# Dell Technologies VEP4600 BIOS

## User guide

**Abstract**

This guide provides information for using the VEP4600 BIOS .

May 2023
Rev. A07

DELL Technologies

## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

**WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

# Contents

# 1

# About this guide

This guide provides information for using the BIOS configuration.

**CAUTION: To avoid electrostatic discharge (ESD) damage, wear grounding wrist straps when handling this equipment.**

**NOTE:** Only trained and qualified personnel can install this equipment. Read this guide before you install and power up this equipment. This equipment contains two power cords. Disconnect both power cords before servicing.

**NOTE:** This equipment contains optical transceivers, which comply with the limits of Class 1 laser radiation.


**Figure 1. Class 1 laser product tag**

**NOTE:** When no cable is connected, visible and invisible laser radiation may be emitted from the aperture of the optical transceiver ports. Avoid exposure to laser radiation. Do not stare into open apertures.

**Topics:**



## Information symbols

This book uses the following information symbols:

**NOTE:** The **Note** icon signals important operational information.

**CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.**

**NOTE:** The **Warning** icon signals information about hardware handling that could result in injury.

**NOTE:** The **ESD Warning** icon requires that you take electrostatic precautions when handling the device.

## Document revision history

**Table 1. Revision history**

| Revision | Date | Description |
|---|---|---|
| A06 | 2022-08 | BIOS 3.41.0.9-23 |
| A05 | 2022-04 | BIOS 3.41.0.9-21 DIAG OS R3.41.3.81-9 |

**Table 1. Revision history (continued)**

| Revision | Date | Description |
|---|---|---|
| A04 | 2021-08 | BIOS 3.41.0.9-19 DIAG OS R3.41.3.81-9 |
| A03 | 2021-01 | BIOS 3.41.0.9-18 DIAG OS R3.41.3.81-8 |
| A02 | 2019-02 | WIFI/LTE expansion cards, BIOS 3.41.0.9-13, DIAG OS 3.41.3.81-4 |
| A01 | 2018-08 | Hardware flow control addition |
| A00 | 2018-05 | Initial release |

# 2

# New and changed features

New features and bug fixes history.

**Topics:**

- BIOS

## BIOS

New features and version history.

**Table 2. New features and version history**

| Functional area | Feature description |
|---|---|
| BIOS 3.41.0.9-23 | VEP4600-3.41.0.9-23<br>● Update to Intel IPU 2021.2 to address security issues:<br>○ Microcode_330 (2006C0A)<br>○ SPS v04.00.04.402.0<br>○ ACM binaries v1.3.61<br>○ PSRC-16050 EDKII HTTP Boot<br>■ CVE-2019-14553<br>○ PSRC-15545 Intel IPU 2021.2 Feb<br>■ CVE-2021-0103, CVE-2021-0107, CVE-2021-0111, CVE-2021-0114, CVE-2021-0115, CVE-2021-0116, CVE-2021-0117, CVE-2021-0118, CVE-2021-0060, CVE-2021-0119, CVE-2021-0124, CVE-2021-0125, CVE-2021-0127<br>○ PSRC-15791 Intel IPU 2021 Nov x710 rNDC FW<br>■ CVE-2021-0200 |
| BIOS 3.41.0.9-21 | VEP4600-3.41.0.9-21:<br>● Addresses the following Intel Security Advisory: INTEL-SA-00463. A security advisory is a statement by the manufacturer when a security vulnerability impacts a product and a remedy is available for the vulnerability. Update requires cold reboot to take effect.<br>○ INTEL-SA-00463: Update Microcode and Intel RC for: CVE-2020-8670, CVE-2020-8700, CVE-2020-12357, CVE-2020-12358, CVE-2020-12359, CVE-2020-12360, CVE-2020-24486, CVE-2020-24509, CVE-2021-0095<br>● Update to AMI label 38<br>● Update BIOS components<br>● Microcode version: v04.00.04.317.0<br>● SPS Firmware version: 02006B06<br>● ACM version: 1.3.51_LBG_BKRV<br>● SINIT version: 1.3.53_LBG_BKRV |
| BIOS 3.41.0.9-19 | 1. Added Secure Boot support. Secure Boot supports Microsoft Key for signed image when enabled. |

**Table 2. New features and version history (continued)**

| Functional area | Feature description |
|---|---|
| | **NOTE:** Secure Boot is **disabled by default**. To configure, see the VEP4600 Operating System Installation Guide.<br>2. Fixed Diag in BIOS test reboot automatically and boot the system into back BIOS.<br>3. Fixed `PSU_test` in embedded BIOS. Shows PSU1 and PSU2 as filed. |
| BIOS 3.41.0.9-18 | 1. Beginning with BIOS VEP4600-BIOS-3.41.0.9-18.BIN Dell has introduced a BIOS setup manual admin user password.<br>a. If your system is running BIOS VEP4600-BIOS-3.41.0.9-18.BIN or later the BIOS setup manual admin user password is `<servicetag>!`<br>**NOTE:** The password is case-sensitive. The password **must match servicetag exactly**.<br>**NOTE:** For example if the service tag is: `GWGRG02` then the password is `GWGRG02!`<br>i. Setup `admin` user manual password: `<servicetag>!`<br>b. If your system is **running less than** BIOS VEP4600-BIOS-3.41.0.9-18.BIN there is **no default** setup manual admin user password.<br>**NOTE: No password** is required for setup manual user account.<br>2. New Intel microcode with security vulnerability fixes (microcode 0x02009606)<br>3. Update AMI BakervillePkg to label 29 to fix security vulnerability. |
| BIOS 3.41.0.9-16 | 1. Micro code security-related fixes<br>2. Intel security vulnerabilities<br>a. Intel-SA-00240: Intel CPU Local Privilege Escalation Advisory<br>i. CVE-2019-0151<br>ii. CVE-2019-0152<br>b. Intel-SA-00280:<br>i. CVE-2019-1113<br>ii. CVE-2019-11137<br>c. Intel-SA-00255:<br>i. CVE-2019-0139<br>ii. CVE-2019-0140<br>iii. CVE-2019-0144<br>iv. CVE-2019-0150<br>d. Intel-SA-00270:<br>i. CVE-2019-11135<br>e. Intel-SA-00271:<br>i. CVE-2019-11139 |
| BIOS 3.41.0.9-15 | 1. Fix for known Intel-SA-00233 Microarchitectural Data Sampling Vulnerabilities.<br>2. Fixed Missing SPF port 1 information with ethtool. |
| BIOS 3.41.0.9-14 | 1. Support for changing BIOS password from Linux<br>2. Fix for infrequent garbled DMI table outputs. |
| BIOS 3.41.0.9-13 | 1. DIAGS in BIOS enabled |

**Table 2. New features and version history (continued)**

| Functional area | Feature description |
|---|---|
| | 2. Add i350 network legacy PXE support.<br>3. Fix system boot from backup BIOS after enabling PCIe PHY test mode.<br>4. Grayed-out the subitems of Driver Health in BIOS Setup |
| BIOS 3.41.0.9-12 | 1. Option ROM dispatches policy:<br>● Restore if failure -> Disabled.<br>● Primary Video Ignore -> Disabled<br>● Device class option ROM dispatches policy (slot number 1, slot number 4, and so forth). All removed except for mass storage controller.<br>●<br>2. PCI subsystem settings:<br>● SR-IOV support -> Enabled<br>3. CSM configuration:<br>● Boot option filter -> UEFI and legacy<br>● Option ROM execution:<br>○ Network -> UEFI<br>○ Storage - > Legacy<br>○ Video - > Legacy<br>○ Other -> UEFI<br>4. Intel Ethernet connection 722 (All four)<br>● NIC configuration -> Wake on LAN - > Disable<br>5. Platform configuration:<br>● PCH configuration -> Azalia -> Disabled<br>6. IIO configuration:<br>● Socket0 configuration -> IOUO, IOu1 -> x8x8<br>7. Server management:<br>● Operating system watchdog timer -> Disabled<br>**NOTE:** Turn this on based on specific OS needs. |

**Table 3. BIOS 3.41.0.9-12 settings changes**

| BIOS 3.41.0.9-12 settings changes | |
|---|---|
| Updated the ECC test function. | PR# BL-90 |
| Added DMI information (Production Version/Serial Number/SKU Number/Family) to DMI Type 1 from FRU. | |
| Fixed the UART 1 that does not print out when BMC stays in uboot. | |
| Set MC slot Bifurcation based on GPIO. | PR# BL-207 |
| Support for new boot order in sequence: Legacy USB, UEFI USB, embedded network (PXE), UEFI hard disk, other UEFI device, legacy hard disk, UEFI shell. | PR# BL-180 |
| Set critical boot device timeout to 60 seconds for final failure to force boot to backup BIOS and disabled critical device test by default. | |
| Added function to read if SR-IOV is enabled and choose the correct PCI device list for POST PCI test. Post PCI test (critical test) will not fail if SR-IOV is enabled or disabled. | PR# BL-227 |
| PchHdAudio default set to disable. | |
| Changed default timeout to break into the setup menu to 10 seconds. | PR# BL-188 |
| Baseline for DIAG in BIOS feature is disabled. | |
| Set Dell proprietary GUID to DMI type 11. | |
| Deemphasis setting of MC1 and MC2. | PR# BL-207 |

# 3

# BIOS

**WARNING: Changing the BIOS may be detrimental to platform operations if the changes are not fully understood. Before you change the BIOS, if you have questions, contact your Dell Technologies technical representative.**

For the most current BIOS update information, see the *VEP4600 Release Notes*.

**Topics:**



# Known hardware behavior

This section provides details on the known hardware behavior corresponding to the VEP platforms.

## LED blink behavior

The network ports corresponding to the VEP platforms continue to glow even after shutting the ports down using the following ESXi command: `esxcli network vmnicX port down`

In the `esxcli network vmnicX port down` command, `X` denotes the physical NIC number.

This LED blink issue is a cosmetic issue, and you can safely ignore it.

You can observe this LED blink hardware behavior in the following VEP platforms: VEP4600 and VEP1400

You can observe this LED blink hardware behavior in the following ESXi versions: ESXi 6.7U3 and ESXi 7.0U3

# BIOS setup

To enter the BIOS setup, press **F2** or **DEL** key during the BIOS boot up.

By default, to enter the BIOS setup, you have three seconds to press the **delete** key during the BIOS boot up. To increase the time allowed, from the **BIOS setup** screen, select the **Boot** tab, then change the **Setup Prompt Timeout** number. The maximum prompt timeout is 10 seconds.

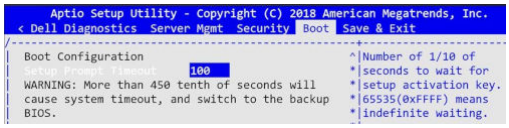



**Figure 2. Setup prompt timout**

The **Main** screen displays the BIOS and platform details such as the processor model, amount of memory, and so forth. Use the **Main** tab to set the date and time, which is saved to the real time clock (RTC).

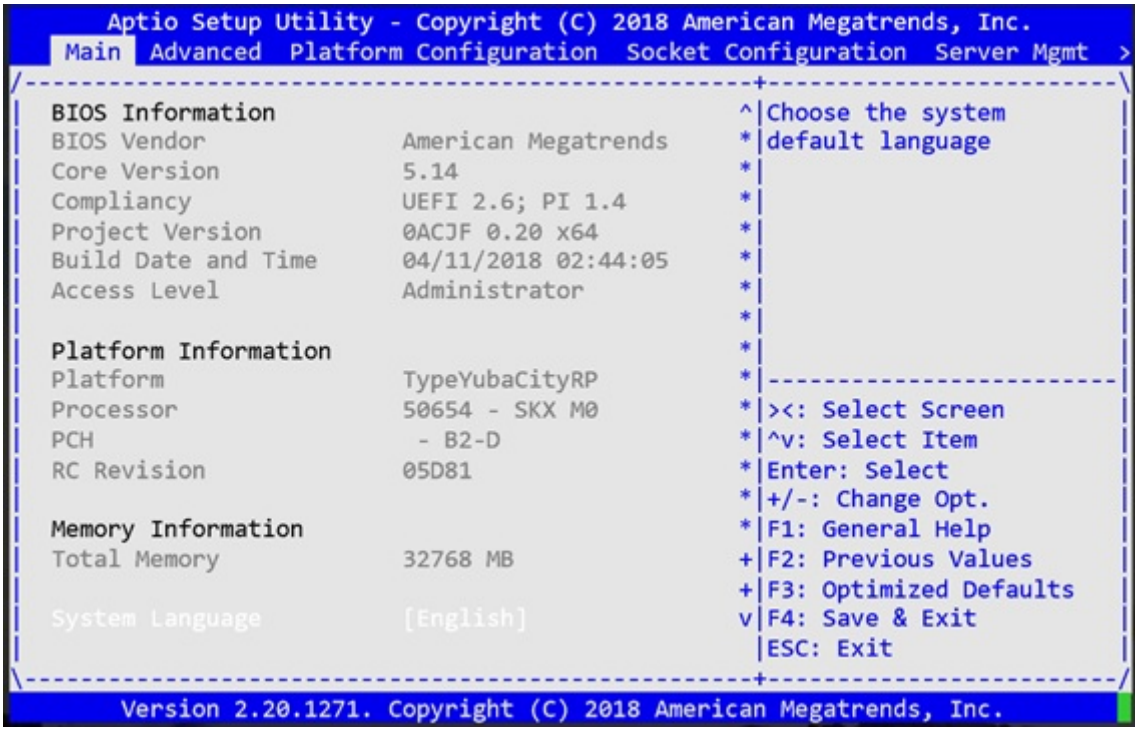
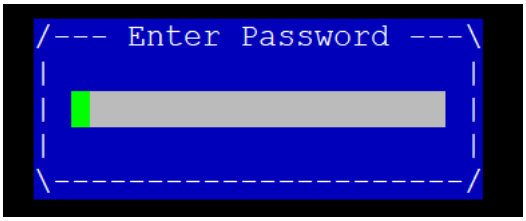



