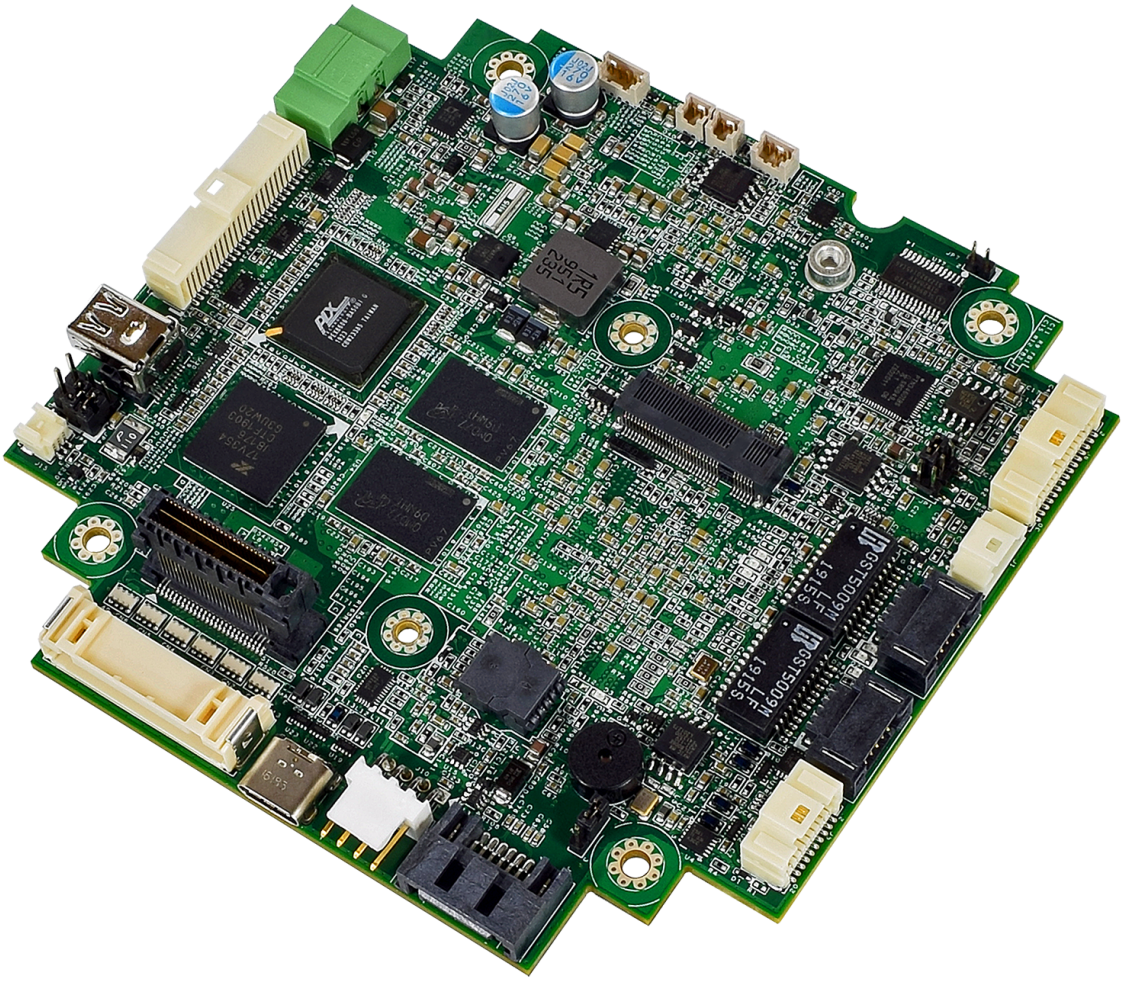
WINSYSTEMS®

# PX1-C441

## Supplemental BIOS Manual



WINSYSTEMS, Inc. | 2890 112th Street, Grand Prairie, Texas 75050 | 817-274-7553 | info@winsystems.com | www.winsystems.com

# Revision History

| BIOS Version | Last Updated Date | Brief Description of Change |
|---|---|---|
| 0.0.7 | 12/06/2021 | Initial release |

# Copyright and Trademarks



## Trademark Acknowledgments

# Table of Contents

# 1. Introduction

The BIOS used in this design is a custom version of the AMI Aptio V x86 BIOS.

## 1.1 References

The following Intel Atom E3900 BIOS specification documents can assist developers in the creation of firmware for the Intel Atom E3900:

- Intel Atom E3900 Platform Intel Architecture Firmware Specification (Volume 1 of 2), Document Number 559810
- Intel Atom E3900 Platform Intel Architecture Firmware Specification (Volume 2 of 2), Document Number 559811
- Intel Dynamic Platform and Thermal Framework (Intel DPTF) v8.x 201 - Rev 1.1, Document Number 556073

## 1.2 Glossary

- **Advanced Configuration and Power Interface (ACPI):** Specification that establishes industry standard interfaces enabling OS directed configuration, power management and thermal management of mobile, desktop, and server platforms.
- **Dynamic Video Memory Technology (DVMT):** Allows dynamic allocation of system memory for use as video memory to ensure the most efficient use of available resources in order to maximize 2D/3D graphics performance.
- **Graphics Processing Unit (GPU):** Specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer.
- **Integrated Graphics Device (IGD):** Graphics processor integrated into the Intel Atom E3900 SOC. The IGD in the Atom E3900 SOC is an Intel 9th Generation GPU, also called Gen9 GPU.
- **Unified Extensible Firmware Interface (UEFI):** Specification that defines a software interface between an operating system and platform firmware. UEFI replaces the basic input/output system (BIOS) firmware interface

# 2. BIOS Update with UEFI Shell

## 2.1 Scope

The Unified Extensible Firmware Interface (EFI or UEFI) is a new model for the interface between operating systems and firmware. It provides a standard environment for booting an operating system and running pre-boot applications.

An optional feature of a UEFI implementation is the ability to boot the system to a built-in shell. The UEFI shell provides a command prompt and a rich set of commands that extend and enhance the capability of the UEFI BIOS.

This section describes the process for updating the PX1-C441 BIOS firmware image using the built-in UEFI shell.

## 2.2 Process

1. Insert a USB flash drive containing the BIOS update program into a USB socket on the PX1-C441 platform.
2. Turn on the PX1-C441 and press **ESC** or **DEL** key during the boot process, which starts the BIOS setup utility.
3. In the BIOS setup utility, use the cursor keys to highlight the **Save & Exit** menu option.
4. Use the cursor keys to select **UEFI: Built-In EFI Shell** from the list of boot devices displayed under the **Boot Override** section.
5. Press **Enter**.

   The PX1-C441 executes the built-in UEFI shell, and displays a list of attached storage devices. The USB flash drive shows up in the list; depending on other boot devices attached, it may be listed as **fs0**, **fs1**, etc.

6. From the UEFI shell command prompt, enter the following command where `N` is the number of the fs device representing the USB flash drive:

   ```
   fsN:
   ```

   The shell prompt changes to indicate that device fsN is now the active storage device. Example: `fs1:`

7. Execute the following command:

   ```
   ls
   ```

   The output of the `ls` command is similar to the display listing available with the Linux or DOS list directory command. If the correct storage device was selected above, the `ls` command should show the BIOS update program in the directory

8. Assuming the BIOS update program is named `Update.efi`, enter the following command at the shell command prompt:

   ```
   Update.efi
   ```

   The BIOS update program begins executing.

