WINSYSTEMS®

SBC35-427

Supplemental BIOS Manual

WinSystems, Inc. | 715 Stadium Drive, Arlington, Texas 76011 | 817-274-7553 | info@winsystems.com | www.winsystems.com

Revision History

BIOS Version	Last Updated Date	Brief Description of Change
42719177	1/1/19	Initial release

Copyright and Trademarks

Trademark Acknowledgments

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 SBC35-427 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 SBC35-427 platform.
2. Turn on the SBC35-427 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 SBC35-427 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 MS-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 SBC35-427 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 SBC35-427 platform.
2. Turn on the SBC35-427 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. 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. 5. Press **Enter**.

   The SBC35-427 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. 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 MS-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 SBC35-427 restarts and boots into the UEFI menu

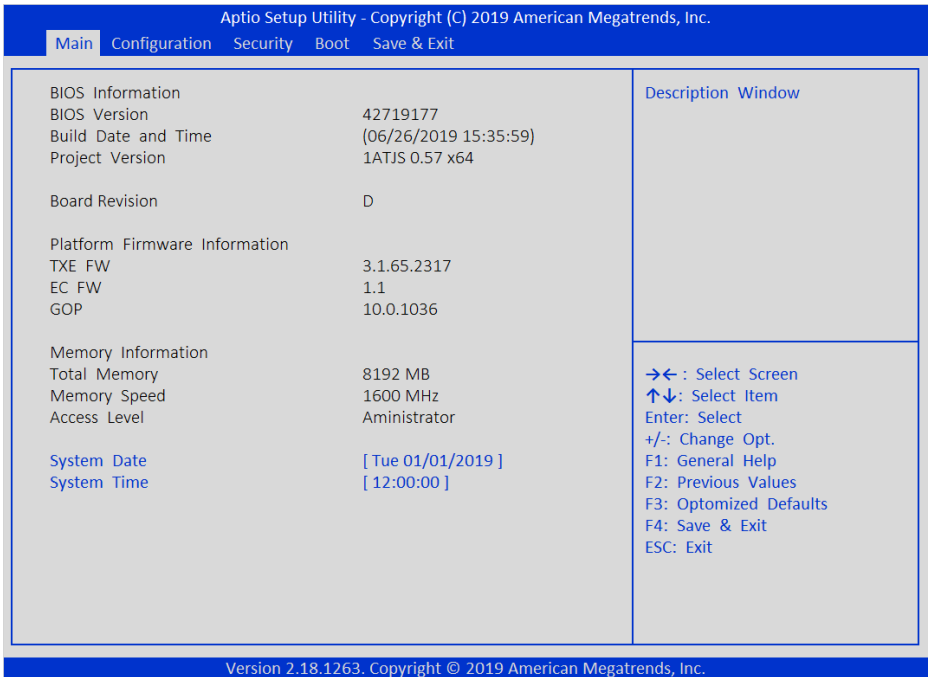
4. Click the **BIOS** button to enter the BIOS.

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.

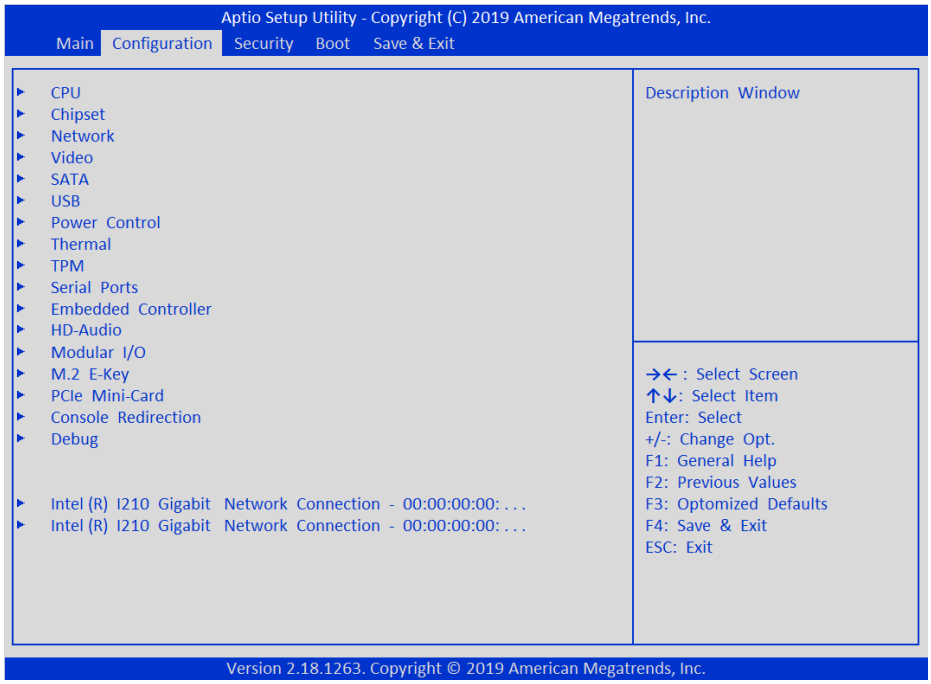
System time and date are configurable on the main BIOS page. An external battery is required to retain time and date if power is removed.