**Figure 3. BIOS setup**

# How to boot into BIOS settings after upgrade

## After upgrading BIOS to the latest release

1. Booting into BIOS settings prompts the user to type in BIOS administrator password.

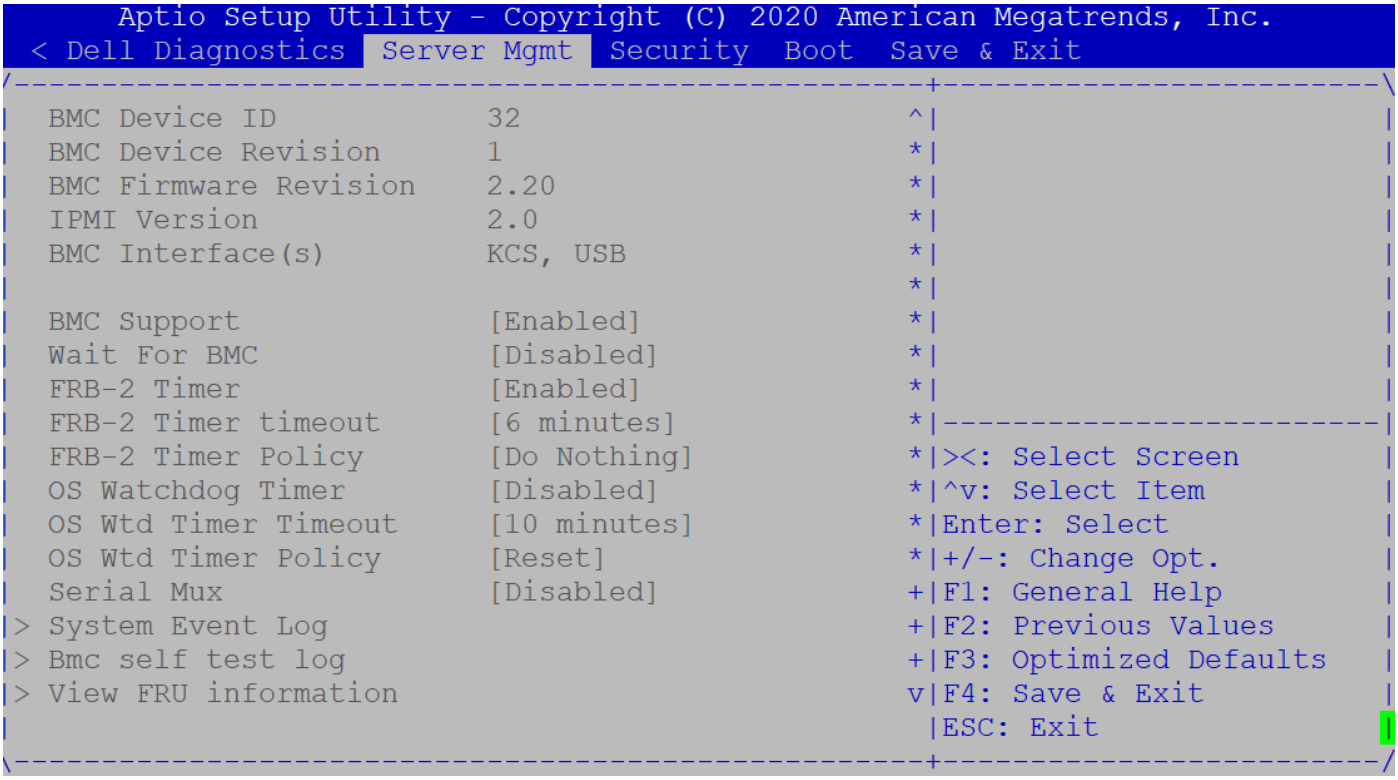



2. The default BIOS administrator password is `<servicetag>!`

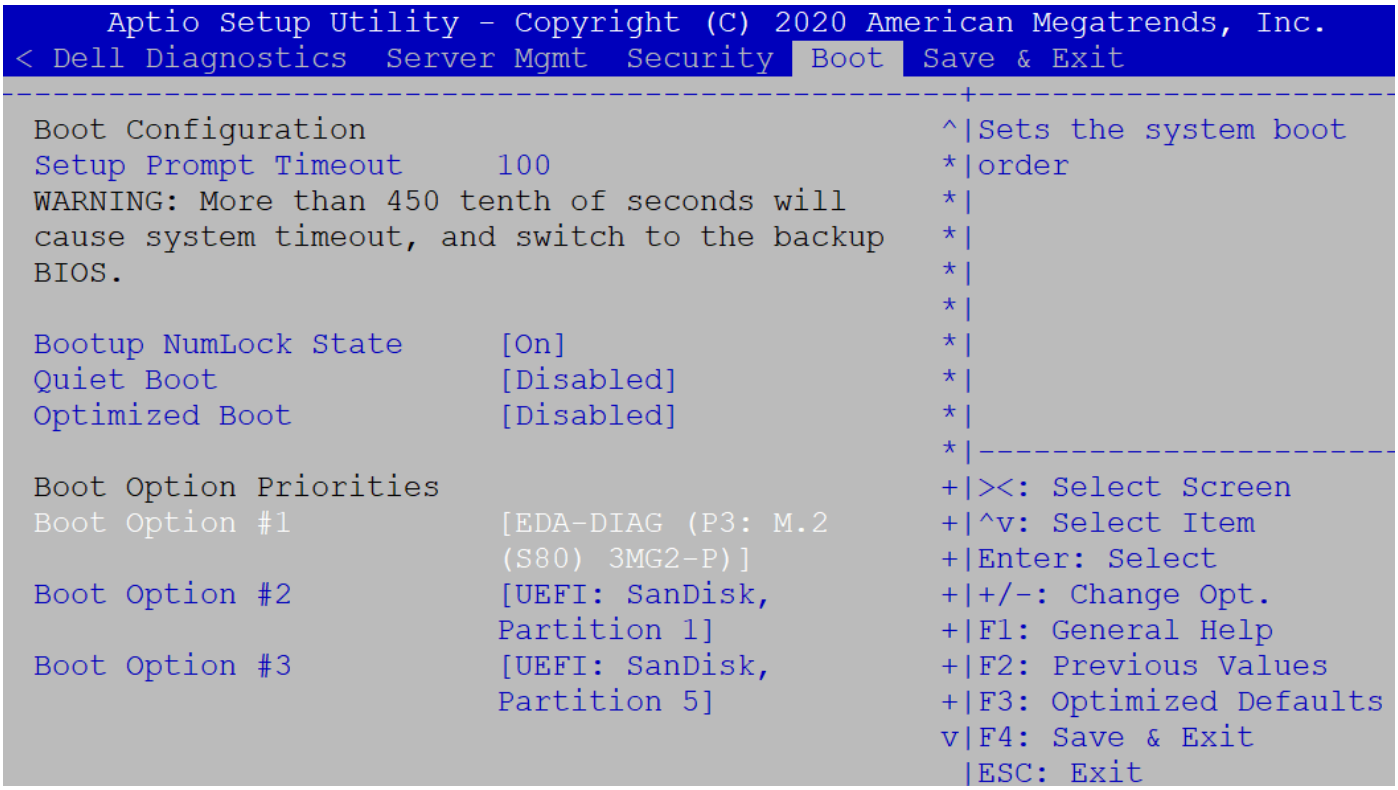
   For example if the service tag is:

   `GWGRG02` then the password is `GWGRG02!`

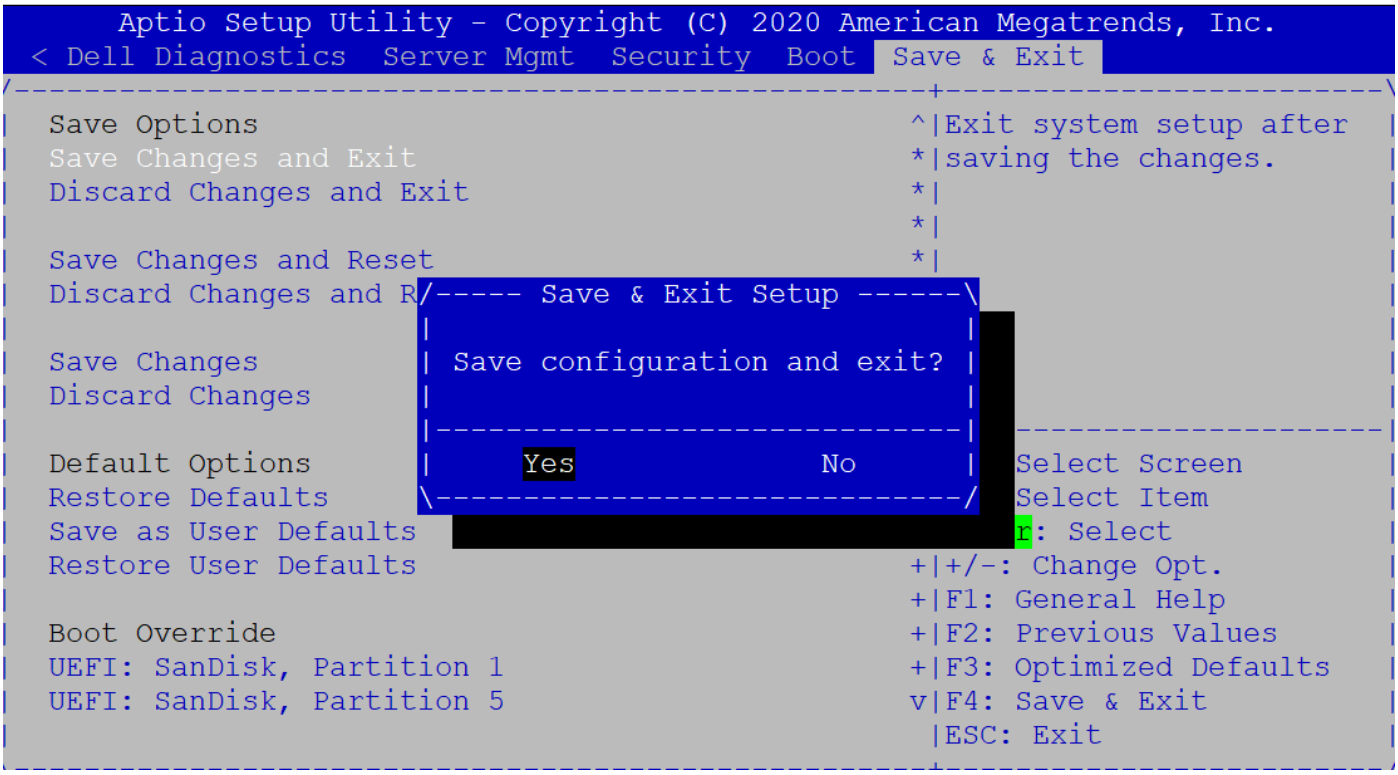
**NOTE:** Press **enter** to skip the password. The BIOS enters read-only mode. Many configuration entries become read-only, not configurable, see the following screenshot.




3. Navigate to the boot tab. You can still boot into all the eligible boot options, see the following boot option menu.




4. Navigate to the `Save & Exit` tab.




There are several ways to retrieve VEP product service tag.

# How to retrieve a VEP4600 product service tag

## Retrieve service tag from BMC, DIAG OS, and luggage tag

Finding service tag through BMC

- Log in and run the following command from the BMC console.

```
ipmitool -I lanplus -H 127.0.0.1 -U admin -P admin fru print | grep "Product
 Serial"
MC1 not present, ignore FRU
MC1 not present, ignore FRU
Product Serial : GWNRG02
```

Finding service tag through DIAG OS

- Boot into DIAG OS and run the following command.

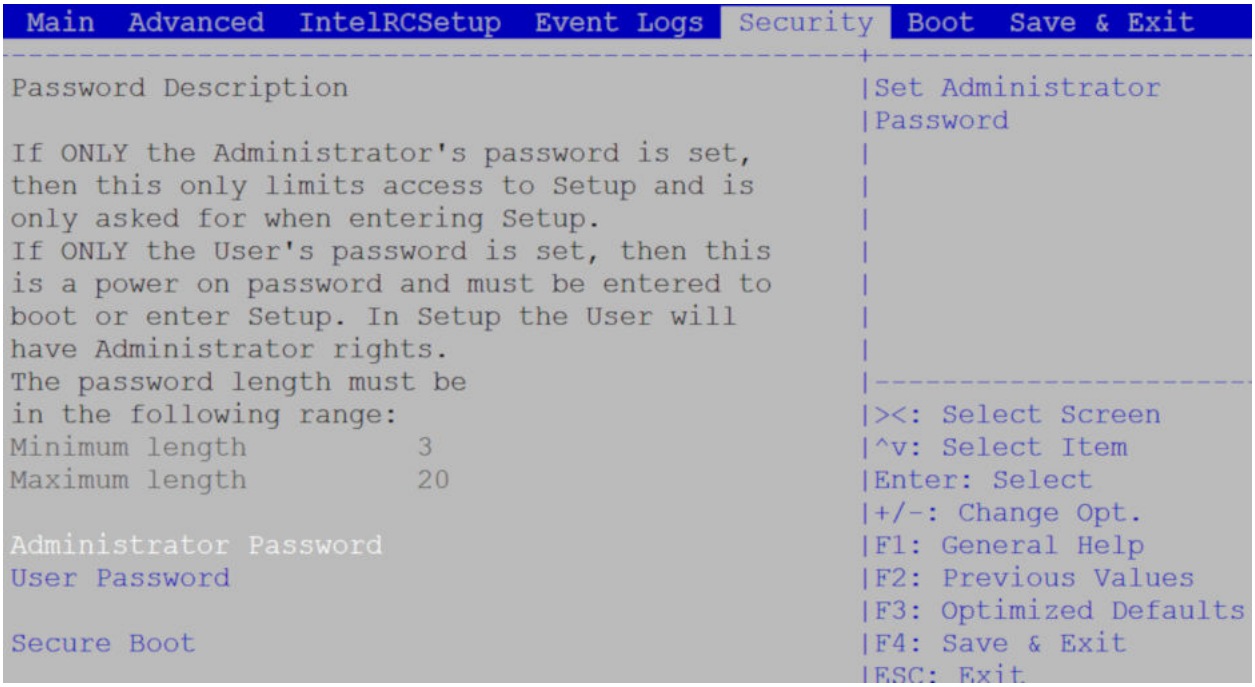
```
dmidecode -t 1 | grep Serial
Serial Number: GWNRG02
```