9. When the update program completes, power cycle the platform to force the new BIOS image to load and execute.

10. Verify that the BIOS update was successful by comparing the displayed BIOS version with the version specified in the BIOS update notification.

# 3. Embedded Controller (EC) Update with UEFI Shell

This section describes the process for updating the PX1-C441 embedded controller (EC) image using the built-in Unified Extensible Firmware Interface (EFI or UEFI for short) shell.

## 3.1 Process

1. Insert a USB flash drive containing the EC update program into a USB socket on the PX1-C441 platform.
2. Turn on the PX1-C441 and press the **ESC** or **DEL** key during the boot process, which starts the BIOS setup utility.
3. In the BIOS setup utility, use the cursor keys to highlight the **Save & Exit** menu option.
4. Use the cursor keys to select **UEFI: Built-In EFI Shell** from the list of boot devices displayed under the Boot Override section.
5. Press **Enter**.

   The PX1-C441 executes the built-in UEFI shell, and displays a list of attached storage devices. The USB flash drive shows up in the list; depending on other boot devices attached, it may be listed as **fs0**, **fs1**, etc.

6. From the UEFI shell command prompt, enter the following command where `N` is the number of the fs device representing the USB flash drive:

   ```
   fsN:
   ```

   The shell prompt changes to indicate that device fsN is now the active storage device. Example: `fs1:`

7. Execute the following command:

   ```
   ls
   ```

   The output of the `ls` command is similar to the display listing available with the Linux or DOS list directory command. If the correct storage device was selected above, the `ls` command should show the EC update program in the directory listing obtained with the `ls` command.

8. Assuming the EC update program is named `Update.efi`, enter the following command at the shell command prompt:

   ```
   Update.efi
   ```

   The EC update program begins executing.

9. When the update program completes, power cycle the platform to force the new EC image to load and execute.
10. Verify that the EC update was successful by comparing the displayed EC version in the BIOS with the version specified in the EC update notification.

# 4. BIOS Settings

This section provides details on the system parameters that are managed by the BIOS. Details on the possible parameter values are included.

## 4.1 Entering the BIOS

Enter the BIOS by pressing **DEL** or **ESC** during POST. If you are running a Windows 10 operating system and you cannot enter the BIOS during POST by pressing either **DEL** or **ESC**, then follow the instructions below.

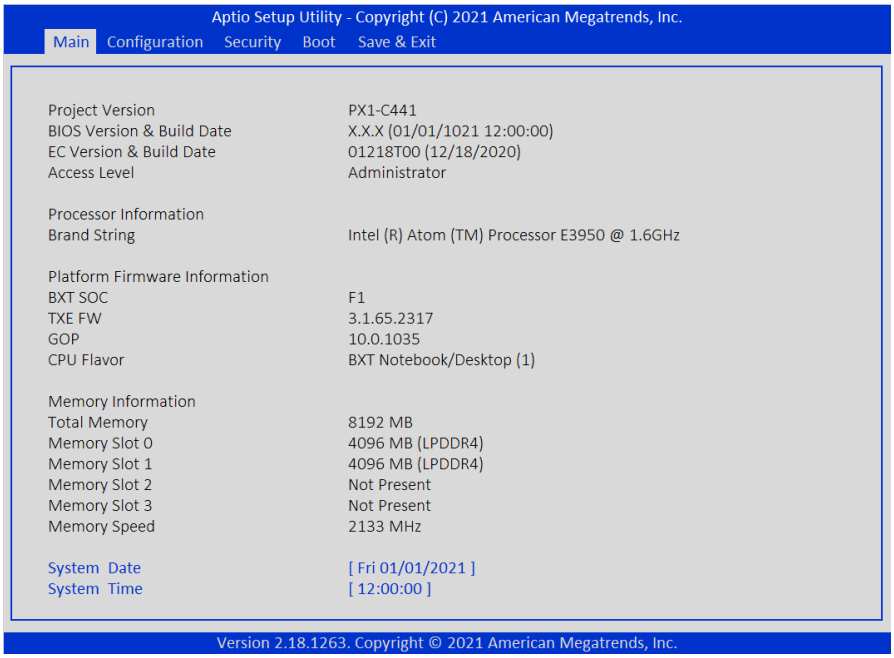
1. Press the **Windows** key on your keyboard and type “recovery options” into the search box.
2. Press **Enter** to open the Windows Recovery settings.
3. Under Advanced startup, click **Restart now**.

   The PX1-C441 restarts and boots into the UEFI menu
4. Click the **BIOS** button to enter the BIOS.

## 4.2 Main

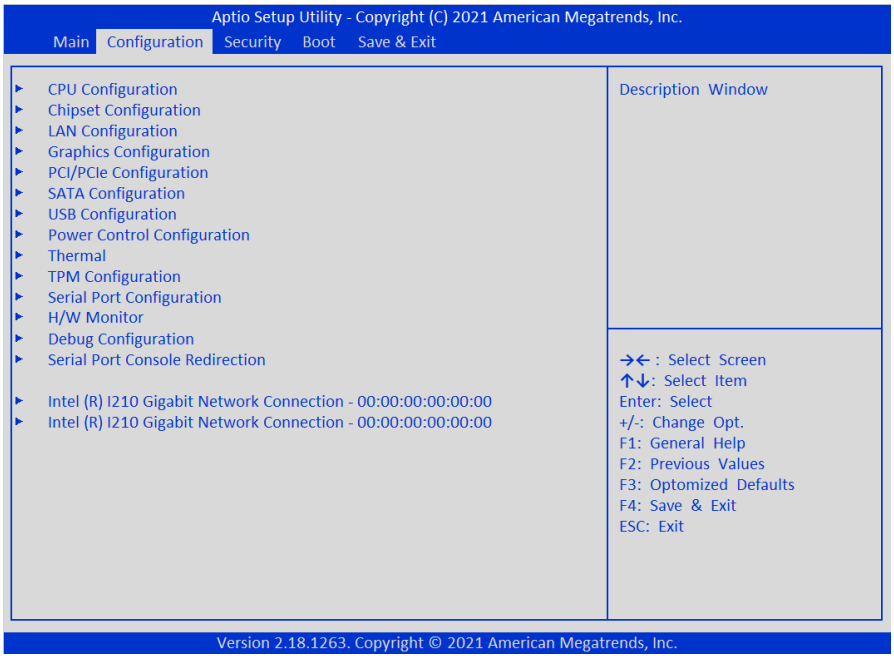
The Main page of the BIOS displays general information related to the current BIOS build, including the BIOS and embedded controller firmware revisions. Information related to the system memory is also displayed on this page.

System time and date are configurable on the main BIOS page. An external battery is required to retain time and date if power is removed. The following BIOS build information is available on the Main BIOS page.



## 4.3 Configuration

The BIOS Configuration page serves as the top-level BIOS page for configuring peripherals and devices present on the PX1-C441 platform. The configuration subpages include pages for the CPU, network interfaces, serial ports, USB ports, SATA, and other features. The settings for each configuration subpage are described in the device sections.