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 SBC35-427 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

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

Feature	Description	Choices	Default
Socket 0 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.		
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
Bi-directional PROCHOT	When a processor thermal sensor trips (any core), the PROCHOT# is driven and the processor is throttled. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.	Enable, Disable	Enable
Thermal Monitor	Uses the thermal control circuit to regulate the processor temperature. Allows the processor to maintain a safe operating temperature without the need for special software drivers or interrupt handling routines.	Enable, Disable	Enable
Monitor Mwait	Allows for efficient partitioning and unpartitioning of shared resources among logical processors. MONITOR sets up an effective address range monitored for write-to-memory activities; MWAIT places the processor in an optimized state until a write to the monitored address range.	Enable, Disable, Auto	Auto
DTS	Two on-die digital thermal sensors can be read via an internal register of the processor. The DTS is the preferred method of reading the processor die temperature because they are located much closer to the hottest portions of the die.	Enable, Disable	Disable

Feature	Description	Choices	Default
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
• Boot Performance Mode	Selects the performance state that the BIOS sets before OS handoff.	Max Performance, Max Battery	Max Performance
• C-States	Enables/disables the use of C-States, which are the “states” that the processor comes to in order to lower power consumption and temperature.	Enable, Disable	Enable
• Enhanced C-States	Enables/disables the use of enhanced C-States. C1 state is when the CPU is idle, but can instantly revert to its working state. C1E (C1 Enhanced) is the updated modern version of same state.	Enable, Disable	Enable
• Max Package C-State	Controls the Max Package C-State that the processor supports.	PC2, PC1, CO	PC2
• Max Core C-State	Limits the depth of the C-States in the HALT state.	Fused Value, Core C10, Core C9, Core C8, Core C7, Core C6, Core C1, Unlimited	Fused Value

4.3.2 Chipset Configuration

Set configuration options that are not CPU-specific.

Feature	Description	Choices	Default
Max Tolud	Sets the maximum Top of Low Usable DRAM (TOLUD) value, which specifies the memory space to be used by internal graphics devices, GTT Stolen Memory, and TSEG, respectively, if these devices are enabled.	2 GB, 2.25 GB, 2.5 GB, 2.75 GB, 3 GB	2 GB
Above 4GB MMIO BIOS assignment	Enables/disables memory mapped I/O for a 64-bit PCIe device to 4 GB or greater address space.	Enable, Disable	Disable
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
Serial IRQ	Enables/disables SERIRQ. Serialized interrupts are transmitted over a single shared SERIRQ line. From a software/OS standpoint, these interrupts are no different than legacy ISA interrupts.	Enable, Disable	Enable

Feature	Description	Choices	Default
Serial IRQ Mode	Sets the Serial IRQ mode as continuous or quiet. In continuous mode, the host continually generates SERIRQ frames to check for device interrupts. In quiet mode, the host waits for a SERIRQ slave to generate a request.	Quiet, Continuous	Continuous
ISH Controller	Enables/disables the Integrated Sensor Hub (ISH) controller. The ISH enables the ability to offload sensor polling and algorithm processing to a dedicated low power co-processor.	Enable, Disable	Enable
Beep Enable	Enables/disables all beeps during boot.	Enable, Disable	Enable

4.3.3 Network

Disable/enable the Intel I210 Ethernet network interface cards.

This section also provides the ability to enable IPv4 and IPv6 PXE boot.

Here are the steps for enabling and setting up IPv4 or IPv6 PXE boot.