Finding service tag through luggage tag

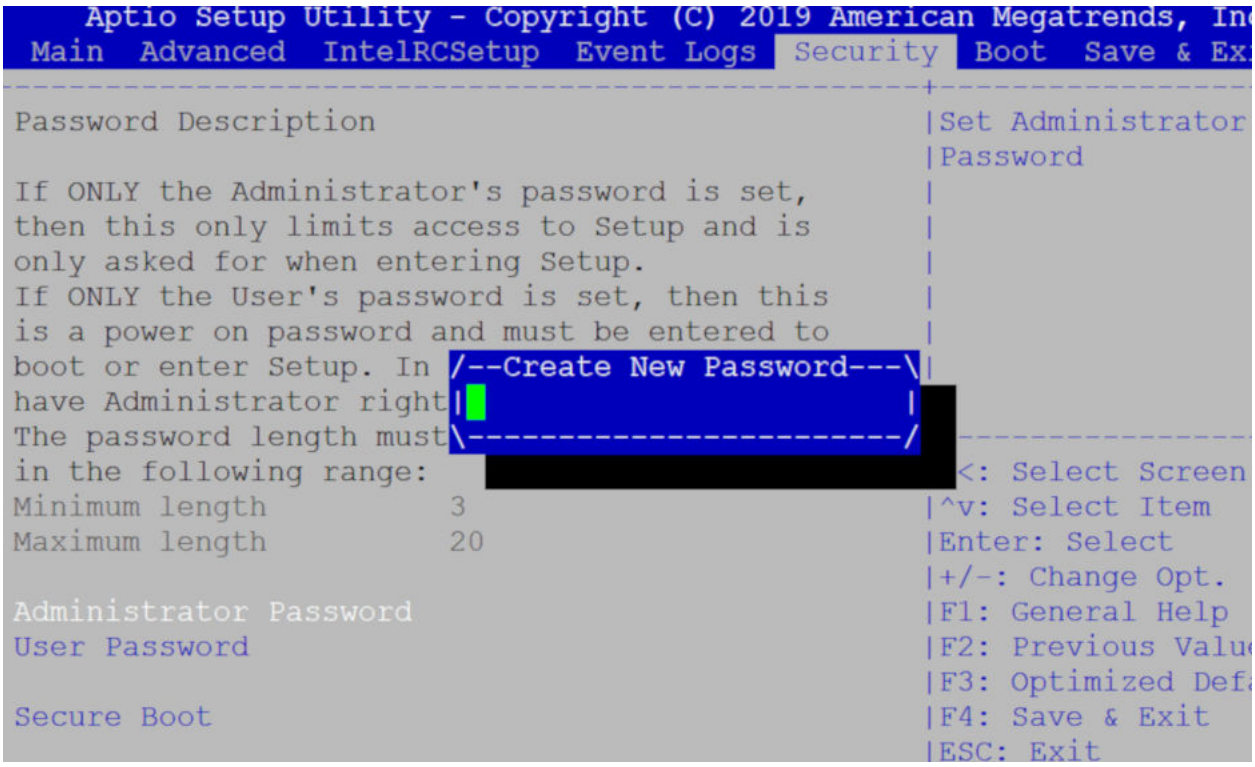
- Pull out the luggage tag from the unit upper right corner.


# How to change the default BIOS password

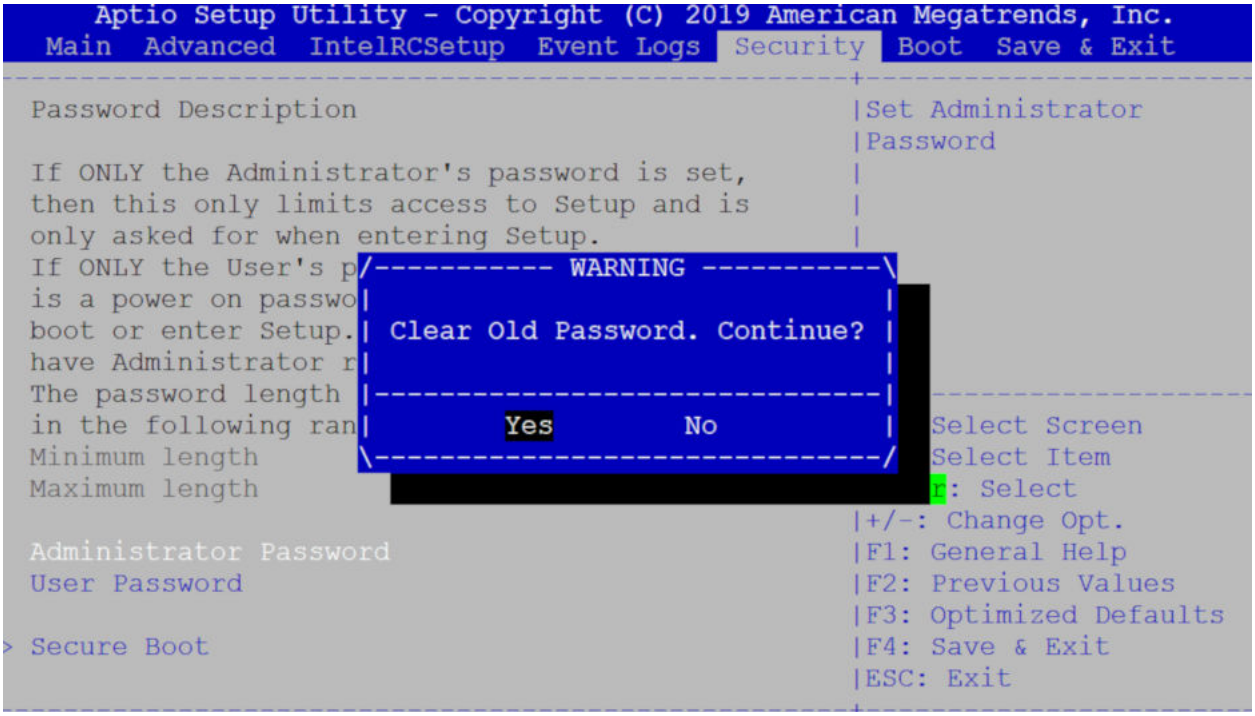
1. Boot into BIOS settings, enter the default password
2. Browse the `Security tab`.



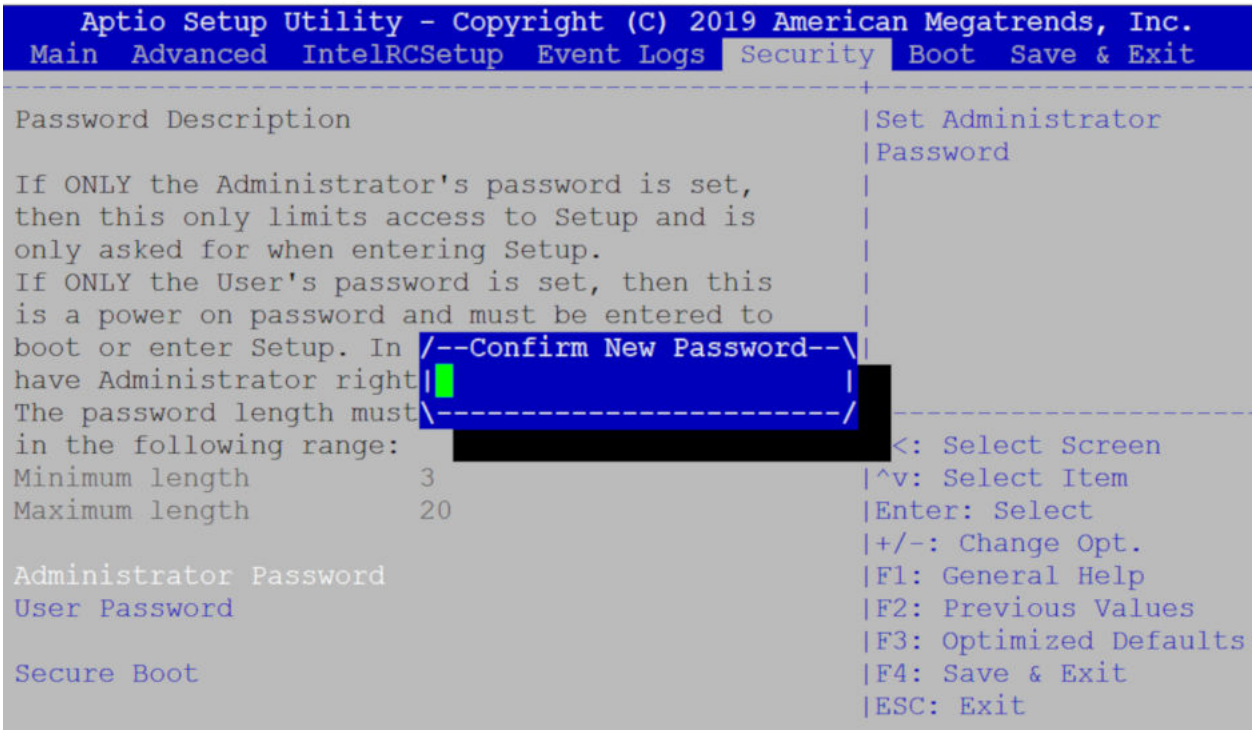

3. Press **enter** on `Administrator Password`.



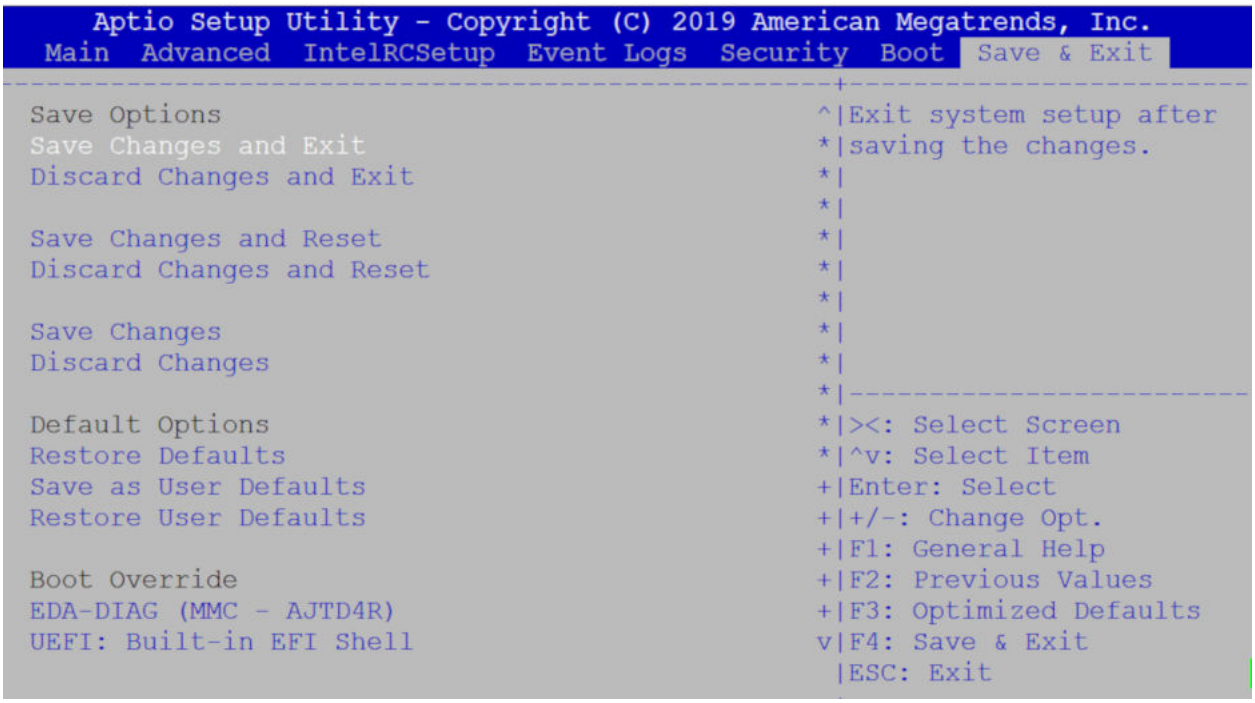

**NOTE:** If you press **enter** with no password, the following appear.



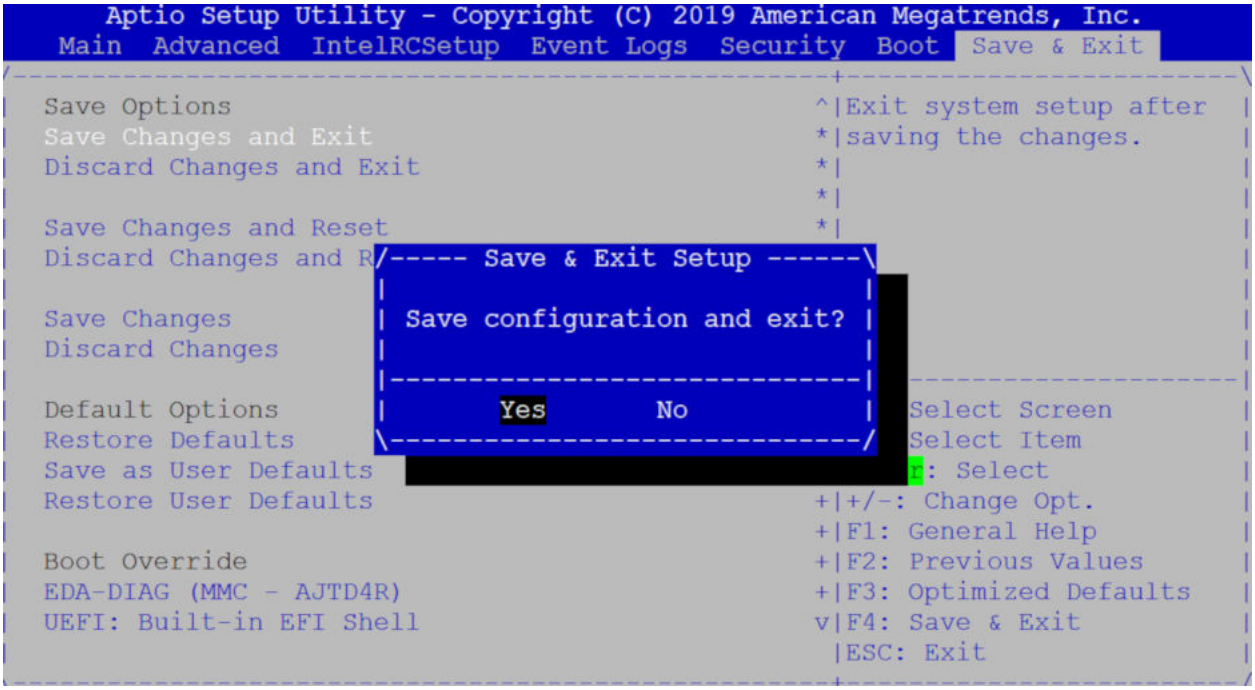

4. Select **Yes** to confirm the old password erased. Once saved and rebooted, no more password required for the subsequent BIOS setting sessions.