### 4.3.1 CPU Configuration

View a summary of the CPU features plus the ability to control vital CPU features including Power Management.

| Feature | Description | Choices | Default |
|---|---|---|---|
| **CPU Information** | CPU values specific to the processor in use. | | |
| Active Processor Cores | Number of cores to enable in each processor package. If disabled, all cores are enabled. If enabled, cores 1, 2, and 3 can be disabled or enabled individually. Core 0 is always enabled and cannot be disabled. | Enable, Disable | Disable |
| Intel Virtualization Technology | Intel VT provides hardware assist to virtualization software, reducing its size, cost, and complexity. Special attention is also given to reduce the virtualization overheads occurring in cache, I/O, and memory. | Enable, Disable | Enable |
| VT-d | Provides hardware assists for Intel Virtualization Technology (VT). This feature can help improve security and reliability, as well as improve performance of I/O devices in a virtual environment. | Enable, Disable | Disable |
| **CPU Power Management** | Provides settings related to CPU power management such as Intel SpeedStep, Turbo Mode, and C-States. | | |
| • EIST | Enhanced Intel SpeedStep allows the CPU to save power by dynamically changing the processor clock frequencies. It calculates the exact frequency needed at any moment by raising or lowering the clock multiplier and also adjusts the CPU voltage. | Enable, Disable | Enable |
| • Turbo Mode | Raises the clock frequency of processor to a manufacturer-defined turbo speed. System load, active cores, estimated current, power consumption, and core temperature are taken into account in the boosting process. | Enable, Disable | Enable |
| • C-States | C-States are the “states” the processor comes to in order to lower power consumption and temperature. | Enable, Disable | Enable |
| • Enhanced C-States | The C1 state is when the CPU is idle, but is able to instantly revert to its working state. C1E (C1 Enhanced) is the updated modern version of the same state. | Enable, Disable | Enable |

### 4.3.2 Chipset Configuration

Set configuration options that are not CPU-specific.

| Feature | Description | Choices | Default |
|---|---|---|---|
| HD-Audio Support | Enables/disables HD-Audio support. | Enable, Disable | Enable |
| 8254 Clock Gating | Enables/disables the legacy 8254 timer and saves power. Some operating systems do not boot if this is enabled. | Enable, Disable | Disable |
| Refresh Rate of 2x | Ensures that the refresh rate never drops below 2x. Enable = 2x, Disable = 1x. | Enable, Disable | Enable |

### 4.3.3 LAN Configuration

| Feature | Description | Choices | Default |
|---|---|---|---|
| Wake On LAN | Enables/disables the Wake on LAN feature. | Enable, Disable | Disable |
| Launch UEFI PXE ROM | Enables/disables the UEFI network stack. Enabling this feature is required for PXE boot. | Enable, Disable | Disable |
| I210 UEFI PXE ROM | Controls the execution of I210 of UEFI PXE OpROM. | Enable, Disable | Enable |
| I210 Legacy PXE ROM | Controls the execution of I210 of Legacy PXE OpROM. | Enable, Disable | Disable |

Enabling and configuring UEFI PXE or Legacy PXE boot:

1. Enable **Launch UEFI PXE Rom** then enable either **UEFI PXE** or **Legacy PXE boot** under the LAN Configuration settings.
2. Navigate to the Boot tab and ensure that **Boot Option #1** under Fixed Boot Order is set to **UEFI Network** if using UEFI PXE boot or **Network** if using Legacy PXE boot.

### 4.3.4 Graphics Configuration

| Feature | Description | Choices | Default |
|---|---|---|---|
| DVMT Pre-Allocated | Selects DVMT 5.0 Pre-Allocated (fixed) graphics memory size used by the internal graphics device. | 64M, 96M, 128M, 160M, 192M, 224M, 256M, 288M, 320M, 352M, 384M, 416M, 448M, 480M, 512M | 64M |
| GOP Driver | Enables/disables the Graphics Output Protocol (GOP) driver. When the GOP driver is enabled, it replaces and turns off the Video BIOS (VBIOS) and enables the use of UEFI pre-boot firmware without CSM. When GOP is disabled, the VBIOS is turned on and requires Compatibility Support Module (CSM) to be enabled as well. To enable CSM, see “Boot” on page 22. | Enable, Disable | Enable |
| **eDP to LVDS Configuration** | Configure eDP and LVDS settings. | | |
| Panel Profile | Selects panel resolution. | 640 x 480, 800 x 480, 800 x 600, 1024 x 768, 1280 x 800, 1280 x 1024, 1366 x 768, 1440 x 900, 1920 x 1080, Custom Profile | 1024 x 768 |

| Feature | Description | Choices | Default |
|---|---|---|---|
| Color Depth and Data Format | Selects color depth and data format. | VESA 24 bpp, JEIDA 24 bpp, VESA and JEIDA 18bpp | VESA and JEIDA 18 bpp |
| Channel Mode | Selects LVDS channel mode. | Single Channel, Dual Channel | Single Channel |
| Clock Mode | Selects clock output for LVDS. | Even Bus, Odd Bus, Both Buses | Even Bus |
| **OEM Profile** | Configure the parameters according to the specific LVDS panel specification. | | |
| Color Depth and Data Format | Selects color depth and data format. | VESA 24 bpp, JEIDA 24 bpp, VESA and JEIDA 18bpp | VESA and JEIDA 18 bpp |
| Channel Mode | Selects LVDS channel mode. | Single Channel, Dual Channel | Single Channel |
| Clock Mode | Selects clock output for LVDS. | Even Bus, Odd Bus, Both Buses | Even Bus |
| • Pixel Clock in kHz | Pixel clock in kilohertz | 10 to 655000 | 2500 |
| • H Active Pixels | Active pixels, horizontal | 480 to 1600 | 640 |
| • H Blank Pixels | Blank pixels, horizontal | 0 to 1000 | 160 |
| • H Offset Pixels | Offset pixels, horizontal | 0 to 1000 | 16 |
| • H Width Pixels | Width pixels, horizontal | 0 to 1000 | 96 |
| • V Active Lines | Active lines, vertical | 480 to 900 | 480 |
| • V Blank Lines | Blank lines, vertical | 0 to 1000 | 45 |
| • V Offset Lines | Offset lines, vertical | 0 to 50 | 10 |
| • V Width Lines | Width lines, vertical | 0 to 50 | 2 |
| H & V sync Signal Polarity | • 0x1E signal polarity is positive<br>• 0x18 signal polarity is negative | Positive, Negative | Positive |

### 4.3.5 PCIe/PCIe Configuration

There are six PCIe lanes (channels 1-6) configured as six x1 PCIe lanes.

| Feature | Description | Choices | Default |
|---|---|---|---|
| PCI Express Root Port | Controls the PCIe root port.<br>• Auto: Disables unused port automatically for optimum power savings.<br>• Enable: Enables port.<br>• Disable: Disables port. | Auto, Enable, Disable | Enable |
| ASPM | Sets Active State Power Management (ASPM), which provides power savings while otherwise in a fully active state. L0s mode is for one direction of the link, usually downstream of the PHY controller. L1 mode is bidirectional and results in greater power reductions though with a greater exit latency. | Disable, L0s, L1, L0sL1, Auto | Disable |
| Hot Plug | Provides support to allow PCIe hotplug. | Enable, Disable | Disable |
| PCIe Speed | Selects the PCIe port speed.<br>• Auto matches the speed of the inserted device.<br>• Gen1 supports up to 2.5 GigaTransfers per second.<br>• Gen2 supports up to 5 GigaTransfers per second. | Auto, Gen1, Gen2 | Auto |
| PCIe Selectable De-emphasis | When the link is operating at 5.0 GT/s, this bit selects the level of de-emphasis for an upstream component.<br>1b -3.5 dB<br>0b -6 dB | Enable, Disable | Enable |