1. Enable either **IPv4** or **IPv6** PXE boot under the Network tab.
2. Navigate to the Save & Exit tab, select **Save Changes and Reset**, then press **Enter**.
3. Enter the BIOS by pressing **DEL** or **ESC** during POST.
4. Navigate to the Boot tab and ensure that **Boot Option #1** under Boot Option Priorities is set to the specific PXE device setup under the Network tab.

4.3.4 Video

Specify video settings.

Feature	Description	Choices	Default
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 23.	Enable, Disable	Enable
VBT Select	Selects the desired video configuration for the Video BIOS Table (VBT) data passed to operating system while it boots. The first source listed is the primary display. NOTE: Use Single-DP1 or Single-LP for Windows OS. • Single = one video source • Dual = two video sources • DP1 = Display Port 1 • DP2 = Display Port 2 • LP = LVDS Panel	Dual-DP1-LP, Dual-DP2-LP, Dual-LP-DP1, Single-LP, Single-DP1	Single-DP1

Feature	Description	Choices	Default
LVDS Bridge	Enables/disables LVDS Bridge, which provides configuration options for the LVDS panel interface. Must be enabled if LP is selected as a video source.	Enable, Disable	Disable
IGD Flat Panel	Selects the panel resolution. If the desired resolution is not available, use the Custom Profile option and adjust the settings to match your panel. **NOTE:** LVDS Bridge must be enabled to view this option.	640 x 480, 800 x 480, 800 x 600, 1024 x 768, 1280 x 720, 1366 x 768, 1600 x 900, 1920 x 1080, Custom Profile	1024 x 768
LCD Panel Brightness	Adjusts the intensity of the LCD panel. **NOTE:** LVDS Bridge must be enabled to view this option.	12.5%, 25%, 37.5%, 50%, 62.5%, 75%, 87.5%, 100%	50%
Bpp Select	Selects the LVDS color depth, either 18 or 24 bits per pixel. **NOTE:** LVDS Bridge must be enabled to view this option.	18 bpp, 24 bpp	18 bpp
Custom Profile Settings	Configure the parameters according to the specific LVDS panel specification. **NOTE:** LVDS Bridge must be enabled, as well as IGD Flat Panel set to Custom Profile to view this option.		
• Pixel Clock in kHz	Pixel clock in kilohertz	10 to 655000	2500
• H Active Pixels	Active pixels, horizontal	480 to 1920	1920
• 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 1080	1080
• 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

4.3.5 SATA

Adjust controls for the two available SATA ports.

Feature	Description	Choices	Default
SATA Port 0	Enables/disables the SATA port at connector J3.	Enable, Disable	Enable
Port 0	Displays “Not Installed” if no device is present. Otherwise, the device information is displayed.		
SATA Port 1	Enables/disables the SATA port on the PCIe Mini-Card.	Enable, Disable	Enable
Port 1	Displays “Not Installed” if no device is present. Otherwise, the device information is displayed.		

4.3.6 USB

Configure the SBC USB ports and view a summary of installed devices.

Feature	Description	Choices	Default
USB 3.0 Port #1	Enables/disables USB port #1. When disabled, any devices plugged into the connector are not detected by BIOS or OS. This is the top socket on the dual stacked connector (J17).	Enable, Disable	Enable
USB 3.0 Port #2	Enables/disables USB port #2. When disabled, any devices plugged into the connector are not detected by BIOS or OS. This is the bottom socket on the dual stacked connector (J17).	Enable, Disable	Enable
USB 2.0 Ports #1-4	Enables/disables the USB 2.0 ports. Provides control to all ports of a 4-port USB 2.0 hub. When disabled, any devices plugged into any of the ports are not detected by BIOS or OS.	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
XHCI Hand-off	Enables/disables a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.	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). **NOTE:** Device power-up delay must be set to manual to view this option.	1 to 40	5

4.3.7 Power Control

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)
OS Reset Select	Selects the reset type in the Fixed ACPI Description (FADT) Table	Warm Reset, Cold Reset	Cold Reset
Wake On Lan	Permits the two Ethernet ports to wake the system from a sleep state.	Enable, Disable	Disable

4.3.8 Thermal

Configure ACPI parameters for operating system thermal management.