5. Enter the same password again to confirm.




6. Browse the **Save & Exit** tab and press **enter** on `Save Changes and Exit`.




# Password reset

Steps to set password to `<servicetag>!` .

## Unified firmware updater admin password reset

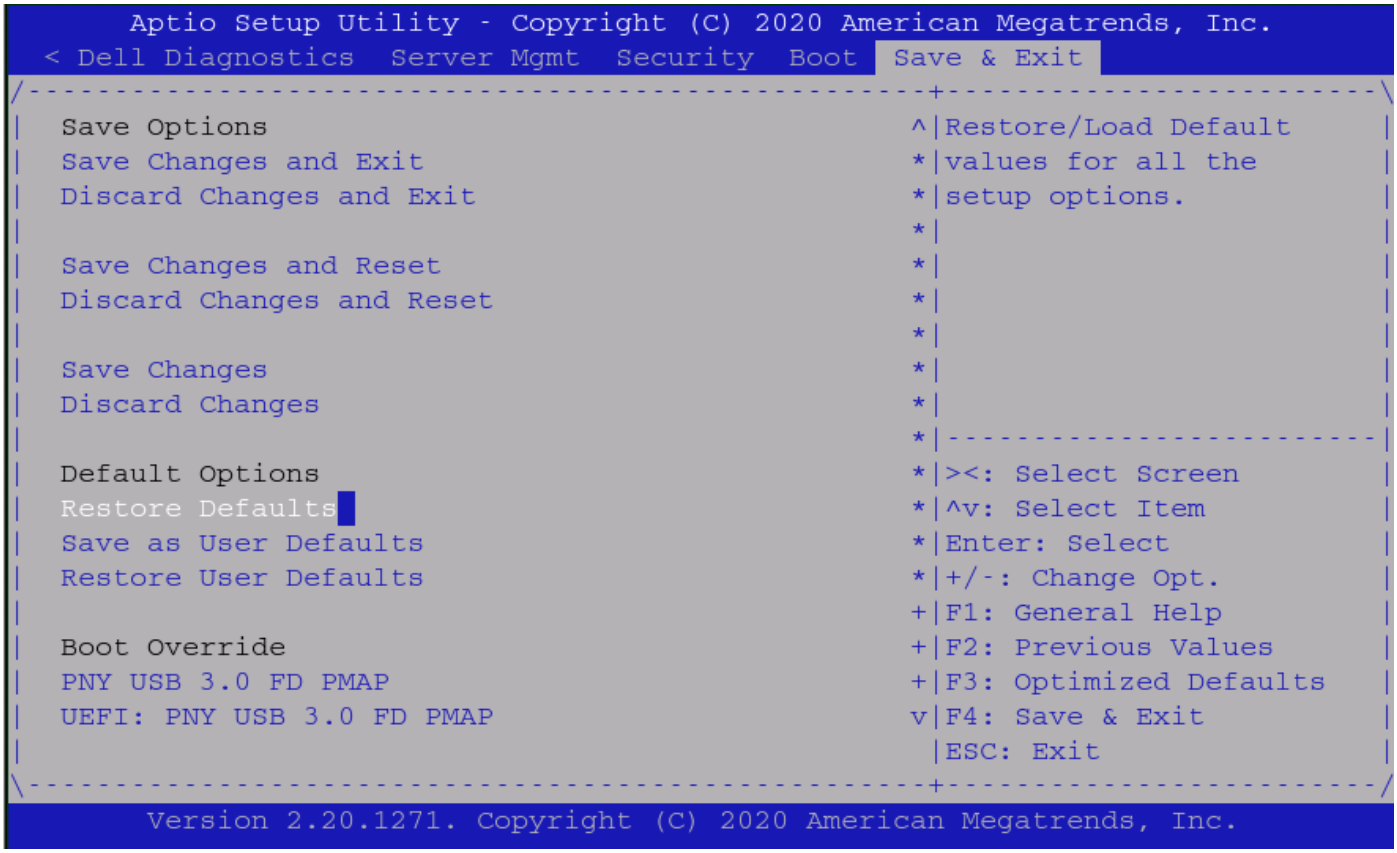
An `admin` user can reset the password in the United firmware updater 3.7.

**NOTE:** This functionality is **only** for an `admin` user.

**NOTE:** **No** password is required for a `user` account.

The following steps permit an user to **reset** an `admin` password to the default `<servicetag>!` password.

1. Select either `Delete` or `F2` to go to the setup menu .
2. Press **enter** to get into the user account.
3. Select `Save & Exit`, then `Restore Defaults`, and finally `Save Changes`.
4. Select `Reset` to return the admin password back to `<servicetag>!`




**NOTE:** The Unified firmware updater **retains** an `admin` old password during the Unified firmware updater update by default **if there is a password setup before the update**.

**NOTE:** The Unified firmware updater tool **cannot recover** the `admin` user's old password if the user has forgotten it.

# Hardware flow control

Hardware flow control is not enabled on the console port by default.

Follow the steps below in BIOS settings to enable the hardware flow control for the console port.

1. Select the **Boot** menu tab. Boot into the BIOS settings using the up and down arrow keys.

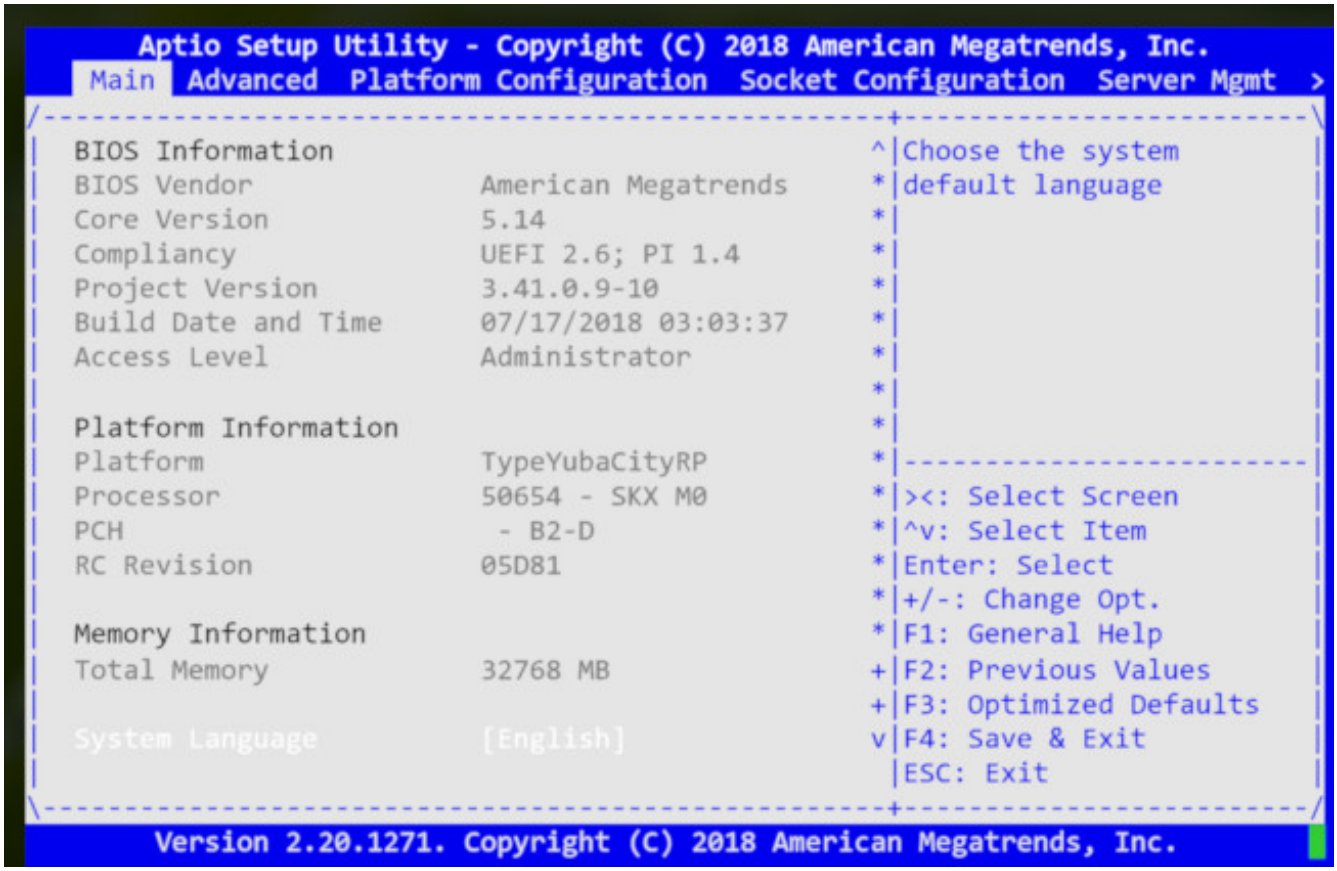



**Figure 4. BIOS main screen**

2. Select **Advanced** then **COM0 (Console Redirection Settings)** and **Hardware RTS/CTS** in the `Flow Control` popup menu.

