DGX Spark UEFI User Guide

NVIDIA Corporation

Nov 13, 2025

UEFI Settings

This guide is also available for download as a PDF.

Chapter 1. Introduction

This guide describes usage of the DGX Spark Unified Extensible Firmware Interface (UEFI).

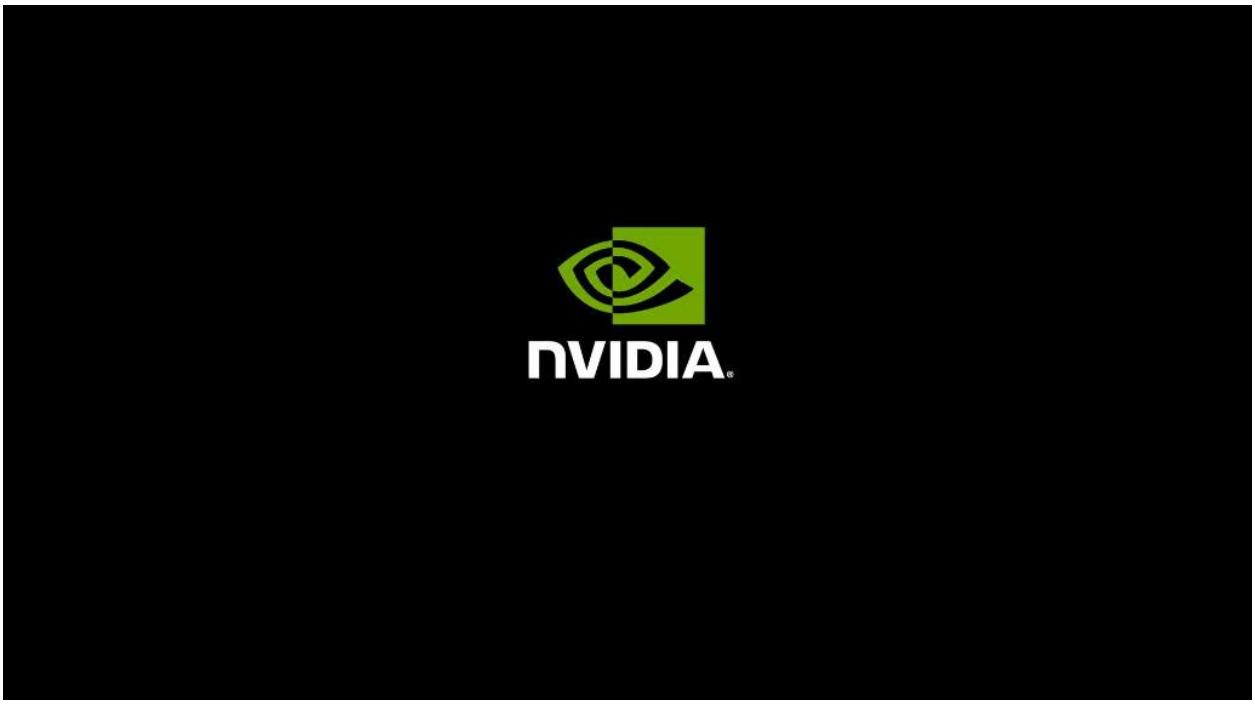
1.1. Table of Contents

1.1.1. Power-On Self-Test (POST) Screen

The first page displayed when the system starts is the POST screen. The version of the POST screen depends on the UEFI settings. The default is the Quiet POST screen.

1.1.1.1 Quiet POST screen

The Quiet POST screen contains only the system logo.



1.1.1.2 Normal POST screen

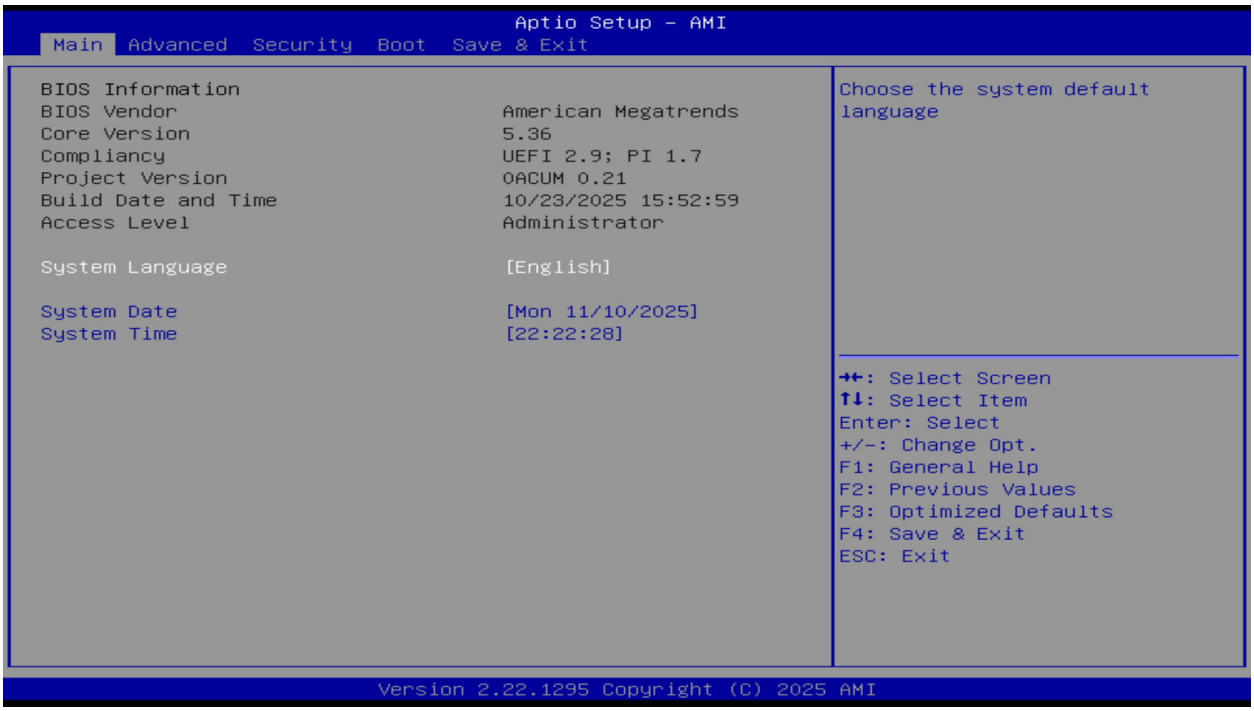
The normal POST screen contains the AMI logo, copyright, and version and product information

1.1.1.3 UEFI Setup Menu

To enter the UEFI setup menu, press the ESC or DEL key immediately after powering on the system and hold it until the UEFI setup menu appears. This process works for both the Quiet POST screen and the Normal POST screen.

1.1.2. Main Tab

The **Main tab** provides additional UEFI and system information, and allows you to change the system language and date and time.



1.1.2.1 System Language

Currently, only English is supported.

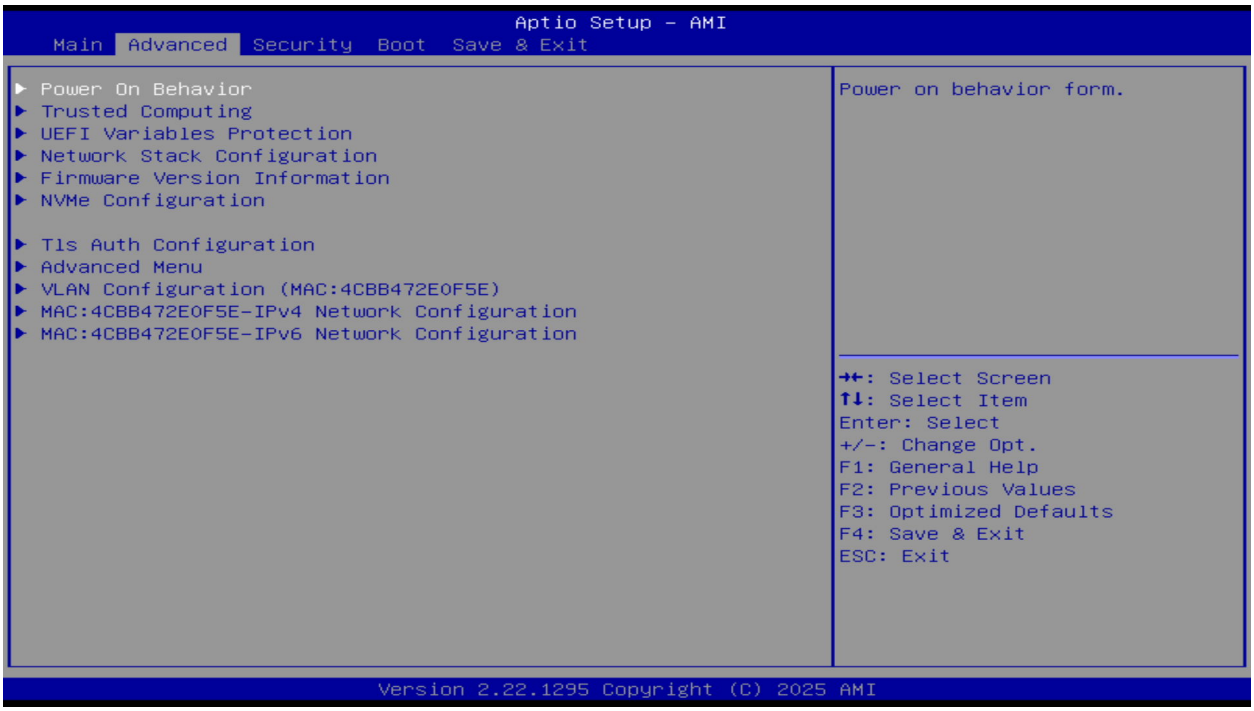
1.1.2.2 System Date and Time

To change the system date, time, and date format, use the following steps:

1. Highlight System Time or System Date using the Up and Down keys.
2. Enter new values using the keyboard.
3. Use the Tab key or the arrow keys to move between fields.
4. The date must be entered in Date MM/DD/YYYY format.
5. The time is entered in HH:MM:SS format.

1.1.3. Advanced Tab

Use the left or right arrow keys to select the **Advanced tab**. Use the up or down arrow keys to select items in the left pane of the tab. Use the `Enter` key to display available submenus for a selected item.



