure.

Board Information

Manufacturer	System Manufacturer string from SMBIOS Type 2 structure.
Product Name	System Product Name string from SMBIOS Type 2 structure.
Version	System Version string from SMBIOS Type 2 structure.
Serial Number	System Serial Number string from SMBIOS Type 2 structure.
Asset Tag	Board Asset Tag string from SMBIOS Type 2 structure.

Chassis Information

Manufacturer	System Manufacturer string from SMBIOS Type 3 structure.
Product Name	System Product Name string from SMBIOS Type 3 structure.
Version	System Version string from SMBIOS Type 3 structure.
Serial Number	System Serial Number string from SMBIOS Type 3 structure.
Asset Tag	Board Asset Tag string from SMBIOS Type 3 structure.

BIOS Version

Type	Information
Aptio V BIOS Page	Main

- Displays the current BIOS version.

Processor Type

Type	Information
Aptio V BIOS Page	Main

- Displays the processor brand.

Max Processor Turbo Frequency

Type	Information
Aptio V BIOS Page	Main

- Displays the max processor turbo frequency.

Max Processor Non Turbo Frequency

Type	Information
Aptio V BIOS Page	Main

- Displays the max processor non-turbo frequency.

Host Clock Frequency

Type	Information
Aptio V BIOS Page	Main

- Displays the default Host Clock Frequency.

L2 Cache

Type	Information
Aptio V BIOS Page	Main

- Displays the total L2 cache memory of the installed processor in megabytes. If the installed processor is multi- core, it is displayed as number of cores x L2 cache per core.

L3 Cache

Type	Information
Aptio V BIOS Page	Main

- Displays the total L3 cache memory of the installed processor in megabytes.

CPUID

Type	Information
Aptio V BIOS Page	Main

- Displays the processor CPUID in hexadecimal.

Microcode Update Revision

Type	Information
Aptio V BIOS Page	Main

- 32-bit processor microcode update revision in hexadecimal.

Total Memory Installed

Type	Information
Aptio V BIOS Page	Main

- Displays the total installed system memory size in gigabytes.

Memory Speed

Type	Information
Aptio V BIOS Page	Main

- Displays the current memory speed. Defined as Current Host Clock Frequency x Memory Reference Multiplier x Memory Multiplier.

SODIMM *n*

Type	Information
Aptio V BIOS Page	Main

- Displays the installed system memory size in SODIMM *n* in gigabytes. One of these lines is displayed for each memory slot present on the motherboard.

Intel® ME FW Version

Type	Information
Requires	ME is present and running
Aptio V BIOS Page	Main

- Displays ME Firmware Version.

EC FW Version

Type	Information
Requires	EC is present on the system
Aptio V BIOS Page	Main

Onboard LAN MAC Address

Type	Information
Aptio V BIOS Page	Main

- MAC Address of onboard LAN device in hexadecimal.

NVIDIA GPU Type

Type	Information
Aptio V BIOS Page	Main

- Displays the manufacturer/model of the Nvidia GPU solution.

NVIDIA GPU VBIOS Version

Type	Information
Aptio V BIOS Page	Main

- Displays the VBIOS version of the Nvidia GPU solution.

System Language

Type	Information
Aptio V BIOS Page	Main

- Displays the system BIOS default language. Currently, only English.

System Date and Time:

- Displays the current time and date in format: MM/DD/YYYY HH:MM:SS XM

Advanced > Storage

SATA Controller(s)

Type	One-of
Enabled	Enables the onboard SATA controller(s)
Disabled	Disables the onboard SATA controller(s)
Aptio V BIOS Page	Advanced > Storage

SATA Mode Selection

Type	One-of
AHCI	PCH SATA controller is configured in AHCI mode.
RAID	PCH SATA controller is configured in RAID mode.
Intel RST Premium With Intel Optane System	PCH SATA controller is configured in Optane mode.
Help	Configures the Chipset SATA controller mode. Warning: OS may not boot if this setting is changed after OS install.
Advanced Help	**AHCI:** Supports advanced SATA features such as Native Command Queuing. **RAID:** Allows multiple drives to be merged into larger volumes for increased performance and/or reliability. Always enables AHCI. **Intel RST Premium With Intel Optane System Acceleration:** Fast Boot will be Grayed-out and disabled under Optane mode. **Warning:** OS may not boot if this setting is changed after OS install.
Requires	Intel RST Premium With Intel Optane System Acceleration will be Grayed-out and not able to be selected when Fast Boot is enabled.
Aptio V BIOS Page	Advanced > Storage

- If a USB keyboard is attached to a USB port that has been disabled via one of these Setup questions, it will be enabled during POST and Setup, but will be disabled before OS boot.
- All non-keyboard devices will be disabled during POST, Setup, and OS. This means that drives attached to disabled USB ports will not appear in the BIOS boot order in Setup.
- If the Portable Device Charging Mode for a USB port is set to Charging Only, then a keyboard attached to that port will not be functional, even during POST.