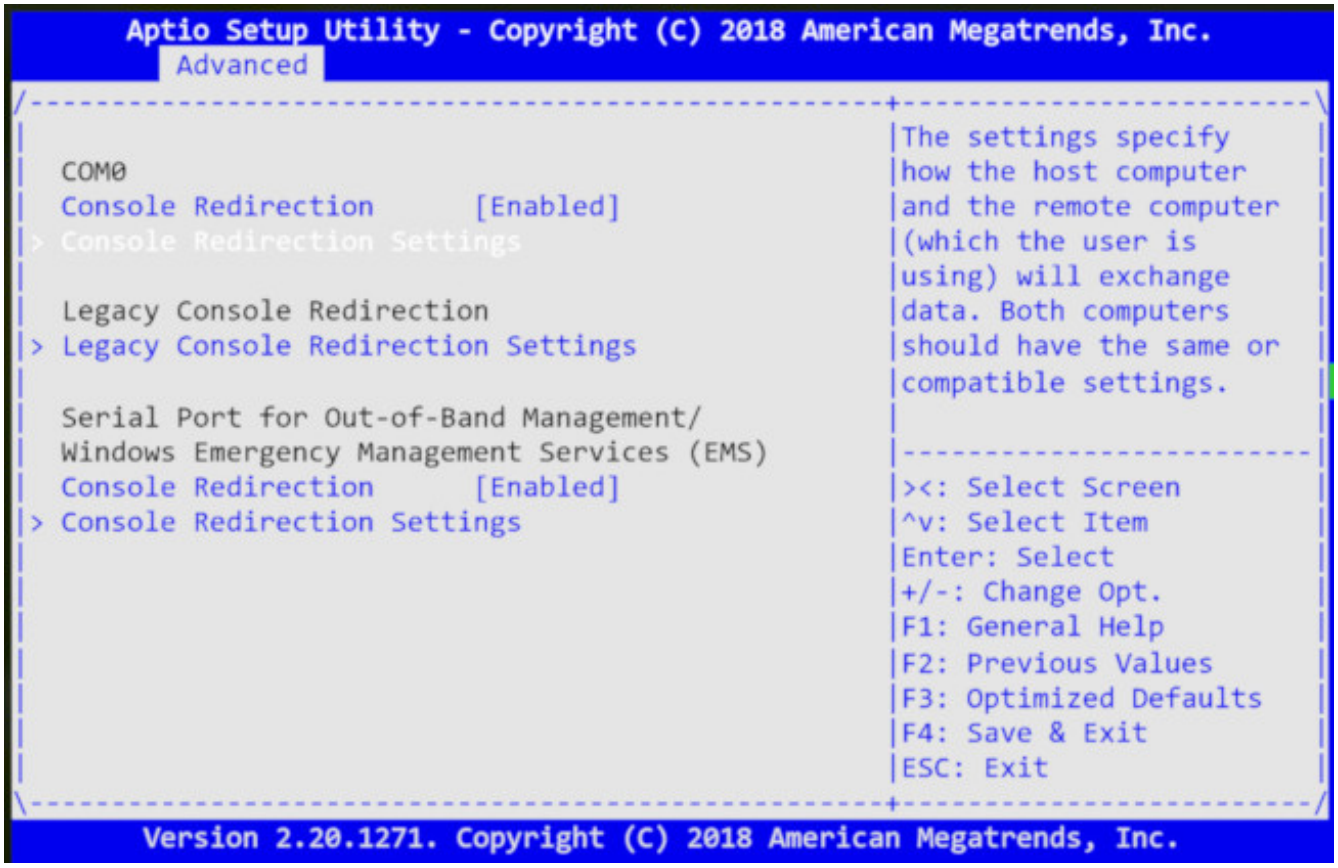



**Figure 5. Advanced tab**

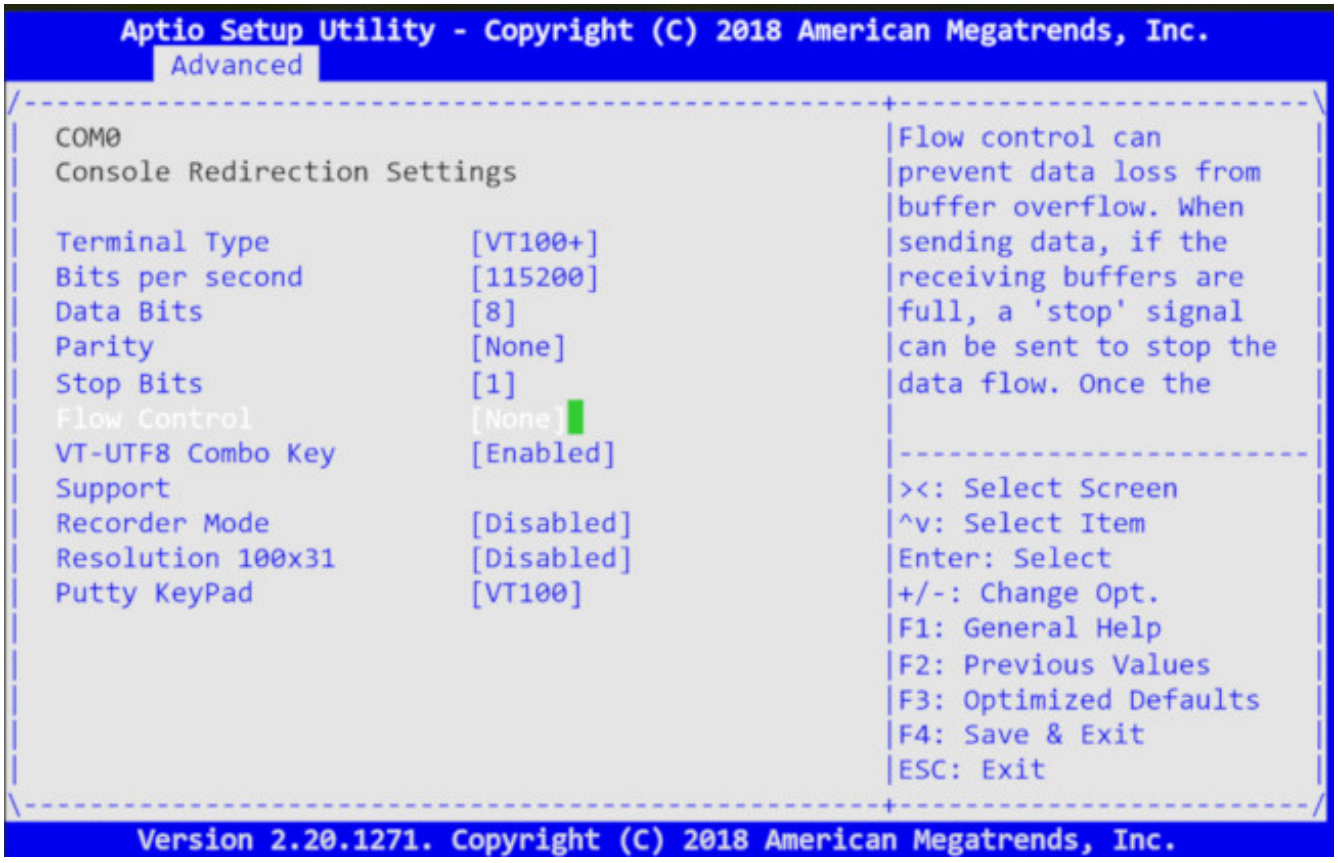



**Figure 6. COM0 (Console Redirection Settings)**

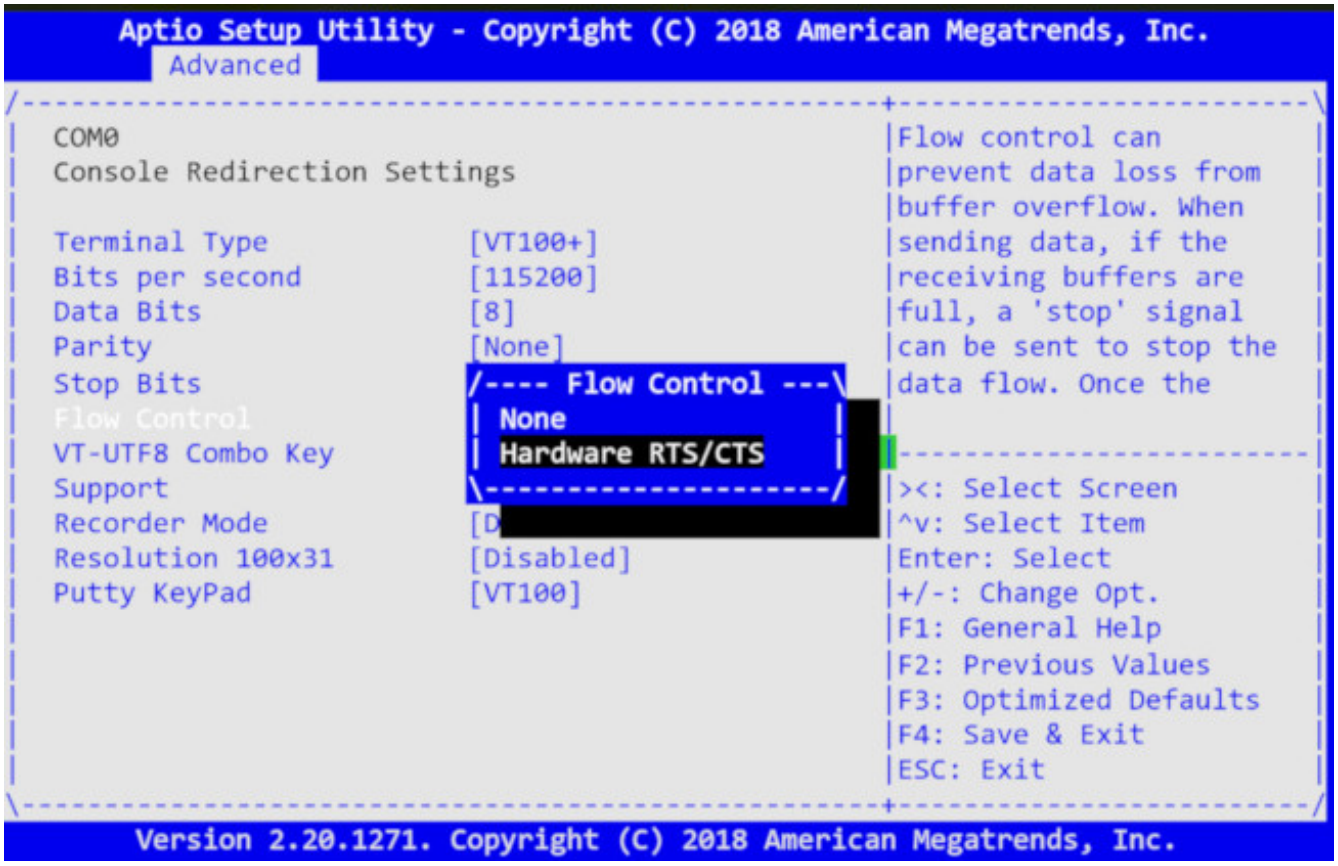



**Figure 7. Hardware RTS/CTS**

3. Press **F4** to save and exit BIOS.

# Super IO configuration

The VEP4600 only has the serial port on the Super I/O (SIO) chip. The chip settings are preconfigured and normally do not need changing.

However, you can use the BIOS to change the Super I/O chip settings, such as the I/O Base, interrupt request line (IRQ), and direct memory access (DMA) channel. To access these settings, from the **BIOS setup** screen, select the **Advanced** tab, then select **SIO Configuration**.

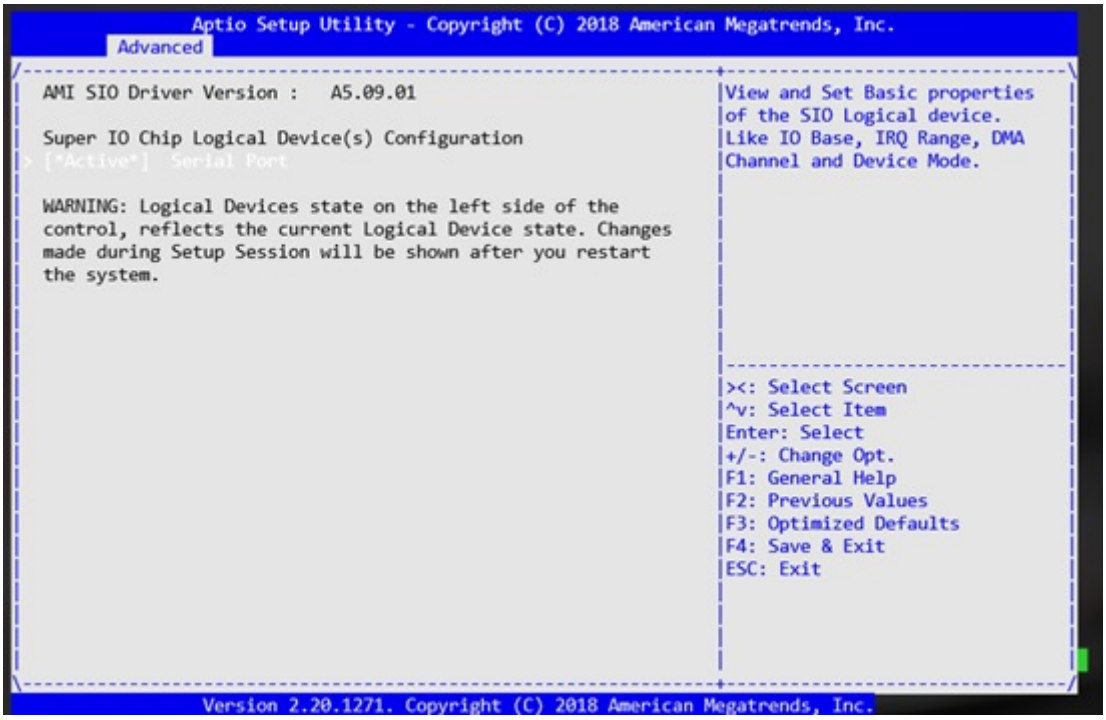



**Figure 8. Super I/O configuration**

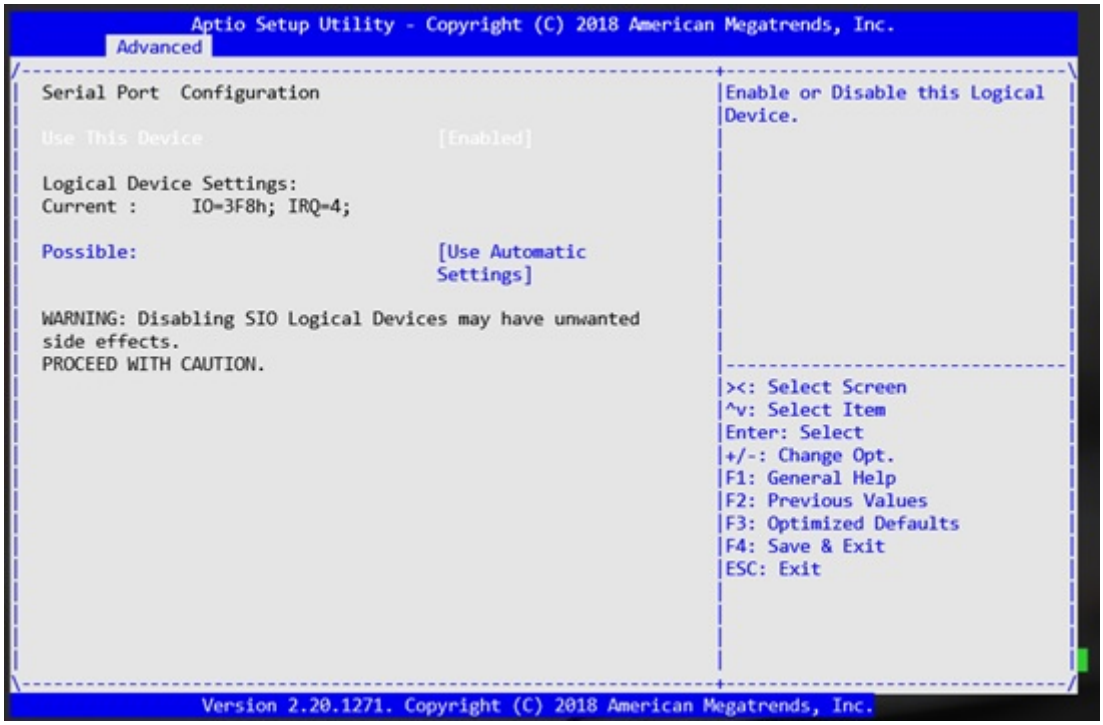



**Figure 9. Super IO configuration**

# Boot order

The BIOS looks for a bootable image in the Boot order setting order list. The BIOS then loads and boots the image. To access the boot order setting, from the **BIOS setup** screen, select the **Boot** tab, then select **Boot Option Priorities**.

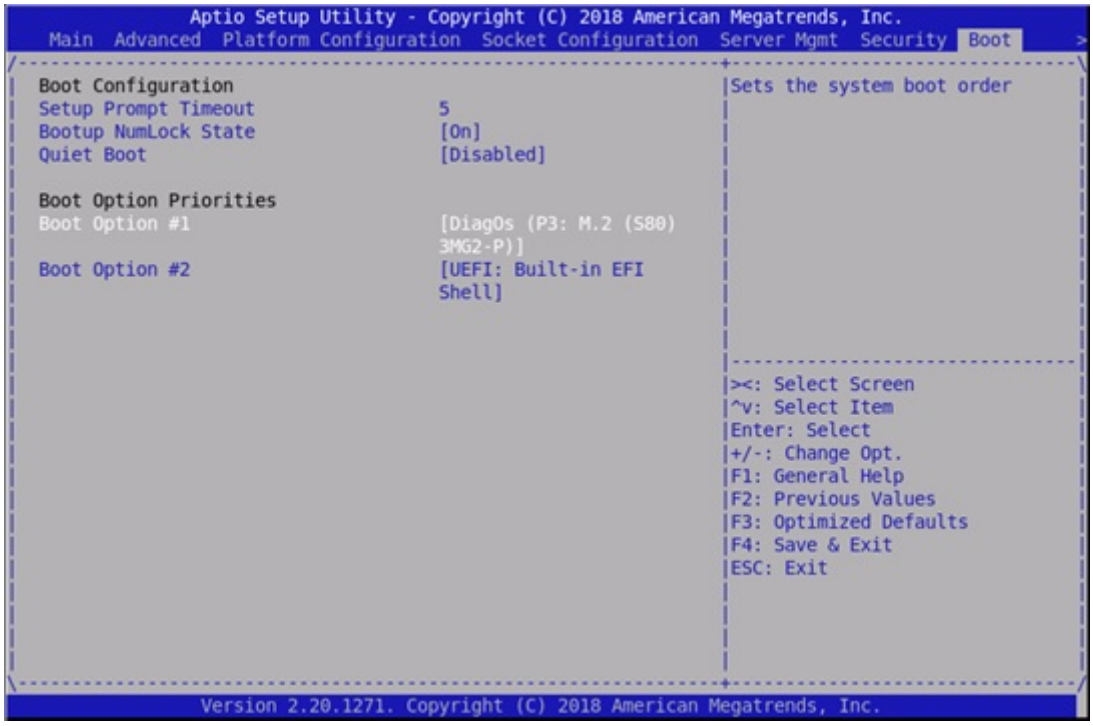



**Figure 10. Boot order**

# Server management

VEP4600 has an on-board baseboard management controller (BMC) to monitor system health. During Boot up, the BIOS communicates with the BMC and exchanges messages with the BMC to log events, get BMC self-test results, and configure BMC network parameters. To configure BMC to use Static IP or dynamic host configuration protocol (DHCP), use the BIOS. To access BMC settings, from the **BIOS setup** screen, select the **Server Mgmt** tab, then **BMC Network Configuration**.