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
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
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
DPTF Policies	Controls the temperature of the ACPI Active Trip Point, which is the point at which the OS turns the fan on.		
• Active Policy	Enables/disables the Active Policy algorithm, which cools a platform through the removal of heat instead of limiting the power or performance of the device. Usually a platform fan is run at various speeds in response to the thermal conditions.	Enable, Disable	Enable

Feature	Description	Choices	Default
• Passive Policy	Sets the Passive Policy, which is responsible for limiting power and performance of components in response to a participant's temperature rising above the platform defined trip point. Passive Policy 2.0 uses a new ACPI object to configure the temperature thresholds. It may not be compatible with Linux.	Disable, Passive Policy 1.0, Passive Policy 2.0	Passive Policy 2.0
• TRT Revision	Sets the Thermal Relationship Table (TRT), which informs the OS the relative thermal contribution of each device to each thermal zone.	Traditional, Priority	Priority
• Critical Policy	Enables/disables the Critical Policy. In the event the platform reaches a critical temperature, the Critical Policy is responsible for gracefully shutting down the system.	Enable, Disable	Enable
• Power Boss	Enables/disables the Power Boss policy. The goal of the policy is to prevent platform shutdown due to a power “brown out” due to a peak or sustained power load that is not supported by the present power source.	Enable, Disable	Enable

4.3.9 TPM

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.	Enable, Disable	Enable
SHA256 PCR Bank	Enables/disables SHA256 PCR Bank.	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.	None, TPM Clear	None

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

4.3.10 Serial Ports

Configure the three serial ports, two ports on the SOC and one legacy port.

Feature	Description	Choices	Default
COM1	Controls and configures SOC Serial Port #1. This port supports RS232, RS485, and RS422 protocols. If using the CBL-SER2-202-12A cable assembly, this port corresponds to the J2 connector.	Enable, Disable	Enable
• Mode	Selects UART mode.	RS-232, RS-485 Half Duplex, RS-422 Full Duplex	RS-232
• Slew	Selects UART slew rate. All drivers can be slew limited to 250 kbps to minimize electro-magnetic interference (EMI) by selecting the Limited option.	Limited, Not Limited	Limited
• Receiver Termination	Selects UART cable receiver termination: no termination or 120 ohms. The receiver inputs are high impedance when termination is disabled. **NOTE:** Only available for RS-485 and RS-422 modes.	None, 120 ohms	None
• Transmitter Termination	Selects UART cable transmitter termination: no termination or 120 ohms. **NOTE:** Only available for RS-422 mode.	None, 120 ohms	None
COM2	Controls and configures SOC Serial Port #2. This port supports RS232, RS485, and RS422 protocols. If using the CBL-SER2-202-12A cable assembly, this port corresponds to the J3 connector.	Enable, Disable	Enable
• Mode	Selects UART mode.	RS-232, RS-485 Half Duplex, RS-422 Full Duplex	RS-232
• Slew	Selects UART slew rate. All drivers can be slew limited to 250 kbps to minimize electro-magnetic interference (EMI) by selecting the Limited option.	Limited, Not Limited	Limited
• Receiver Termination	Selects UART cable receiver termination. The receiver inputs are high impedance when termination is disabled. **NOTE:** Only available for RS-485 and RS-422 modes.	None, 120 ohms	None
• Transmitter Termination	Selects UART cable transmitter termination. **NOTE:** Only available for RS-422 mode.	None, 120 ohms	None
Legacy UART	Controls and configures the Legacy UART on the EC. This port only supports the RS232 protocol.		
• Address	Selects Legacy UART address. **NOTE:** Legacy UART settings are mirrored in the Embedded Controller section of the BIOS options.	3F8, 2F8, 3E8, 2E8	2F8
• Interrupt	Selects Legacy UART interrupt.	IRQ3	IRQ3
• Baud Rate	Selects Legacy UART baud rate in kbps.	9600, 19200, 38400, 57600, 115200	115200

4.3.11 Embedded Controller

Configure the embedded controller functions (Legacy UART and Watchdog Timer) and view ambient temperature and SOC voltages.