M.2 Slot x RST PCIe Storage Remapping

Type	One-of
Help	Configures the PCIe storage remapping. **Warning**: OS may not boot if this setting is changed after an OS install and a RAID volume is not configured.
Requires	The Chipset SATA controller supports the PCIe storage remapping. Chipset SATA Mode is set to RAID. Remapping is enabled and grey out if Optane mode in Chipset SATA mode is set.
Aptio V BIOS Page	Advanced > Storage

M.2 Port x

Type	One-of
Help	Enables or Disables M.2 Port.
Aptio V BIOS Page	Advanced > Storage

M.2 Slot x

Type	Information
Aptio V BIOS Page	Advanced > Storage

- Displays the manufacturer/model of the M.2 device installed

M.2 Slot x Vendor ID:Device ID:Port

Type	Information
Aptio V BIOS Page	Advanced > Storage

- Displays the vendor ID of the M.2 device(s) installed

Hard Disk Pre-Delay

Type	Numeric
Help	Delay (in seconds) before hard drives are initialized. This can be used to increase the amount of time that the BIOS Splash Screen displays.
Aptio V BIOS Page	Advanced > Storage

SMART Self-Test

Type	Checkbox / One-of
Help	Enables or Disables S.M.A.R.T - Self-Monitoring, Analysis, and Reporting Technology. If supported on any attached drives, BIOS will monitor drive health.
Aptio V BIOS Page	Advanced > Storage

Advanced > Onboard Devices

HD Audio

Type	One-of
Disabled	Disables HD audio
Enabled	Enables HD audio
Auto	
Aptio V BIOS Page	Advanced > Onboard Devices

LAN

Type	One-of
Disabled	Disables the onboard Ethernet LAN controller
Enabled	Enables the onboard Ethernet LAN controller
Aptio V BIOS Page	Advanced > Onboard Devices

Thunderbolt™ Support

Type	One-of
Disabled	Disables the onboard Thunderbolt controller
Enabled	Enables the onboard Thunderbolt controller
Aptio V BIOS Page	Advanced > Onboard Devices

WLAN

Type	Checkbox / One-of
Help	Enables or Disables the onboard Wireless LAN Controller.
Aptio V BIOS Page	Advanced > Onboard Devices

Bluetooth

Type	Checkbox / One-of
Help	Enables or Disables the onboard Bluetooth Controller.
Aptio V BIOS Page	Advanced > Onboard Devices

SDCard 3.0 Controller

Type	One-of
Disabled	
Enabled	
Aptio V BIOS Page	Advanced > Onboard Devices

Gaussian Mixture Models and Neural Networks Accelerator (GNA)

Type	One-of
Disabled	
Enabled	
Help	Enables or Disables the GNA functionality.
Aptio V BIOS Page	Advanced > Onboard Devices

Failsafe Watchdog

Type	Checkbox / One-of
Help	After a boot failure, uses BIOS defaults to allow the system to boot back into BIOS Setup while retaining the last used BIOS Setup values set by the user.
Aptio V BIOS Page	Advanced > Onboard Devices

Visual Numberpad

Type	One-of
Help	Turns the Virtual Numpad on or off.
Aptio V BIOS Page	Advanced > Onboard Devices

intel.

Webcam

Type	One-of
Disabled	
Enabled	
Help	Enables or Disables the webcam.
Aptio V BIOS Page	Advanced > Onboard Devices

Advanced > USB

Legacy USB Support

Type	One-of
Enabled	USB Legacy allows USB support under non-USB-aware OSes.
Disabled	Disabling USB Legacy will not disable USB keyboards during BIOS POST, including
Auto	Disables legacy support if no USB devices are connected.
Aptio V BIOS Page	Advanced > USB

Left USB Port / Right USB Rear Port / Rear USB Front Port

Type	One-of
Enable	Enables USB port
Disable	Disables USB port
No Detect	Disables USB port during POST only
Help	*Help is specific to each supported motherboard header/back panel port layout.*
Advanced Help	**Enable**: All devices on this port will be available to BIOS and OS. **Disable:** USB keyboard/Mouse will be available to BIOS, and all devices on this port will be unavailable to OS. **No Detect:** No devices on this port will be detected by BIOS, but all will be available to OS. Use this option to speed up BIOS boot.
Requires	Grayed out and set to **Disable** if corresponding **Portable Device Charging** question is set to **Charging Only**
Aptio V BIOS Page	Advanced > USB

- One of these questions is displayed for each USB port present on the motherboard.
- If a USB keyboard is attached to a USB port that has been disabled via one of these Setup questions, it will be enabled during POST and Setup, but will be disabled before OS boot.
- All non-keyboard devices will be disabled during POST, Setup, and OS. This means that drives attached to disabled USB ports will not appear in the BIOS boot order in Setup.
- If the Portable Device Charging Mode for a USB port is set to Charging Only, then a keyboard attached to that port will not be functional, even during POST.

intel.