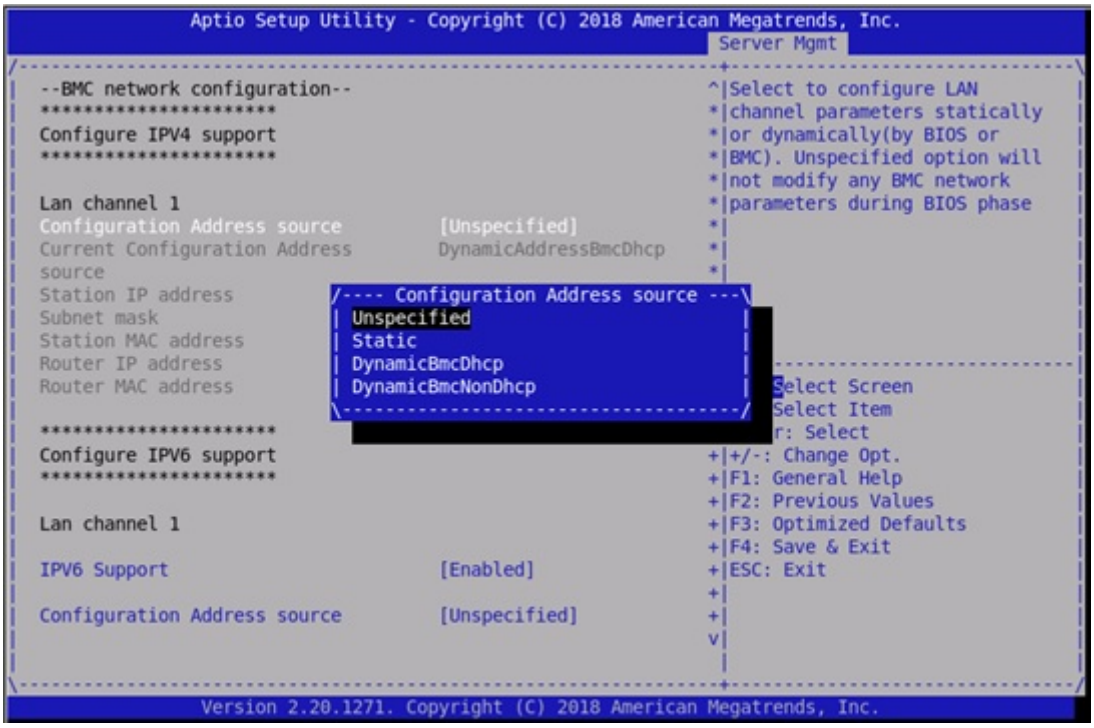



**Figure 11. Server management**

After an event, the BIOS logs a message to the BMC. The BMC stores these messages in nonvolatile storage. Apart from the BIOS, health monitoring software and system software also logs messages to the BMC system event log (SEL). View these messages from the **BIOS setup** screen, select the **Server Mgmt** tab, then select **View System Event Log**.

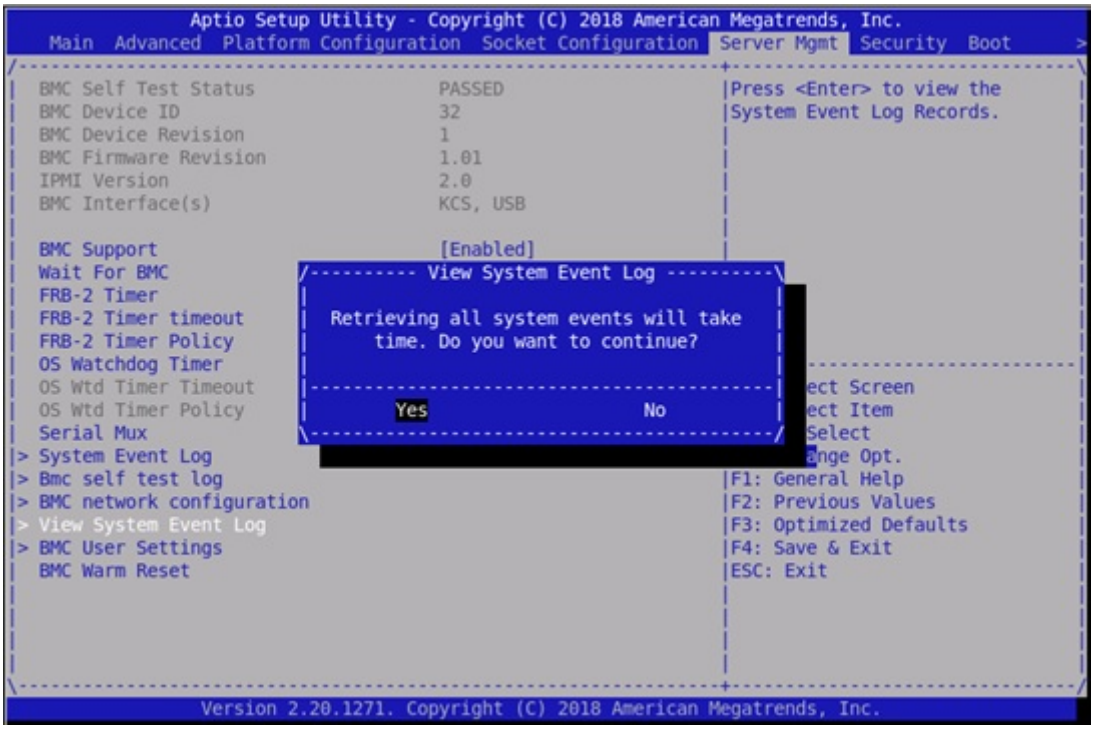



**Figure 12. View system event logs**

You can add, delete, access, or modify user rights. Manage the BMC user account from the **BIOS setup** screen, select the **Server Mgmt** tab, then select **BMC User Settings**.

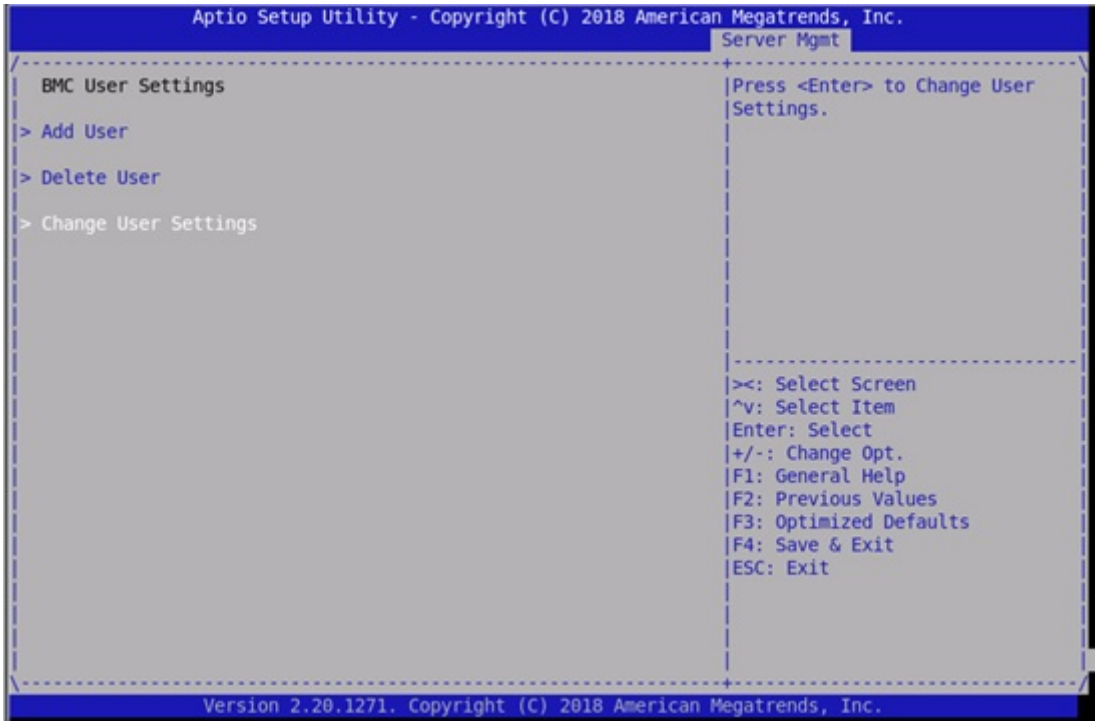



**Figure 13. BMC user settings**

# Option ROM dispatch policy

Option read-only memory (ROMs) contain firmware that the BIOS executes. The values listed on this screen and in the **Compatibility Support Module** screen use default values when the **Restore if Failure** setting is **true** and the BIOS fails to boot up.

**NOTE:** Changing the *option ROM* settings may effect the BIOS boot up. Dell Technologies recommends keeping the default value of *Restore if Failure* equals *true*.

Access the option ROM dispatch policy screen from the **BIOS setup** screen, select the **Advanced** tab, then select **Option ROM Dispatch Policy**.

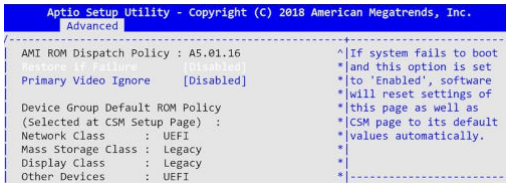
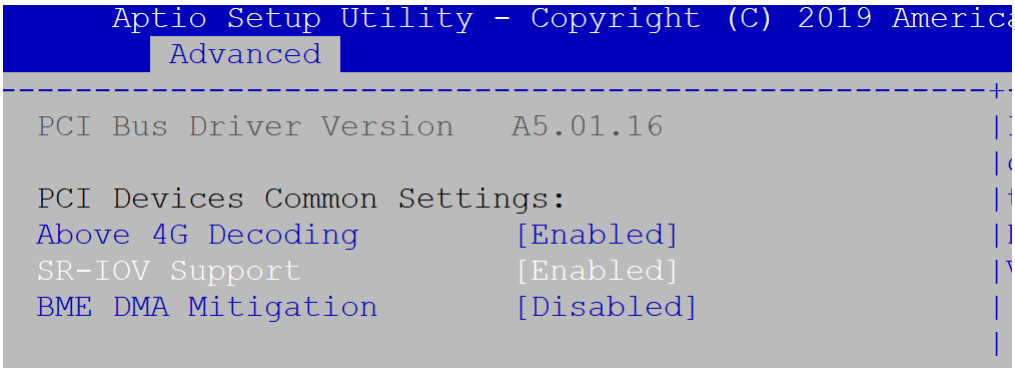



**Figure 14. Option ROM dispatch policy**

# SR-IOV support

If VEP4600 uses Virtualization Technologies, you must enable the single root I/O virtualization (SR-IOV) **SR-IOV support** option.

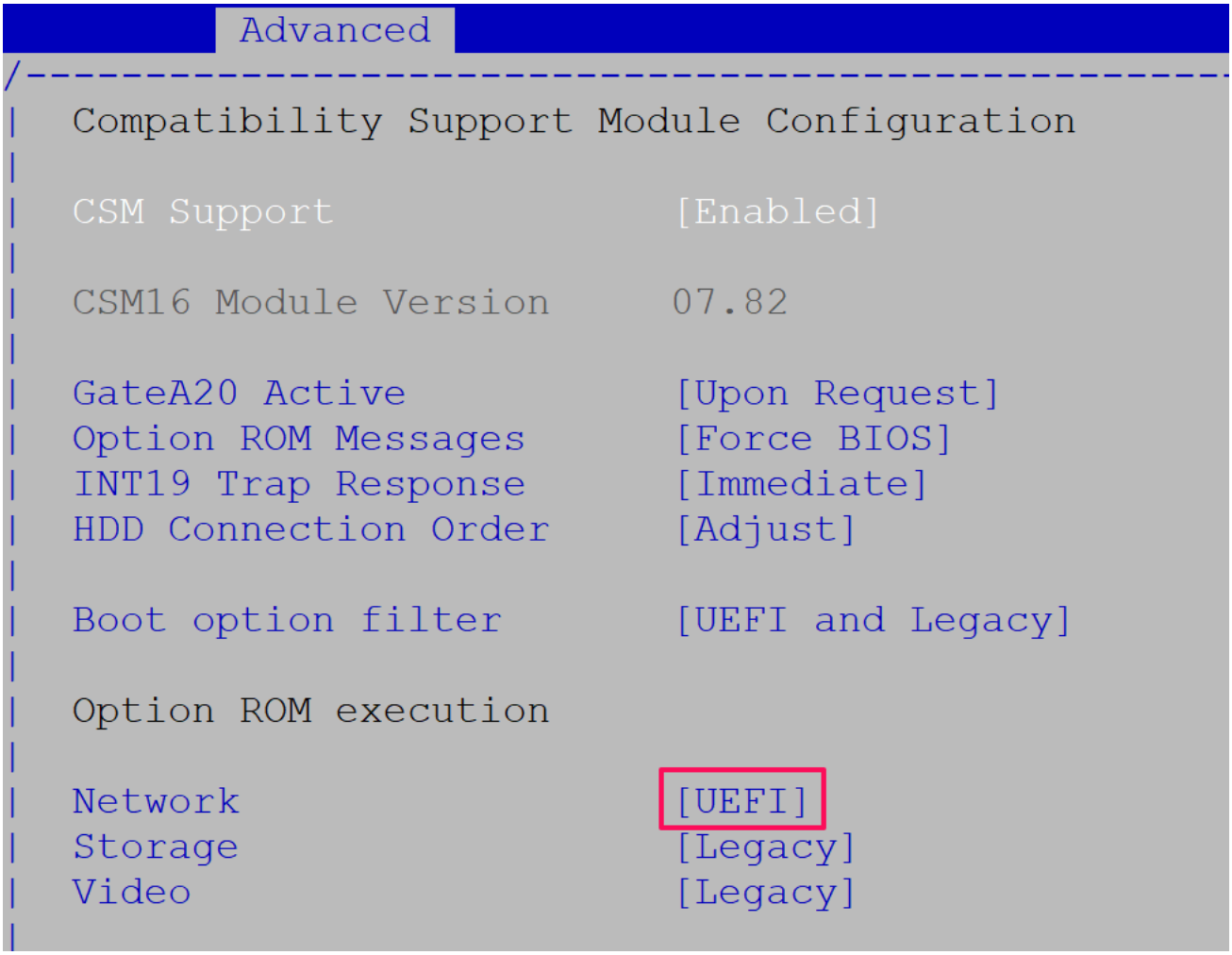
Access this option from the `BIOS setup screen`, select the `Advanced` tab, then select `SR-IOV Support.`



