Diebold Nixdorf

M1 and M2 POS Motherboard

(with BIOS Setup)

User Manual (Edition March 2019)

We would like to know your opinion on this publication.
Please send us a copy of this page if you have any constructive criticism.
We would like to thank you in advance for your comments.

With kind regards,

Your opinion:

Diebold Nixdorf International GmbH
Documentation R&D BLN 2
Wohlrabedamm 31
D-13629 Berlin
E-Mail: retail.documentation@dieboldnixdorf.com
Order No.: ***01750297725A***

M1 and M2 POS Motherboard

User Manual

Edition March 2019

Overview

Introduction

This manual describes the features of two variants of a Motherboard based on the Intel 100 series chipset Q170 and H110, formerly known as Skylake.

These **M1** and **M2** Motherboards were primarily designed for the Diebold Nixdorf POS System BEETLE /M-III.

Some Highlights of the M1 and M2 Motherboard

- 6th and 7th Generation Intel® Core™ Processors, formerly known as Skylake and Kaby Lake
- Intel 100 series chipset Q170 and H110
- CPU integrated graphic controller up to Intel® HD Graphics 630, depending on used processor
- AMT 11.6 support at M1 motherboards
- 2x WN Panellink 2 interfaces
- 1x VGA interface
- Gigabit LAN onboard (Intel® Ethernet Connection; Q170: i219-LM, H110: i219-V)
- 3 SATA III ports
- 2x DDR4 SODIMM sockets, supporting up to 32GB (2x16GB) at 2133/2400MHz. Only ~2GB available for 32bit OS
- 1x PCI Express x16 gen3
- 2x PCI Express x1 gen3
- 6 COM ports. COM1 is unpowered, COM2-6 have the option to be powered
- 1 LPT port
- MiniPCIe socket (full size) supporting the WN NVRAM module

- M.2 (PCIe x4/SATA) on M1
- 1x PS2 (KBD/MS)
- 2 USB3.0 ports
- up to 10 USB2.0 ports (H110: 6 ports)

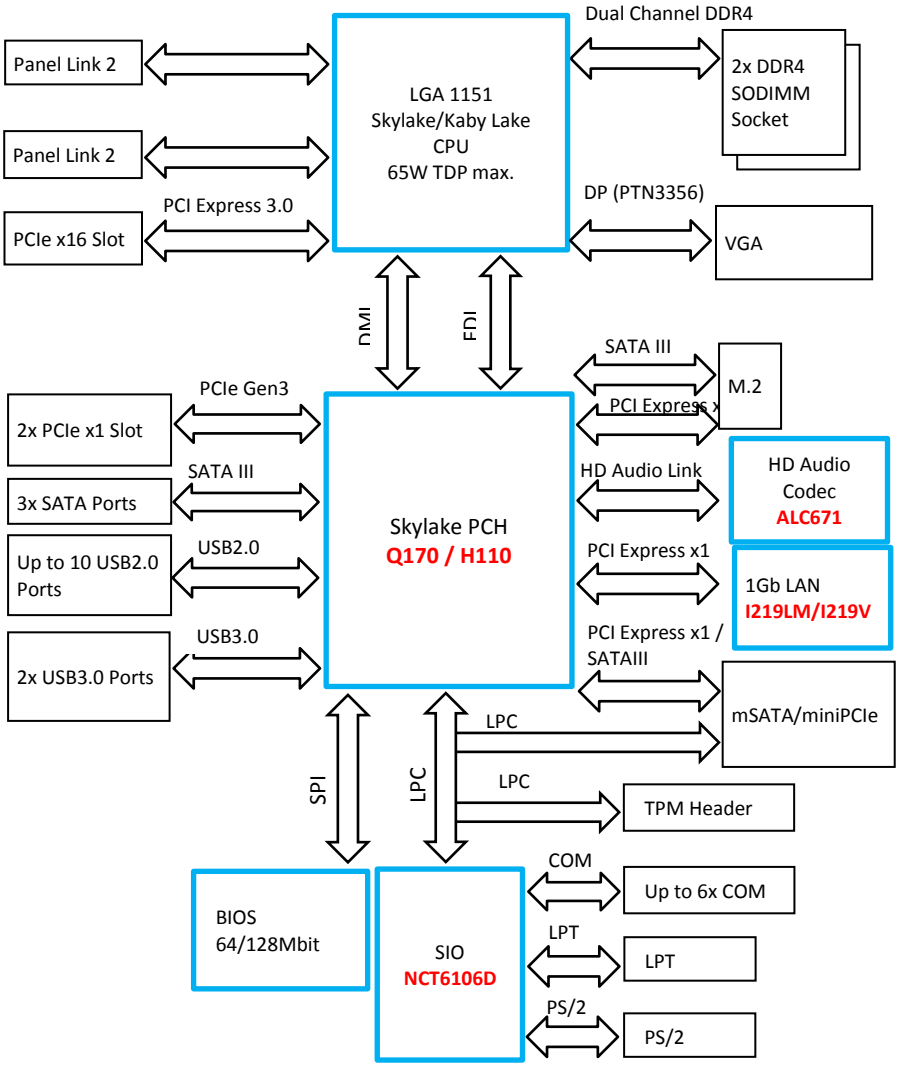
TFT- displays without DDC are not supported.

Motherboard Specification

Mainboard assembly variants

As mentioned above there are two motherboard variants: The **M1** board with Q170 chipset supporting AMT, RAID, M.2 and mPCIe and the **M2** board with H110 chipset as value edition supporting lesser features.

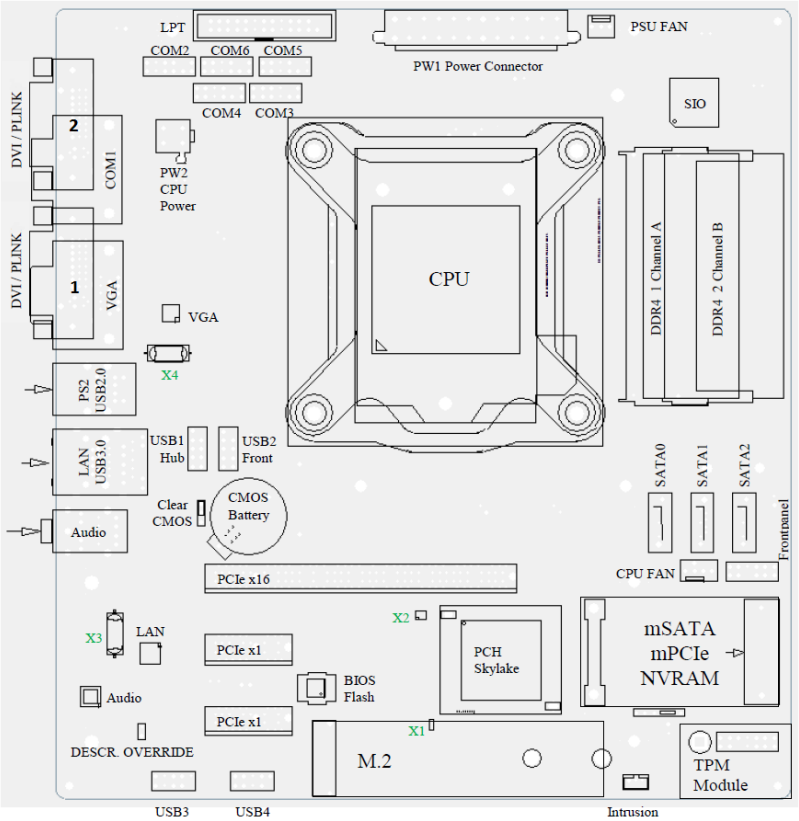
Block Diagram



CPU support

CPU	CPU#	#CPU core	#Threads	Base (Turbo) Freqency	GFX	Cache size	TDP [W]
i5 (Kaby Lake)	i5-7500	4	4	3.4 (3.8)	HD 630	6MB	65
i5 (Skylake)	i5-6500	4	4	3.2 (3.6)	HD 530	6MB	65
i3 (Kaby Lake)	i3-7101E	2	4	3.9	HD 630	3MB	54
I3 (Skylake)	I3-6100	2	4	3.7	HD 530	3MB	51
Pentium (Skylake)	G4400	2	2	3.3	HD 510	3MB	54
Celeron (Skylake)	G3900	2	2	2.8	HD 510	2MB	51

Mainboard internal connectors and onboard features



Memory (internal)

The mainboard provides two DDR4 unbuffered SODIMM sockets supporting up to 32GB in dual channel mode. The horizontal mounting of the SODIMM sockets ensures an optimal air flow.
DDR4 I/O Voltage of 1.2 V.
4Gb and 8Gb DDR4 DRAM device technologies are supported.
The amount of installed memory that can be used may vary based on the BIOS settings and the used OS.
Total Video memory size up to 1536MB of the installed memory.
(Pre-allocated Video memory size up to 1GB)

Serial ports (internal)

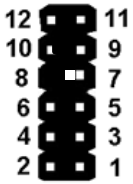
The mainboard provides 1 external and 5 internal COM ports (with FIFO, 16550 compatible) from NCT6106D.
COM2 -6 are configurable to standard or powered COM ports with an internal COM cable option (max current for powered COM: single port 300mA@5V; all ports together not more than 500mA@5V; single port 600mA@12V; all ports together not more than 900mA@12V).

Maximum voltage drop on 12V is 300mV, on 5V it is 150mV at full load. This output is designed according to UL regulations and is protected by a self-resettable fuse.

COM1 is a standard 9 pin DSUB connector in I/O shield.

2x 6 pin header, 2.54 mm pitch

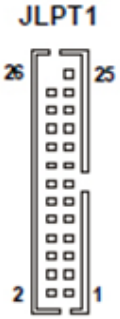
Pin	Signal
1	DCD
2	RX
3	TX
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI
10	Key Pin
11	+5 V
12	+12 V



LPT (internal)

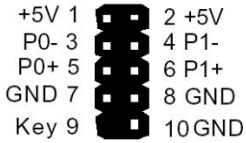
LPT (IEEE1284 compliant) via NCT6106D.
Connector type: 26 pin shrouded header, 2.54mm pitch

Pin	Function	Pin	Function
1	STR#	14	GND
2	AFD#	15	D6
3	D0	16	GND
4	ERR#	17	D7
5	D1	18	GND
6	PINIT#	19	ACK#
7	D2	20	GND
8	LPT_SLIN#	21	BUSY
9	D3	22	GND
10	GND	23	PE
11	D4	24	GND
12	GND	25	SLCT
13	D5	26	Key



USB 2.0 (internal)

7 USB ports at M1 board and 3 USB ports at M2 are routed to 10pin double row headers with 2.54 mm pitch. These headers are intended to connect optional front USB modules or USB hubs.