Feature	Description	Choices	Default
Legacy UART	Controls and configures the Legacy UART on the EC. This port only supports the RS-232 protocol. **NOTE:** Legacy UART settings are mirrored in the Serial Ports section of the BIOS options.	Enable, Disable	Enable
Address	Selects Legacy UART address.	3F8h, 2F8h, 3E8h, 2E8h	2F8
Interrupt	Selects Legacy UART interrupt.	IRQ3, IRQ4, IRQ5	IRQ3
Baud Rate	Selects Legacy UART baud rate.	9600, 19200, 38400, 57600, 115200	115200
Watchdog Timer	Controls the watchdog timer (WDT) on the EC. If enabled, mode and time-out can be configured.	Enable, Disable	Disable
Time-Out	Selects WDT time-out value.	1 to 255	0
Mode	Selects WDT time units.	Seconds, Minutes	Minutes

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

- Ambient Temperature
- Core Voltage
- +5V Voltage
- +3.3 Voltage
- +12V Voltage
- VDDQ Voltage
- Battery Voltage

4.3.12 HD-Audio

Enable/disable high-definition (HD) audio.

Feature	Description	Choices	Default
HD-Audio Support	Enables/disables high-definition audio.	Enable, Disable	Enable

4.3.13 Modular I/O

Configure the WINSYSTEMS Modular IO80 port such as USB 2.0 ports, PCIe, and SPI.

Feature	Description	Choices	Default
USB Port #2	Enables/disables the USB port. When disabled, any devices plugged into the connector is not detected by BIOS or OS.	Enable, Disable	Enable
USB Port #3	Enables/disables the USB port. When disabled, any devices plugged into the connector is not detected by BIOS or OS.	Enable, Disable	Enable
PCI Express Root Port 5	Controls the PCIe root port. • Auto: Disables unused port automatically for optimum power savings. • Enable: Enables port. • Disable: Disables port.	Auto, Enable, Disable	Auto
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	Auto
PCIe Speed	Selects the PCIe port speed. • Auto matches the speed of the inserted device. • Gen1 supports up to 2.5 GigaTransfers per second. • Gen2 supports up to 5 GigaTransfers per second.	Auto, Gen1, Gen2	Auto
SPI #2	Controls the SPI interface. Enabled only if there is an SPI device on an IO80 add-in board.	Enable, Disable	Disable
Sensor Hub I2C	Enables/disables the sensor hub, which offloads sensor polling and algorithm processing to a dedicated low-power co-processor.	Enable, Disable	Disable
Sensor Hub I2C Speed	Selects the I2C speed. Standard Mode runs at 100 kHz and Fast Mode runs at 400 kHz.	Standard Mode, Fast Mode	Standard Mode

4.3.14 M.2 E-Key

Configure options for the M.2 Socket such as USB 2.0 ports, PCIe, High Speed UART, and GPIO.

Feature	Description	Choices	Default
USB Port #4	Enables/disables the USB port. When disabled, any devices plugged into the connector are not detected by BIOS or OS.	Enable, Disable	Enable
PCI Express Root Port 1	Controls the PCIe root port. • Auto: Disables unused port automatically for optimum power savings. • Enable: Enables port. • Disable: Disables port.	Auto, Enable, Disable	Auto

Feature	Description	Choices	Default
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
PCIe Speed	Selects PCIe port speed. • Auto matches the speed of the inserted device. • Gen1 supports up to 2.5 GigaTransfers per second. • Gen2 supports up to 5 GigaTransfers per second.	Auto, Gen1, Gen2	Auto
High Speed UART #2	Enables/disables High Speed UART.	Enable, Disable	Disable
SDIO	Enables/disables the SDIO interface.	Enable, Disable	Disable

4.3.15 PCIe Mini-Card

Configure options for the PCIe Mini-Card socket such as a USB 2.0 port, a SATA channel, and PCIe.

Feature	Description	Choices	Default
USB Port #5	Enables/disables the USB port. When disabled, any devices plugged into the connector are not detected by BIOS or OS.	Enable, Disable	Enable
SATA Port 1	Enables/disables the SATA channel.	Enable, Disable	Enable
Port 1	Displays “Not Installed” if no device is present. Otherwise, the device information is displayed.		
PCI Express Root Port 3	Controls the PCIe root port. • Auto: Disables unused port automatically for optimum power savings. • Enable: Enables port. • Disable: Disables port.	Auto, Enable, Disable	Auto
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
PCIe Speed	Selects the PCIe port speed. • Auto matches the speed of the inserted device. • Gen1 supports up to 2.5 GigaTransfers per second. • Gen2 supports up to 5 GigaTransfers per second.	Auto, Gen1, Gen2	Auto

4.3.16 Console Redirection

Enable console redirection to mirror the console output to Serial Port 2 on connector J4. Console Redirection settings are only available when Console Redirection is enabled.