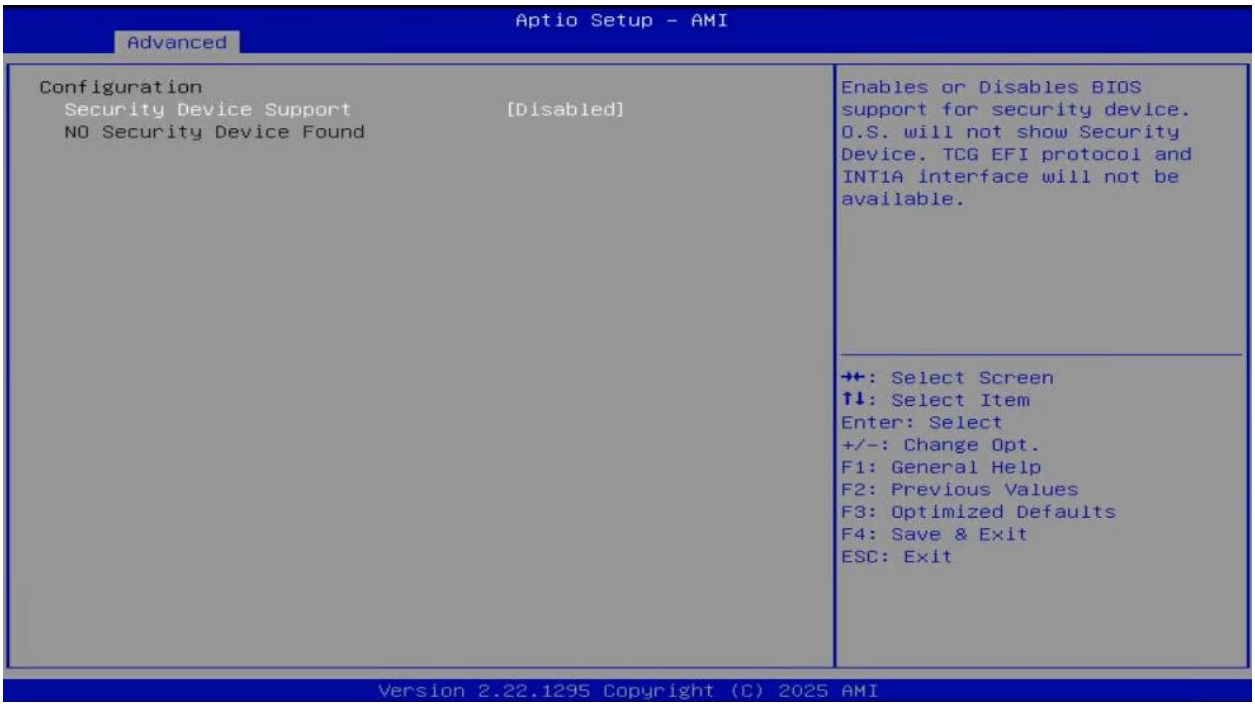
If the system is unstable after changing any settings in advanced configuration, revert to the default settings on the **Save & Exit** tab.

1.1.3.1 Power On Behavior

Power On Behavior Table

Setting	Description
After Power Loss Behavior	`Auto Boot` (default) or `Power Button Press`

1.1.3.2 Trusted Computing



Trusted Computing Settings Table

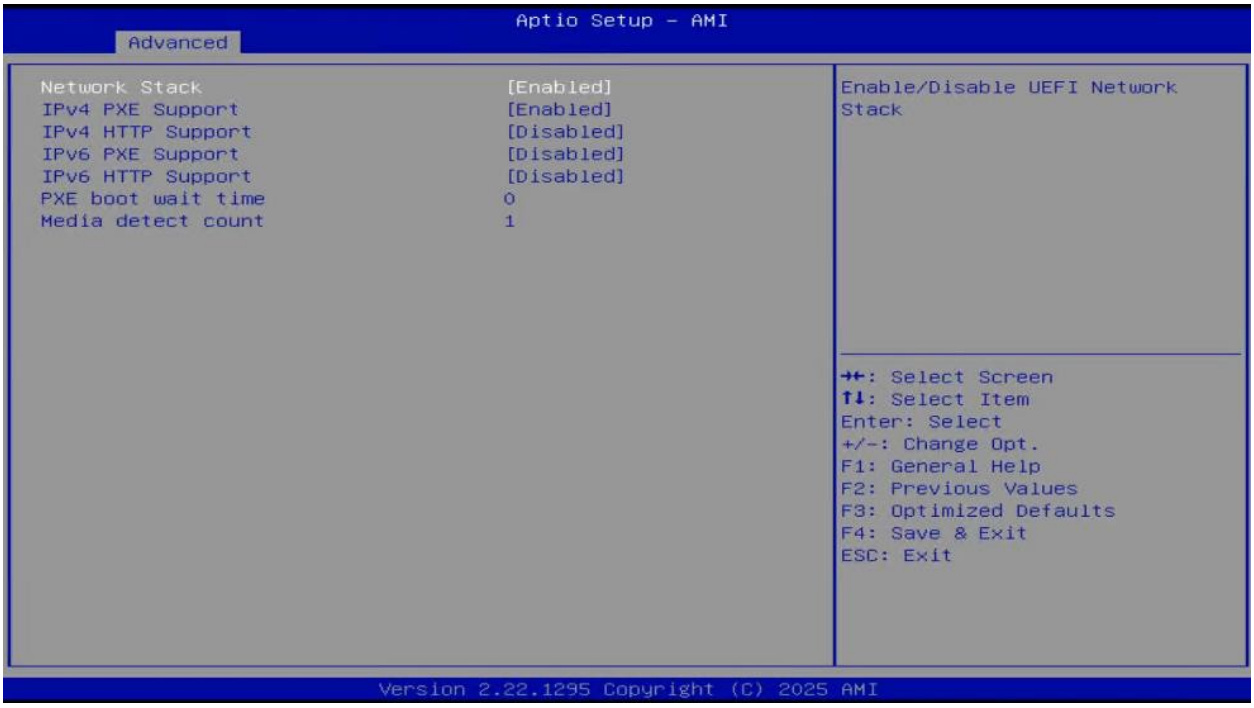
Setting	Description
Security Device Support	Select `Enable` or `Disable` to enable or disable the Security TPM Device Support.

1.1.3.3 UEFI Variables Protection

UEFI Variables Protection Settings

Setting	Description
Password protection of Runtime Variables	Control the NVRAM Runtime Variable protection through System Admin Password.