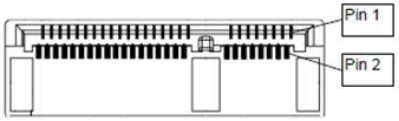


USB1_Hub port header contains only 1 USB port (pins 1,3,5,7)

Mini PCI Express /mSATA (internal)

The mainboard provides a full size mini PCI Express / mSATA connector. It is placed on top, thus being accessable without removing other components. It supports LPC signals to support optional NVRAM modules.
The power supply is only available in S0. There is no PCIe WAKE support. The interface (SATA or PCIe) is automatically detected using Pin 51 of the mSATA connector (GND = SATA; N.C = PCIe).

PCIe functionality is only supported on M1 motherboard.
Connector type: Standard MiniPCIe connector full size



Pin	Signal
1	Not connected
3	Not connected
5	Not connected
7	Not connected
9	GND
11	CLK 100M -
13	CLK 100M +
15	GND
Key	
17	RESET
19	CLK_LPC
21	GND
23	RX + (upstream)
25	RX - (upstream)
27	GND
29	GND
31	TX - (downstream)
33	TX + (downstream)
35	GND
37	GND
39	3,3V
41	3,3V
43	GND
45	Not connected
47	Not connected
49	Not connected
51	DET_SATA#

Pin	Signal
2	3,3V
4	GND
6	1,5V
8	LPC_FRAME
10	LPC_LAD3
12	LPC_LAD2
14	LPC_LAD1
16	LPC_LAD0
Key	
18	GND
20	Not connected
22	RESET
24	3,3V
26	GND
28	1,5V
30	SMB CLK
32	SMB DAT
34	GND
36	Not connected
38	Not connected
40	GND
42	Not connected
44	Not connected
46	Not connected
48	1,5V
50	GND
52	3,3V

M.2 (internal)

The M.2 connector supports M.2 Key M modules with SATA or PCIe up to x4 interface and a size of 2260 and 2280. The interface (SATA or PCIe) is automatically detected using the PEDET Pin 69 of the M.2 connector (GND = SATA; N.C = PCIe).

Pin	Signal
1	GND
3	GND
5	RX3 - (upstream)
7	RX3 + (upstream)
9	GND
11	TX3 - (downstream)
13	TX3 + (downstream)
15	GND
17	RX2 - (upstream)
19	RX2 + (upstream)
21	GND
23	TX2 - (downstream)
25	TX2 + (downstream)
27	GND
29	RX1 - (upstream)
31	RX1 + (upstream)
33	GND
35	TX1 - (downstream)
37	TX1 + (downstream)
39	GND
41	RX0 + (upstream)
43	RX0 - (upstream)
45	GND
47	TX0 - (downstream)
49	TX0 + (downstream)
51	GND
53	CLK 100M -
55	CLK 100M +
57	GND
13	Key
15	Key
17	Key
19	Key
67	Not connected
69	DET_SATA#
71	GND
73	GND
75	GND

Pin	Signal
2	3,3V
4	3,3V
6	Not connected
8	Not connected
10	HDLED#
12	3,3V
14	3,3V
16	3,3V
18	3,3V
20	Not connected
22	Not connected
24	Not connected
26	Not connected
28	Not connected
30	Not connected
32	Not connected
34	Not connected
36	Not connected
38	DEVSLP
40	Not connected
42	Not connected
44	Not connected
46	Not connected
48	Not connected
50	RESET
52	Not connected
54	Not connected
56	Not connected
58	Not connected
60	Key
62	Key
64	Key
66	Key
68	Not connected
70	3,3V
72	3,3V
74	3,3V

SATA (internal)

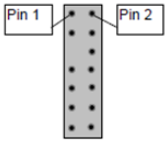
The mainboard provides three standard SATA ports. The ports SATA0 (white) and SATA1 (blue) and SATA2 (black) supporting SATA III connectivity speed. SATA3 port is connected to mSATA connector and SATA4 port is connected to M.2 connector.
The RAID functionality is only supported by the M1 motherboard.

TPM (internal)

Trusted Platform Modules are a Trusted Computing Group (TCG) security solution to increase the system security.
The Platform supports Intel PTT or TPM1.2 / TPM2.0 Modules connected to the TPM connector.

Pin	Signal
1	GND
3	CLK_LPC
Key	
7	RESET
9	3,3V
11	Not connected
13	3,3V STBY

Pin	Signal
2	LPC_FRAME
4	LPC_LAD3
6	LPC_LAD2
8	LPC_LAD1
10	LPC_LAD0
12	LPC_SERIRQ
14	Not connected



PCI Express Slots (internal)

There are two PCIe slots x1 Gen3 and one 1 PCIe slot x16 Gen3.

PCIe cards are able to wake up the system.

Thermal management: The input power of a single PCIe x1 card must not exceed 10W and x16 card does not exceed 30W.

The PCIe slot at the outer side of the mainboard supports USB signals on PCIe pins A5 (D-) and A8 (D+) as USB uplink connection and A6+A7 (VBUS) to support specific Retail PCIe card.

Front panel connector (internal)

The mainboard supports a front panel connector to support service elements (like POWER ON pushbutton, HDD and power LEDs).

Indicator	Signaling	Description	ACPI State	
Systemstate	'Power On'	System is full working	G0	S0
	'Power On' LED is blinking equably 500ms on / 500ms off	System is sleeping.	G1	S3
	'Power on' LED is off 'Sleep' LED (orange) is on	System is sleeping and the contents is saved on disk.	G1	S4
	'Power On' LED is off 'Sleep' LED (orange) is off	System is off.	G2	Deep Sleep
			G3	
	'Power On' LED is blinking 4x short then repeated after intermission 100ms on/ 900ms off 1	Failure in Power Supply		

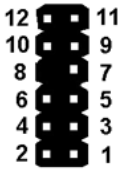
	‘Power On’ LED is blinking 2x short then repeated after intermission: 100ms on/ 100ms off 100ms on/ 700ms off …	Failure in CPU Power Supply, CPU or BIOS		
Harddisk	‘Harddisk’ LED is flashing	Drive access	G0	S0
	Off	No drive access		
			G1	S1 – S4
			G2	S5
			G3	

The BIOS is able to disable the power button during S0. Then it is not possible to shut down the system by the power button, even when pressed longer than 4s. Power on from S5 is still possible.

The front panel header also supports speaker connection.

Type: 2x6 pin header, 2.54 mm pitch.

Pin Number	Function
1	Power switch +
2	Reset switch +
3	Power switch -
4	Reset switch -
5	Power LED +
6	Speaker -
7	Power LED -
8	Coding
9	HDD LED +
10	GND
11	HDD LED -
12	Speaker +



Chassis intrusion connector (internal)

The mainboard supports a chassis intrusion connector connected to the PCH.
The intrusion monitoring is used to protect the system against unauthorized opening. This is detected, even if no AC is connected. However, this will not be indicated until the system is operating again.
Type: 3 pin shrouded header, B3B-PH-K-S (JST) or equivalent.

Pin Number	Function
1	GND
2	Intrusion input (switch to GND if chassis is open)
3	n.c.

Clear CMOS jumper (internal)

Pin	Signal
1	GND
2	RTC – Reset and load BIOS setup defaults
3	NC – Not Connected

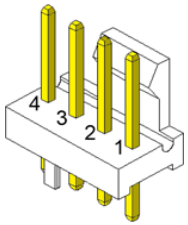
Fan (internal)

The mainboard provides two fan connectors. The CPU fan connector supports PWM fans with 4 pin connection.

Connector details are: 2.54mm (.100") Pitch Vertical Header, with Friction Lock, 4 (3) Circuits, PC Tail Length: 3.50mm (.138"). Molex Part Nr: 47053-1000 or similar. The connector follows the Intel "4-Wire Pulse Width Modulation (PWM) Controlled Fans" specification.

PWM Fan

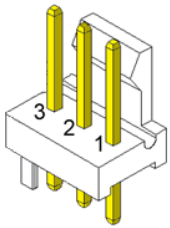
Pin	Signal	Signal Description
1	GND	GND
2	12 V	Fan operation voltage
3	Sense	Tachometric signal
4	Control	PWM control signal (only 4 pin connector)



The PSU fan connector has 3 pin connection with DC fan speed regulation.

DC Fan

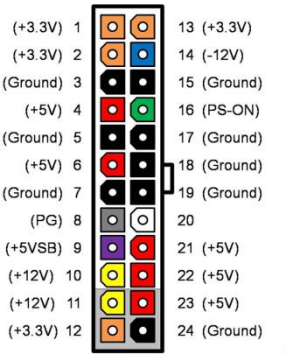
Pin	Signal	Signal Description
1	GND	GND
2	PWR	Operation Voltage 5-12 V
3	Sense	Tachometric signal



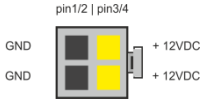
ATX / 12V Power connector (internal)

The mainboard provides a 4 pin and a 24 pin ATX power connector.

Pin Number	Function
1,2,12,13	+3.3V
3,5,7,15,17,18,19,24	GND
4,6,21,22,23	+5V
8	Power ok
9	5V SB
10, 11	+12V
14	-12V
16	PSON
20	n.c.



Pin Number	Function
1,2	GND
3,4	+12V



A 20 pin ATX power cable can be plugged into the 24 pin connector on the motherboard, too. In this case the pins 11,12,23 and 24 are not used and left open. The 4 pin ATX power connector has to be connected to the PSU anyway, otherwise the motherboard will not work.

Voltage regulator

IMVP8: 65 W TDP desktop and server/workstation SKUs
High efficient CPU VR 12.5 Design

XHCI USB controller

The PCH contains an eXtensible Host Controller Interface (XHCI) host controller which supports up to 10 USB 3.0 ports and 14 USB 2.0 ports. This controller allows data transfers up to 5 Gb/s. The controller supports SuperSpeed (SS), high-speed (HS), full-speed (FS) and low speed (LS) traffic on the bus.
Windows 7 does not natively support the Skylake USB controller. Therefor a PS2 keyboard/mouse is recommended for OS setup.
Current BIOS versions include a workaround (USB/PS2 emulation) in order to use USB keyboard / mouse
during MS Windows 7 installation
For Windows 7 installation a SATA DVD drive has to be used or the XHCI driver has to be integrated into the installation files to be able to use any USB drive during installation.

Processor Graphics

DirectX* Video Acceleration (DXVA) support for accelerating video processing.
Full AVC/VC1/MPEG2 HW Decode
Advanced Scheduler 2.0, 1.0, XPDM support.
Windows* 10, Windows* 8, Windows* 8.1, Windows* 7, OSX, Linux* OS support.
DirectX* 12.0, DirectX* 11.1, DirectX* 11, DirectX* 10.1, DirectX* 10, DirectX* 9 support.
OpenGL* 4.4, OpenGL* 4.0 support.
Max Display Resolutions:

DVI	1920x1200@60Hz
VGA	Any resolution and refresh rates are supported from 25 MHz up to 180 MHz pixel clock rate at 24 bpp, or up to 240 MHz pixel clock rate at 18 bpp

Display Modes: Single Display, Display Clone, Extended Desktop:
3 Independent displays on M1 only

Audio

Chip vendor and type: Realtek ALC 671

Audio Codec Ports	**Default**
A	N
B	M
C	L
D	N
E	N
F	N
G	N
H	N
I	L
SP	N

Remark: System Beeps are audible on Line_Out1 at Rear Connector.