4.3.17 Debug

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 is not enabling DCI feature.	Enable, Disable	Disable
DCI Auto Detect Enable	Enables/disables DCI Auto Detect. When set to Auto Detect, it detects DCI being connected during BIOS post time and enables DCI. Otherwise it disables DCI.	Enable, Disable	Enable

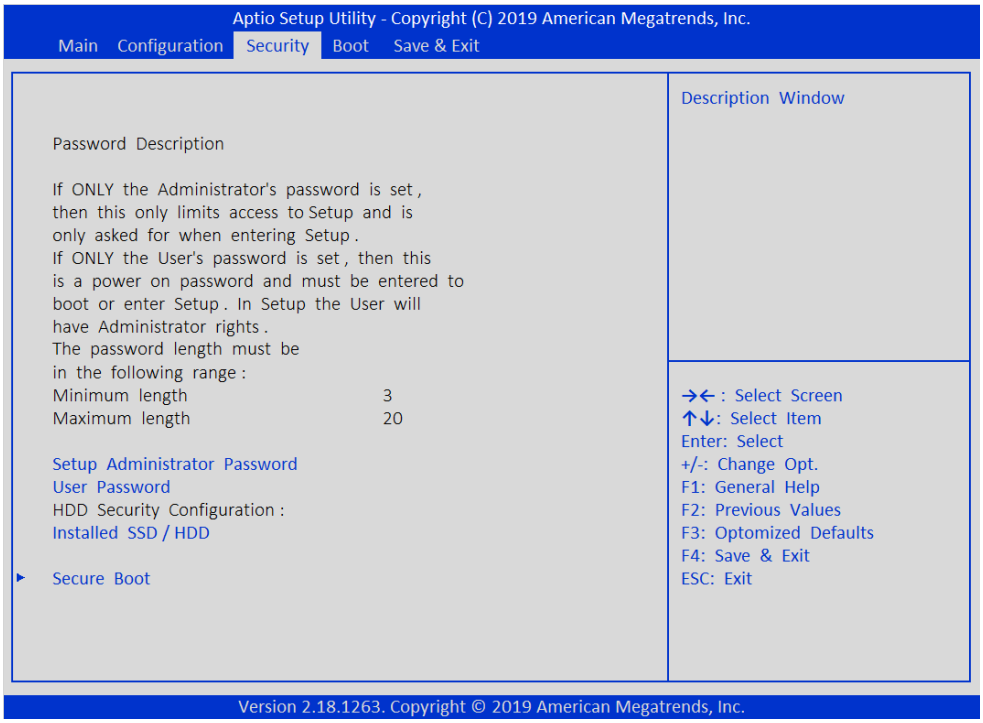
4.3.18 Intel I210 Gigabit Network Connection 1 & 2

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 the server to be powered on using an in-band 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 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.

4.4.2 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.

4.4.3 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.