1.1.3.4 Network Stack Configuration

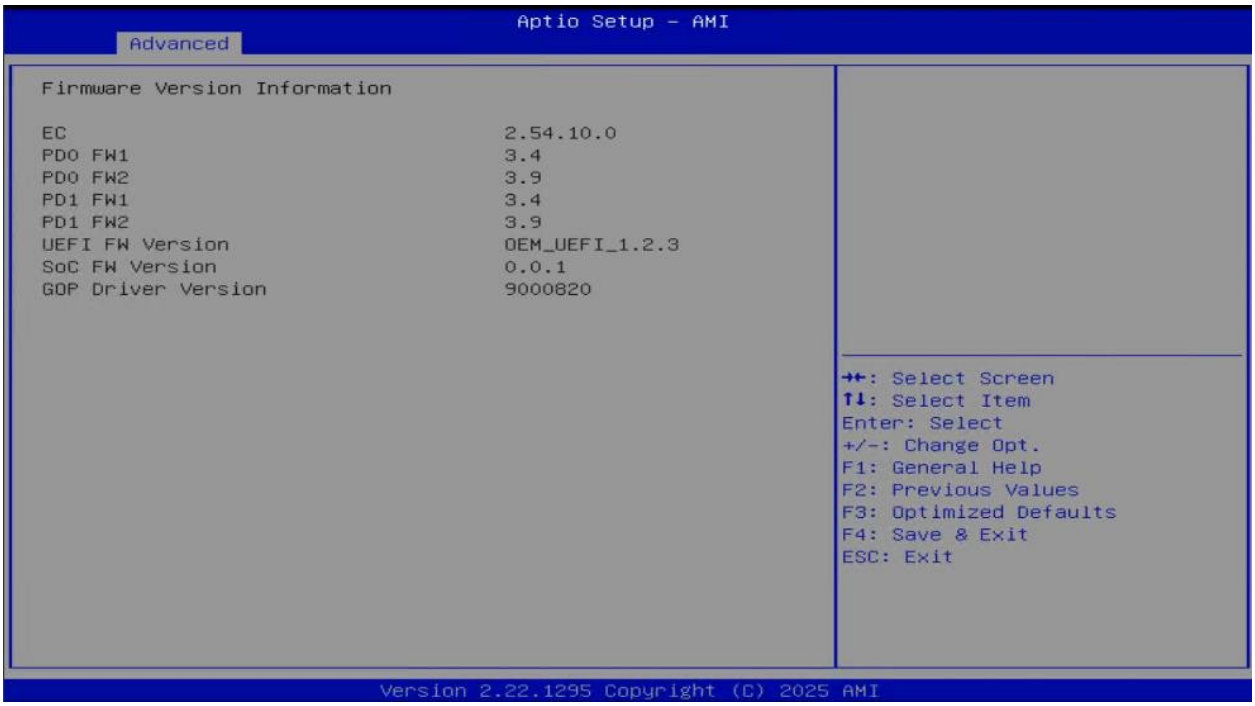


Network Configuration Table

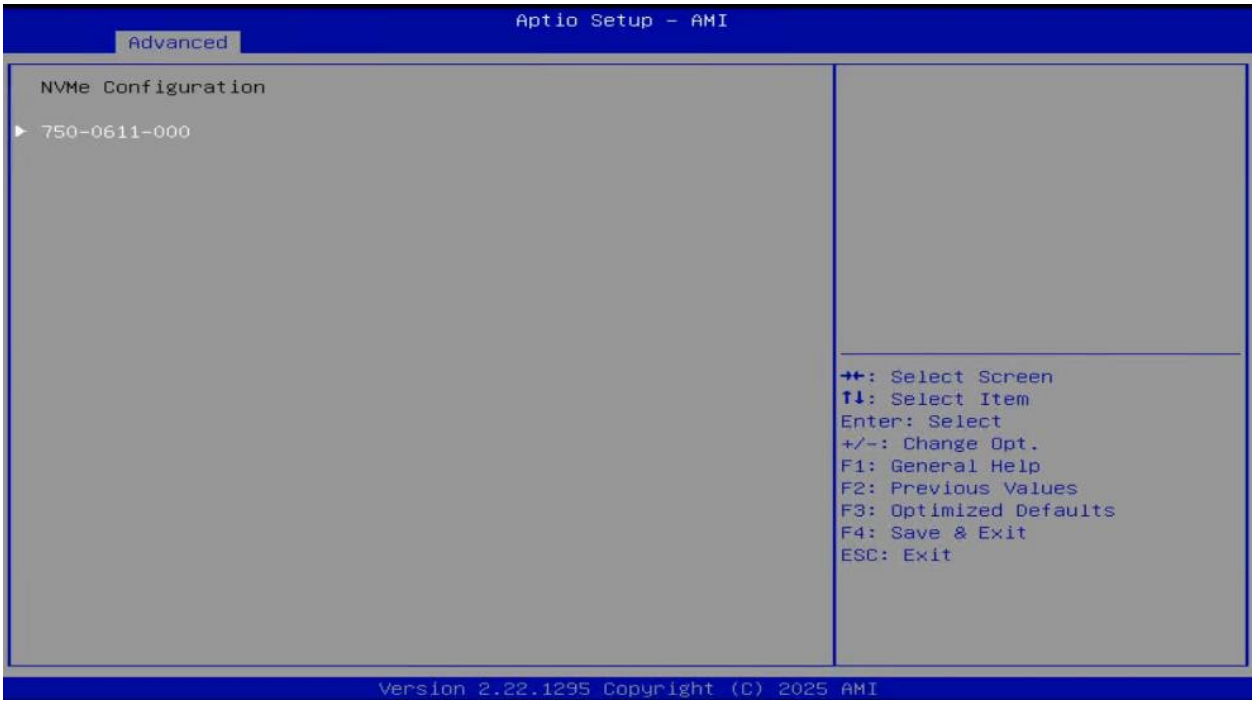
Network Configuration Setting	Description
Network Stack	Enable and Disable the UEFI network stack.
Ipv4 PXE Support	Enable and Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support is unavailable.
Ipv4 HTTP Support	Enable and Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support is unavailable.
Ipv6 PXE Support	Enable and Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support is unavailable.
Ipv6 HTTP Support	Enable and Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support is unavailable.
PXE boot wait time	Wait time in seconds to press ESC to abort the PXE boot. Use the +/- keys or numeric keys to set the value. The default is 0.
Media detect count	Number of times the presence of the media is checked. Use the +/- keys or numeric keys to set the value. The default is 1.

1.1.3.5 Firmware Version Configuration

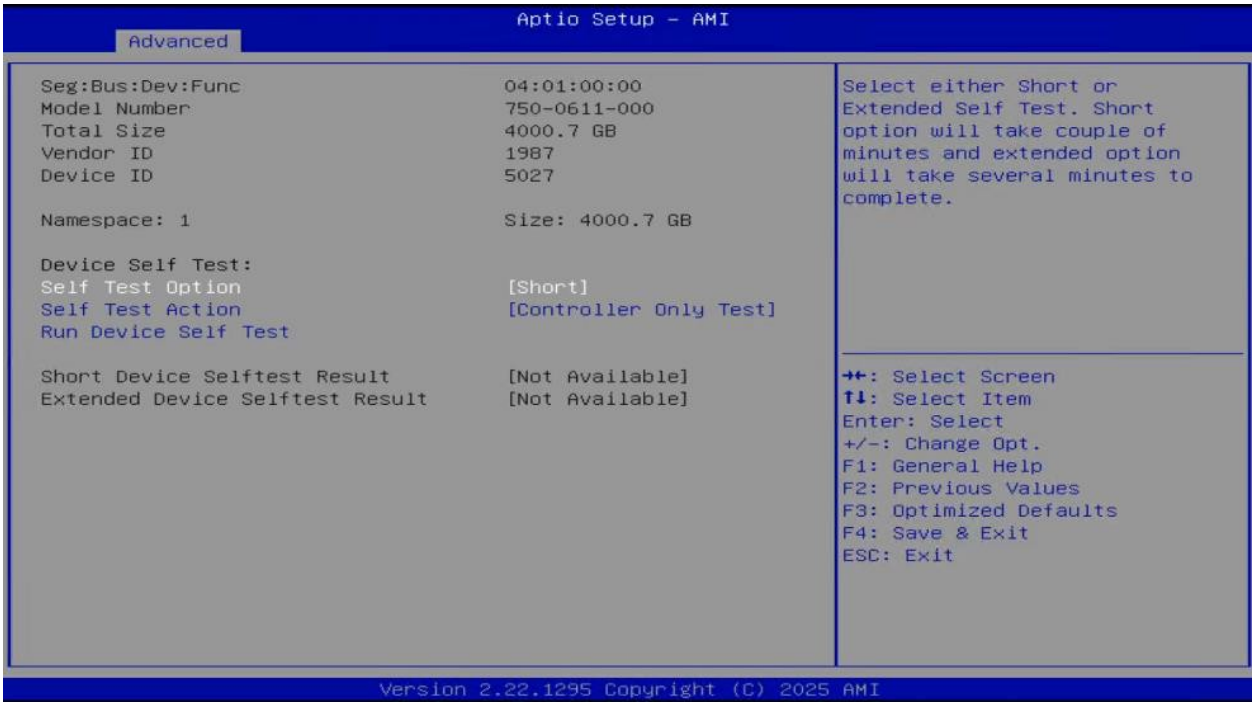
This screen displays **EC**, **PD**, and **Retimer** firmware version information.



1.1.3.6 NVMe Configuration



Selecting a device name displays more information as shown in the screenshot below.



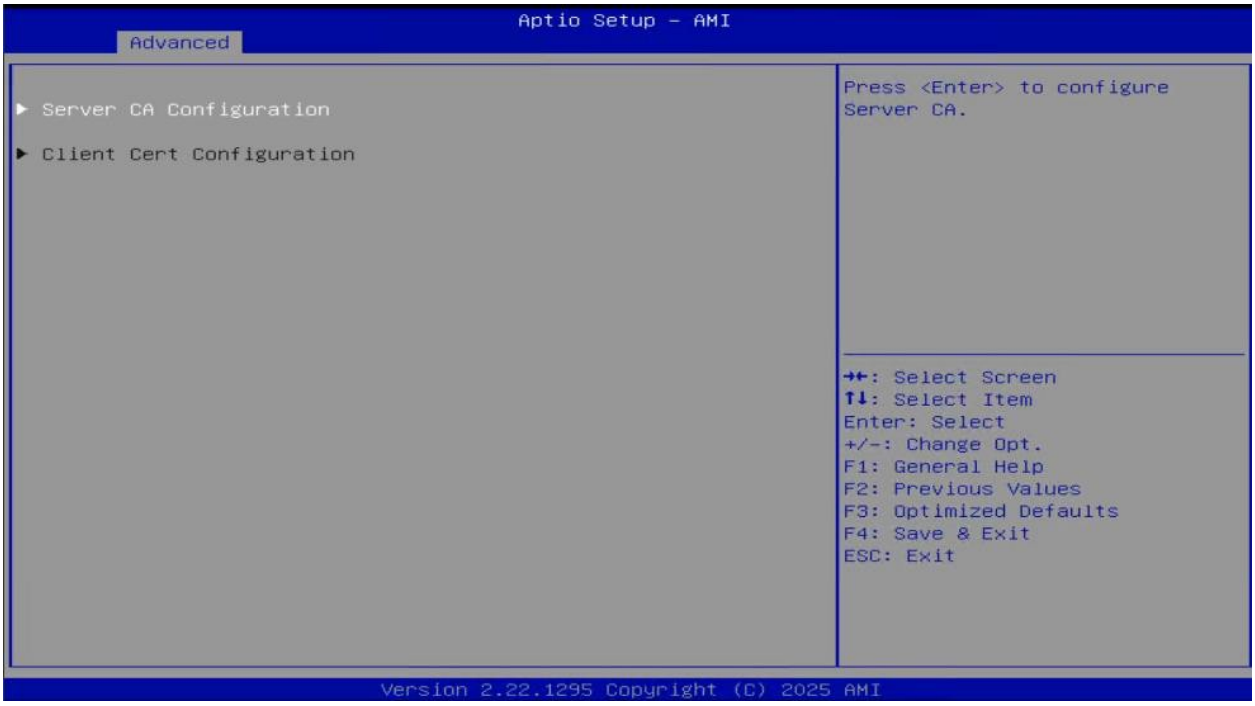
Additional NVMe Information Settings

A device self-test operation is a diagnostic testing sequence that tests the integrity and functionality of the controller and may include testing of the media associated with namespaces. The operation is broken into a series of segments. The segment number in the Self-test Result Data Structure is used for reporting purposes to indicate where a test failed.

Additional NVMe Information Settings Table

Additional NVMe Information Setting	Description
Self Test Option	User can also select the type of Self Test operation, (A) Short or (B) Extended. A short device self-test operation will take couple of minutes, whereas Extended Self Test will take several minutes to complete.
Self Test Action	User can select the type of Self Test action, (A) Controller Only test or (B) Controller and Namespace test, to specify on whether Self Test operation should be done only on Controller or both Controller and Namespace.
Run Device Self Test	User can also select the type of Self Test operation, (A) Short or (B) Extended. A short device self-test operation will take couple of minutes, whereas Extended Self Test will take several minutes to complete.