### 4.3.6 SATA Configuration

| Feature | Description | Choices | Default |
|---|---|---|---|
| SATA Controller | Enable or disable the chipset SATA controller. This controller supports two internal SATA ports | Enable, Disable | Enable |
| SATA Speed Selection | Selects the SATA interface speed:<br>• Gen 1 = 1.5 Gbps<br>• Gen 2 = 3 Gbps<br>• Gen 3 = 6 Gbps (Default) | Auto, Gen 1, Gen 2, Gen 3 | Auto |
| SATA Port 0 | Displays “Not Installed” if no device is present. Otherwise, the device information is displayed. | | |
| Port 0 | Enables/disables the SATA port at connector J8. | Enable, Disable | Enable |
| SATA Port 0 Hotplug Capability | If enabled, SATA port will be reported as hotplug capable. | Enable, Disable | Disable |
| SATA Device Type | Identify if the SATA port is connected to a solid state drive or hard disk drive. | Hard Disk Drive, Solid State Drive | Hard Disk Drive |
| SATA Port 1 | Displays “Not Installed” if no device is present. Otherwise, the device information is displayed. | | |

| Feature | Description | Choices | Default |
|---|---|---|---|
| Port 1 | Enables/disables the SATA channel at M.2 connector J9. | Enable, Disable | Enable |
| SATA Device Type | Identify if the SATA port is connected to a solid state drive or hard disk drive. | Hard Disk Drive, Solid State Drive | Hard Disk Drive |

### 4.3.7 USB Configuration

Configure the PX1-C441 USB ports and view a summary of installed devices.

| Feature | Description | Choices | Default |
|---|---|---|---|
| USB 2.0 Ports #0-7 | Enables/disables the USB 2.0 ports. Provides control to each port of an 8-port USB 2.0 hub. | Enable, Disable | Enable |
| Legacy USB Support | Enables/disables Legacy USB support. The Auto option disables legacy support if no USB devices are connected. The Disable option keeps USB devices available only for EFI applications. | Auto, Enable, Disable | Enable |
| USB Mass Storage Driver Support | Enables/disables USB mass storage driver support. The USB mass-storage specification provides an interface to a number of industry-standard command sets, allowing a device to disclose its subclass. | Enable, Disable | Enable |
| USB transfer time-out | Sets the time-out value for Control, Bulk, and Interrupt transfers. | 1 sec, 5 sec, 10 sec, 20 sec | 20 sec |
| Device reset time-out | Sets the USB mass storage device Start Unit command time-out. | 10 sec, 20 sec, 30 sec, 40 sec | 20 sec |
| Device power-up delay | Specifies the maximum time the device takes before it properly reports itself to the host controller. Auto uses default value: for a Root port it is 100 milliseconds, and for a Hub port the delay is taken from the Hub descriptor. | Auto, Manual | Auto |
| Device power-up delay in seconds | Specifies the delay before the device begins to power up (seconds).<br>**NOTE:** Device power-up delay must be set to manual to view this option. | 1 to 40 | 5 |

### 4.3.8 Power Control Configuration

Specify settings for CPU hibernation and ACPI sleep states.

| Feature | Description | Choices | Default |
|---|---|---|---|
| Enable Hibernation | Enables/disables the system's ability to Hibernate (S4 Sleep State). This option may be not effective with some operating systems. | Enable, Disable | Enable |
| ACPI Sleep State | Selects the highest ACPI sleep state the system enters when the SUSPEND button is pressed. | Suspend Disable, S3 (Suspend to Ram) | S3 (Suspend to Ram) |
| RTC Wakeup | Enables/disables system wakeup on alarm event. When enabled the system will wake on the hour: minute: second specified. If Disabled the RTC wakeup feature is off. | Enable, Disable | Disable |

### 4.3.9 Thermal

Configure ACPI parameters for operating system thermal management.

NOTE The features listed after DTPF are shown only if DTPF is enabled.

| Feature | Description | Choices | Default |
|---|---|---|---|
| Automatic Thermal Reporting | Permits the BIOS to automatically configure critical, passive, and active trip points to ACPI enabled operating systems. Set to Disable for manual configuration. | Enable, Disable | Disable |
| Critical Trip Point | Controls the temperature of the ACPI Critical Trip Point, which is the point at which the OS shuts the system off. | 15 to 125 C | 125 C |
| Passive Trip Point | Controls the temperature of the ACPI Passive Trip Point, which is the point at which the OS begins throttling the processor. | 15 to 111 C, Disable | 111 C |
| Active Trip Point | Controls the temperature of the ACPI Active Trip Point, which is the point at which the OS turns the fan on. | 15 to 110 C | 60 C |
| DPTF | Enables/disables Intel Dynamic Platform and Thermal Framework (DPTF), which provides various platform level power and thermal management technologies that enable quiet and cool platform designs. | Enable, Disable | Disable |
| **NOTE:** The features below are shown only if DTPF is enabled. | | | |
| DPTF Configuration | An integer containing the DPTF configuration bitmap. Enter a value between 0 - 63.<br>• bit 0: Generic UI Access Control (0=enable, 1=disable)<br>• bit 1: Restricted UI Access Control (0=enable, 1=disable)<br>• bit 2: Shell Access Control (0=enable, 1=disable)<br>• bit 3: Environment Monitoring Report Control (0=report, 1=silent)<br>• bit 4: Thermal Mitigation Report Control (0=silent, 1=report)<br>• bit 5: Thermal Policy Report Control (0=silent, 1=report) | 0 - 63 | 0 |
| DPTF Processor | Enables/disables the Processor Participant Device. | Enable, Disable | Enable |
| Active Thermal Trip Point | Controls the temperature of the ACPI Active Thermal Trip Point. A value of 0 causes the DPTF driver to disable the trip point. | 0 to 127 | 90 |
| Passive Thermal Trip Point | Controls the temperature of the ACPI Passive Thermal Trip Point. A value of 0 causes the DPTF driver to disable the trip point. | 0 to 127 | 100 |
| S3/CS Thermal Trip Point | Controls the temperature of the ACPI Critical Thermal Trip Point for entering S3 or CS. A value of 0 causes the DPTF driver to disable the trip point. | 0 to 127 | 110 |
| Hot Thermal Trip Point | Controls the temperature of the ACPI Hot Thermal Trip Point. A value of 0 causes the DPTF driver to disable the trip point. | 0 to 127 | 110 |

| Feature | Description | Choices | Default |
|---|---|---|---|
| Critical Thermal Trip Point | Controls the temperature of the ACPI Critical Thermal Trip Point. A value of 0 causes the DPTF driver to disable the trip point. | 0 to 127 | 105 |
| Thermal Sampling Period | Specifies the polling interval in 10ths of seconds. A value of 0 tells the driver to use interrupts. The granularity of the sampling period is 0.1 seconds. For example, if the sampling period is 30 seconds, then _TSP needs to report 300; if the sampling period is 0.5 seconds, then choose 5. | 0 to 100 | 0 |