Supported Sleep States

S0	**Normal Operation (“ON”)**
S3	**Suspend to RAM / “Stand By”**
S4	**Suspend to Disk / “Hibernation”**
S5	**Soft Off**

System wake up

System wake up is supported from the following devices and power states:

USB	S3 S4/S5 with keyboard only
PS/2	S3
Power button	S3/S4/S5/DS4/DS5
PCIe/PCI PME wakeup	S3/S4/S5
RTC	S3/S4/S5/DS4/DS5
WoL	S3/S4/S5

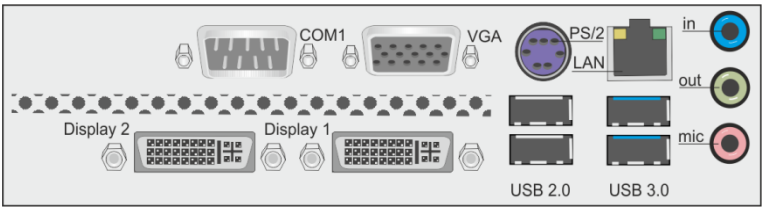
DeepSleep

When no wake up sources are set in BIOS, the system will go into DeepSleep, when shutting down the system to S5. Most of the onboard components will be powered off and also the power LED will stay off. In this case the system power consumption is below 0.5W, depending on PSU in use.
In this state the System can be switched on by power button or RTC WakeUp only.

Mainboard onboard connectors with external access

Motherboard I/O shield overview (external)

The picture below shows the arrangement of the onboard I/O connectors.



PanelLink 2.0 (external)

The PanelLink 2.0 interface is based on a DVI-I connector and uses DVI-D signals. There is no analog VGA connection even if it is a DVI-I connector. Unused pins of the connector are connected to USB signals.

Pin assignment

Pin	DVI-D	Function PL2.0
1	TMDS Data 2-	TMDS Data 2-
2	TMDS Data 2+	TMDS Data 2+
3	TMDS Data shield	TMDS Data shield
4	n.c.	+12V
5	n.c.	+12V
6	DDC CLK	DDC CLK
7	DDC DATA	DDC DATA
8	n.c. (VSYNC)	Power button RMT
9	TMDS Data 1-	TMDS Data 1-
10	TMDS Data 1+	TMDS Data 1+
11	TMDS Data shield	TMDS Data shield
12	n.c.	+12V
13	n.c.	+12V
14	5V	+5V SB
15	GND	GND
16	Hotplug detect	Hotplug detect
17	TMDS Data 0-	TMDS Data 0-
18	TMDS Data 0+	TMDS Data 0+
PIN	**DVI-D**	**Function PL2.0**
19	TMDS Data shield	TMDS Data shield
20	n.c.	+12V
21	n.c.	+12V
22	TMDS Data shield	TMDS Data shield
23	TMDS CLK+	TMDS CLK+
24	TMDS CLK-	TMDS CLK-
C1	n.c. (red)	
C2	n.c. (green)	n.c.
C3	n.c. (Blue)	USB-
C4	n.c. (HSYNC)	USB+
C5	GND	GND

The +12V signals are protected by a self-resettable fuse and are able to deliver a current of 2.5A.

This voltage rail is only enabled if a monitor DDC identification is passed and a PL2-capable monitor was detected, e.g. vendor ID is Diebold Nixdorf (05dh 0d8h) and device ID is in the range of 30000…34999.
This output is designed according to UL regulations. This output is switched off when PL2 connector is removed and is only switched on again after PL2 connector was attached and DDC identification detected a supported monitor again.

5VSB (pin 14) supply is enabled in S3, S4 and S5.

RMT pin 8 is a low active input and represents an ACPI button. This button supports system wakeup and system sleep functionality. It does not immediately power down the system if it is pressed for longer than 4s (power button overwrite).

The RMT feature for each Plink2 port can be enabled/disabled in BIOS setup.

VGA (external)

This interface uses a 15 pin DSUB connector in the upper row of I/O shield. Sync signals VSYNC and HSYNC have 5V logic high level.

PS/2 Keyboard / Mouse (external)

The Keyboard/Mouse connector is a part of the motherboard I/O shield. It also supports mouse and keyboard connection simultaneously by using a PS/2 Y-cable.

LAN (external)

The mainboard supports 1Gbit connection to a Local Area Network (LAN). Indication **LED** for link and activity is available.

Right LED	**Speed Indication**
10mbit	off
100mbit	green
1000mbit	yellow

Left LED	**Link&Activity**
Link at every speed	Green on
Traffic at every speed	Green blinking

WOL (wake on LAN) and Intel PXE are supported.

USB 2.0 / USB 3.0 (external)

Four USB ports (two for USB2.0 and two for USB3.0) are located in the mainboard I/O connector area.

Audio (external)

The mainboard supports a microphone-in (pink), a line-out (green) and a line-in (blue)
connector in I/O shield. The connector type is stereo 3.5mm diameter.

Power supply requirements

Power supply requirements only for onboard components w/o add-in cards and USB devices:

MultiRail:

Source	Voltage	Regulation Tolerance	Minimum system board current	Maximum system board current
Main power supply	+12V	+/- 5%	0,05A	8A/12A
	-12V	+/- 10%	0,0A	0,3A
	+5V	+/- 5%	0,2A	6A
	+3,3V	+/- 5%	0,0A	0,5A
Auxil-iary	+5V AUX	+5% / -3%	0,0A	2,5A

Power load ability

Fuse Number	Max. current	Function Description	Max. Current per
1	750mA	Keyboard/Mouse port	500mA
2	750mA	VGA	500mA
3	750mA	DVI 1 (5V)	500mA
4	750mA	DVI 2 (5V)	500mA
5	5A	DVI 1 (PLINK)	
6	5A	DVI 2 (PLINK)	
7	2A	COM(5V)	
8	1,5A	COM(12V)	
9	2A	USB3/LAN Port 0	900mA
		USB2/PS2 Port 2	500mA
10	2A	USB3/LAN Port 1	900mA
		USB2/PS2 Port 3	500mA
11	2A	USB2 Internal “USB1_HUB” Port 5	500mA
		USB2 Internal “USB2_Front” Port	500mA
		USB2 Internal “USB2_Front” Port	500mA
12	2A	USB2 Internal “USB3” Port 10	500mA
		USB2 Internal “USB3” Port 11	500mA
13	2A	USB2 Internal “USB4” Port 12	500mA
		USB2 Internal “USB4” Port 13	500mA

SMBus address table

This table describes the used part of the possible SMBus address map.

SMBus Address		Function	Description
88h	0001 001xb	Intel Skylake PCH	SMBus Slave Address
A0h	1010 000xb	EEPROM of the DIMM 1, channel A	Module 1
A4h	1010 010xb	EEPROM of the DIMM 1, channel B	Module 2
C8h	1100 100xb	Management Engine (iAMT)	

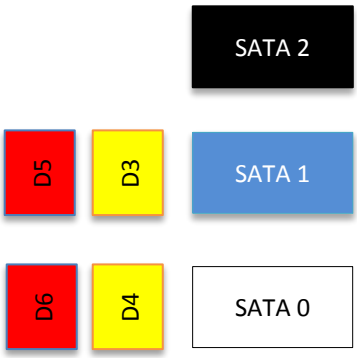
Frequency and bandwidth overview

Source	Frequency /MHz	Bandwidth
Skylake CPU		
Memory DDR4	2133/2400	Up to 34,1 GB/s per chan-
PCIe 2.0 x16	2500	8 GByte/s
PCIe 3.0 x16	4000	16 GByte/s
Skylake PCH		
DMI Gen 3	4000	8.0 Gb/s per Lane
PCIe	1250	2.5 Gb/s per Lane
PCIe 2.0	2500	5 Gb/s per Lane
PCIe 3.0	4000	8,0 Gb/s per Lane
SATA	750	150 MB/s
SATA 2	1500	300 MB/s
SATA 3	3000	600 MB/s
HD-Audio	24	
LPC-Bus	24	
USB (low-, full-, high speed, SuperSpeed)	2500	1,5Mb/s \ 12Mb/s \ 480Mb/s \ 5Gbit/s
Real time clock	32,768 kHz	
SMBus	100 kHz	

RAID (M1 Motherboard)

The M1 motherboard provides RAID functionality for the SATA interface. Raid level 0 (striping), 1 (mirroring) and 5 (striping with distributed parity) are supported. For RAID 5 three HDD/SSD devices are needed.
To enable the RAID functionality please see the corresponding chapter in the BIOS setup description.

For SATA ports 0 and 1 there are onboard LEDs indicating the status of the attached HDD/SSD within the RAID Array. The functionality of the SATA LEDs depends on host software (Intel SATA/RAID driver ("Rapid Storage Technology" – driver at the time of writing)). The host software needs to be installed and running for LED indication to work.



LED	Color	Function
D3	Yellow	Read/Write activity indication for SATA 1 port
D4	Yellow	Read/Write activity indication for SATA 0 port
D5	Red	Failure indication for SATA1 port
D6	Red	Failure indication for SATA0 port

Technical Data

Topic	Remarks
Form Factor	µATX 226x210mm
Processor	6th/ 7th Generation Intel® Core™ Processors
Chipset	Intel Series 100 (**M1**: Q170; M**2**: H110)
CPU Socket	LGA1151
Graphics	Celeron / Pentium: Intel HD 510 Core i3/i5 Skylake: Intel HD 530 Core i3/i5 Kaby Lake: Intel HD 630
Main Memory	Dual channel memory architecture 2 sockets supporting unbuffered non-ECC DDR4 memory modules supporting up to 32GB system memory SODIMM. 2133/2400 MHz
Storage	3x SATA III RAID support (M1 only)
LAN	onboard Gigabit LAN, status LED activity and link
Audio	Realtek HD audio Codec ALC 671
PS/2	Mouse and keyboard (PS/2) connector in I/O shield
USB	2x USB 3.0 9x USB 2.0 (M1) 5x USB 2.0 (M2)
Expansion Slots	2x PCIe x1 Gen3 1x PCIe x16 Gen3 1x MiniPCIe (on M**1** only)+mSATA, additional LPC signals 1x M.2 M key (PCIe x4/SATA) 1x TPM pin header
Motherboard External I/O Connectors (at I/O Shield)	2x Plink2.0 / DVI-D 1x LAN (RJ45) + 2x USB3.0 1x PS/2 + 2x USB2.0 1x VGA 1x COM **Audio**: Line in (blue) Line out (green) Microphone in (pink)

Internal I/O Connectors	4x USB 2.0 headers supporting 7 total USB (M1) 2x USB 2.0 headers supporting 3 total USB (M2) 1x PCIe x16 2x PCIe x1 1x MiniPCIe 1x M.2 2x DDR4 SODIMM 3x SATA 1x CPU fan 4pin 1x PSU fan 3pin 5x COM header 1x LPT header 1x Chassis intrusion 1x 24pin ATX 1x 4pin ATX 1x TPM header 1x Front panel header
Other Special Features	1x CMOS clear jumper 1x PW clear jumper 1x BIOS recovery jumper
Product Lifecycle	5 years without changing OS software driver critical components e.g. audio codec, LAN, Super-I/O, Chipset
AMT	Version 11.6 at M1 board only

Hardware Monitor

The requirements for the hardware monitoring are described in the BIOS chapter Hardware Monitor.