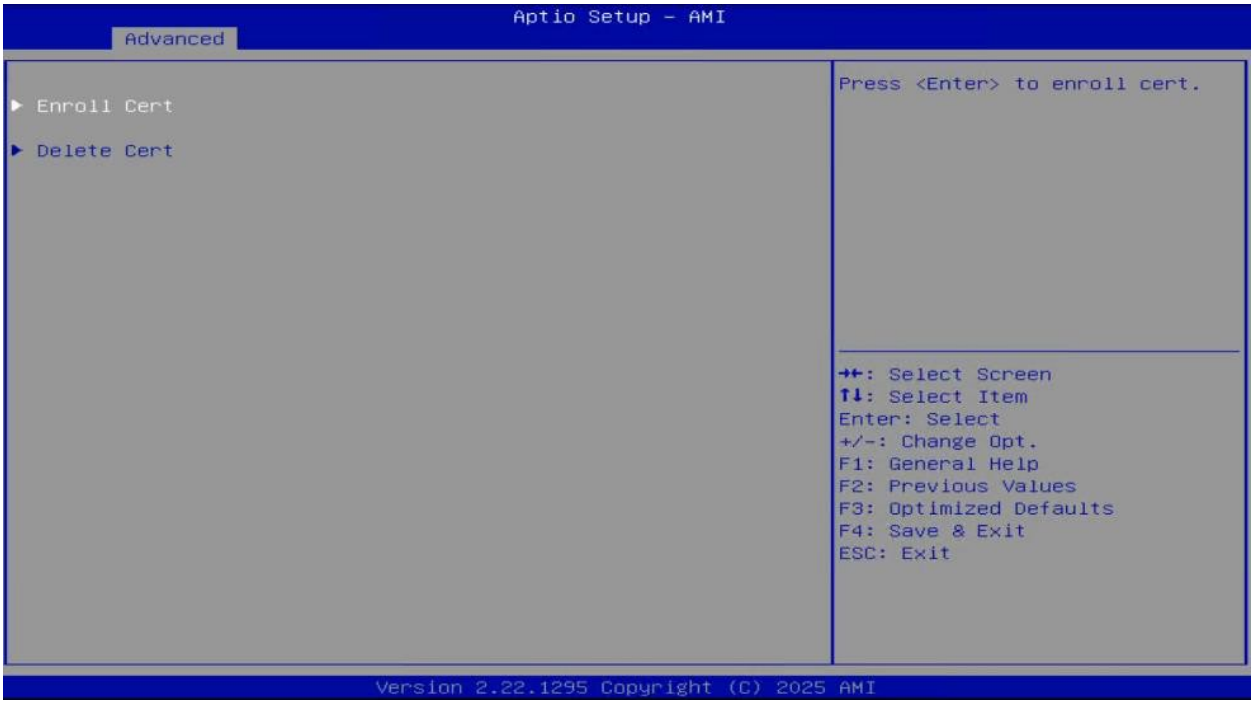
1.1.3.7 Transport Layer Security (TLS) Auth Configuration



This screen can be used to add the Server Certificate Authority (CA) certification and Client Cert to use for secure communication between UEFI and an external server.

Note

Client Cert configuration is currently unsupported.

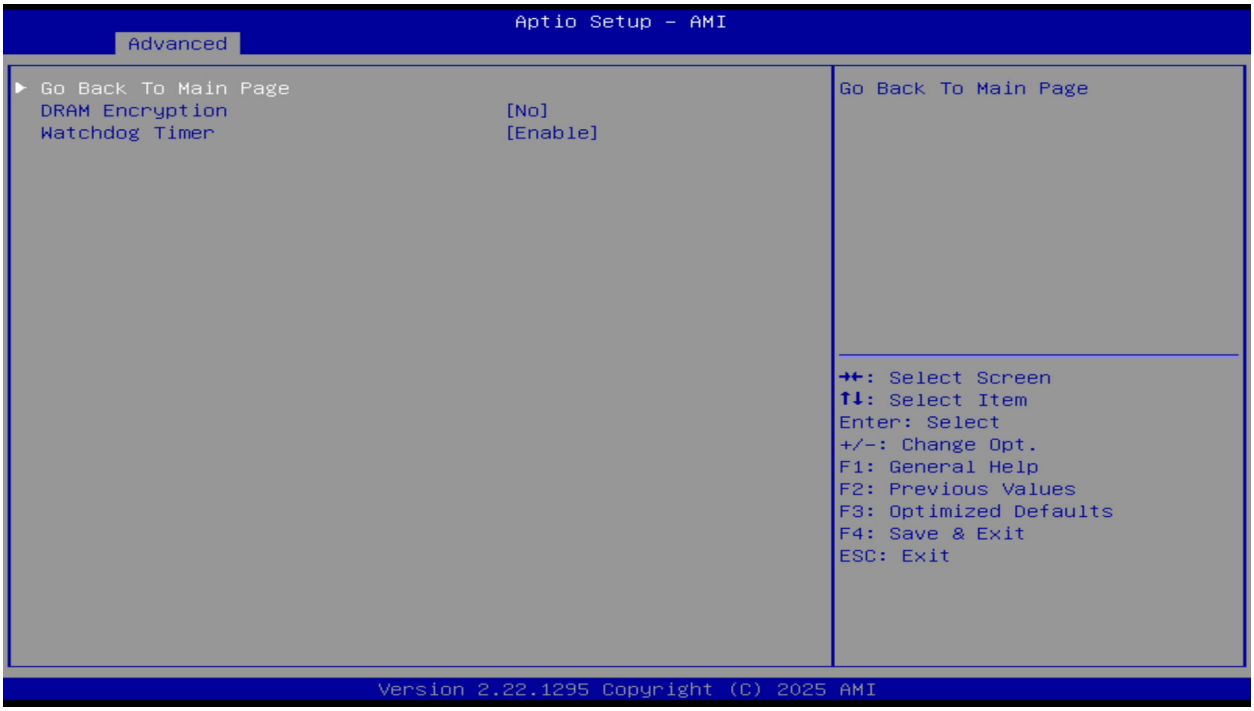


Certificate Management Settings Table

Certificate Management Setting	Description
Enroll Cert	Enables enrolling a CA Cert from the file system or using GUID with the following GUID format: <1111111-2222-3333-4444-1234567890ab>.
Delete Cert	Enables or disables the deletion of an enrolled CA Cert from the system.

1.1.3.8 Advanced Menu

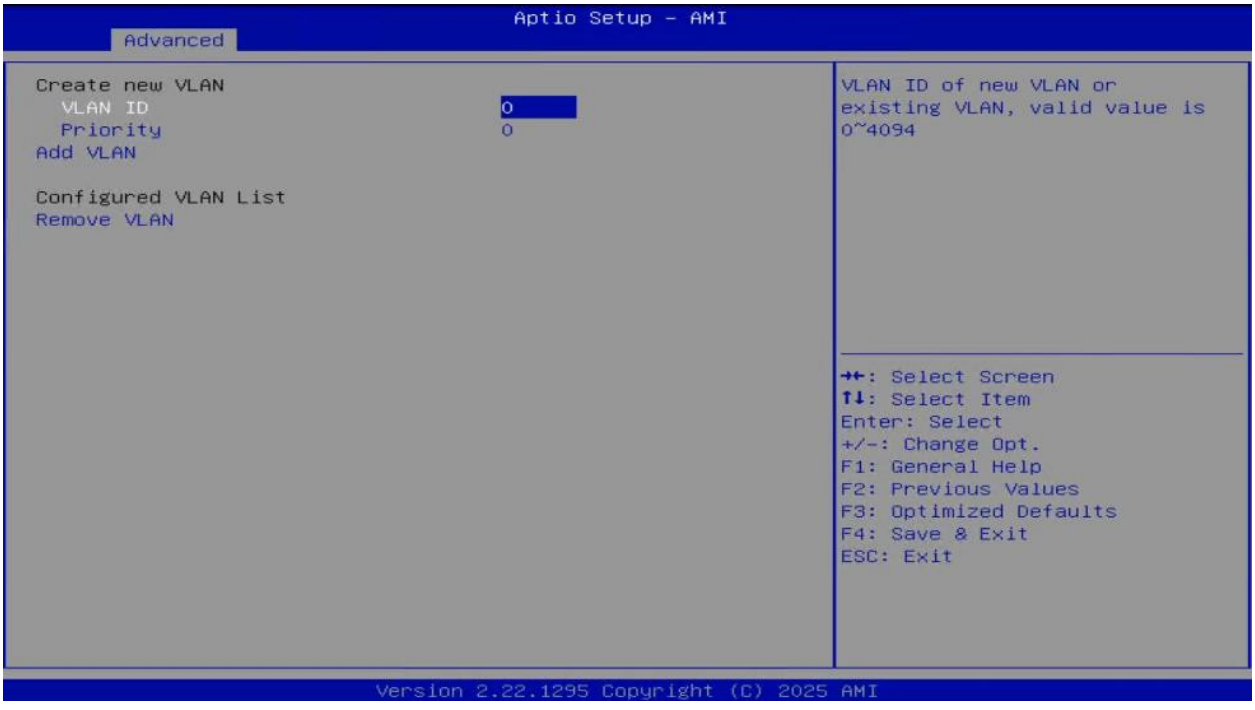
1.1.3.8.1 Platform Configuration



Platform Configuration Settings Table

Platform Configuration Setting	Description
DRAM Encryption	Enable and Disable DRAM Encryption. Options: Yes or No (default).
Watchdog Timer	Timer to reset the system in case of a failure.

1.1.3.9 VLAN Configuration Screens



1.1.3.10 MAC:XXXXXXXXXXXX-IPv4 Network Configuration

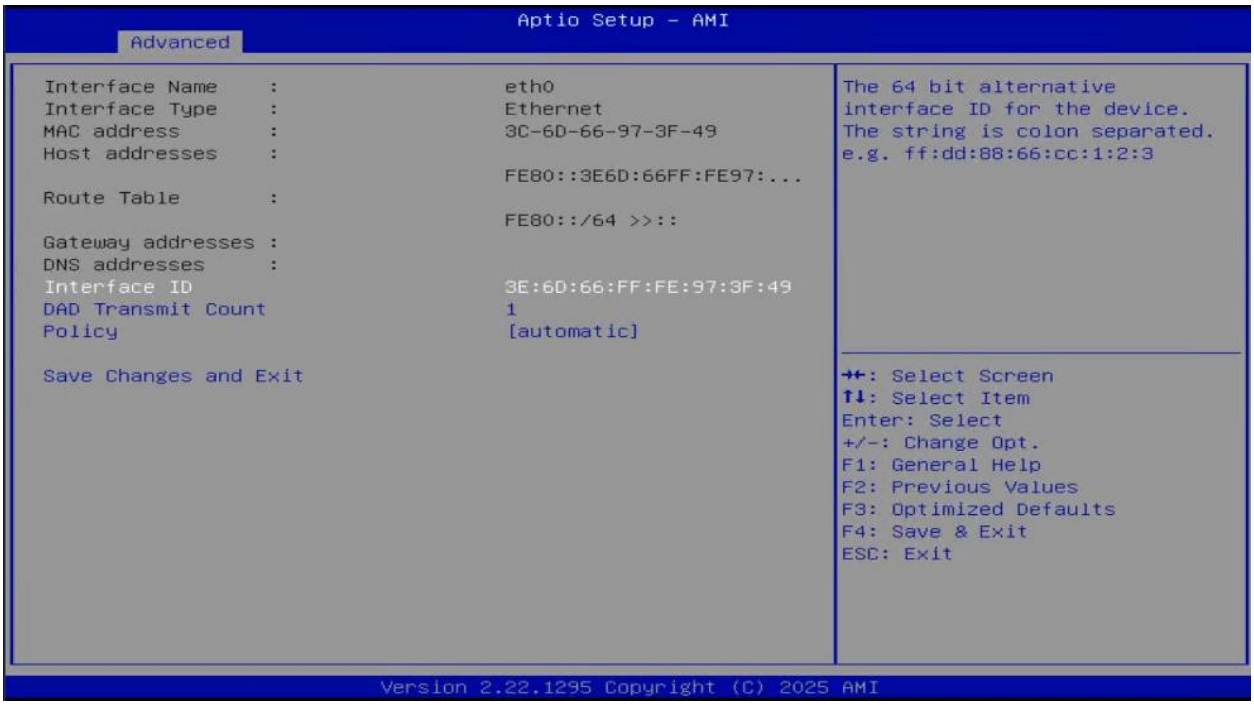
When Network Stack is enabled on the Network Configuration screen, this screen enables IPv4 network configuration for the device having MAC address XXXXXXXXXXXX.