### 4.3.10 TPM Configuration

Disable/enable the onboard TPM 2.0 device as well as the Platform Configuration Registers (PCR) for each supported hash algorithm.

| Feature | Description | Choices | Default |
|---|---|---|---|
| Security Device Support | Enables/disables BIOS support for security device. If disabled, the OS does not show a security device and the TCG EFI protocol and INT1A interface are not available. | Enable, Disable | Enable |
| SHA-1 PCR Bank | Enables/disables SHA-1 PCR Bank.<br>**NOTE:** Only available if Security Device Support is enabled. | Enable, Disable | Enable |
| SHA256 PCR Bank | Enables/disables SHA256 PCR Bank.<br>**NOTE:** Only available if Security Device Support is enabled. | Enable, Disable | Enable |
| Pending operation | Selecting TPM Clear schedules a reset operation for the security device and executes after saving the BIOS and rebooting the system.<br>**NOTE:** Only available if Security Device Support is enabled. | None, TPM Clear | None |
| Platform Hierarchy | Enables/disables platform hierarchy. | | |
| Storage Hierarchy | Enables/disables storage hierarchy. | | |
| Endorsement Hierarchy | Enables/disables endorsement hierarchy. | | |
| TPM 2.0 UEFI Spec Version | Selects the TCG2 spec version support.<br>• TCG_1_2 = compatible mode for Win8/ Win10.<br>• TCG_2 = Support TCG2 protocol and event format for Win10 and later. | TCG_1_2, TCG_2 | TCG_2 |
| Physical Presence Spec Version | Selects to inform the operating system to support PPI Spec version 1.2 or 1.3. Note some HCK test may not support 1.3. | 1.2, 1.3 | 1.3 |
| Device Select | Selects which TPM spec to use. TPM 1.2 restricts support for TPM 1.2 devices. TPM 2.0 restricts support for TPM 2.0 devices. Auto supports both with default set to TPM 2.0. TPM 1.2 devices are enumerated. | 1.2, 2.0, Auto | Auto |

NOTE You must navigate to the Save & Exit tab, select **Save Changes and Reset**, then press **Enter** for the TPM reset to occur.

### 4.3.11 Serial Port Configuration

Configure the three serial ports.

| Feature | Description | Choices | Default |
|---|---|---|---|
| **Module Serial Port 1** | Controls and configures UART 1. This port supports only RS-232 protocol. | Enable, Disable | Enable |
| **COM C Mode** | Selects serial port mode. | RS-232, RS-485 Half-Duplex, RS-485/422 Full Duplex | RS-232 |
| **COM D Mode** | Selects serial port mode. | RS-232, RS-485 Half-Duplex, RS-485/422 Full Duplex | RS-232 |
| Watchdog Timer | Controls the watchdog timer (WDT) on the EC. If enabled, mode and timeout can be configured. | Enable, Disable | Disable |
| Timer Unit | Selects WDT time units. | Seconds, Minutes | Minutes |
| Timer Value | Selects WDT timeout value. | 1 to 255 | 0 |

### 4.3.12 H/W Monitor

Monitor hardware status.

The following parameters are provided for reference and are updated every half-second:

- CPU Temperature
- Vcore
- +3.3V Voltage
- +5.0V Voltage
- +12V Voltage
- VDIMM Voltage

### 4.3.13 Debug Configuration

Control the Direct Connect Interface (DCI), which allows debugging using a USB3 port.

| Feature | Description | Choices | Default |
|---|---|---|---|
| DCI Enable (HDCIEN) | Enables/disables Direct Connect Interface (DCI). When DCI is enabled, it is taken as user consent to enable DCI, which allows debug over the USB3 interface. When disabled, the host control does not enable the DCI feature. | Enable, Disable | Disable |

### 4.3.14 Serial Port Console Redirection

Enable console redirection to mirror the console output to COM 0. Console Redirection settings are only available when COM 0 is enabled in the Serial Port Configuration section of the BIOS.

| Feature | Description | Choices | Default |
|---|---|---|---|
| Console Redirection | Enables/disables console redirection on COM 0 | Enable, Disable | Disable |
| Terminal Type | Selects terminal type. | VT100, VT100+, VT-UTF8, ANSI | ANSI |
| Bits per Second | Selects the baud rate | 9600, 19200, 38400, 57600, 115200 | 115200 |
| Data Bits | Selects the data bit | 7,8 | 8 |
| Parity | Selects parity bit setting | None, Even, Odd, Mark, Space | None |
| Stop Bits | Selects stop bits setting | 1, 2 | 1 |
| Flow Control | Selects whether to use Flow Control or not. | None, Hardware RTS/CTS | None |
| VT-UTF8 Combo Key Support | Enables/disables VT-UTF8 combination key support for ANSI/VT100 terminals. | Enable, Disable | Enable |
| Recorder Mode | Only text is sent when recorder mode is enabled. This is for capturing terminal data. | Enable, Disable | Disable |
| Resolution 100x31 | Enables/disabled extended terminal resolution. | Enable, Disable | Disable |
| Putty Keypad | Selects function key and keypad on Putty. | VT100, Linux, XTERM86, SCO, ESCN, VT400 | VT100 |

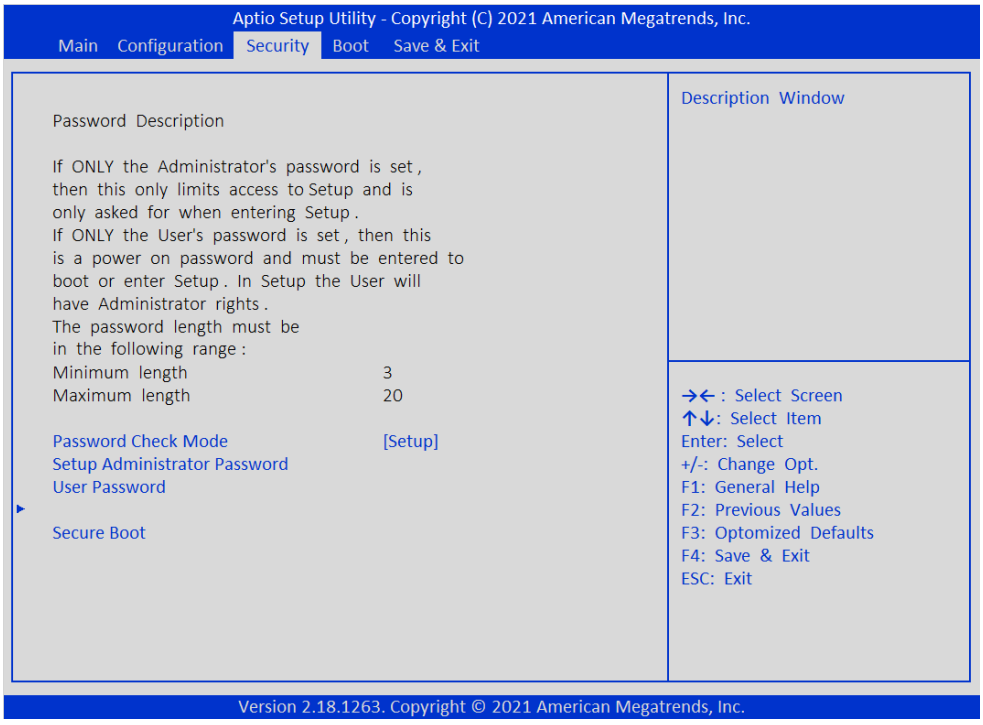
### 4.3.15 Intel I210 Gigabit Network Connection 1 & 2