Changing the Battery

The systems are equipped with a lithium battery on the motherboard to ensure data retention, the time and the setup parameters. The battery should be changed approximately every five years.

When inserting the new battery, make sure the polarity is correct. This is marked in the socket. Incorrect replacement of the battery may lead to the danger of explosion.

The battery is located in a socket on the Motherboard.
To gain access to the battery, proceed as described in the according chapters of your **BEETLE User Manual.**

The lithium battery must be replaced only by identical batteries or types recommended by Diebold Nixdorf International.

You can return the used batteries to your Diebold Nixdorf International sales outlet. Batteries containing harmful substances are marked accordingly.
The chemical denotations are as follows: **CD** = Cadmium; **Pb** = Lead, **Li** = Lithium.

This symbol on a battery tells you that batteries containing harmful substances must not be disposed of as household waste. Follow the country specific laws and regulations. Within the European Union you are legally bound to return these batteries to the service organization where you purchased the new battery.

The setup parameters must be reset each time the battery has been changed.

UEFI BIOS Setup

UEFI / BIOS General Information

The classic BIOS was replaced by the "Unified Extensible Firmware Interface (UEFI)". The term "BIOS" is still strongly anchored in the PC and will continue to be used as "UEFI BIOS" in this document.

Some setup settings are displayed differently for the motherboards M1 or M2. This depends on the chipset used on the motherboard, as well as on the use of different processors. In this manual these chipset and processor options are provided with the following hints:

For the dependency to the chipset M1--> Q170 or M2--> H110
For the dependency to the processor --> CPU

There is also an operating mode that can be switched between "Legacy" and "UEFI". In the "Legacy" mode a Compatibility System Module (CSM) is active that still supports older operating systems. For this purpose, options are switched on or off in the setup.

For the dependency to Legacy mode --> Legacy
For the dependency to UEFI mode --> UEFI

Information

The mainboard M1.x-Q170-uATX and M2.x-H110-uATX comes with an AMI UEFI BIOS chip that contains the ROM Setup information of your system. This chip serves as an interface between the processor and the rest of the mainboard's components. This section explains the information contained in the Setup program and tells you how to modify the settings according to your system configuration.

Even if you are not prompted to use the Setup program, you might want to change the configuration of your system in the future. For example, you may want to enable the Security Password Feature or make changes to the power management settings. It will then be necessary to reconfigure your system using the BIOS Setup program so that the system can recognize these changes and record them in the NVRAM. All setup data is stored

in a non-volatile memory (NVRAM). When you remove the battery, all settings, except the BIOS password, are set to default.

Standard UEFI BIOS Version

The UEFI BIOS ROM of the system holds the Setup utility. When you turn on the system, it will provide you with the opportunity to run this program. This appears during the Power-On Self-Test (POST). Press <F2> or click setup in the upper right corner to call the Setup utility. If you missed the opportunity to pressing the mentioned key, POST will continue with its test routines, thus preventing you from calling Setup. If you still need to call Setup, reset the system by pressing <Ctrl> + <Alt> + <Del>. You can also re-start by turning the system off and then on again. But do so only if the first method fails.

If you like to change the boot order only once, you can press the <F10> key or click on BBS in the upper right corner during the POST is running. At the end you will see a Pop-Up window with all the devices the system has found. With the keys <UP> and <DOWN> you select the boot device.

The Setup program has been designed to make it as easy as possible. It is a menu-driven program, which means you can scroll through the various sub-menus and make your selections among the predetermined choices. You can also use the mouse or the touch screen to navigate through the menus.
When you invoke Setup, the main program screen will appear. Read more about the Setup entries on the following pages.

Because the UEFI BIOS software is constantly being updated, the following UEFI BIOS screens and descriptions are for reference purposes only and may not reflect your UEFI BIOS screens exactly.

UEFI BIOS Menu Bar

Press the ON/OFF button until a beep is emitted. Press then the F2 button to start the BIOS menu. The top of the screen has a menu bar with the following sections:

Info	Use this menu for information only
Main	Use this menu to make changes to the basic system configuration.
Advanced	Use this menu to enable and make changes to the advanced features.
Security	Use this menu to enable a supervisor or user password and Intrusion Detection.
Power	Use this menu to configure the chipset specific options
Event Logs	Use this menu to change the Smbios Log configuration.
Boot	Use this menu to configure the default system device used to locate and load the Operating System.
Save & Exit	Use this menu to exit the current menu or specify how to exit the Setup program.

To access the menu bar items, press the right or left arrow key on the keyboard until the desired item is highlighted.

Legend Screen

The right frame displays the key legend. The keys in the legend frame allow you to navigate through the various setup menus. The following table lists the keys found in the legend with their corresponding alternates and functions.

Navigation Key(s)	Description of Functions
← or → (keypad arrows)	Select the menu item to the left or right.
↑ or ↓ (keypad arrows)	Moves the highlight up or down between fields.
Enter	Move into sub menu or change selected menu items
+ (plus key) - (minus key)	Change field contents.
<Tab>	Jumps from one field to the next.
<F1>	Opens a general Help Screen with extended information.
<F2>	Load previous values (Load last saved values)
<F3>	Load optimized values (Factory reset)
<F4>	Saves changes and exits Setup.
<Esc>	Opens a windows to select between exit and return to setup

General Help

In addition to the Item Specific Help window, the UEFI BIOS setup program also provides a General Help screen. This screen can be called from any menu by simply pressing <F1>. The General Help screen lists the legend keys with their corresponding alternates and functions.

Scroll Bar

When a scroll bar appears to the right of a help window, it indicates that there is more information to be displayed that will not fit in the window. Use <PgUp> and <PgDn> or the up and down keys to scroll through the entire help document.

Press <Home> to display the first page, press <End> to reach the last page. To exit the help window, press the <Enter> or <Esc> key.

Sub-Menu

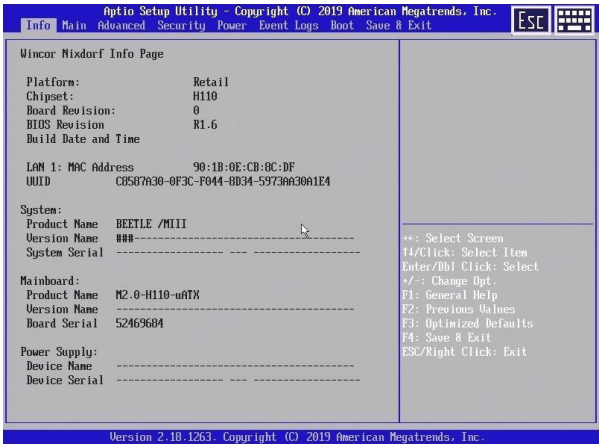
Note that a right pointer symbol "➢" appears left of certain fields. This pointer indicates that a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter.

To call a sub-menu, simply move the highlight to the field and press <Enter>. The sub-menu then will appear immediately. Use the legend keys to enter values and move from field to field within a sub-menu just as you would do within a menu. Use the <Esc> key to return to the main menu.

Take some time to familiarize yourself with each of the legend keys and their corresponding functions. Practice navigating through the various menus and sub-menus. If you accidentally make unwanted changes to any of the fields, use the set default hot key <F3>. While moving around through the Setup program, note that explanations appear in the Item Specific Help window located to the right side of each menu. This window displays the help text for the currently highlighted field.

Info Screen

When the Setup program is accessed, the following info screen appears:



This screen is for information only. There is nothing that could be changed within Setup. All information is intended to facilitate the support of your system.

BIOS Revision:

The UEFI BIOS version is displayed in the format Rxx.yy.zz

xx	Core Version, never changes
yy	Release Version, changes with every update
zz	Internal Release, for tests only

The UEFI BIOS Date is displayed the date of release in international format: MM/DD/YYYY

LAN1 MAC Address:

The Ethernet MAC-Address of the on board LAN Controller is displayed at this line if this device is enabled.

UUID Info:

A UUID is an identifier standard used in software construction, standardized by the Open Software Foundation. The intent of UUIDs is to enable distributed systems to uniquely identify information without significant central coordination.

Product Name:

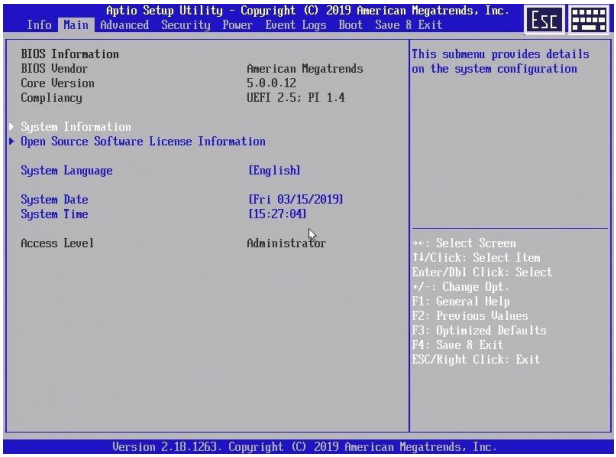
This text is fixed for your mainboard with standard UEFI BIOS. This board is called “M1.x-Q170-uATX” or “M2.x- H110-uATX”

System, Mainboard, Power Supply:

The default placeholders may be replaced by specific data from factory, describing configuration, serial number etc. for each device.

Main Menu

The Main Menu is entered, to determine the basic system configuration and to provide an overview. Some of the parameters are only available under certain conditions.



System Information

The System Information submenu gives you an overview of the system configuration. This includes information about the CPU, memory and LAN configuration.

Open source software license information

This submenu provides the licence information for the open source software that is used in this system board.

System Language

Specifies the language used in the BIOS Setup.

System date

Set the date.
Use Tab to switch between date elements.
Default ranges:
Year: 2005-2099
Days: dependent on month

System time

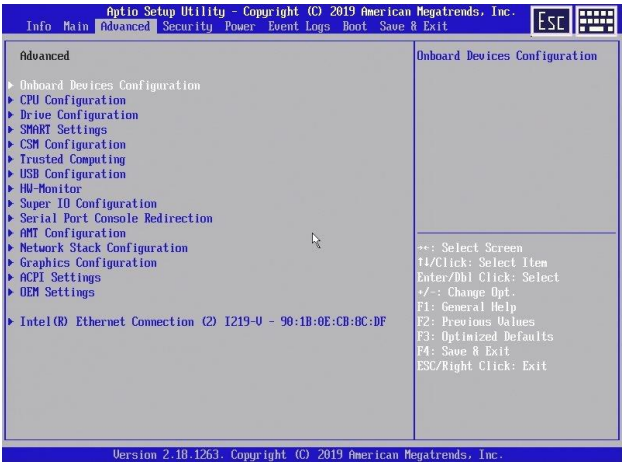
Set the time.
Use Tab to switch between time elements.