IPv4 Network Configuration Settings

IPv4 Network Configuration Setting	Description
Configured	Enable and Disable IPv4 configuration for this device. When Enabled, settings described in this table are available.
Enable DHCP	Enter DHCP mode. The default is `Disabled`.
Local IP Address	Enter an IP address in dotted decimal notation for this device, for example, `192.168.1.2`.
Local NetMask	When Enable DHCP mode is disabled, enter a NetMask in dotted decimal notation for this device, for example, `255.255.255.0`.
Local Gateway	When Enable DHCP mode is disabled, enter the Gateway address in dotted decimal notation for this device, for example, `192.168.1.1`.
Local DNS	When Enable DHCP mode is disabled, enter the DNS server addresses in dotted-decimal notation for this device, for example, `192.166.1.100`.
Save Changes and Exit	Press `Enter` to save changes and exit.

1.1.3.11 MAC:XXXXXXXXXXXX-IPv6 Network Configuration

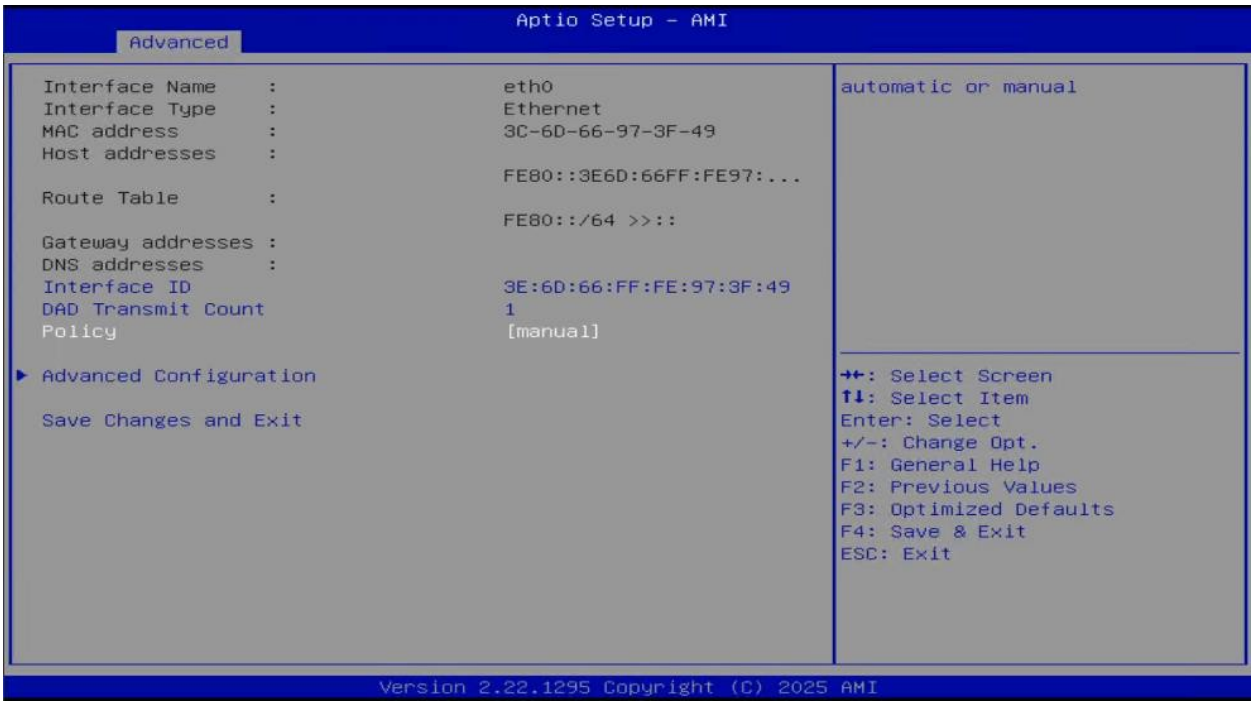
When Network Stack is enabled on the Network Configuration screen, this screen enables IPv6 network configuration for the device having MAC address XXXXXXXXXXXX.



IPv6 Network Configuration Settings

Setting	Description
Interface ID	Enables changing the 64-bit alternative interface ID for the device. The string is colon separated, for example, `ff:dd:88:66:cc:1:2:3`.
DAD Transmit Count	Enables changing the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) on a tentative address. A value of 0 indicates that DAD is not performed. The default is 1.
Policy	The options are `Automatic` and `Manual`. Using `Automatic`, IPv6 configuration is set automatically. Using `Manual` enables manual IPv6 configuration of the IP address, gateway address, and DNS address.

The screen in the screenshot below is available when Policy is set to `Manual` and Advanced Configuration is selected. This supports manual network address configuration.

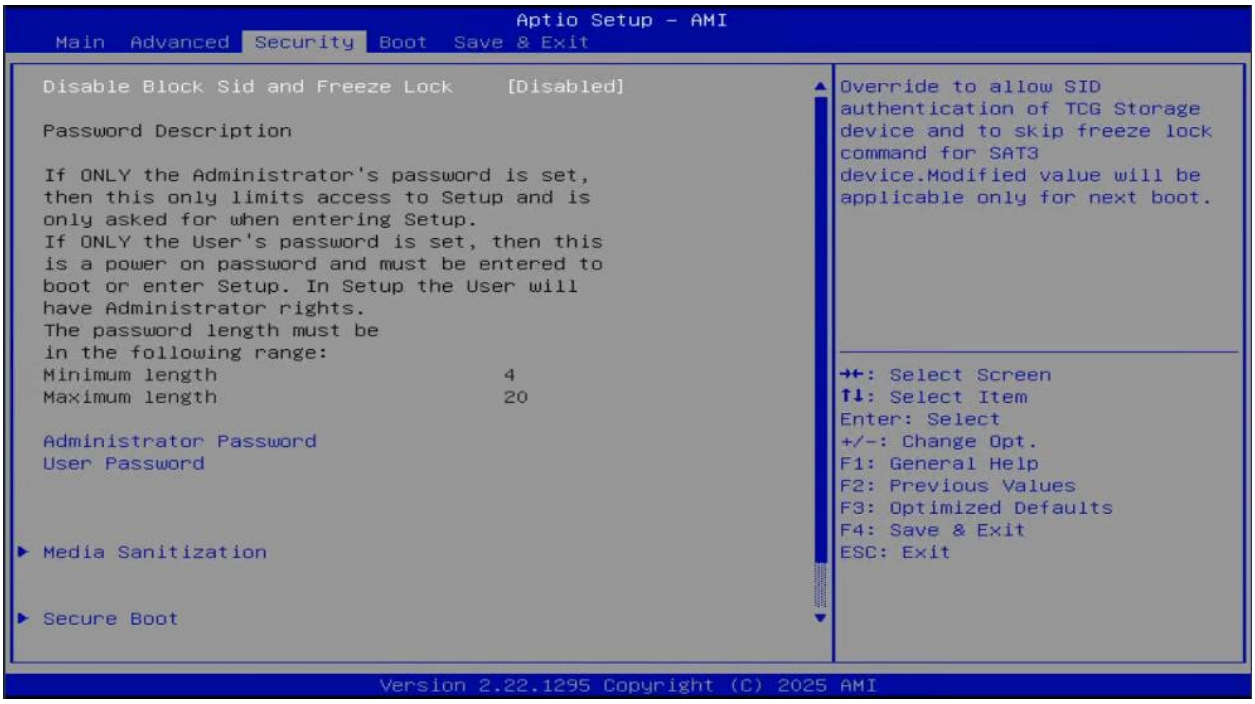


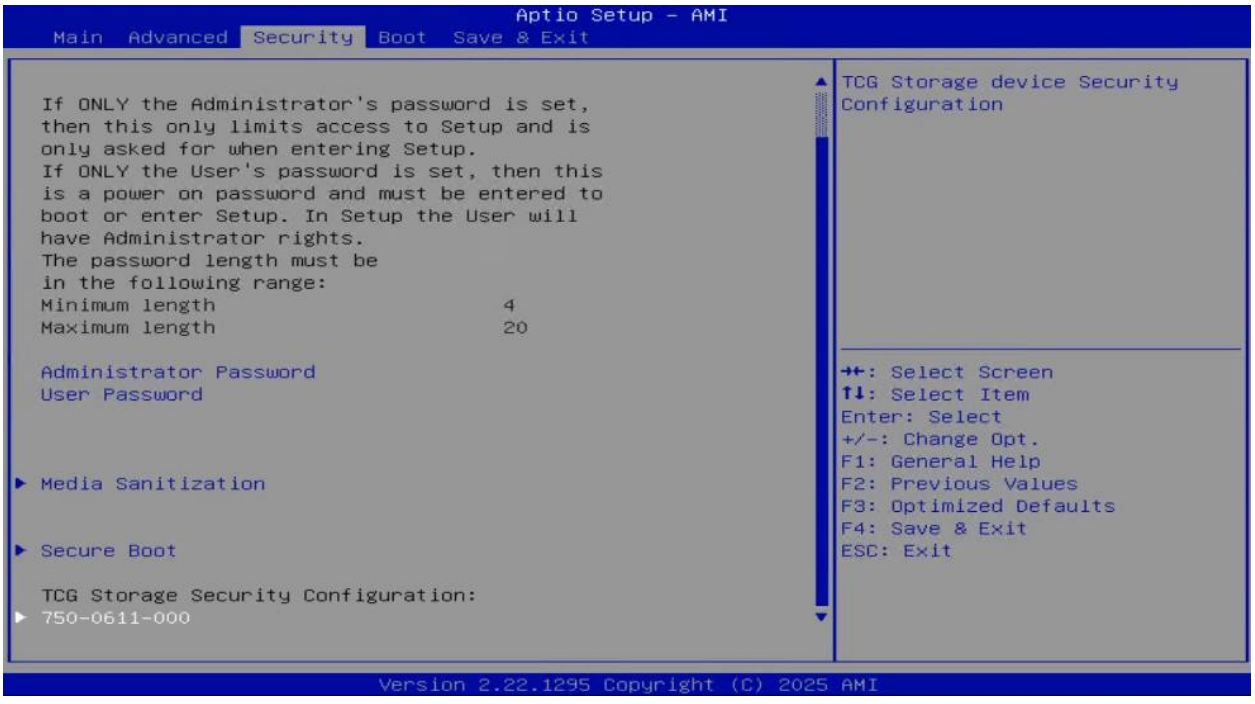
Manual IPv6 Address Configuration Settings