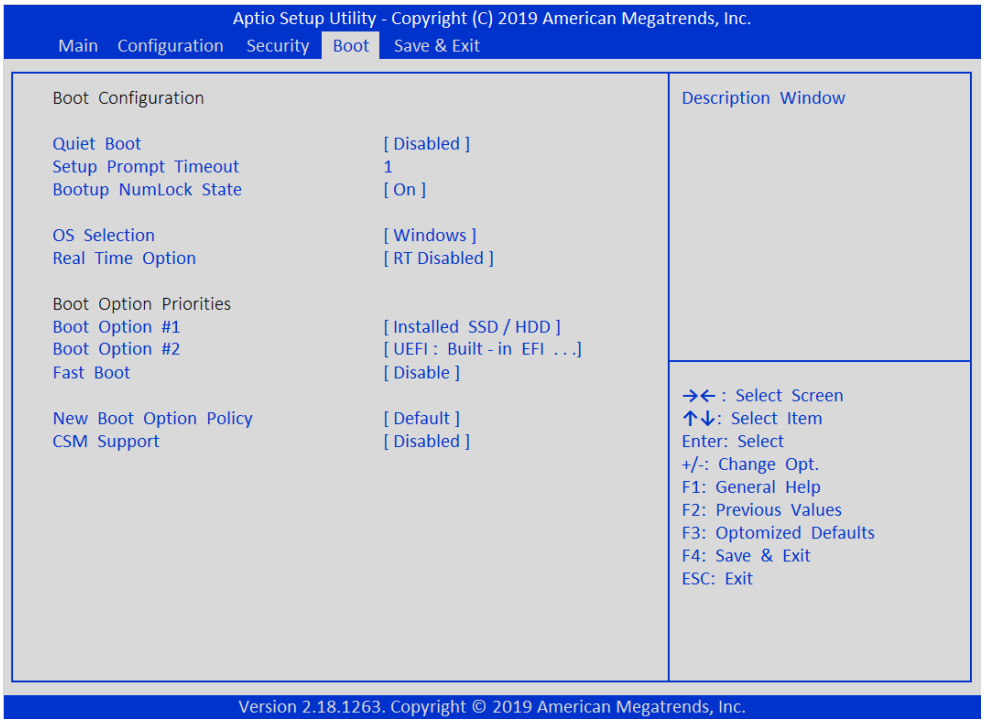
4.4.4 Secure Boot

Navigate to the appropriate HDD or SSD drive and press **Enter** to 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 Mode - Custom and Standard	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. **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. **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 SBC35-427 such as BIOS bootup and logo display, device boot order, and CSM support.



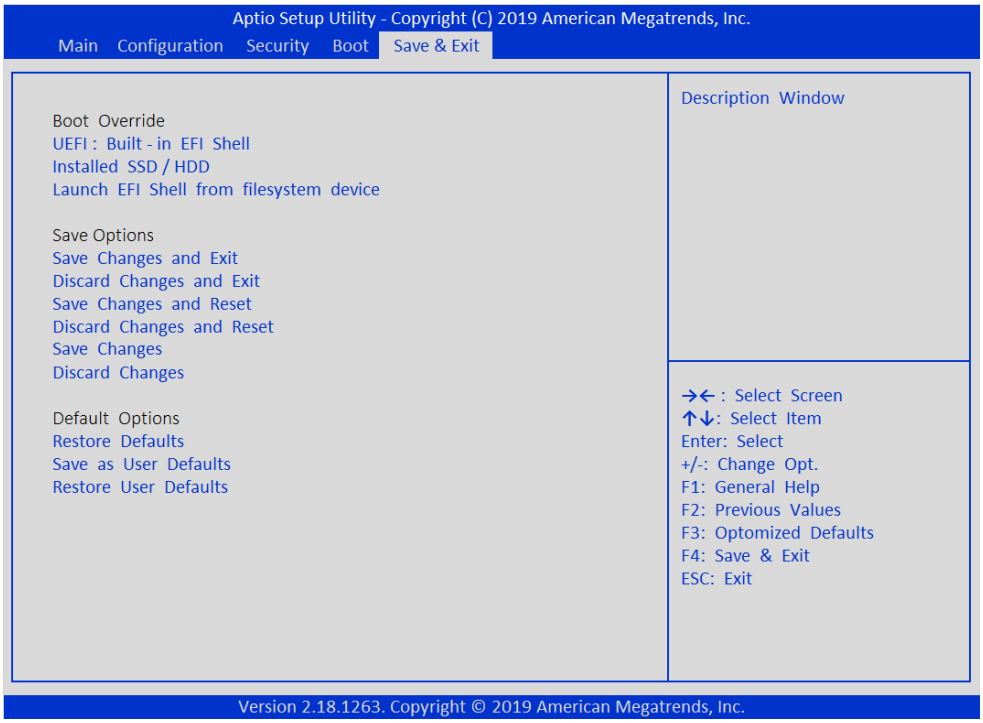
Feature	Description	Choices	Default
Quiet Boot	Enables/disables quiet boot. Enabling this option hides the BIOS post messages on bootup and displays the AMI BIOS logo. This logo is configurable for custom OEM applications. Contact a WINSYSTEMS Applications Engineer at 1-817-274-7553 for more information.	Enable. Disable	Disable
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
OS Selection	Selects the target operating system. Other menu options may change based on the OS selection. This is proper behavior.	Windows, Linux, MS-DOS	Windows
Real Time Option	Enables/disables the following real time features: • L2 cache partitioning to decrease access latency • PCIE packet prioritization based on traffic class • Hardware-assisted time synchronization	RT Disabled, RT Enabled	RT Disabled
Boot Option Priorities	All bootable options are listed in the order of boot priority. The list can be rearranged to the desired boot device order.		
• Fast Boot	Enables/disables the Fast Boot features, which shorten the normal boot path for booting into an OS rapidly. Most device probes are skipped to reduce boot time.	Enable. Disable	Disable
• New Boot Option Policy	Controls the placement in the boot order of newly detected UEFI boot options. If default is selected, a new device is moved to the bottom of the boot priority list but in front of the UEFI shell. Other options are the top or the bottom of the list.	Default, Place First, Place Last	Default
• 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
• Primary IGFX Boot Display	Selects the video device which will be activated during POST. Secondary boot display selection appears based on your selection. **NOTE:** This option is only available when CSM Support is enabled.	Auto, Display Port 1, Display Port 2, LVDS	Auto
• GateA20 Active	Enabling the Gate-A20 line is an early step that a protected-mode x86 operating system does in the bootup process. • Upon Request - can be disabled using BIOS services. • Always - GA20 never disabled; this option is useful when any RT code is executed above 1 MB. **NOTE:** This option is only available when CSM Support is enabled.	Upon Request, Always	Upon Request
• INT19 Trap Response	Specifies the timing for executing an INT19 trap. INT 19h is a low-level system command normally used just after POST to boot the OS. • Immediate - execute the trap right away. • Postponed - execute the trap during legacy boot. **NOTE:** This option is only available when CSM Support is enabled.	Immediate, Postponed	Immediate