Advanced Menu

The advanced functions which are available to the system are configured in this menu for the advanced system configuration.

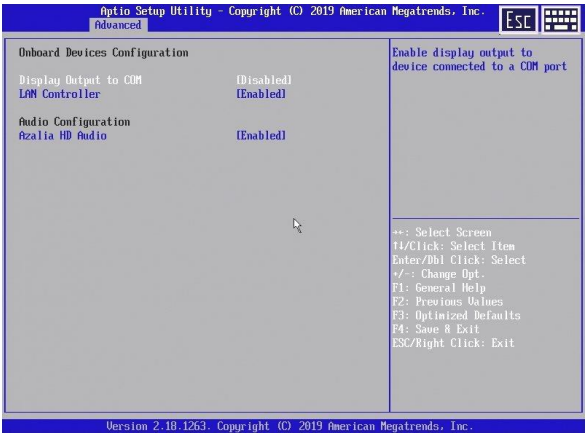
Only change the default settings if required for a special purpose.

Incorrect settings can cause malfunctions.



Onboard Devices Configuration

Opens the submenu to configure devices on the system board. Some of them are only available under certain conditions.



Display Output to COM [Disabled]

Enable display output to device connected to a COM port.

LAN Controller [Enabled]

Specifies whether the LAN controller on the system board is available.

Enabled	The LAN controller on the system board is available.
Disabled	The LAN Controller on the system board is not available.

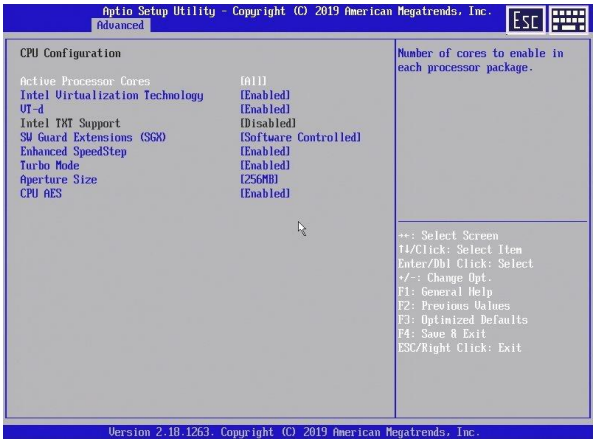
Azalia HD Audio [Enabled]

Allows the onboard Azalia HD (High Definition) audio controller to be enabled.

Enabled	The onboard audio controller is enabled.
Disabled	The onboard audio controller is disabled.

CPU Configuration

Opens the CPU Configuration submenu. Some of the parameters are only available under certain conditions.



CPU Active Processor Cores [All]

On processors which contain multiple processor cores, the number of active processor cores can be limited. Inactive processor cores will not be used and are hidden from the operating system.
All available processor cores are active and can be used.
1..n Only the selected number of processor cores is active. The other processor cores are disabled.
The choice made here allows possible problems with certain software packages or system licences to be solved.

Intel Virtualization Technology [Enabled]

Used to support the visualisation of platform hardware and multiple software environments. Based on Virtual Machine Extensions (VMX), to support the application of multiple software environments under the use of virtual computers.

The virtualisation technology enhances the processor support for virtualisation purposes on the over 16 bit and 32 bit protected modes and on the Intel® Extended Memory 64 Technology (EM64T) mode.

In active mode, a Virtual Machine Monitor (VMM) can use the additional performance features of the Vanderpool Technology Hardware.

Disabled A Virtual Machine Monitor (VMM) cannot use the additional performance features of the hardware.

Enabled A VMM can use the additional performance features of the hardware.

VT-d [Enabled]

Enable/Disable Intel Virtualisation Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.

SW Guard Extensions (SGX) [Software Controlled]

Enable/Disable Software Guard Extensions (SGX).

Enhanced SpeedStep [Enabled]

When enabled, OS sets CPU frequency according load. When disabled, CPU frequency is set at max non-turbo.

CPU Turbo Mode [Enabled]

Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceed CPU defined limits.

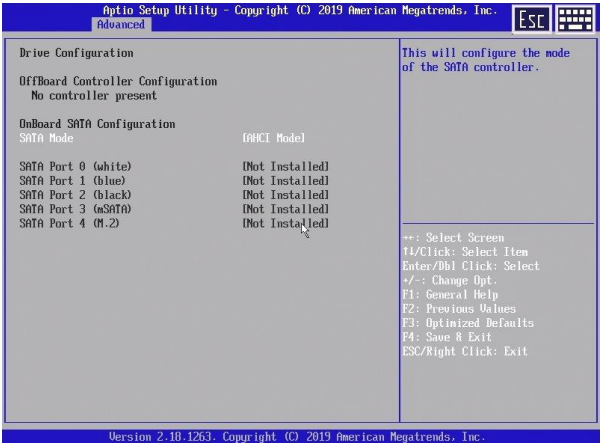
Aperture Size [256 MB]

Select the Aparture Size Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.

CPU AES [Enabled]

Enable/Disable AES (Advanced Encryption Standard).

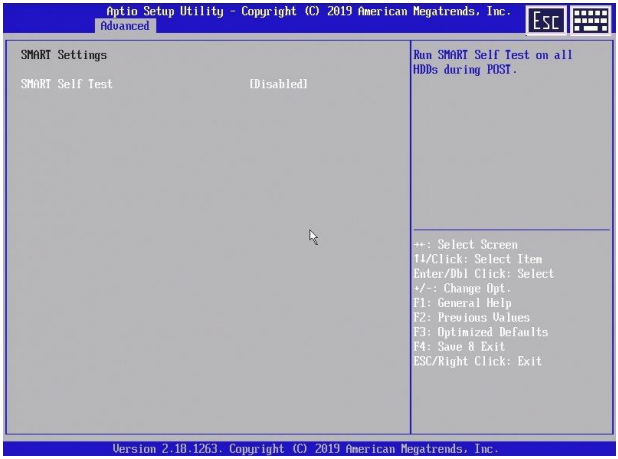
Drive Configuration



Q170 SATA Mode [AHCI Mode]

This will configure the mode of the SATA controllers. Possible options are AHCI or RAID mode.
This option is not available for chipset H110.

SMART Settings



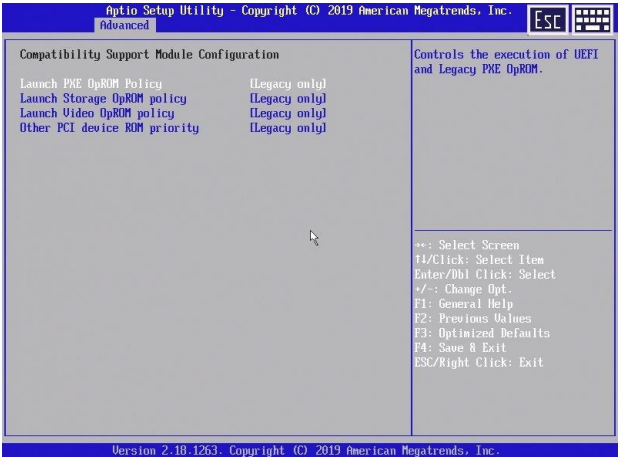
Smart Self Test [Disabled]

Run SMART Self Test on all HDDs during POST.

CSM Configuration

Opens the submenu for configuring the Compatibility Support Module (CSM).

This submenu is only available if Secure Boot Control is disabled under Setup –> Security –> Secure Boot Configuration.



Launch PXE OpROM Policy [Legacy only]

Controls the execution of UEFI and Legacy PXE OpROM.

Launch Storage OpROM Policy [Legacy only]

Controls the execution of UEFI and Legacy Storage OpROM.

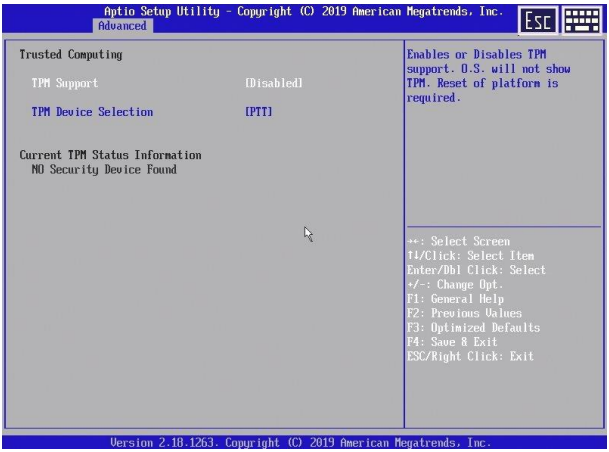
Launch Storage OpROM Policy [Legacy only]

Controls the execution of UEFI and Legacy Video OpROM.

Other PCI device ROM priority [Legacy only]

For PCI devices other than Network, Mass storage or Video defines which OpROM to launch.

Trusted Computing



TPM Support [Disabled]

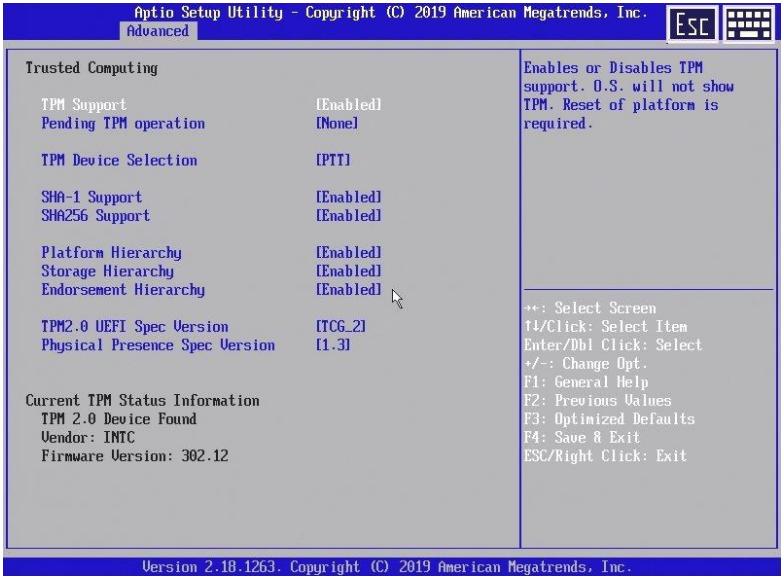
Enables or disables TPM support. O.S. will not show TPM. Reset of platform is required.

TPM Device Selection [PTT]

Selects TPM device: PTT or dTPM.

PTT	Enables PTT in SkuMgr
dTPM 1.2	Disables PTT in SkuMgr Warning! PTT/dTPM will be disabled and all data saved on it will be lost.