Setting	Description
New IPv6 address	A manual IP address can be configured only under manual policy, for example, `2002::1/64`.
New Gateway addresses	A gateway IP address can be configured only under manual policy. Use a space to separate IP addresses to configure more than one gateway address. For example, `2002::2 2002::3`.
New DNS addresses	A DNS IP address can be configured only under manual policy. Use a space to separate IP addresses to configure more than one DNS address, for example, `2002::4/64 2002::5/64`..
Discard Changes and Exit	Press `Enter` to discard all changes and exit.

1.1.4. Security Tab

Use the left or right arrow keys to select the **Security tab**. Use the up or down arrow keys to select items on the left pane of the tab. Use the `Enter` key to display available submenus for a selected item.





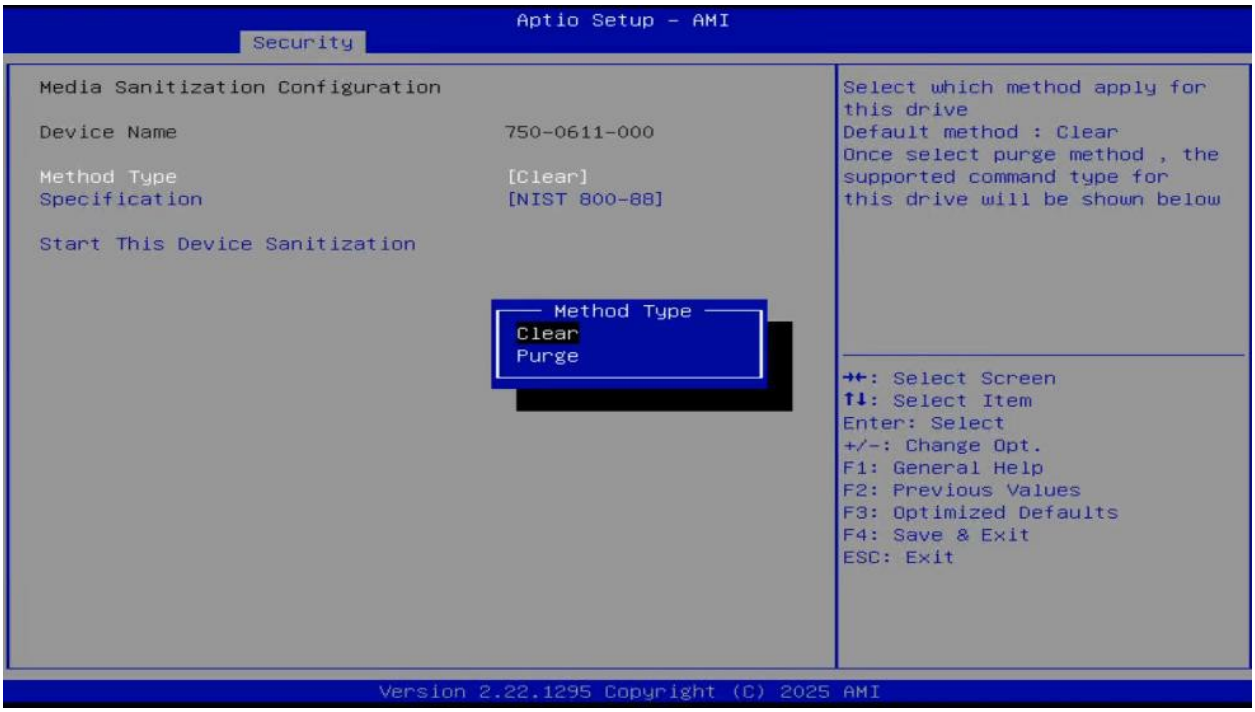
Security Tab

Setting	Description
Disable Block Sid and Freeze Lock	Override to allow SID authentication of TCG Storage device and to skip freeze lock command for SAT3 device. Modified value will be applicable only for next boot.
Administrator Password	Selecting this option enables users to set the Administrator password.
User Password	Selecting this option enables users to set the User password.

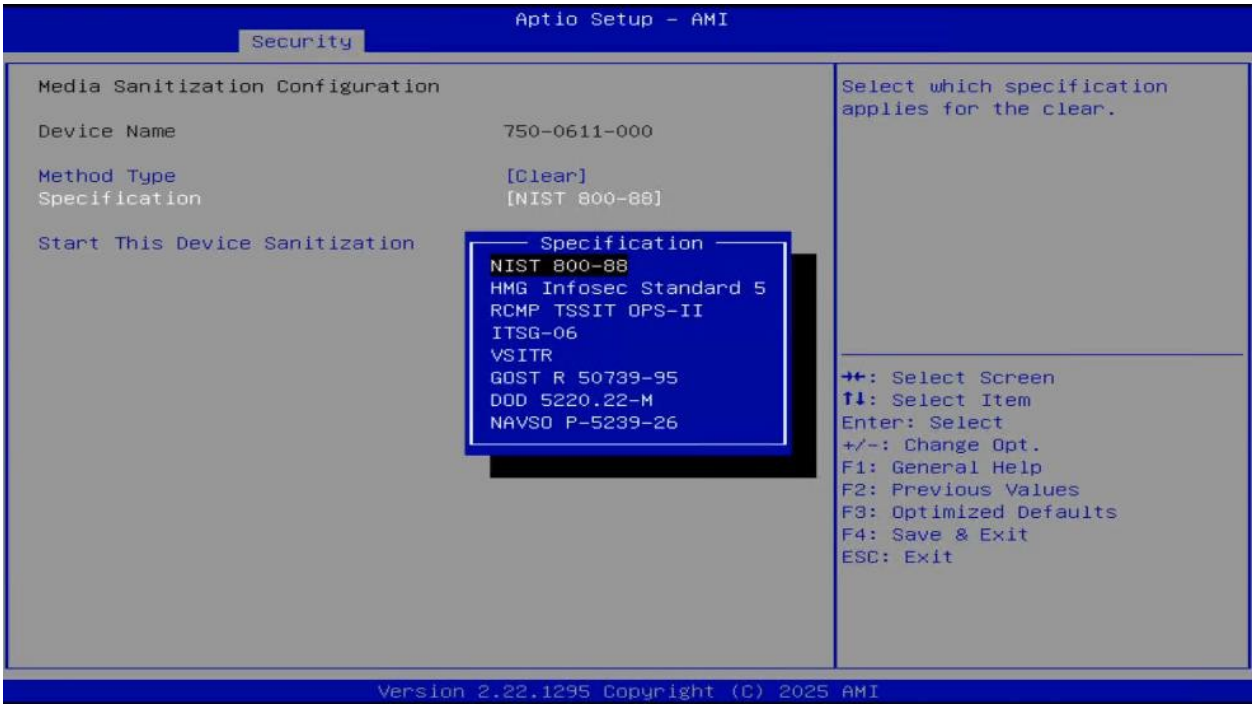
1.1.4.1 Media Sanitization

Device Name : Select the Device Name

Method Type : Select the Method Type



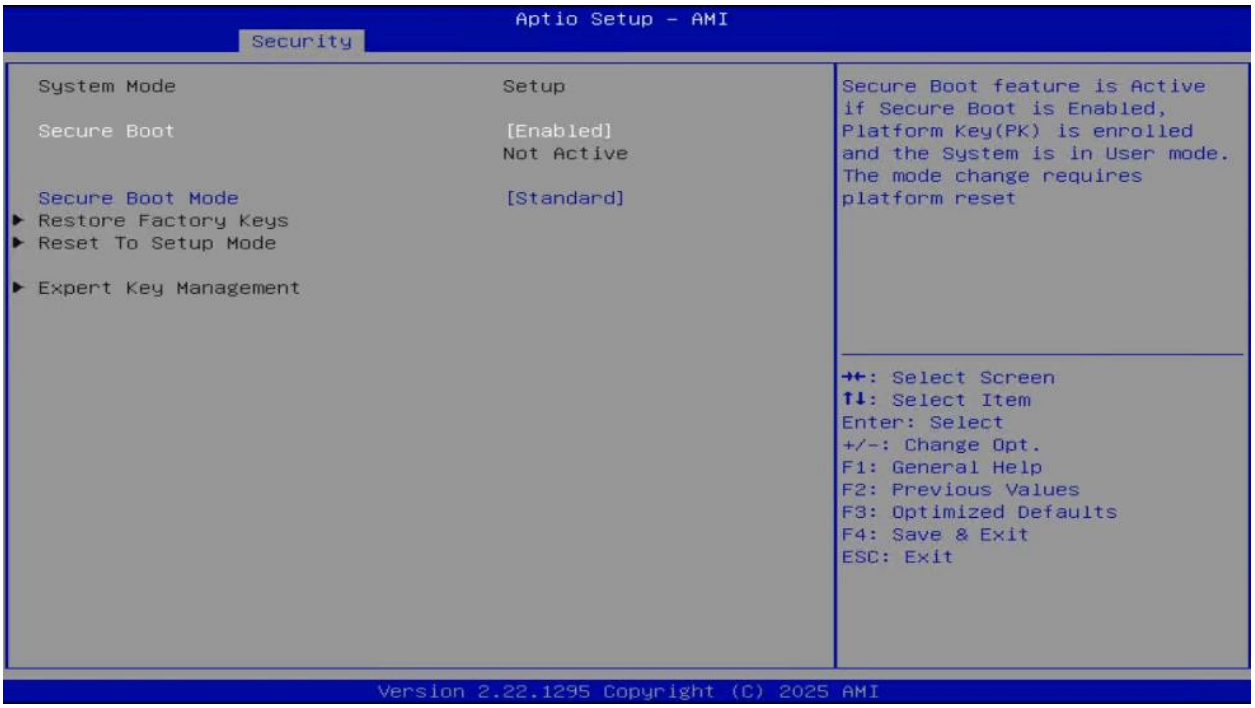
Specification: Select the Specification



Start This Device Sanitization : Start sanitizing will set up the configuration

1.1.4.2 Secure Boot

Select **Secure Boot** to configure boot mode and manage keys.