Advanced > Video

IGD Minimum Memory

Type	One-of
32 MB	
64 MB	
128 MB	Note: Kaby Lake platform does not support 128 MB option.
Aptio V BIOS Page	Advanced > Video

IGD Aperture Size

Type	One-of
128 MB	
256 MB	
512 MB	
1024 MB	Platform memory address space resource dependent. BIOS may hide this option if memory address space is not enough.
2048 MB	UEFI mode only. Platform memory address space resource dependent. BIOS may hide this option if memory address space is not enough.
Help	Selects the aperture size for the Integrated Graphics Device (IGD). Requires motherboard supports at least one video port tied to an Intel Graphics Device (IGD).
Aptio V BIOS Page	Advanced > Video

Advanced > Add-In Config

Information about Wi-Fi and/or LAN, RAID configuration options and preferences for onboard or add-in devices.

Advanced > Event Log

SMBIOS Event Log

Type	One-of
Enabled	
Disabled	
Help	Enables or Disables Event Logging. If Enabled, BIOS will log POST Errors in NVRAM.
Aptio V BIOS Page	Advanced > Event Logs > Change SMBIOS Event Log Settings

Erase Event Log

Type	One-of
No	
Yes, Next reset	
Yes, Every reset	
Help	Choose option for erasing SMBIOS event logs. Erasing is done prior to any logging activation during reset.
Aptio V BIOS Page	Advanced > Event Logs > Change SMBIOS Event Log Settings

When Log is Full

Type	One-of
Do nothing	
Erase immediately	
Help	Choose option for reactions to a full event log.
Aptio V BIOS Page	Advanced > Event Logs > Change SMBIOS Event Log Settings

View SMBIOS Event Log

Type	Information
Aptio V BIOS Page	Advanced > Event Logs > View SMBIOS Event Log

- A line is displayed for each Event Type with a non-zero occurrence value.
- *Timestamp* is the time and date of the most recent occurrence of the event. It is displayed in the format MM/DD/ YYYY HH:MM:SS
- *Error code* is the name of the POST Error.
- *Count* is the number of times that event has occurred since the Event Log was last cleared.

Advanced > Undervolting

Core Voltage Offset

Type	Numeric
Help	Specifies the offset voltage applied to the IA Core domain, in millivolts. Use the + or – key to adjust in increments of 10.
Aptio V BIOS Page	Advanced > Undervolting

GT Voltage Offset

Type	Numeric
Help	Specifies the offset voltage applied to the GT domain, in millivolts. Use the + or – key to adjust in increments of 10.
Aptio V BIOS Page	Advanced > Undervolting

GTU Voltage Offset

Type	Numeric
Help	Specifies the offset voltage applied to the GTU domain, in millivolts. Use the + or – key to adjust in increments of 10.
Aptio V BIOS Page	Advanced > Undervolting

Power Mode

Type	One-of
Performance	
Balanced	
Battery Saver	
Help	Configures the system power mode.
Aptio V BIOS Page	Advanced > Undervolting

Intel Speed Shift Technology

Type	One-of
Disabled	
Enabled	
Help	Enable or disable Intel Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controller P-states.
Aptio V BIOS Page	Advanced > Undervolting

Advanced > Battery

Design Capacity

Type	Information
Help	Defines the typical capacity of the battery when new.
Aptio V BIOS Page	Advanced > Battery

Battery Health

Type	Information
Help	Specifies the health of the battery from the following choices: • Normal • Fair • Low
Aptio V BIOS Page	Advanced > Battery

Battery Mode

Type	Information
Help	Displays the current charge information for the battery. Charging or Discharging.
Aptio V BIOS Page	Advanced > Battery

Advanced > Fan

Minimum Fan Duty Cycle

Type	Numeric
Range	0-100
Help	Selects the minimum duty cycle that the fan will never go below.
Aptio V BIOS Page	Advanced > Fan

Disable Passive Cooling Mode

Type	One-of
Disabled	
Enabled	
Aptio V BIOS Page	Advanced > Fan

intel.

Advanced > Auto RTC Reset

Auto RTC Reset

Type	Checkbox
Help	If the system is reset by the watchdog timer three times and still cannot boot, the system will proceed with a BIOS recovery.
Aptio V BIOS Page	Advanced > Auto RTC Reset

Performance

Host Clock Frequency

Type	Information
Aptio V BIOS Page	Performance

- Displays the default Host Clock Frequency.

Max Processor Turbo Frequency

Type	Information
Aptio V BIOS Page	Performance

- Displays the max processor turbo frequency.

Max Processor Non-Turbo Frequency

Type	Information
Aptio V BIOS Page	Performance

- Displays the max processor non-turbo frequency.

Processor Ring Frequency

Type	Information
Aptio V BIOS Page	Performance

- This information line is constructed from the calculation of the Processor Ring Frequency (Host Clock Frequency x Processor Ring Max Multiplier).