Configure the Intel I210 Network Interface Controller (NIC), and view specific technical information such as link status, and MAC address.

| Feature | Description | Choices | Default |
|---|---|---|---|
| **NIC Configuration** | Provides options to configure the link speed and enables/disables Wake on Lan. | | |
| Link Speed | Specifies the port speed used for the selected boot protocol. | Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full | Auto Negotiated |
| Wake on LAN | Enables/disables the server to be powered on using an inband magic packet. | Enable, Disable | Disable |
| Blink LEDs | Specifies the number of seconds to blink LEDs. This function provides the ability to physically view which Ethernet NIC is #1 or #2. To blink the integrated LEDs on the RJ45 connector, type a number from 0 to 15 (seconds) then press Enter to blink the LEDs for that amount of time. | 0 - 15 | 0 |

## 4.4 Security

Set various passwords, and specify how and when these passwords are used to protect the system.



### 4.4.1 Password Check Mode

Select whether to check for password when entering the BIOS (Setup) or on every boot up sequence (Power On).

### 4.4.2 Setup Administrator Password

If only the administrator password is set, then this password is required to enter the BIOS setup and grants you administrative privileges.

### 4.4.3 User Password

If only the user password is set, then this password is required during boot or entering the BIOS setup with administrative privileges.

NOTE If both the administrator and user passwords are set, then either password is required to boot the machine or enter the BIOS setup, however the user password does not have administrative privileges on the security page.

### 4.4.4 HDD Security Configuration

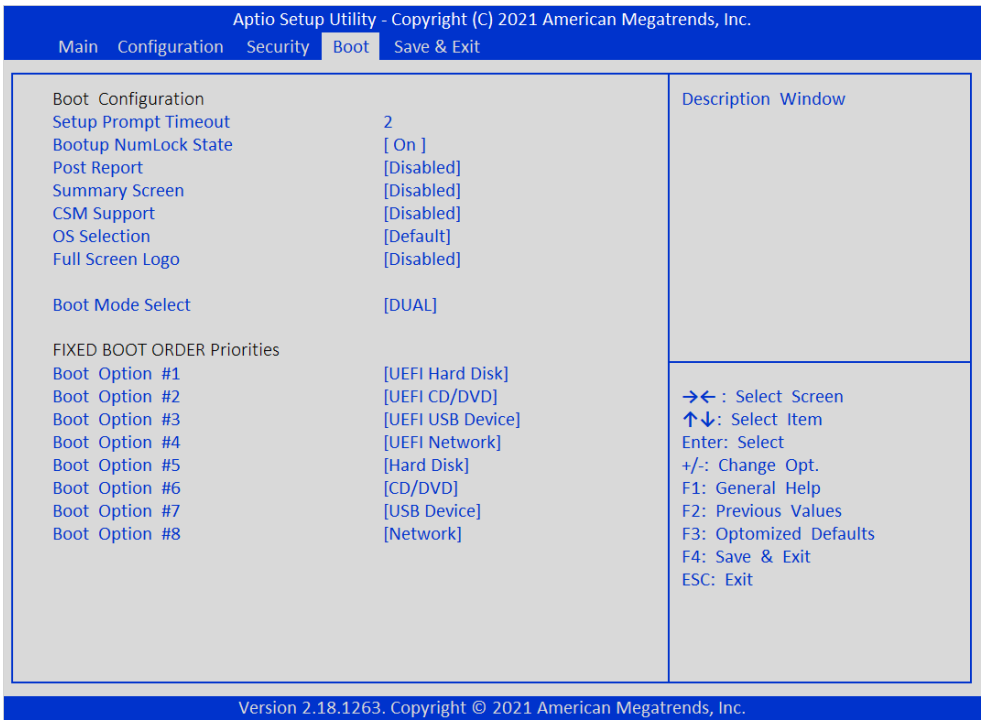
Navigate to the appropriate HDD or SSD drive to set, modify, and clear the hard disk user and master passwords. User password setup is required for enabling security.

### 4.4.5 Secure Boot

| Feature | Description | Choices | Default |
|---|---|---|---|
| Secure Boot | Enables/disables Secure Boot. When enabled, Secure Boot activated, Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM is disabled. | Enable, Disable | Enable |
| Secure Boot Customization | Sets UEFI Secure Boot Mode to Standard mode or Custom mode, this change is in effect after save. After reset, the mode returns to Standard mode. | Standard, Custom | Standard |
| Restore Factory Keys | Forces the system to user mode. Configure NVRAM to contain OEM-defined factory default Secure Boot keys.<br>**NOTE:** This is a one time push button that restores the factory keys. There are no choices. | — | — |
| **Key Management** | Enables expert user to modify Secure Boot Policy variables without full authentication.<br>**NOTE:** These settings are for advanced users only. Contact a WINSYSTEMS application engineer for additional information. | | |

## 4.5 Boot

Configure advanced boot options for the PX1-C441 such as BIOS bootup and logo display, device boot order, and CSM support.