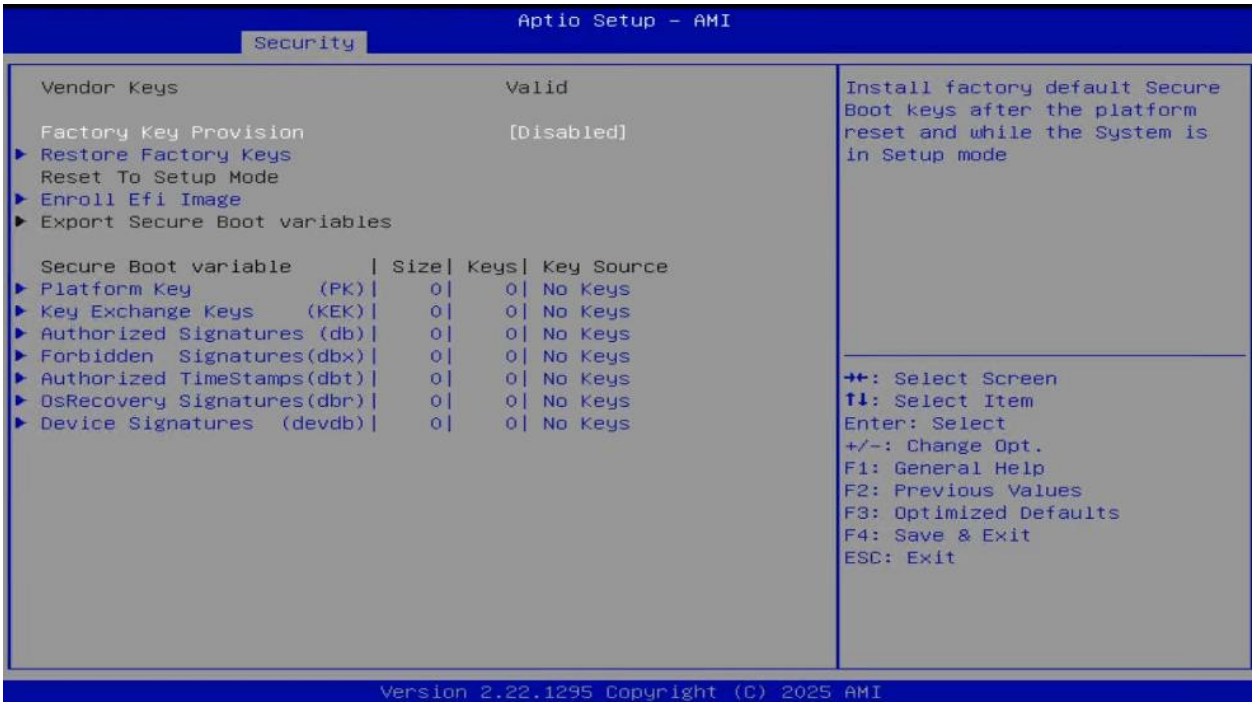
Secure Boot: Allows users to enable and disable the secure boot feature. The default is **Enabled**. The secure boot feature is active when secure boot is enabled, Platform Key (PK) is enrolled, and the system is in User mode. A mode change requires a platform reset.

Restore Factory Keys: Forces the system to User mode and installs factory-default secure boot key databases.

Reset To Setup Mode: Delete the NVRAM content of all UEFI secure boot keys.

Expert Key Management: Enables a user to configure key management settings.

1.1.4.2.1 Expert Key Management



The expert key management accesses these formats:

- **Public Key Certificate:** EFI Signature List, EFI CERT X509 (DER Encoded), EFI CERT RSA2048 (Bin), EFI SERT SHAXXX
- **Authenticated UEFI Variable**
- **Authenticated UEFI Variable**
- **Key Source**: Factory, External, Mixed

Settings for key management:

- **Factory Key Provision:** If enabled, install factory-default Secure Boot keys after platform reset. This applies only when the system is in setup mode.
- **Restore Factory Keys:** To force the system to user mode, configure NVRAM to contain OEM-defined factory default secure boot keys.
- **Reset to Setup Mode:** Delete all secure boot key databases from NVRAM.
- **Enroll EFI Image:** Enables the image to run in secure boot mode. Enroll the SHA256 Hash certificate of a PE image into Authorized Signature database.
- **Export Secure Boot variables:** Copy the NVRAM content of secure boot variables to files in a root folder on a file system device.

Secure Boot Variables

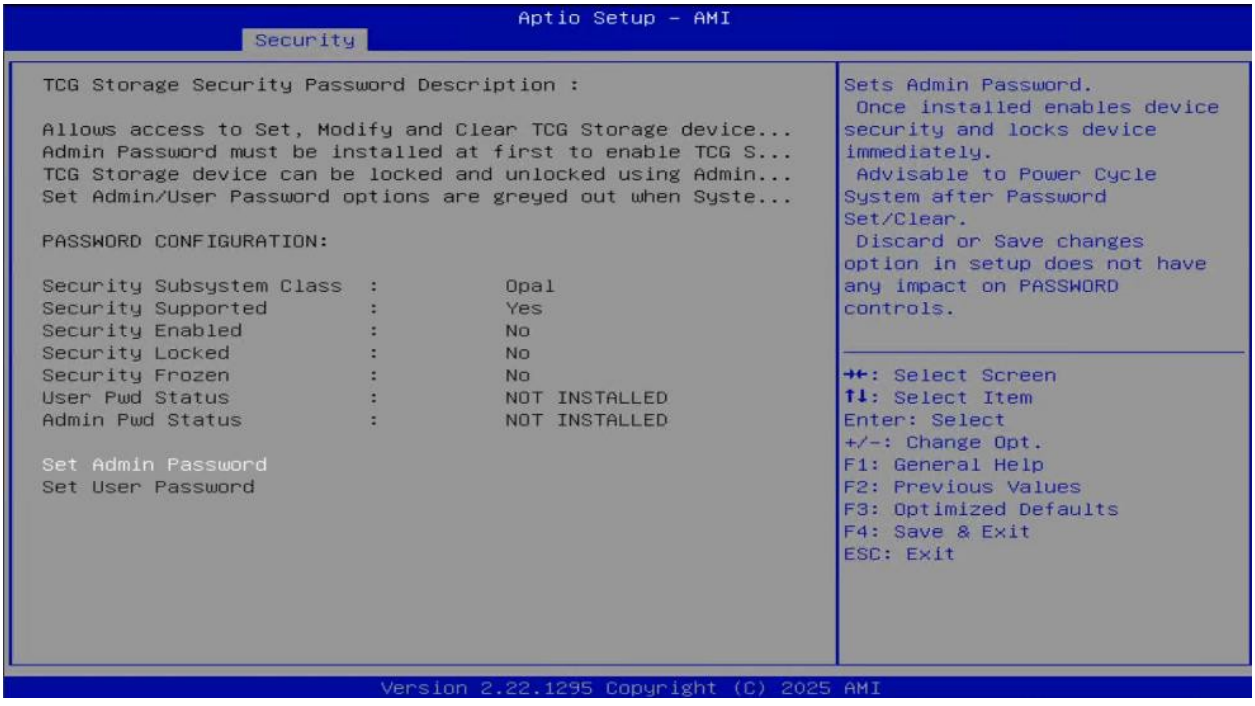
- **Platform Key (PK):** Enables users to configure PK settings. Users can update the settings using a value from factory defaults or from a file in the file system.
- **Key Exchange Key (KEK):** Enables users to configure KEK settings. Users can update or append this using value from factory defaults or from a file in the file system.
- **Authorized Signatures:** Enables users to configure Authorized Signatures settings. Users can update or append this using value from factory defaults or from a file in the file system.
- **Forbidden Signatures:** Enables users to configure Forbidden Signatures settings. Users can update or append this using value from factory defaults or from a file in the file system.
- **Authorized TimeStamps:** Enables users to configure the settings of the Authorized TimeStamps. Users can update or append this using a value from factory defaults or from a file in the file system.
- **OsRecovery Signatures:** Enables users to configure the settings of the OsRecovery Signatures. Users can update or append this using a value from factory defaults or from a file in the file system.