TPM enabled and device PTT



SHA-1 Support [Enabled]

Enable or disable SHA-1 PCR Bank.

SHA256 Support [Enabled]

Enable or disable SHA256 PCR Bank.

Platform Hierachy [Enabled]

Enable or disable the TPM ownership hierarchy for platform protection.

Storage Hierachy [Enabled]

Enable or disable the TPM ownership hierarchy for general cryptographic usage.

Endorsement Hierachy [Enabled]

Enable or disable the TPM ownership hierarchy for privacy control.

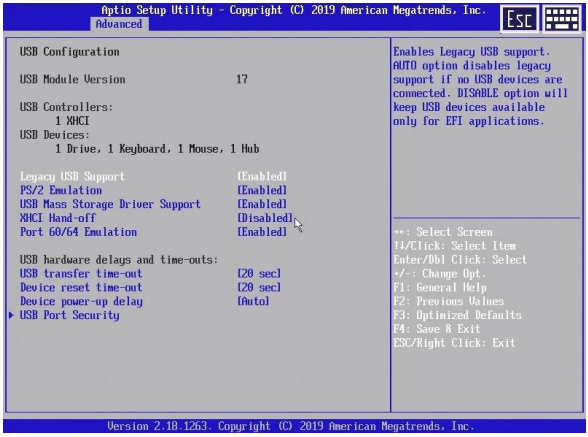
TPM 2.0 UEFI Spec Version [TCG_2]

Select the TCG2 specification version support.
TCG_1_2: Compatible mode for Windows 8 or 10
TCG_2 : Compatible mode for Windows 10 or later

Physical Presence Spec Version [1.3]

Support the operating system with PPI specification version 1.2 or 1.3.
Please note that some HCK tests might not support PPI version 1.3

USB Configuration



USB Devices

Shows the number of available USB devices, USB keyboards, USB mice and USB hubs.

Legacy USB Support [Enabled]

Specifies whether legacy USB support is available. This function should always be enabled or set to Auto so that the operating system can be booted from a USB device if required.

Disabled	Legacy USB support is not available. A USB keyboard or USB mouse can only be used if this is supported by the operating system. Booting the operating system from a USB device is not possible.
Enabled	Legacy USB support is available. A USB keyboard or USB mouse can also be used if the operating system does not support USB. Booting the operating system from a USB device is possible.
Auto	Legacy USB support will be disabled if no USB devices are connected.

PS/2 Emulation [Enabled]

Emulates PS/2 Keyboard and Mouse. This allows USB Keyboard and Mouse to be used in OS like Windows 7 that do not support XHCI natively.

USB Mass Storage Driver Support [Enabled]

Enable/Disable USB Mass Storage Driver Support.

XHCI Hand-off [Disabled]

This is a workaround for OSes without XHCI hand-off support.
The XHCI ownership change should be claimed by XHCI driver.

Port 60/64 Emulation [Enabled]

Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.

USB transfer time-out [20 sec]

The time-out value for Control, Bulk and Interrupt transfers.

Device reset time-out [20 sec]

USB mass storage device Start Unit command time-out.

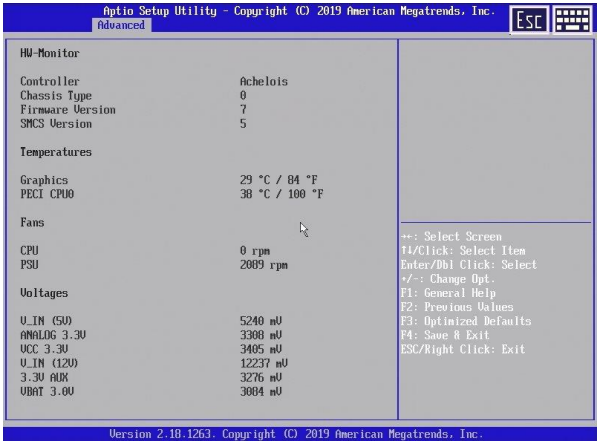
Device power-up delay [Auto]

Maximum time the device will take before it properly reports itself to the Host Controller. AUTO uses default value time: for a Root port it is 100 ms, for a Hub port, the delay is taken from Hub descriptor.

USB Port Security

Configures USB ports according to device classes. Any disabled USB ports are also not available under the operating system.

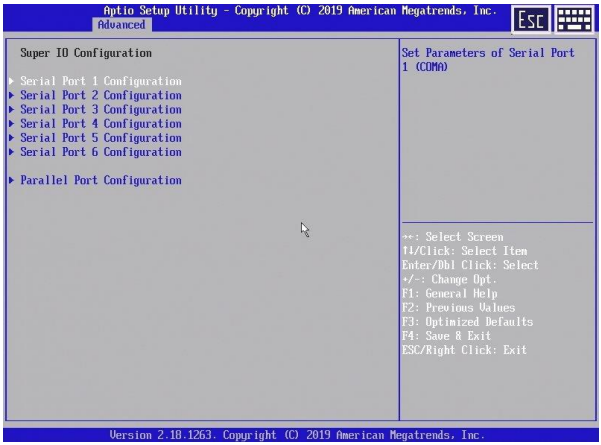
Hardware Monitor



Get here information about the system health status.

Super IO Configuration

See the configuration settings for serial and choose the configuration of parallel ports.



Serial Port Configuration

Serial ports 2-6 can be disabled.

Parallel Port

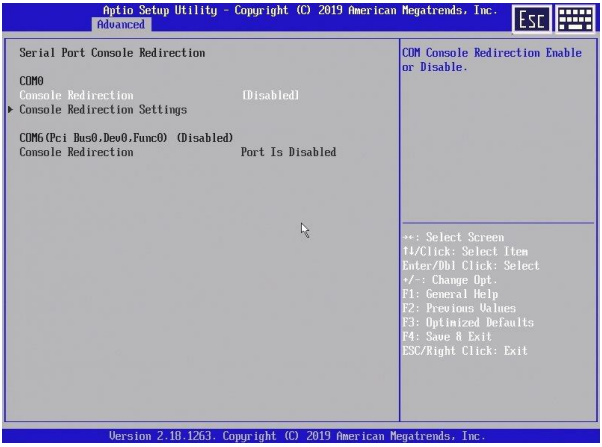
Disabled	The parallel port is not available.
Enabled	The parallel port is available.

Device Mode

Change here the printer port mode:

STP Printer Mode
SPP Mode
EPP 1.9 and SPP Mode
EPP 1.7 and SPP Mode

Serial Port Console Redirection

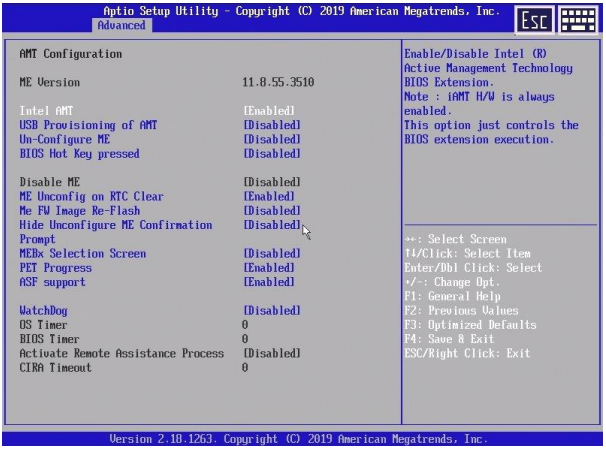


Console Redirection [Disabled]

Enable or disable the COM Console Redirection.

AMT Configuration

Opens the submenu to configure Intel® Active Management Technology.



ME Version

Shows the current AMT/ME version.

Intel AMT [Enabled]

Enables/Disables Intel (R) Active Management Technology BIOS Extension.

iAMT H/W is always enabled. This option simply controls the execution of the BIOS Extension.

USB Provisioning of AMT [Disabled]

Enables/disables AMT-USB provisioning.

Unconfigure ME [Disabled]

If this option is enabled, an MBEx (Management Engine BIOS eXtension) query occurs at the next reboot to establish whether the AMT/ME configuration should be reset to the default values.

Disabled Do not change the AMT/ME configuration.
Enabled Start the reset of the AMT/ME configuration. The option is then automatically reset to Disabled.

BIOS Hot Key pressed [Disabled]

Select Enabled to automatically enter MEBX Setup once during next POST.

ME Unconfigure on RTC Confirmation [Enabled]

When disabled ME will not be unconfigured on RTC Clear.

ME FW Image Re-Flash [Disabled]

Enable/Disable ME FW Image Re-Flash function.

Hide Unconfigure ME Confirmation Prompt [Disabled]

OEMFlag Bit 6:
Hide Unconfigure ME configuration prompt when attempting ME unconfiguration.

MEBx Selection Screen [Disabled]

OEMFlag Bit 2:
Enable MEBx selection screen with 2 options:
Press 1 to initiate a remote connection
Note:
Network Access must be activated from MEBx Setup for this screen to be displayed.

PET Progress [Enabled]

Enable/Disable PET events progress to receive PET events.

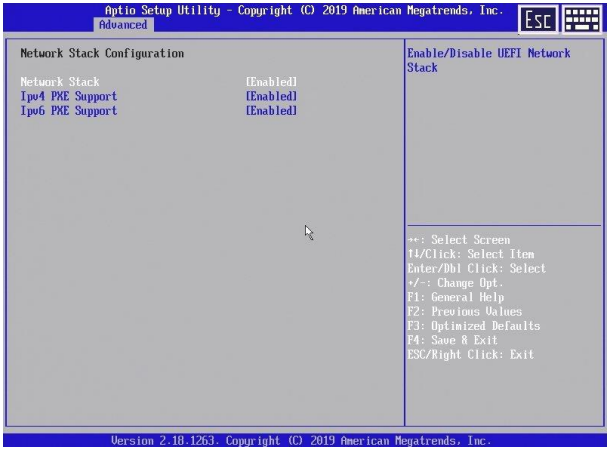
ASF support [Enabled]

Enable/Disable Alert Standard Format support.

WatchDog [Disabled]

Enable/Disable WatchDog timer.

Network Stack Configuration



Network Stack [Enabled]

Enable/Disable UEFI Network Stack.

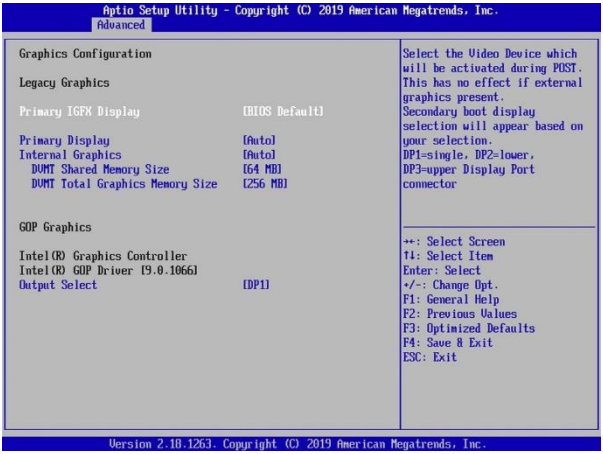
Ipv4 PXE Support [Enabled]

Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created.