Intel Graphics Dynamic Frequency

Type	Information
Aptio V BIOS Page	Performance

Total Memory Installed

Type	Information
Aptio V BIOS Page	Advanced > Performance > Memory
Aptio V BIOS Page	Performance

- Displays the total installed system memory size in gigabytes.

Memory Speed

Type	Information
Requires	Host Clock Frequency, Memory Reference Multiplier, and Memory Multiplier have not been overridden.
Aptio V BIOS Page	Advanced > Performance > Memory
Aptio V BIOS Page	Performance

- Displays the current memory speed. Defined as Current Host Clock Frequency x Memory Reference Multiplier x Memory Multiplier.

Memory Clock

Type	Information
Aptio V BIOS Page	Performance

SODIMM *n*

Type	Information
Aptio V BIOS Page	Advanced > Performance > Memory
Aptio V BIOS Page	Performance

- Displays the installed system memory size in SODIMM *n* in gigabytes.
- One of these lines is displayed for each memory slot present on the motherboard.
- DIMM numbering is based on the suggested order of memory loading and should match the label on the board silkscreen.

Memory Voltage

Type	Information
Aptio V BIOS Page	Performance

- Display the current memory voltage.

Performance > Processor

Hyper-Threading

Type	One-of
Enabled	
Disabled	
Help	When disabled, only one thread per active core will be available.
Requires	Enabled and grayed-out if **Intel® Trusted Execution Technology** is set to **Enable**
Aptio V BIOS Page	Performance > Processor

Intel® Turbo Boost Technology

Type	Checkbox / One-of
Help	Enable to automatically allow processor cores to run faster than the base operating frequency when running below power, current, and temperature limits.

Advanced Help	Enable to automatically allow processor cores to run faster than the base operating frequency when running below power, current, and temperature limits. Disable to limit processor speed based on Maximum Non-Turbo Ratio. Enabling Intel® Turbo Boost Technology will also Enable Enhanced Intel SpeedStep® Technology.
Requires	Hidden if processor does not support Intel® Turbo Boost Technology
Aptio V BIOS Page	Performance > Processor

Active Processor Cores

Type	One-of
ALL	Enables all available Cores in the Processor.
1	Enables only 1 Core in the Processor.
2	Enables 2 Cores in a multi-core Processor.
3	Enables 3 Cores in a multi-core Processor.
4	Enables 4 Cores in a multi-core Processor.
5	Enables 5 Cores in a multi-core Processor.
6	Enables 6 Cores in a multi-core Processor.
7	Enables 7 Cores in a multi-core Processor.
Help	Number of cores to enable in each processor package
Requires	Set to **ALL** and grayed-out if **Intel® Trusted Execution Technology** is set to **Enable**
Aptio V BIOS Page	Performance > Processor

Intel Speed Shift Technology

Type	One-of
Disabled	
Enabled	
Help	Enable or disable Intel Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controller P-states.
Aptio V BIOS Page	Advanced > Performance > Processor

Security

- Valid length for passwords is 2 to 20 characters.
- Valid characters for passwords are case-sensitive alpha-numeric: 0-9, A-Z, a-z.

Supervisor Password

Type	Information
Installed	
Not Installed	
Aptio V BIOS Page	Security

- Displays whether a supervisor password has been set.

User Password

Type	Information
Installed	
Not Installed	

Aptio V BIOS Page	Security

- Displays whether a user password has been set.

[Set] Administrator Password

Type	Password
Text Entry Prompt	Please type in your password
Text Entry Prompt	Please type in your new password
Text Entry Prompt	Please confirm your new password
Help	Passwords must be between 2 and 20 characters and are case sensitive.
Advanced Help	Fast Boot will be disabled if a User Password is installed.
Aptio V BIOS Page	Security

- The first Text Entry Prompt is only used when attempting to change a password that is already installed.
- To delete an existing Supervisor password, enter a blank password after entering
  the existing Supervisor password.

[Set] User Password

Type	Password
Text Entry Prompt	Please type in your password
Text Entry Prompt	Please type in your new password
Text Entry Prompt	Please confirm your new password
Help	Passwords must be between 2 and 20 characters and are case sensitive. If a User Password is created, it must be entered each boot before OS access.
Advanced Help	Fast Boot will be disabled if a User Password is installed.
Aptio V BIOS Page	Security

- The first Text Entry Prompt is only used when attempting to change a password that is already installed.
- To delete an existing User password, enter a blank password after entering the existing User password.

TCG Storage Security Configuration

- Security Subsystem Class
- Security Supported
- Security Enabled
- Security Locked
- Security Frozen
- User Pwd Status
- Admin Pwd Status

Type	Information
Aptio V BIOS Page	Security > TCG Storage Security Configuration

- Displays the current status of these security features.