Device Signatures:

1.1.4.3 TCG Storage Security Configuration

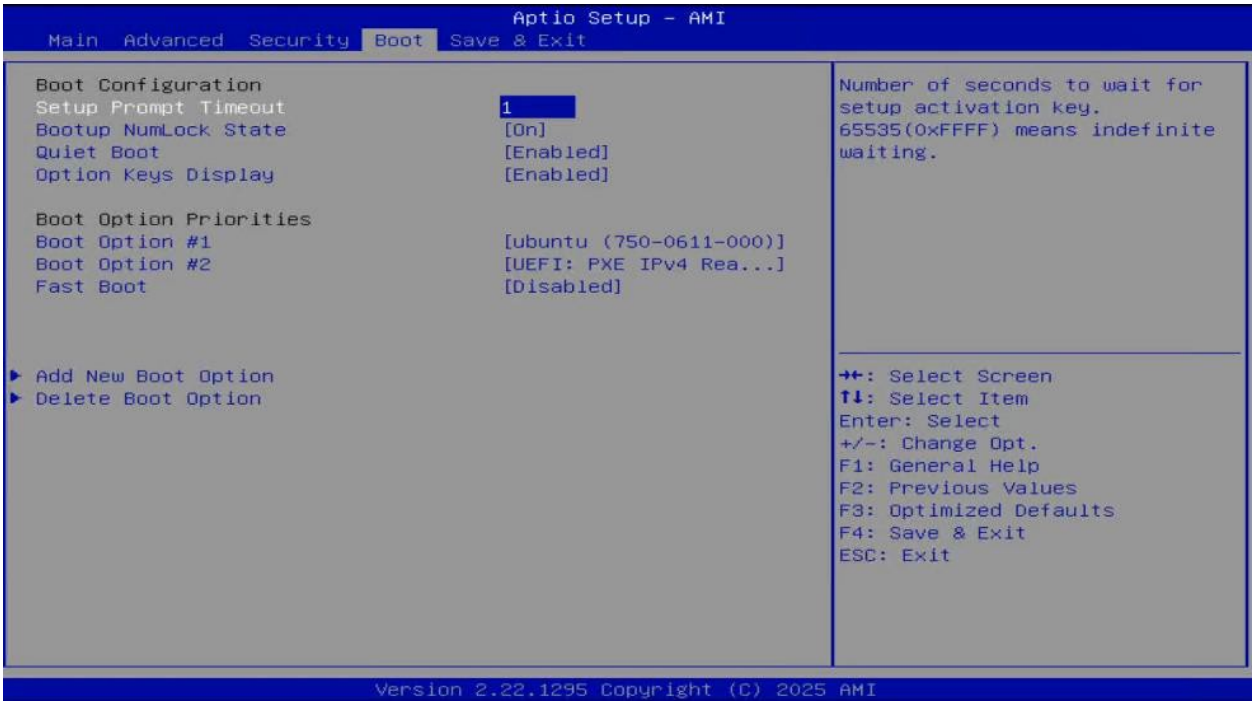
The TCG Storage Security Configuration screen is available when the TCG Storage device is selected.

This allows access to Set, Modify and Clear TCG Storage device Admin and User Password. The Admin Password must be installed first to enable TCG Storage Security. User Password can be created only when Admin password is installed. TCG Storage device can be locked and unlocked using Admin password alone, User password acts as optional credential to unlock the Device in POST. Set Admin/User Password options are greyed out when System enters Setup after Boot fail as Device security is frozen. Power-off, Power-on and press hot key to enter setup.



1.1.5. Boot Tab

Use the left or right arrow keys to select the **Boot** tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the `Enter` key to display available submenus for a selected item.



1.1.5.1 Boot Configuration

- **Setup Prompt Timeout:** Set the number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. The default is 1 second.
- **Bootup NumLock State:** Select the keyboard NumLock state when booting. The options are On and Off.
- **Quiet Boot:** Enables or disables the Quiet Boot option. The default value is Enabled.

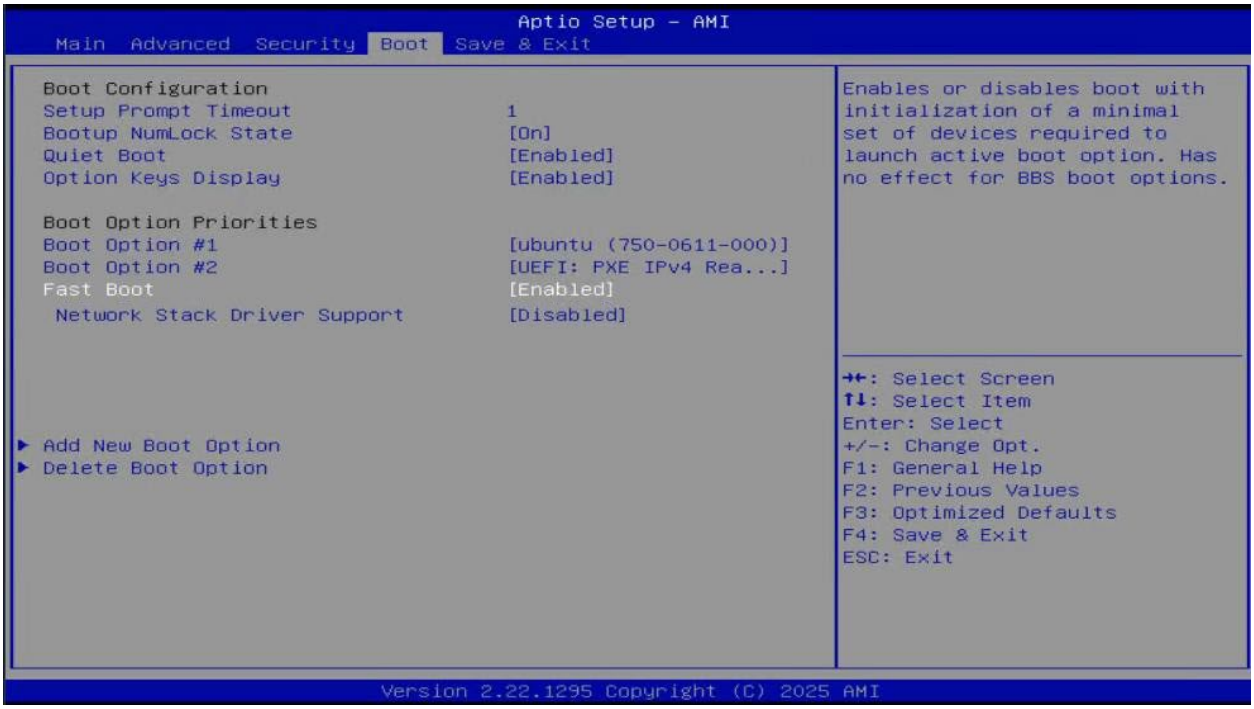
1.1.5.2 Boot Option Priorities

This prioritizes the order of bootable devices from which the system boots. To select devices, press `Enter` on each entry from top to bottom.

New UEFI OS Boot Option Policy controls the placement of newly detected UEFI boot options. The default is Place First so that any newly installed OS has the highest priority. The options are Default, Place First, and Place Last.

1.1.5.2.1 Fast Boot

Set this value to enable the user to allow the system to boot in fast boot mode. Once Fast Boot is enabled, below sub items will be visible.



Network Stack Driver Support

Enabled - Network Stack driver is supported in fast boot path.

Disabled - Network Stack drivers would NOT be started in fast boot path.

Add New Boot Option

Add Boot Option - Specify name for new boot option

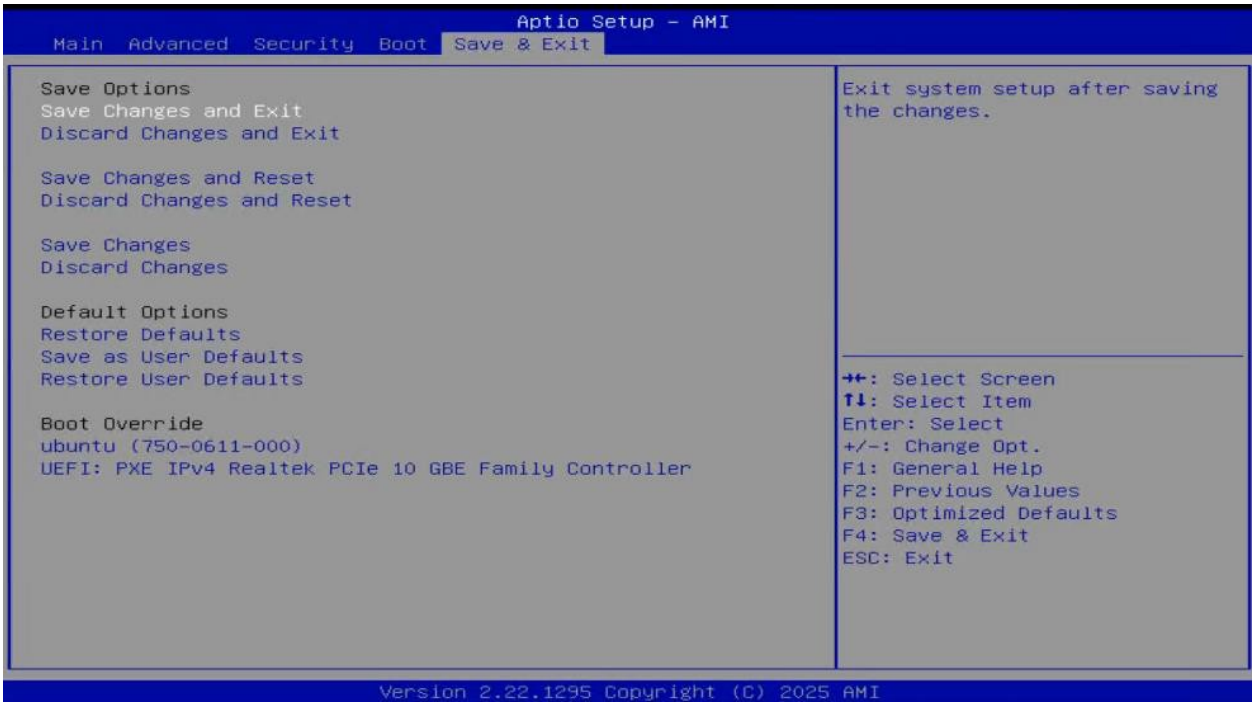
Path for Boot Option - Enter the path to the boot option

Create - Creates the newly formed boot option

Delete Boot Option - Remove an EFI boot option from the boot order

1.1.6. Save & Exit Tab

Use the `Left Arrow` or `Right Arrow` keys to select the **Save & Exit** tab. Use the `Up Arrow` or `Down Arrow` keys to select items on the left pane of the tab. Use the `Enter` key to display available submenus for a selected item.



1.1.6.1 Save Options

- **Save Changes and Exit:** Set this option to exit system setup after saving the changes.
- **Discard Changes and Exit:** Select this option to quit the BIOS Setup without making any permanent changes to the system configuration.
- **Save Changes and Reset:** Select this option to reset the system after saving the changes.
- **Save Changes**: Save the changes from users and allow users to continue to make changes.
- **Discard Changes:** Revert the system to its previous state.
- **Discard Changes and Reset:** Select this option to reset the system without changing the system configuration.

> **Note**
>
> UEFI is reset after **Save Changes and Exit** is selected.

1.1.6.2 Default Options

- **Restore Defaults:** Set this option to restore factory settings, which are designed for maximum system stability rather than maximum performance.
- **Save as User Defaults:** Select this option to enable a user to save changes to the UEFI setup for future use.
- **Restore User Defaults:** Select this option to retrieve previously saved user-defined settings.

1.1.6.3 Boot Override

This section lists the boot options for the system. Select an option, press `Enter`, and the system boots using the selected boot option.

Copyright