Ipv6 PXE Support [Enabled]

Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created.

Graphics Configuration



Primary IGFX Display

Select the Video Output Device which will be activated during POST. This has no effect if an external graphics card is present.

BIOS Default	POST on all screens
Display 1	POST on display 1 only
Display 2	POST on display 2 only
VGA	POST on VGA display only; possibility to mount a secondary display

If other than BIOS default is selected, you can specify an additional secondary sceen.

Primary Display

Selects which graphics controller has connected the primary display.

Internal Graphics

The BIOS detects automatically if the internal graphics controller can be disabled, but it can manually be forced to enabled or disabled.

DVMT Shared Memory Size

Select DVMT 5.0 pre-allocated (fixed) memory size used by the internal graphics controller.

DVMT Total Graphics Memory Size

Select DVMT 5.0 total memory size used by the internal graphics controller.

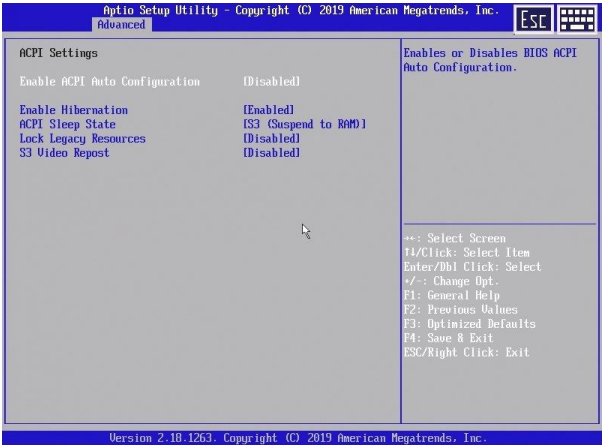
UEFI The following option is only available if the option *Launch Video OpROM Policy* is set to [UEFI only]

GOP Graphics

Output Select [DP1]

This option enables the chosen display. Only connected displays are available

ACPI Settings



Enable ACPI Auto Configuration [Disabled]

Being an ACPI BIOS system, the operating system is allowed to control the Power Management features of the computer and the setting for Advanced Power Management (APM) BIOS mode are ignored.
Not all operating systems support ACPI BIOS mode.

Enable Hibernation [Enabled]

Enables or Disables System ability to Hibernate (OS/S4 Sleep State).
This option may not be effective with some operating systems.

ACPI Sleep Sate [S3 (Suspend to RAM)]

Select the highest ACPI sleep state the system will enter when SUSPEND button is pressed.

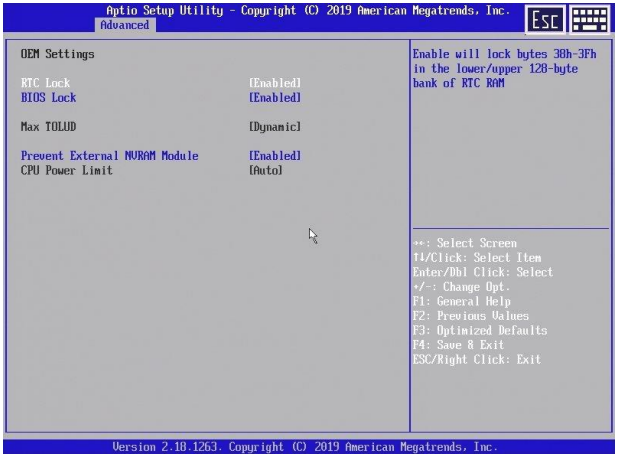
Lock Legacy Resources [Disabled]

Enables or Disables Lock Legacy Resources.

S3 Video Repost [Disabled]

Enable or Disable S3 Video Repost.

OEM Settings



RTC Lock [Enabled]

Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.

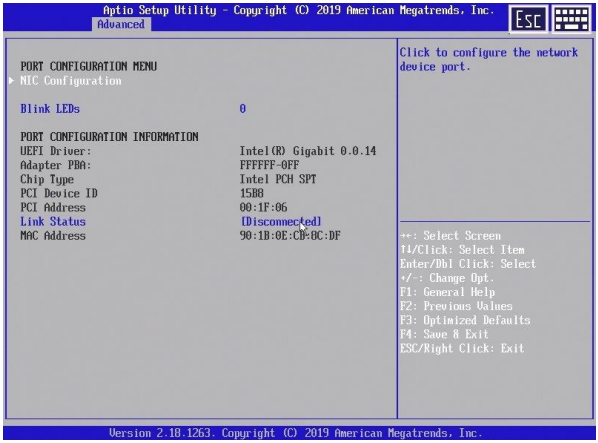
BIOS Lock [Enabled]

Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash

Prevent External NVRAM Module [Enabled]

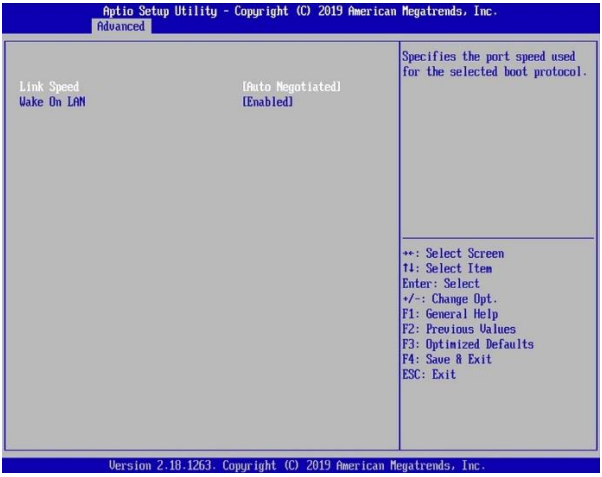
For using NVRAM set to Disabled.

Intel Ethernet Connection



NIC Configuration

Click to configure the network device port.



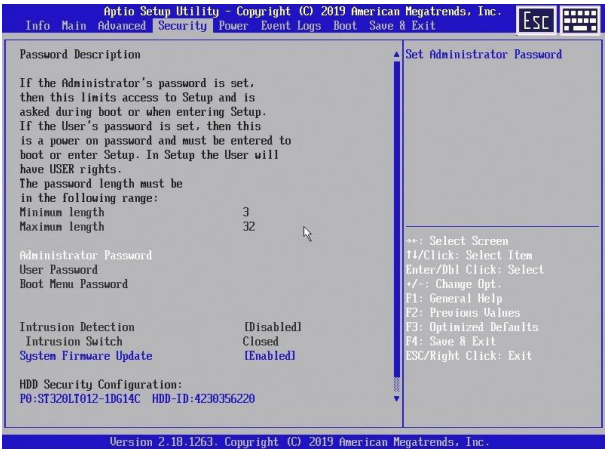
Link Speed [Auto negotiated]

Specifies the port speed for the selected boot protocol.Options: 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 10 Mbps Full

Wake on LAN [Enabled]

Enables power on of the system via LAN.
Note that configuring Wake on LAN in the operating system does not change the value of this settings but does override the behaviour of Wake on LAN in OS controlled power states.

Security



Administrator Password

This field allows you to set the password. Highlight the field and press <Enter>. Type a password and press <Enter>, you can type **3 to 20** alphanumeric characters. Symbols and other characters are ignored. To confirm the password, type the password again and press <Enter>. This password allows full access to the UEFI BIOS Setup menu. To clear the password, highlight this field and press <Enter>. Enter your current password. Then you will be asked to enter the new password. Press <Enter> and the password will be deleted.

Intrusion Detection [Disabled]

Intrusion is just possible when admin password is set, if the system cover is removed and the Intrusion Detection is [Enabled].

The system stops during the next reboot or power up process and display a warning message. After this warning the boot process stops and the user has to power off and on the system and then enter the UEFI BIOS setup which resets the open case detection automatically. Additionally is a viewing point of the case open switch below the enable/disable entry point placed. This message will signalize the actual case open status directly. Configuration Options: [Disabled] [Enabled]

Administrator Password

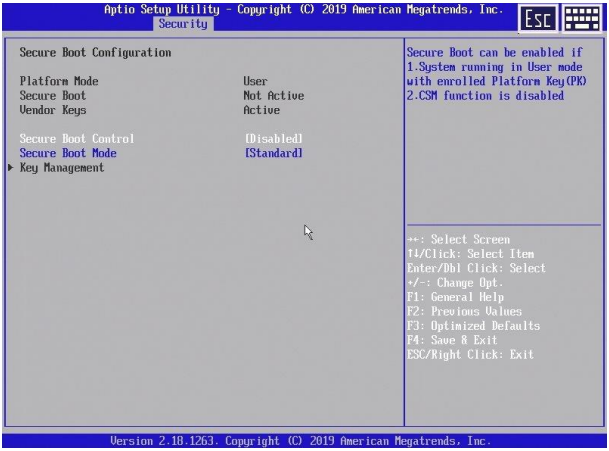
Set here the administrator password.

System Firmware Update [Enabled]

Changing the system firmware version is possible only if Enabled or Restricted.

Enabled	Windows Update (WU) and BIOS update tools can change/update the system firmware version.
Restricted	Only BIOS update tools can change/update the system firmware version. Windows Update (WU) is blocked.

Secure Boot configuration



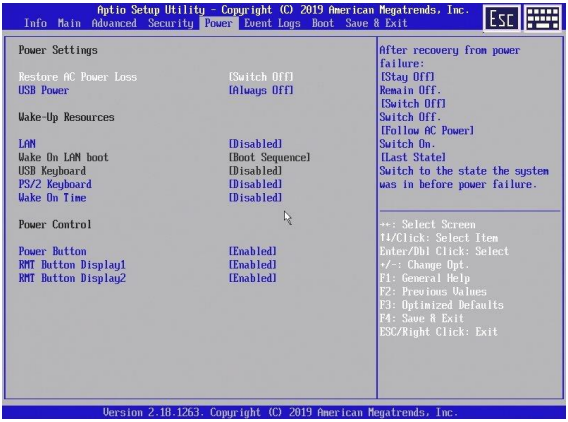
Secure Boot Control [Disabled]

This option can be enabled if:
1. System running in User mode with enrolled Platform Key
2. CSM function is disabled
Configuration options: [Disabled] [Enabled]

Secure Boot Mode [Standard]

This is the secure mode selector. The ‘Custom’ mode enables user to change the Image Execution policy and mange Secure Boot Keys
Configuration options: [Standard] [Custom]

Power



Restore AC Power Loss [Switch off]

After recovery from power failure:

Disabled	Remain off
Switch Off	Switch off after a short POST
Switch On	Switch on
Last State	Switch to the state the system was in before power failure.

USB Power[Always off]

When the system is switched off (S4/S5 the USB-Ports):

[Always Off]	Remain powered off
[Always ON]	Remain powered on

Wake-Up Resources

LAN [Disabled]

Enabled	The system can be switched on via a LAN controller.
Disabled	The system cannot be switched on via a LAN controller.