Set Admin Password

Type	Password
Text Entry Prompt	Please type in your password
Text Entry Prompt	Please type in your new password
Text Entry Prompt	Please confirm your new password
Confirmation Prompt	Hard Drive Passwords are not recoverable and cannot be removed without an original password. The drive will remain inaccessible unless the User or Master Hard Drive
Help	Passwords must be between 2 and 19 case-sensitive alpha-numeric characters. If a User Hard Drive Password is created, it must be entered each boot before OS access.
Advanced Help	The drive must be attached to Chipset SATA Port 0 and in either IDE or ACHI Mode.
Requires	Hidden if there is not a Hard Drive attached to Chipset SATA Port 0 or Chipset SATA Mode is not IDE or AHCI.
Aptio V BIOS Page	Security > HDD Password Configuration

- The first Text Entry Prompt is only used when attempting to change a password that is already installed.
- To delete an existing Hard Drive password, enter a blank password after entering the existing Hard Drive password.

Set User Password

Type	Password
Text Entry Prompt	Please type in your password
Text Entry Prompt	Please type in your new password
Text Entry Prompt	Please confirm your new password
Confirmation Prompt	Hard Drive Passwords are not recoverable and cannot be removed without an original password. The drive will remain inaccessible unless the User or Master Hard Drive
Help	Passwords must be between 2 and 19 case-sensitive alpha-numeric characters. The Master Hard Drive password is only used to unlock a drive if the User Hard Drive password is forgotten.
Advanced Help	The Master Hard Drive password does not lock a drive by itself. The drive must be attached to Chipset SATA Port 0 and in either IDE or ACHI Mode.
Requires	Hidden if there is not a Hard Drive attached to Chipset SATA Port 0 or Chipset SATA Mode is not IDE or AHCI.
Aptio V BIOS Page	Security > HDD Password Configuration

- The first Text Entry Prompt is only used when attempting to change a password that is already installed.
- To delete an existing Master Hard Drive password, enter a blank password after entering the existing Master Hard Drive password.

Security > Security Features

Allow UEFI 3rd Party Driver Loaded

Type	Checkbox
Help	**Enable**: Allow UEFI 3rd party driver to be loaded during Boot Device Selection (BDS) stage. **Disable**: Prohibit UEFI 3rd party driver to be loaded during BDS stage.
Aptio V BIOS Page	Security > Security Features

Intel® Virtualization Technology

Type	Checkbox
Help	Enables or Disables features that provide hardware support for virtualization. Requires power cycling and specific hardware/software installed to take effect.
Requires	Processor supports VT. Enabled and grayed-out if Intel® Trusted Execution Technology is set to Enable.
Aptio V BIOS Page	Security > Security Features

Intel® VT for Directed I/O (VT-d)

Type	Checkbox
Help	Enables or Disables Intel® VT for Directed I/O (VT-d) which provides additional hardware support for managing I/O virtualization. If Enabled, BIOS will publish a DMA Remapping ACPI table.
Requires	Processor and chipset combination support VT-d. Enabled and grayed-out if Intel® Trusted Execution Technology is set to Enable
Aptio V BIOS Page	Security > Security Features

Fixed Disk Boot Sector

Type	One-of
Normal	BIOS will allow writes to the MBR on fixed disks.
Write Protect	BIOS will block writes to the MBR on fixed disks.
Help	Write Protect provides some Master Boot Record protection. Set to Normal while installing an operating system.
Advanced Help	Only applicable to Legacy BIOS interfaces.
Aptio V BIOS Page	Security > Security Features

Intel® Software Guard Extensions (SGX)

Type	One-of
Disabled	Hides all SGX related items: **SGX Owner EPOCH, Reset SGX Owner EPOCHs to Factory Default, and SGX Reserved Memory Size.**
Enabled	Enable SGX.
Software Controlled	Grayed-out and set **SGX Reserved Memory Size** to **<Auto>.**
Help	Enables or Disables Intel® Software Guard Extensions (SGX). Software Controlled: SGX is disabled initially. When SGX application and ME FW driver are installed, SGX will be enabled via a UEFI OS-BIOS runtime interface.
Aptio V BIOS Page	Security > Security Features

intel.

SGX Owner EPOCHs

Type	One-of
Factory Default	Use factory default Owner EPOCHs. .
New Random Owner EPOCHs	Generate a new random Owner EPOCHs on next boot. Display Reset SGX Owner EPOCHs to Factory Default setup item from next boot. Display New Radom SGX Owner EPOCHs is activated if new random EPOCH is used. Hide SGX Owner EPOCHs item from next boot.
User Defined Owner EPOCHs	Extract the customer defined EPOCHs value from EPOCH variable on next boot. Display Please install 128 bit EPOCH to "EPOCH" UEFI variable. Display Reset SGX Owner EPOCHs to Factory Default item on next boot. Display User Defined SGX Owner EPOCHs is activated if user defined EPOCHs value is used. Hide SGX Owner EPOCHs item from next boot.
Help	Keep or change the SGX Owner EPOCHs value. SGX sealing key is derived from Owner EPOCHs. Warning: after change the Owner EPOCH value, previously Intel SGX sealed data cannot be accessed.
Advanced Help	Factory Default to use default Owner EPOCH value. New Random Owner EPOCHs to generate and use a new random Owner EPOCHs. User Defined Owner EPOCHs will extract customer defined EPOCHs value from EPOCH variable.
Requires	Hide if **Intel® Software Guard Extensions (SGX)** set to **<Disabled>.** Hide if new random owner EPOCHs or user defined owner EPOCHs is activated.
Aptio V BIOS Page	Security > Security Features