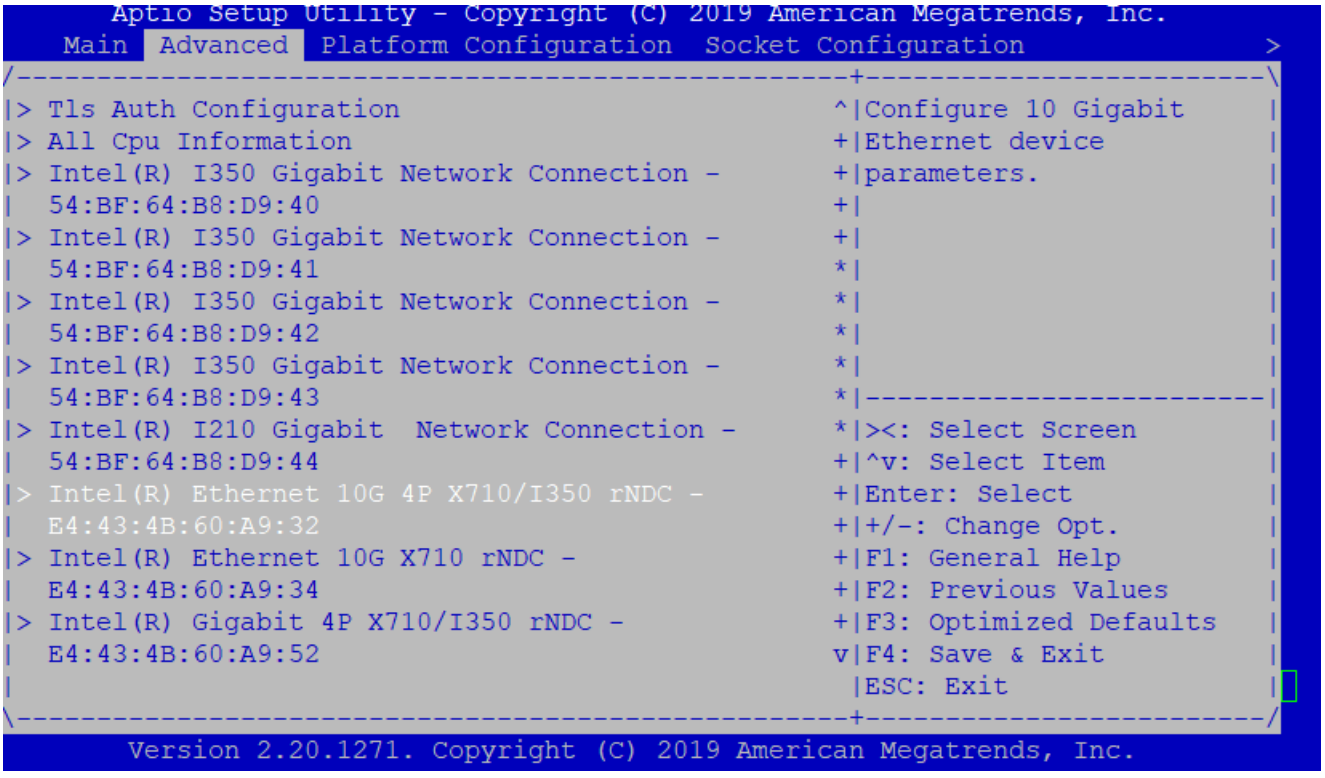

**NOTE:** This SR-IOV feature is **enabled** in the BIOS factory **default** configuration.

Configure SR-IOV in X710 rNDC card.

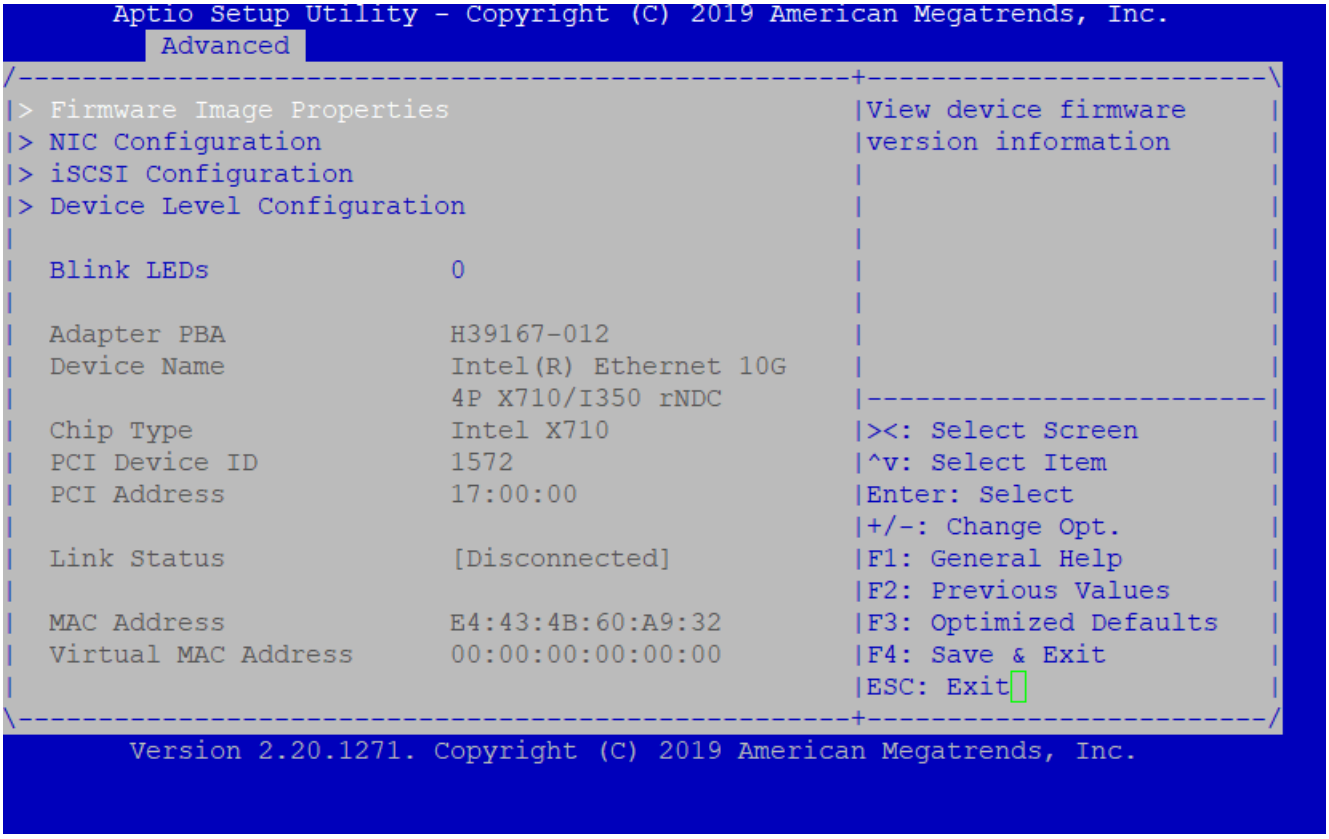
- Check Network UEFI Configuration



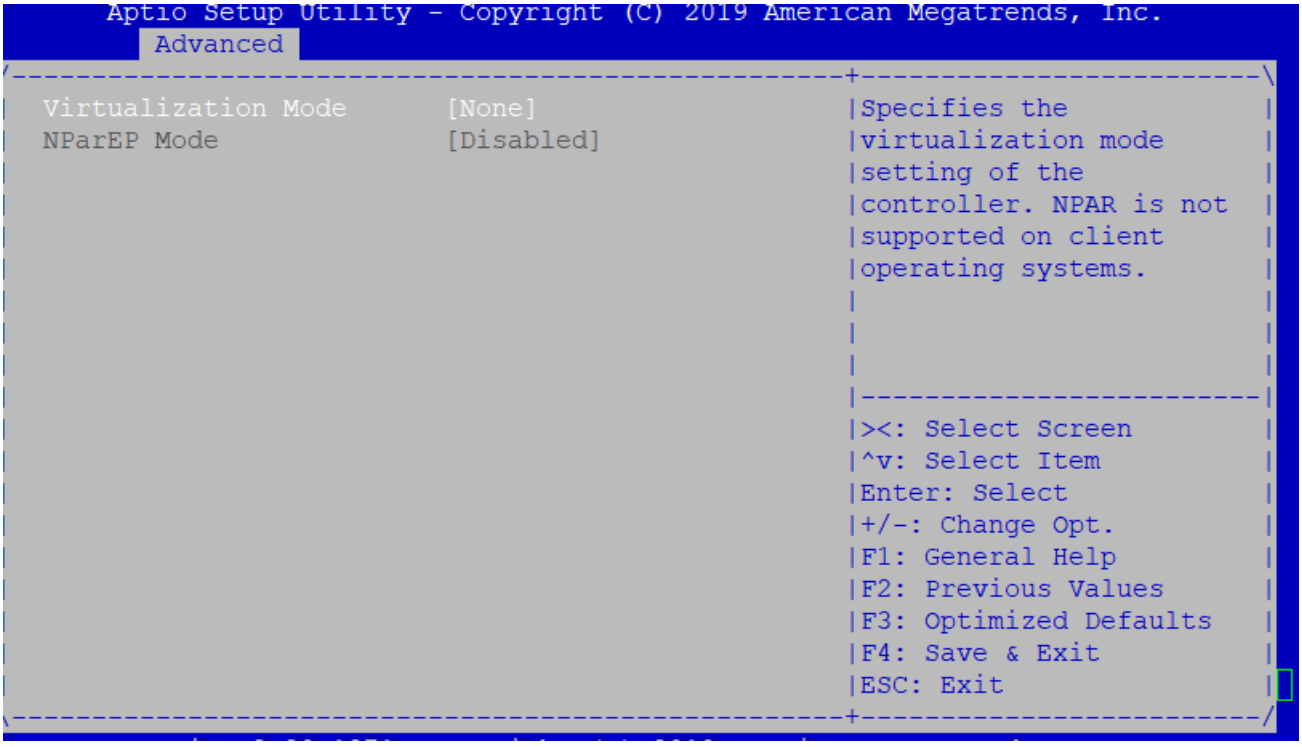

- Scroll down and select the X710 interface card.



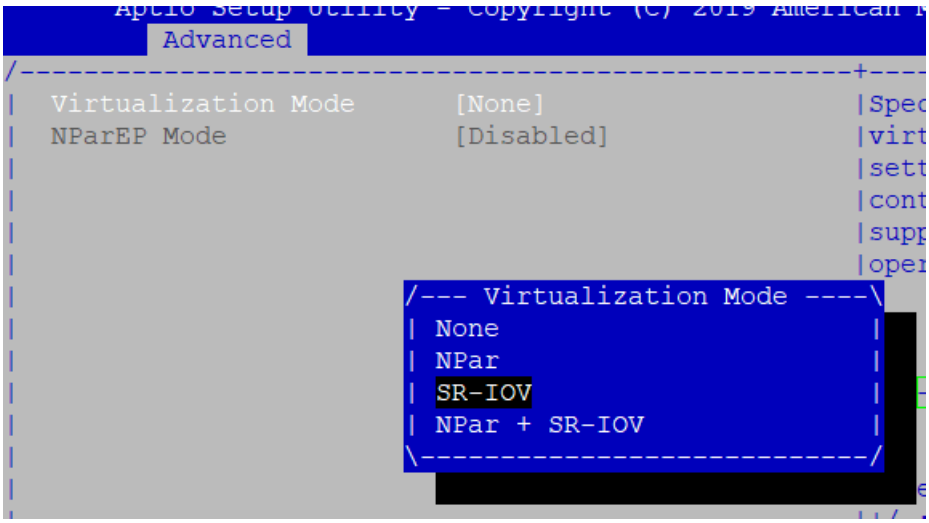

- Select `Device Level Configuration` and press the **enter** key for the selected X710 card.




- Select `Virtualization Mode` for device level configuration and press the **enter** key.




- Select `SR-IOV` in the `Virtualization Mode` popup menu and press the **enter** key.




# USB 3.0

To support universal serial bus (USB) 3.0 in operating systems, set the extensible host controller interface (xHCI) **XHCI Hand-off** option to **enabled**. Access this setting from the **BIOS setup** screen, select the **Advanced** tab, then select **USB Configuration**.

If the BIOS must support USB 2.0 devices—legacy USB devices—leave **Legacy USB Support** set to **enabled**, shown below.

Because the box is connected using the universal asynchronous receiver-transmitter (UART) console, traditional keyboard or mouse are not connected to the USB ports.

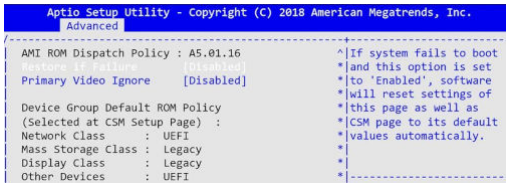



**Figure 15. USB 3.0 option**

# PXE and HTTP boot support

VEP4600 allows the platform to boot an operating system using Preboot Execution Environment (PXE) boot. To enable PXE boot, set the **Network Stack** option to **enabled**. Access this setting from the **BIOS setup** screen, select the **Adanced** tab, then select **Network Stack**.

The BIOS also supports hypertext transfer protocol (HTTP) boot. Use both HTTP and PXE boot over IPv4 or IPv6.