Wake on LAN Boot

LAN must be enabled to enable Wake On LAN Boot.

[Boot Sequence]
Use Boot Sequence order after Wake On LAN

[Force LAN Boot]
Force LAN Boot after Wake On LAN (Option “Launch PXE OpROM” must be enabled to actually force a network boot).

USB keyboard [Disabled]

If enabled, any USB keyboard button press will power on the system
USB power option must be enabled to support USB power on.

PS/2 Keyboard [Disabled]

If enabled, any PS/2 keyboard button press will power on the system
USB power option must be enabled to support PS/2 power on.

Wake On Time [Disabled]

Allows the system to be switched on via an internal timer.

Power Control

Power Button [Enabled]

If disabled, power button will not work in S0. You cannot shut down the system from OS, but you can enable system from S5

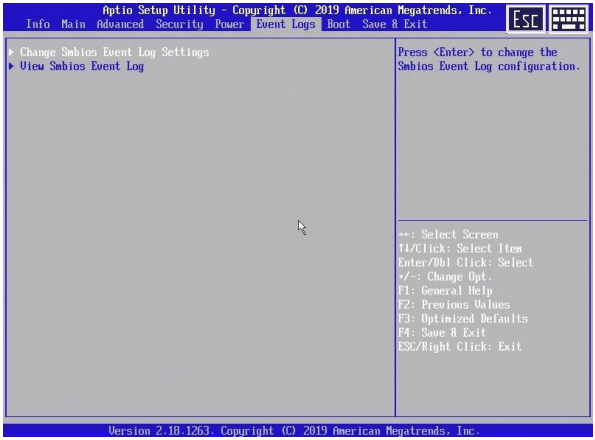
RMT Button Display1 [Enabled]

Enable or disable the remote button of display1.

RMT Button Display2 [Enabled]

Enable or disable the remote button of display2.

Event Logs



Change SMBIOS event log settings

SMBIOS Event Log [Enabled]

Specifies whether the SMBIOS event log is enabled.

Enabled	The SMBIOS event log is disabled.
Disabled	The SMBIOS event log is enabled.

Erase Event Log [No]

Specifies whether the SMBIOS event log should be deleted.

No	The SMBIOS event log will not be deleted.
Yes, next reset	The SMBIOS event Log is deleted once during the next system boot up. Afterwards, this option is automatically reset to No.
Yes, every reset	The SMBIOS event log is deleted every time the system is booted.

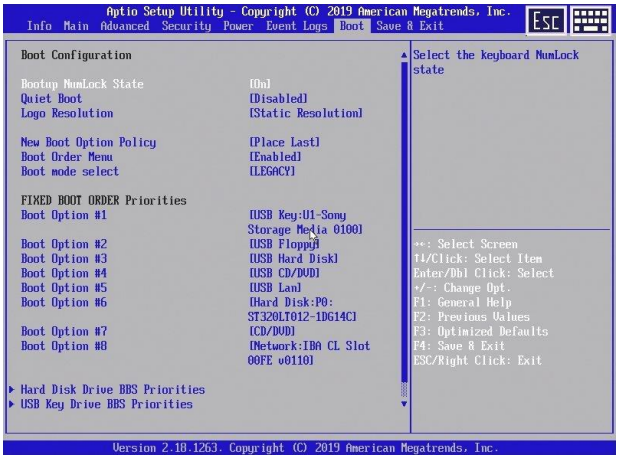
When Log is full [Do Nothing]

Specifies the course of action to be taken when the SMBIOS event log is full.

Do Nothing	When the SMBIOS event log is full, no further entries are added. The SMBIOS event log must first be deleted before new entries can be added.
Erase Immediately	When the SMBIOS event log is full, it will be erased immediately. All existing entries will be deleted!

Boot

The Boot Menu enables you to set the order of bootable devices to a regular base. Pressing the function key <F10> while POST is running will change the boot order only once. You will see a Pop-Up window listing all devices the system is able to boot from. Select the boot device with keys <Up> and <Down>. Press <Enter> key to start the selected device booting.



Bootup NumLock State [On]

The setting of the NumLock function after a system boot is provided here. Controls the functionality of the numeric keypad.

On	NumLock is enabled, the numeric keypad can be used.
Off	NumLock is disabled, the numeric keypad keys can be used to control the cursor.

The Num indicator light on your keyboard shows the current boot up NumLock state. The Num key on the keyboard can be used to toggle between ON and OFF.

Quiet Boot [Disabled]

The boot logo is shown on the screen instead of the POST boot up information.

Enabled	The boot logo is displayed.
Disabled	The POST boot up information is shown on the screen.

Configures the screen resolution [Static Resolution]

Default Resolution	Default screen resolution is used.
Native Resolution	Native display resolution is used.
Static Resolution	Limit screen resolution to 800x600

Boot Order Menu [Enabled]

Specifies whether the boot order menu can be invoked during the POST process by pressing the F10 key.

Enabled	The boot order menu can be invoked
Disabled	The boot order menu cannot be invoked

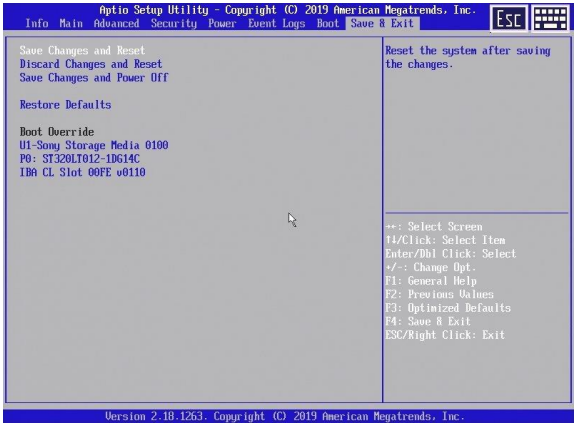
Boot mode select [LEGACY]

This option selects the boot mode.
Configuration options: [LEGACY] [UEFI]

Fixed Boot Order Priorities '#n' Boot Device

These menu entries are used to specify the boot sequence from the available devices. Every entry (from #1 till #7) specifies a boot group. Each boot device found while POST is running will be sorted in one of a BBS group. Enter a BBS group to swap the boot order of the BBS device.

Save & Exit



Save Changes and Reset

Once finished changing setup values, this option from the Exit menu ensure that values are saved to the NVRAM. The NVRAM is sustained by an onboard backup battery and stays on even when the BEETLE is turned off. Once this option is selected, a confirmation is asked. Select [Ok] to save changes and reset the system.

Discard Changes and Reset

This option should only be used if the changes made in Setup should not save. If made some changes to fields other than system date, system time, and password, the system will ask for confirmation before exiting and reset the system.

Save Changes and Power off

Powers off the system after saving changes. Changed Power Settings become effective after next Power On.

Restore Defaults

This option loads the default values for each of the values on the Setup menu. When this option is selected or if <F3> is pressed, a confirmation is requested. Select [Ok] to load default values. Now select Exit Saving to save the default values or make other changes before saving the values to the non-volatile RAM.

Boot Override

With this option choose a boot device that is listed below this menu entry. Every entry specifies a boot device that enumerate during POST.

Status And Error Codes

At the beginning of each POST routine, the UEFI BIOS outputs status and error codes to I/O port address 80h. Use this code during trouble shooting to establish where the system failed and what routine has been performed.

Checkpoint Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

Standard Checkpoints

Phase SEC

Status Code	Description
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization

0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C	PEI phase BMC self-test failure

0x5C-0x5F	Reserved for future AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is stared (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AMI progress codes
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AMI error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

PEI Beep Codes

# of Beeps	Description
1	Memory not installed
2	Recovery started
3	Typically for development use. The beep code is generated when DXEIPL PPI or DXE Core is not found.
4	Recovery failed
4	S3 Resume failed
7	Typically for development use. The beep code is generated when platform cannot be reset because reset PPI is not available.

DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started

0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect

0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure

DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Typically for development use. The beep code is generated when some of the-Architectural Protocols are not available.
5	No Console Input or Output Devices are found **1,2**
6	Flash update is failed
7	Typically for development use. The beep code is generated when platform cannot be reset because reset protocol is not available.
8	Platform PCI resource requirements cannot be met

1 Note serial console redirection is considered a console out device if enabled

2 Note serial console redirection is considered a console in device if enabled. Also, depending on configuration PS/2 driver may always report a console in device even if one is not connected.

ACPI/ASL Checkpoints

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

OEM-Reserved Checkpoint Ranges

Status Code	Description
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes

Abbreviations

ADM	AMI Display Manager
ACPI	Advanced Configuration and Power Interface
AGTL+	Assisted Gunning Transceiver Logic
APC	Advanced Power Control
APIC	Advanced Peripheral Interrupt Controller
APM	Advanced Power Management
AT	Advanced Technology
ATA	AT Attachment
BAT	Basic Access Test
BBS	BIOS Boot Specification
BDA	BIOS Data Area
BGA	Ball Grid Array
BIOS	Basic Input and Output System
CMOS	Complementary Metal Oxide Semiconductor
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CRT	Cathode-ray Tube
DIM	Device Initialization Manager
DIMM	Dual Inline Memory Module
DMA	Direct Memory Access
DMI	Desktop Management Interface
DVMT	Dynamic Video Memory Technology
DVI	Digital Video Interface
EBDA	Extended BIOS Data Area
ECP	Extended Capabilities Port
EEPROM	Electrical Erasable Read Only Memory
EFI	Extensible Firmware Interface
E-IDE	Enhanced Integrated Drive Electronics
EMS	Expanded Memory System
ESCD	Extended System Configuration Data
EPP	Enhanced Parallel Port
FSB	Front Side Bus

GPNV	General Purpose Non-Volatile (RAM)
GTL	Gunning Transceiver Logic
HW	Hardware
IDE	Integrated Drive Electronics
IGD	Internal Graphic Device
IPL	Initial Program Load (Device)
LAN	Local Area Network
LBA	Logical Block Addressing
LCD	Liquid Crystal Display
MAC	Media Access Control
MTRR	Memory Type Range Register
MP	Multiple Processors
NA	Power failure
NVRAM	Non-volatile Random Access Memory
P-ATA	Parallel AT Attachment (old version of hard disk interface)
POS	Point of Sales
PCI	Peripheral Component Interconnect
PnP	Plug and Play
POST	Power On Self Test
RAM	Random Accessible Memory
RI	Ring Indicator
ROM	Read Only Memory
RS	Retail Systems
SATA	Serial AT Attachment (new version of hard disk interface)
SLP	System Locked Pre-Installation
SMI	System Management Interrupt
SMM	System Management Mode
SMRAM	System Management RAM
SPGA	Staggered Pin Grid Array

TFT	Thin-film transistor
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UUID	Universal Unique Identifier
VGA	Video Graphics Array
WOL	Wake On LAN
WOM	Wake On Modem

Wincor Nixdorf International GmbH
D-33094 Paderborn

Order No.: ***01750297725A***