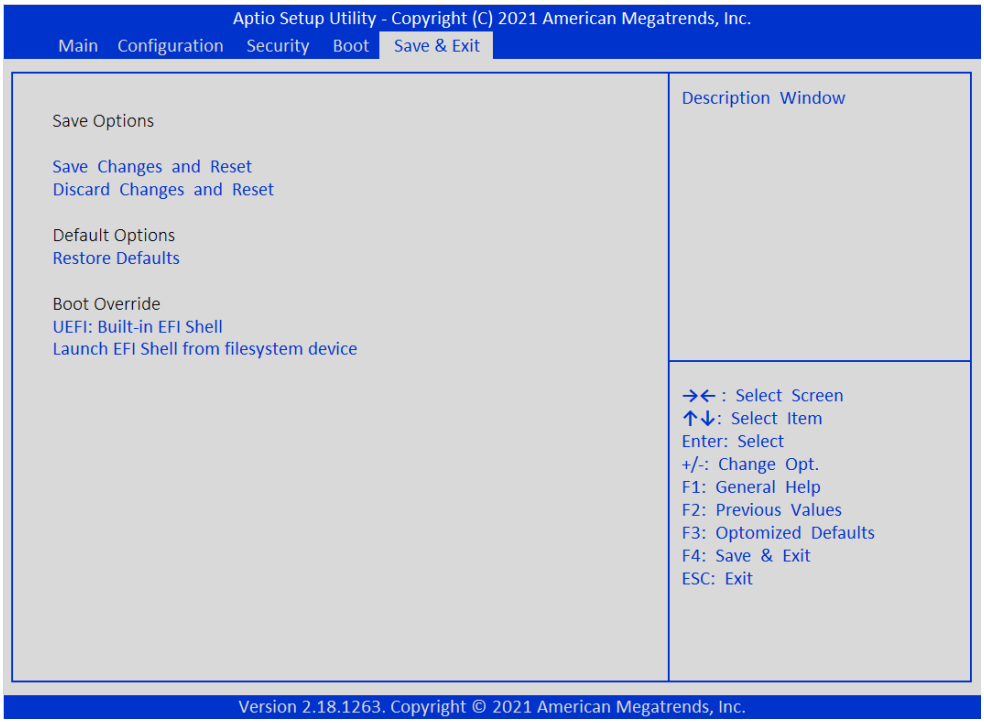



| Feature | Description | Choices | Default |
|---|---|---|---|
| Setup Prompt Timeout | Sets the number of seconds to wait for the setup activation key. A value of 65535 (0xFFFF) means indefinite waiting. | 1 to 65535 | 1 |
| Bootup NumLock State | Selects the default keyboard NumLock state. | On, Off | On |
| POST Report | Enables/disables POST screen report. | Enable, Disable | Disable |
| Summary Screen | Enables/disables Summary screen report. | Enable, Disable | Disable |
| CSM Support | Enables/disables Compatibility Support Module (CSM), which provides legacy BIOS compatibility by emulating a BIOS environment, allowing legacy operating systems and some option ROMs that do not support UEFI to still be used. | Enable, Disable | Disable |
| OS Selection | Selects the target operating system. Other menu options may change based on the OS selection. This is proper behavior. | Default, Android, Legacy System, Intel Linux | Default |
| Full Screen Logo | Enables/disables quiet boot. Enabling this option hides the BIOS post messages on bootup and displays the WINSYSTEMS logo. This logo is configurable for custom OEM applications. Contact a WINSYSTEMS applications engineer at 1-817-274-7553 for more information. | Disable, Enable | Disable |

## 4.6 Save & Exit

Save custom BIOS options to the CMOS ROM.

Additionally, booting to the UEFI shell is as easy as selecting UEFI: Built-in EFI Shell under Boot Override and pressing **Enter**.




### 4.6.1 Save Options

| Feature | Description |
|---|---|
| Save Changes and Reset | Saves all custom configured BIOS settings, then immediately reboots the computer. |
| Discard Changes and Reset | Reverts any custom configured BIOS settings back to default, then reboots the computer. |

### 4.6.2 Default Options

| Feature | Description |
|---|---|
| Restore Defaults | Clears any changes to BIOS settings and reverts all settings back to factory defaults. |

### 4.6.3 Boot Override

Temporarily override the Boot Option Priorities table located in the Boot tab of the BIOS to boot to any storage device.

# 5. BIOS Factory Defaults

Reset the BIOS settings to factory defaults using either of the two methods described below.

## 5.1 Software

To reset the BIOS CMOS parameters to factory defaults:

1. Turn on the PX1-C441 and press **ESC** or **DEL** during the boot process to enter the BIOS.
2. In the BIOS, use the arrow keys to highlight the **Save & Exit** menu option.
3. Using the arrow keys, highlight **Restore Defaults** and press **Enter**.
4. Select **Save Changes and Exit** or press **F4**.

NOTE For a quick restore of the BIOS settings you can press **F3**, **Enter**, then **F4**, **Enter**. This operation can be helpful in case video has accidentally been turned off in the BIOS.

## 5.2 Hardware

A jumper provided onboard enables you to reset the BIOS CMOS settings to factory defaults. The BIOS reads this pin during system boot and forces the settings to reset if the pin is at ground.

To reset the BIOS CMOS parameters to factory defaults using Clear CMOS:

1. Remove power from the board.
2. Place the jumper at **JP7** on pins 2 and 3.
3. Apply power to the board, and let it boot into the BIOS.
4. Power off the board, and restore **JP7** to the Normal operation position (pins 1 and 2).

# 6. Software Description

This section describes the AMI BIOS components to be used in the implementation of the PX1-C441 BIOS firmware.

## 6.1 Software Design Specification: UEFI Operating System Support

The BIOS supports booting the following UEFI-compliant operating systems:

- Windows 10 x64, IoT Core, and Professional
- Linux x64

- Most x86 operating systems

## 6.2 Software Design Specification: Legacy Operating System Support

The BIOS supports booting the following legacy OS capabilities:

- Compatibility support module (CSM)
- Legacy boot support
- Legacy option ROM support

## 6.3 Software Design Specification: Boot Device Configuration

The BIOS supports booting an OS from the following devices:

- USB mass storage device
- Serial ATA (SATA) device
- Network boot - PXE
- eMMC
- M.2 mass storage device

## 6.4 Software Design Specification: BIOS Update Mechanisms

The BIOS supports the following update mechanisms:

- BIOS update with UEFI shell
- Software utilities
- Flash recovery via USB mass storage device
- Flash recovery via eMMC device
- Embedded controller (EC) firmware update with UEFI shell

## 6.5 Software Design Requirements: BIOS Components

The BIOS includes the following components:

- **Advanced Host Controller Interface (AHCI) support:** Provides SATA host controller functionality.
- **Display switching in setup:** Implements display switching using the UEFI GOP driver under the SETUP environment.
- **Boot order:** Generates the default boot order on the platform's first boot.
- **Boot/resume from S4 device:** Allows the platform to boot from the last S4 hibernated device, disregarding the current boot priority.
- **Cryptographic support:** Provides cryptographic related libraries, PPI, and UEFI protocols for security modules (secure FW update, secure boot, etc.)

- **Source level support:** Provides source-level debug functionality for the BIOS project.
- **Fastboot:** Provides optimization of the boot time.
- **Fixed boot order:** Provides infrastructure that allows custom handling of available boot options to meet specific customer needs. Custom boot behavior may include different requests, such as always boot from specific device, and default support of various kinds of grouping of boot devices.
- **Generic error logging:** Provides support for logging POST and runtime errors to the GPNV area.
- **Keyboard controller emulation:** Used for USB keyboard/mouse.
- **Physical memory testing:** Supports testing of physical memory present in the system.
- RTC registration and ability to handle wakeup from S5 sleep state.
- **Secure boot support:** Provides support and functionality to conform with UEFI 2.3.1 secure boot requirements and includes the following components:
  - Extended functionality of EFI NVRAM driver with support for authenticated EFI variables
  - EFI image authentication module that installs EFI security architecture protocol with image authentication and image execution policy
  - Secure boot variable (PK, KEK, db, and dbx) provisioning
- • Support for the booting to the built in UEFI shell.