SGX Reserved Memory Size

Type	One-of
32MB	
64MB	
128MB	
Help	Configure the SGX Reserved Memory Size.
Requires	Platform supports SGX. Gray-out if Intel® Software Guard Extensions (SGX) set to <Software Controlled>. Hide if Intel® Software Guard Extensions (SGX) set to <Disabled>.
Aptio V BIOS Page	Security > Security Features

Intel® Platform Trust Technology

Type	Checkbox
Help	Enables or Disables Intel® Platform Trust Technology.
Requires	Boards does not stuff discrete TPM 2.0. Cleared and grayed-out if Intel® Trusted Execution Technology is set to Enable
Aptio V BIOS Page	Security > Security Features

iSetupCfg Password Check

Type	One-of
Enabled	
Bypass	

Temporarily Bypass	
Help	Configuring the BIOS Setup via iSetupCfg requires BIOS Admin/Supervisor password for access. **Enable**: Actual BIOS Admin/Supervisor password is required. **Bypass or Temporarily Bypass**: a 'dummy' Admin password is accepted.
Aptio V BIOS Page	Security > Security Features

Thunderbolt Security Level

Type	One-of
Legacy Mode	No security - allows legacy Thunderbolt devices to auto connect
Unique ID	User Authorization - the connection manager requests connection approval from the host software; auto approval may be given based on the unique ID of the connecting
One time saved key	Secure Connect - the connection manager requests connection approval from the host software; auto approval is only given if the host challenge to the device acceptable.
DP++ only	Display Port Only - allows only DP sinks to be connected.
Help	Configures the Thunderbolt security level
Aptio V BIOS Page	Security > Security Features

Power

After Power Failure

Type	One-of
Stay Off	System will stay in power-off state after AC power restore.
Last State	System will return to last power state before AC power lost.
Power On	System will automatically power-on after AC power is restored.
Help	Configures system behavior after AC power is lost.
Advanced Help	If set to Stay Off, the System will stay in a power-off state after AC power is restored. If set to Last State, the System will return to the last power state before AC power was lost. If set to Power On, the System will automatically power-on after AC power is restored.
Aptio V BIOS Page	Power

Wake on LAN from S4/S5

Type	One-of
Stay Off	System will not wake from S4/S5 power state if Wake on LAN packet is received.
Power On – Normal Boot	System will wake from S4/S5 power state if Wake on LAN packet is received. BIOS will follow normal boot order.
Power On – PXE Boot	System will wake from S4/S5 power state if Wake on LAN packet is received. BIOS will attempt to boot to PXE. If PXE boot fails, BIOS will attempt to boot to other devices according to normal boot order.
Help	Configures behavior when Wake on LAN packet is received during S4/S5. Wake on LAN must also be enabled in OS LAN driver.
Advanced Help	**Stay Off -** System will not wake. **Power On - Normal Boot:** System will wake and use normal boot order. **Power On - PXE Boot**: System will wake and attempt boot to PXE.

Aptio V BIOS Page	Power

Battery Charge Top Limit

Type	One-of
100%	
90%	
80%	
70%	
60%	
Help	Allows you to select when the battery will stop charging. For example, if you select 80%, the battery stops charging when it becomes 80% full.
Aptio V BIOS Page	Power

Wake System from S5

Type	Checkbox
Help	Enables or Disables Wake System from S5. If Enabled, system will wake at the selected date/time via RTC alarm.
Requires	Grayed-out and disabled if **Intel® Rapid Start Technology** is enabled.
Aptio V BIOS Page	Power

Recurrence when Wake System from S5 is Selected

Type	One-of
Monthly	System will wake at the selected date/time via RTC alarm monthly.
Weekly	System will wake at the selected week day/time via RTC alarm weekly.
Daily	System will wake at the selected time daily.
Help	Select Daily/Weekly/Monthly to wake the system.
Requires	**Wake System from S5** is set to **Enable**
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

Sunday / Monday / Tuesday / Wednesday / Thursday / Friday / Saturday

Type	Checkbox
Help	If enabled, system will wake at the selected time via RTC alarm on the day selected.
Requires	**Wake System from S5** is set to **Enable.** **Recurrence is set to Weekly.**
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

Wakeup Date

Type	Numeric
Range	0-31
Help	Select day of each month to wake the system. Select 0 for daily wakeup.
Requires	**Wake System from S5** is set to **Enable.** Recurrence is set to Monthly.
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

Wakeup Hour

Type	Numeric
Range	0-23
Help	Select wakeup hour in 24-hour format. For example, 15 means 3 PM.
Requires	**Wake System from S5** is set to **Enable**
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