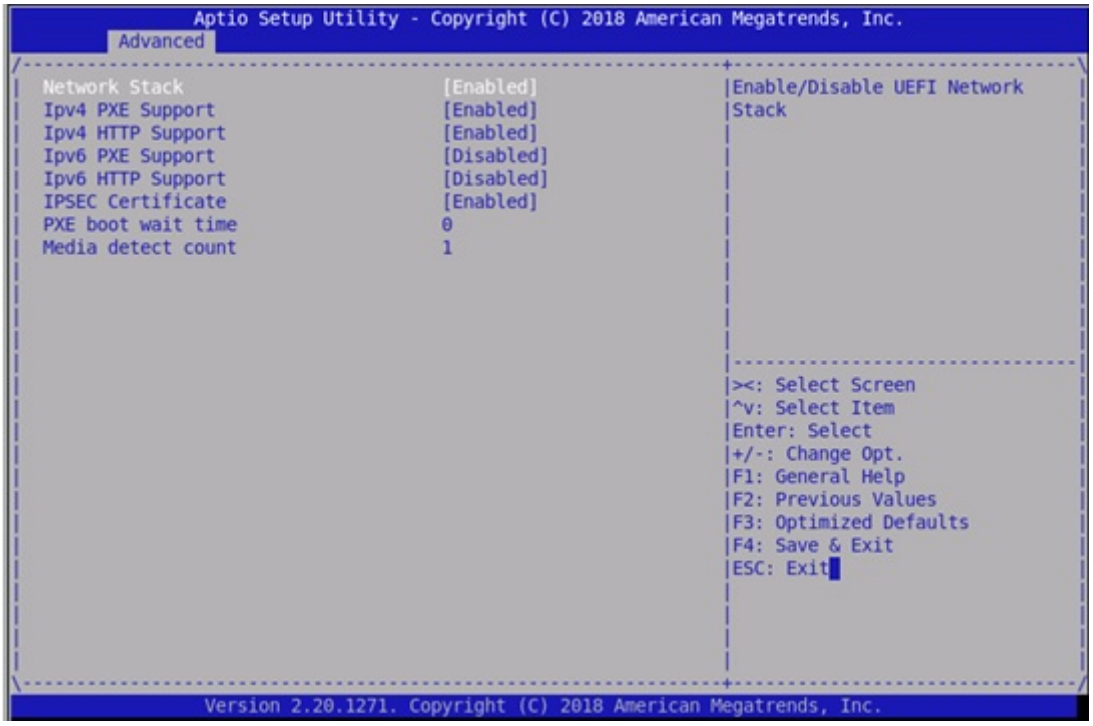



**Figure 16. PXE and HTTP boot support**

# Network interface configuration

VEP4600 has two 10GbE small form-factor pluggable plus (SPF+) ports, four Gigabit ports, and one Gigabit management port.

The BIOS uses these ports for PXE boot. You can configure the **wake on LAN** setting. You can also configure the one Gigabit port to auto configure or set to a specific speed. Access these settings from the **BIOS setup** screen, select the **Advanced** tab, then select the **Intel(R) I350 Gigabit Network Connection**, **Intel(R) I210 Gigabit Network Connection**, or **Intel(R) Ethernet Connection X722 for 10GbE SFP+** settings.

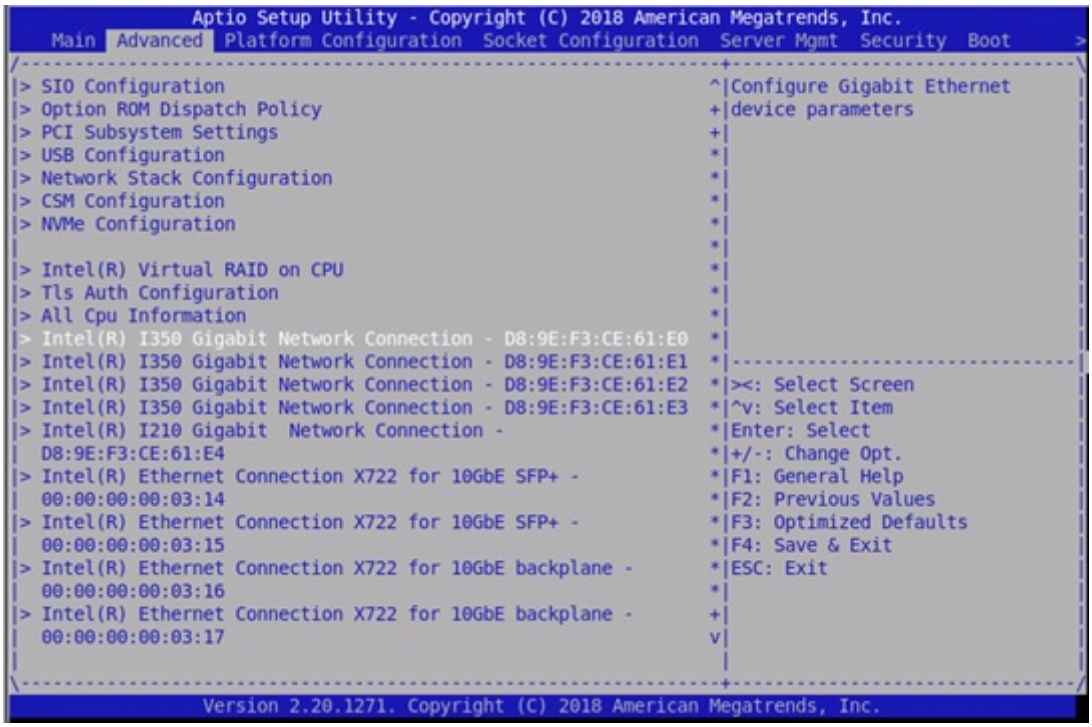



**Figure 17. Network interface options**

# Advanced power management

Access the settings for power management from the **BIOS setup** screen, then select the **Socket Configuration** tab. On the **Advanced Power Management Configuration** screen, select **Memory Power & Thermal Configuration**.

By default, **SpeedStep(P states)** and **Autonomous Core C-State** are disabled.

The **Software controlled T-States** option is also disabled by default.

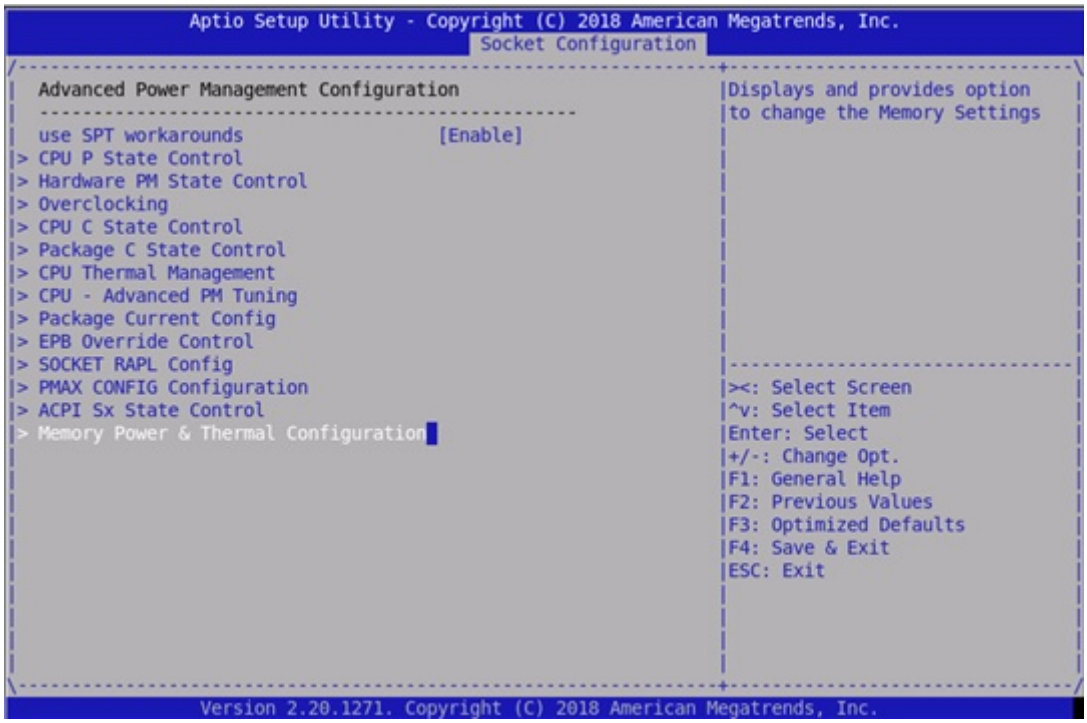



**Figure 18. Advanced power management options**

# Trusted computing

The BIOS provides options to enable or disable trusted platform module (TPM) security. BIOS has two provision coverage ratio (PCR) banks and provides options to select **SHA-1** or **SHA256** for these banks. Access the TPM settings from the **BIOS setup** screen, then select the **Advanced** tab, then select **Trusted Computing BIOS settings**.

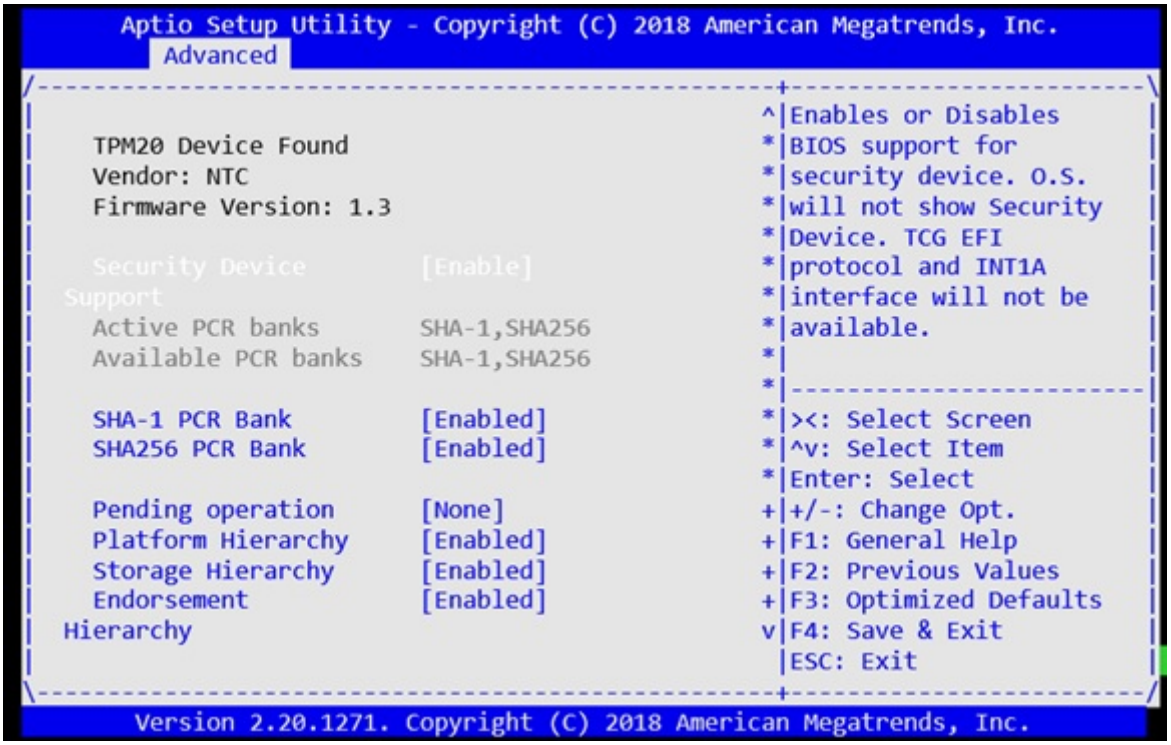



**Figure 19. Trusted computing options**

# Embedded DIAGS

Embedded DIAGS are available in BIOS 3.41.0.9-23 release and DIAG OS R3.41.3.81-9 release.

Embedded DIAGS in the BIOS validates and verifies all the system's components are operating normally.

System diagnostics include:

1. PSU
2. Fan
3. I2C
4. RTC/CMOS
5. PCI
6. DIMM
7. IPMI
8. Storage
9. Critical Device
10. Temperature

**NOTE:**

See uCPE Networking DIAG OS Guide for details at https://www.dell.com/support.

# Secure Boot

## Secure Boot activation steps

**NOTE:** Secure Boot is disabled by default.

This functionality is designed to work with Microsoft keys which are embedded into the BIOS.

**NOTE:** Must enable a signed image for **non-Microsoft** operating systems.

1. Select `Secure Boot` from the `Security` BIOS window.

2. Select `Enabled` from the open `Secure Boot` BIOS window.


# System Security Settings details

**About this task**

The **System Security Settings** screen details are explained as follows:

| | |
|---|---|
| **Secure Boot** | Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to **Disabled** by default. |
| **Secure Boot Policy** | When Secure Boot policy is set to **Standard**, the BIOS uses the system manufacturer key and certificates to authenticate pre-boot images. When Secure Boot policy is set to **Custom**, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to **Standard** by default. |
| **Secure Boot Mode** | Enables you to configure how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx).<br>If the current mode is set to **Deployed Mode**, the available options are **User Mode** and **Deployed Mode**. If the current mode is set to **User Mode**, the available options are **User Mode**, **Audit Mode**, and **Deployed Mode**. |

| Options | Description |
|---|---|
| **User Mode** | In **User Mode**, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.<br>BIOS allows unauthenticated programmatic transitions between modes. |
| **Audit Mode** | In **Audit mode**, PK is not present. BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.<br>**Audit Mode** is useful for programmatically determining a working set of policy objects. |

| Options | Description |
| --- | --- |
| | BIOS performs signature verification on pre-boot images and logs the results in the image Execution Information Table, but approves the images whether they pass or fail verification. |
| **Deployed Mode** | **Deployed Mode** is the most secure mode. In **Deployed Mode**, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.<br>**Deployed Mode** restricts the programmatic mode transitions. |
| **Secure Boot Policy Summary** | Specifies the list of certificates and hashes that Secure Boot uses to authenticate images. |
| **Secure Boot Custom Policy Settings** | Configures the Secure Boot Custom Policy. To enable this option, set the **Secure Boot Policy** to **Custom**. |

# 4

# Dell Technologies support

The Dell Technologies support site provides documents and tools to help you effectively use Dell Technologies equipment and mitigate network outages. Through the support site you can obtain technical information, access software upgrades and patches, download available management software, and manage your open cases. The Dell Technologies support site provides integrated, secure access to these services.

To access the Dell Technologies support site, go to www.dell.com/support/. To display information in your language, scroll down to the bottom of the web page and select your country from the drop-down menu.

- To obtain product-specific information, enter the 7-character service tag, known as a luggage tag, or 11-digit express service code of your switch and click **Submit**.
- To view the platform service tag or express service code, pull out the luggage tag on the upper-right side of the platform or retrieve it remotely using the `ipmitool -H <bmc ip address> -I lanplus -U <user name> -P <password> fru` command
- To receive more technical support, click **Contact Us**. On the Contact Information web page, click **Technical Support**.

To access switch documentation, go to www.dell.com/manuals/.

To search for drivers and downloads, go to www.dell.com/drivers/.

To participate in Dell Technologies community blogs and forums, go to www.dell.com/community.