# 7. AMI POST Codes

## 7.1 POST Codes

These codes are displayed during a normal boot process. If the boot fails, the last code displayed provides an indicator of the failing code.

| Regular Boot POST Codes | Code |
|---|---|
| PEI_CORE_STARTED | 0x10 |
| PEI_CAR_CPU_INIT | 0x11 |
| PEI_CAR_NB_INIT | 0x15 |
| PEI_CAR_SB_INIT | 0x19 |
| PEI_MEMORY_SPD_READ | 0x2B |
| PEI_MEMORY_PRESENCE_DETECT | 0x2C |
| PEI_MEMORY_TIMING | 0x2D |
| PEI_MEMORY_CONFIGURING | 0x2E |
| PEI_MEMORY_INIT | 0x2F |
| PEI_MEMORY_INSTALLED | 0x31 |

| Regular Boot POST Codes | Code |
|---|---|
| PEI_CPU_INIT | 0x32 |
| PEI_CPU_CACHE_INIT | 0x33 |
| PEI_CPU_AP_INIT | 0x34 |
| PEI_CPU_BSP_SELECT | 0x35 |
| PEI_CPU_SMM_INIT | 0x36 |
| PEI_MEM_NB_INIT | 0x37 |
| PEI_MEM_SB_INIT | 0x3B |
| PEI_DXE_IPL_STARTED | 0x4F |
| DXE_CORE_STARTED | 0x60 |
| DXE_NVRAM_INIT | 0x61 |
| DXE_SBRUN_INIT | 0x62 |
| DXE_CPU_INIT | 0x63 |
| DXE_NB_HB_INIT | 0x68 |
| DXE_NB_INIT | 0x69 |
| DXE_NB_SMM_INIT | 0x6A |
| DXE_SB_INIT | 0x70 |
| DXE_SB_SMM_INIT | 0x71 |
| DXE_SB_DEVICES_INIT | 0x72 |
| DXE_ACPI_INIT | 0x78 |
| DXE_CSM_INIT | 0x79 |
| DXE_BDS_STARTED | 0x90 |
| DXE_BDS_CONNECT_DRIVERS | 0x91 |
| DXE_PCI_BUS_BEGIN | 0x82 |
| DXE_PCI_BUS_HPC_INIT | 0x93 |
| DXE_PCI_BUS_ENUM | 0x94 |
| DXE_PCI_BUS_REQUEST_RESOURCES | 0x95 |
| DXE_PCI_BUS_ASSIGN_RESOURCES | 0x96 |
| DXE_CON_OUT_CONNECT | 0x97 |
| DXE_CON_IN_CONNECT | 0x98 |
| DXE_SIO_INIT | 0x99 |
| DXE_USB_BEGIN | 0x9A |
| DXE_USB_RESET | 0x9B |
| DXE_USB_DETECT | 0x9C |
| DXE_USB_ENABLE | 0x9D |
| DXE_IDE_BEGIN | 0xA0 |
| DXE_IDE_RESET | 0xA1 |
| DXE_IDE_DETECT | 0xA2 |
| DXE_IDE_ENABLE | 0xA3 |
| DXE_SCSI_BEGIN | 0xA4 |
| DXE_SCSI_RESET | 0xA5 |
| DXE_SCSI_DETECT | 0xA6 |
| DXE_SCSI_ENABLE | 0xA7 |

| Regular Boot POST Codes | Code |
|---|---|
| DXE_SETUP_VERIFYING_PASSWORD | 0xA8 |
| DXE_SETUP_START | 0xA9 |
| DXE_SETUP_INPUT_WAIT | 0xAB |
| DXE_READY_TO_BOOT | 0xAD |
| DXE_LEGACY_BOOT | 0xAE |
| DXE_EXIT_BOOT_SERVICES | 0xAF |
| RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN | 0xB0 |
| RT_SET_VIRTUAL_ADDRESS_MAP_END | 0xB1 |
| DXE_LEGACY_OPROM_INIT | 0xB2 |
| DXE_RESET_ SYSTEM | 0xB3 |
| DXE_USB_HOTPLUG | 0xB4 |
| DXE_PCI_BUS_HOTPLUG | 0xB5 |
| DXE_NVRAM_CLEANUP | 0xB6 |
| DXE_CONFIGURATION_RESET | 0xB7 |

| S3 Resume POST Codes | Code |
|---|---|
| PEI_S3_STARTED | 0xE0 |
| PEI_S3_BOOT_SCRIPT | 0xE1 |
| PEI_S3_VIDEO_REPOST | 0xE2 |
| PEI_S3_OS_WAKE | 0xE3 |

| Recovery POST Codes | Code |
|---|---|
| PEI_RECOVERY_AUTO | 0xF0 |
| PEI_RECOVERY_USER | 0xF1 |
| PEI_RECOVERY_STARTED | 0xF2 |
| PEI_RECOVERY_CAPSULE_FOUND | 0xF3 |
| PEI_RECOVERY_CAPSULE_LOADED | 0xF4 |

# 8. Error Codes

These post codes indicate that an error has occurred.

| Regular Boot Error Codes | Code |
|---|---|
| PEI_MEMORY_INVALID_TYPE | 0x50 |
| PEI_MEMORY_INVALID_SPEED | 0x50 |
| PEI_MEMORY_SPD_FAIL | 0x51 |
| PEI_MEMORY_INVALID_SIZE | 0x52 |
| PEI_MEMORY_MISMATCH | 0x52 |
| PEI_MEMORY_NOT_DETECTED | 0x53 |
| PEI_MEMORY_NONE_USEFUL | 0x53 |

| Regular Boot Error Codes | Code |
|---|---|
| PEI_MEMORY_ERROR | 0x54 |
| PEI_MEMORY_NOT_INSTALLED | 0x55 |
| PEI_CPU_INVALID_TYPE | 0x56 |
| PEI_CPU_INVALID_SPEED | 0x56 |
| PEI_CPU_MISMATCH | 0x57 |
| PEI_CPU_SELF_TEST_FAILED | 0x58 |
| PEI_CPU_CACHE_ERROR | 0x58 |
| PEI_CPU_MICROCODE_UPDATE_FAILED | 0x59 |
| PEI_CPU_NO_MICROCODE | 0x59 |
| PEI_CPU_INTERNAL_ERROR | 0x5A |
| PEI_CPU_ERROR | 0x5A |
| PEI_RESET_NOT_AVAILABLE | 0x5B |
| DXE_CPU_ERROR | 0xD0 |
| DXE_NB_ERROR | 0xD1 |
| DXE_SB_ERROR | 0xD2 |
| DXE_ARCH_PROTOCOL_NOT_AVAILABLE | 0xD3 |
| DXE_PCI_BUS_OUT_OF_RESOURCES | 0xD4 |
| DXE_LEGACY_OPROM_NO_SPACE | 0xD5 |
| DXE_NO_CON_OUT | 0xD6 |
| DXE_NO_CON_IN | 0xD7 |
| DXE_INVALID_PASSWORD | 0xD8 |
| DXE_BOOT_OPTION_LOAD_ERROR | 0xD9 |
| DXE_BOOT_OPTION_FAILED | 0xDA |
| DXE_FLASH_UPDATE_FAILED | 0xDB |
| DXE_RESET_NOT_AVAILABLE | 0xDC |

| S3 Resume Error Codes | Code |
|---|---|
| PEI_MEMORY_S3_RESUME_FAILED | 0xE8 |
| PEI_S3_RESUME_PPI_NOT_FOUND | 0xE9 |
| PEI_S3_BOOT_SCRIPT_ERROR | 0xEA |
| PEI_S3_OS_WAKE_ERROR | 0xEB |

| Recovery Error Codes | Code |
|---|---|
| PEI_RECOVERY_PPI_NOT_FOUND | 0xF8 |
| PEI_RECOVERY_NO_CAPSULE | 0xF9 |
| PEI_RECOVERY_INVALID_CAPSULE | 0xFA |