Wakeup Minute

Type	Numeric
Range	0-59
Help	Select wakeup minute.
Requires	**Wake System from S5** is set to **Enable**
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

Wakeup Second

Type	Numeric
Range	0-59
Help	Select wakeup second.
Requires	**Wake System from S5** is set to **Enable**
Aptio V BIOS Page	Advanced > Power > Secondary Power Settings

DeepSx Power Policies

Type	One-of
Disabled	
Enabled in S4-Battery	
Enabled in S5-Battery	
Enabled in S4	
Enabled in S5	
Help	Configure the DeepSx Mode configurations
Aptio V BIOS Page	Advanced > Power

Boot

Secure Boot / UEFI Boot / Legacy Boot

Type	Information
Aptio V BIOS Page	Boot

- Displays if these boot modes are enabled or disabled.

System Mode

Type	Information
Aptio V BIOS Page	Boot > Secure Boot

- Displays the current secure boot mode.

intel.

Secure Boot

Type	One-of
Enabled	
Disabled	
Help	If Enabled, BIOS will only boot to trusted operating system images. Secure Boot is supported only via UEFI Boot.
Advanced Help	Enabling Secure Boot will allow boot only to trusted operating system installations. Enabling Secure Boot will also enable UEFI Boot and disable Legacy Boot.
Requires	Disabled if **UEFI Boot** is Disabled. Disabled if Legacy Boot is Enabled.
Aptio V BIOS Page	Boot > Secure Boot

Secure Boot Mode

Type	One-of
Standard	
Custom	
Help	In Custom mode, Secure Boot policy variables can be configured by a physically present user without full authentication.
Aptio V BIOS Page	Boot > Secure Boot

Restore Factory Keys

Type	Action
Help	Installs factory defaults.
Requires	Secure Boot Mode is set to **Custom**.
Aptio V BIOS Page	Boot > Secure Boot

Reset To Setup Mode

Type	Action
Help	Deletes all variables and resets the system to Setup Mode.
Requires	Secure Boot Mode is set to **Custom**.
Aptio V BIOS Page	Boot > Secure Boot

UEFI Boot

Type	Checkbox
Help	If Enabled, BIOS will attempt to boot via UEFI before using the legacy boot sequence. UEFI Boot must be enabled in order to boot to a drive larger than 2 TB (terabytes).
Advanced Help	If both UEFI Boot and Legacy Boot are enabled, BIOS will attempt to boot via UEFI before using the legacy boot sequence. Enabling Secure Boot will also enable UEFI Boot and disable Legacy Boot.
Requires	Enabled if **Legacy Boot** is Disabled. Enabled if Secure Boot is Enabled.
Aptio V BIOS Page	Boot > Boot Priority

intel.

Legacy Boot

Type	Checkbox
Help	If Enabled, BIOS can attempt to boot via the legacy (non-UEFI) boot sequence.
Advanced Help	If both UEFI Boot and Legacy Boot are enabled, BIOS will attempt to boot via UEFI before using the legacy boot sequence. Enabling Secure Boot will also enable UEFI Boot and disable Legacy Boot.
Requires	Enabled if UEFI Boot is Disabled. Disabled if Secure Boot is Enabled. Disabled and gray out if Optane mode in Chipset SATA mode and RST PCIe Storage Remapping are set for Optane support.
Aptio V BIOS Page	Boot > Boot Priority

Boot Option

Type	Ordered List
Help	Select the boot order for all detected bootable devices.
Requires	Hidden if **UEFI Boot** is Disabled
Aptio V BIOS Page	Boot > Boot Priority

- All detected UEFI boot options will be included in the list.
- The user can change the order of boot options within the list.
- The BIOS will attempt to boot to each option in the order of this list.

Fast Boot

Type	Checkbox
Help	If Enabled, Boot from Network/Optical/Removable Devices and RAID configuration will be disabled. In addition, Video and USB devices (keyboards and drives) will not be available until after OS boot.
Advanced Help	This feature cannot be enabled while a User Password or Hard Disk Drive Password is installed, and when Chipset SATA Mode set to Intel RST Premium With Intel Optane System Acceleration. This feature does not affect USB and video capabilities after OS boot. In order to disable Fast Boot without entering BIOS Setup: Power down the system, then hold down the power button until the system beeps.
Requires	Fast Boot will be Grayed-out and Disabled if Chipset SATA Mode set to Intel RST Premium With Intel Optane System Acceleration.
Aptio V BIOS Page	Boot > Boot Priority

Boot USB Devices First

Type	Checkbox
Help	If Enabled, the BIOS will attempt to boot to supported USB devices before any other devices. If Disabled, the normal boot order will be used.
Requires	Grayed-out and set to **Disable** if **Fast Boot** is set to **Enable**
Aptio V BIOS Page	Boot > Boot Priority