Feature	Description	Choices	Default
• Boot Option Filter	Selects the search criteria for bootable devices. Legacy looks for bootable drives that use an MBR partitioning scheme. UEFI looks for bootable drives that use a GPT partitioning scheme. **NOTE:** This option is only available when CSM Support is enabled.	UEFI and Legacy, Legacy only, UEFI only	UEFI and Legacy
Option ROM Execution	**NOTE:** These option are only available when CSM Support is enabled.		
• Network	Controls the execution of PXE Boot as UEFI or Legacy.	Do not launch, UEFI, Legacy	UEFI
• Storage	Controls the execution of the UEFI connected storage device as UEFI or Legacy.	Do not launch, UEFI, Legacy	UEFI
• Video	Controls the execution of the Video as UEFI or Legacy.	Do not launch, UEFI, Legacy	UEFI

4.6 Save & Exit

Save custom BIOS options to the CMOS ROM.

These options can be saved as temporary changes or saved as user defaults. 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 Boot Override

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

4.6.2 Save Options

Feature	Description
Save Changes and Exit	Saves all custom configured BIOS settings, then immediately boots to the first boot device set in Boot Option Properties (see "Boot" on page 23)
Discard Changes and Exit	Reverts any custom configured BIOS settings to default, then boots to your first boot device.
Save Changes and Reset	Saves all custom configured BIOS settings, then immediately reboots the computer.
Discard Changes and Exit	Reverts any custom configured BIOS settings back to default, then reboots the computer.
Save Changes	Saves all custom configured BIOS settings.
Discard Changes	Reverts any custom configured BIOS settings during this session back to default.

4.6.3 Default Options

Feature	Description
Restore Defaults	Clears any changes to BIOS settings and reverts all settings back to factory defaults.
Save as User Defaults	Saves any changes to BIOS settings as custom defaults. This does not affect factory defaults.
Restore User Defaults	Similar to Restore defaults, this option restores the BIOS settings originally saved as User Defaults.

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 SBC35-427 and press **ESC** or **DEL** during the boot process, which starts the BIOS setup utility.
2. In the BIOS setup utility, use the arrow keys to highlight the **Save & Exit** menu option.
3. Using the arrow keys, highlight **Restore Defaults** and press **Enter**.
4. 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

Jumpering pins 1-2 on jumper JP1 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 JP1:

1. Remove power from the board.
2. Place a jumper across 1-2.
3. Apply power to the board, and let it boot into the BIOS.
4. Power off the board, and remove the jumper at 1-2.

6. Software Description

This section describes the AMI BIOS components to be used in the implementation of the SBC35-427 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:

- MS-DOS 6
- 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 8.1.5 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
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

Regular Boot POST Codes	Code
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
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
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

Regular Boot Error Codes	Code
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