Boot Network Devices Last

Type	Checkbox
Help	If Enabled, Network devices will always be placed after non-Network devices in the boot priority. If Disabled, Network devices can be placed at any position in the boot priority but will default to last.
Aptio V BIOS Page	Boot > Boot Priority

Unlimited Boot to Network Attempts

Type	Checkbox
Help	If Enabled, network devices will receive unlimited boot attempts after the normal boot order has been exhausted. If Disabled, each boot device will only receive a single boot attempt.
Aptio V BIOS Page	Boot > Boot Priority

BIOS Setup Auto-Entry

Type	Checkbox
Help	If set to Enable, BIOS will halt and prompt to boot normally or enter Setup. This must be set to Disable to allow OS boot without user intervention.
Advanced Help	This feature is not available while Fast Boot USB Optimization is set to Enable.
Requires	Grayed-out and set to **Disable** if **Fast Boot** is set to **Enable**.
Aptio V BIOS Page	Boot > Boot Priority

Internal UEFI Shell

Type	Checkbox
Help	Enables or Disables the Internal UEFI Shell.
Requires	Grayed-out and Disabled if **Secure Boot** is **Enabled**
Aptio V BIOS Page	Boot > Boot Priority

USB

Type	Checkbox
Help	Enables or Disables the ability to boot from supported USB devices.
Requires	Grayed-out and Disabled if **Fast Boot** is **Enabled**
Aptio V BIOS Page	Boot > Boot Priority

Optical

Type	Checkbox
Help	Enables or Disables the ability to boot to Optical devices.
Requires	Grayed-out and Disabled if **Fast Boo**t is **Enabled**
Aptio V BIOS Page	Boot > Boot Priority

Network Boot

Type	One-of
Disable	Disable network boot.
Legacy PXE	Enable PXE boot in legacy boot.

intel.

Legacy iSCSI	Enable iSCSI boot in legacy boot.
UEFI PXE & iSCSI	Enable iSCSI and PXE boot in UEFI boot for platform supports both UEFI PXE and iSCSI boot.
UEFI PXE	Enable PXE boot in UEFI boot for platform does not support UEFI iSCSI boot.
Help	Enables or Disables the ability to boot from the network. Note: UEFI network boot option is automatically disabled if Legacy Boot setting is enabled.
Requires	Hide Legacy PXE option if Legacy Boot is set to Disabled. Hide Legacy iSCSI option if Legacy Boot is set to Disabled. Hide UEFI PXE & iSCSI option if Legacy Boot is set to Enabled or UEFI Boot is set to Disabled. Legacy PXE and Legacy iSCSI options in current value must switch to UEFI PXE & iSCSI option automatically if switching from Legacy Boot to UEFI Boot. UEFI PXE & iSCSI option in current value must switch to Legacy PXE option if Legacy Boot is enabled.
Aptio V BIOS Page	Boot > Boot Priority

Suppress Alert Messages At Boot

Type	Checkbox
Help	If enabled, BIOS will display POST error messages for five seconds without requiring user action (keyboard input) before continuing to boot. Subsequent error messages of the same type will be suppressed from the display but recorded in the Event Log.
Aptio V BIOS Page	Boot > Boot Display Configuration

POST Function Hotkeys Displayed

Type	Checkbox
Help	If set to Enable, BIOS will display Function key prompts during POST. Function key input will still be accepted even if prompts are disabled.
Aptio V BIOS Page	Boot > Boot Display Configuration

Display F2 to Enter Setup

Type	Checkbox
Help	If set to Enable, BIOS will display "F2 to Enter Setup" prompt. F2 key input will still be accepted if this prompt is disabled.
Requires	**POST Function Hotkeys Displayed** is set to **Enable**
Aptio V BIOS Page	Boot > Boot Display Configuration

Display F7 to Update BIOS

Type	Checkbox
Help	If set to Enable, BIOS will display "F7 to Update BIOS" prompt. F7 key input will still be accepted if this prompt is disabled.
Requires	**POST Function Hotkeys Displayed** is set to **Enable**
Aptio V BIOS Page	Boot > Boot Display Configuration

Display F10 to Enter Boot Menu

Type	Checkbox

Help	If set to Enable, BIOS will display "F10 to Enter Boot Menu" prompt. F10 key input will still be accepted if this prompt is disabled.
Requires	**POST Function Hotkeys Displayed** is set to **Enable**
Aptio V BIOS Page	Boot > Boot Display Configuration

Display F12 for Network Boot

Type	Checkbox
Help	If set to Enable, BIOS will display "F12 for Network Boot" prompt. F12 key input will still be accepted if this prompt is disabled.
Requires	**POST Function Hotkeys Displayed** is set to **Enable**
Aptio V BIOS Page	Boot > Boot Display Configuration

Enable Fn Lock+Esc

Type	One-of
Enabled	Function keys work as standard functions (such as F2, F7, etc.).
Disabled	The alternate function of the key works (such as audio level increase, screen brightness adjustment, etc.)
Aptio V BIOS Page	Boot