R1/R2 Motherboard (with UEFI BIOS)

User manual

01750340075A

Copyright

Contents

1 Symbols

DANGER

This warning note describes a hazard with a high degree of risk, which, if not avoided, will result in death or grave bodily injury.

WARNING

This warning note describes a hazard with a medium degree of risk, which, if not avoided, will result in death or grave bodily injury.

CAUTION

This warning note describes a hazard with a low degree of risk, which, if not avoided, will result in death or grave bodily injury.

NOTICE

This note provides application tips and information that help prevent errors and material damage.

2 Warranty

Generally Diebold Nixdorf guarantees a warranty engagement for 12 months beginning with the date of delivery. This warranty engagement covers all damages which occur despite a normal use of the product.

Damages because of

- improper or insufficient maintenance,
- improper use of the product or unauthorized modifications of the product,
- inadequate location or surroundings

will not be covered by the warranty.

For further information on the stipulation consult your contract.

All parts of the product which are subject to wear and tear are not included in the warranty engagement. For detailed warranty arrangements please consult your contract documents.

NOTICE

Please contact your local service provider for all questions concerning your service contract.

3 ESD (Electrostatic Sensitive Devices)

Electrostatic sensitive devices (ESD) may be marked with this sticker.

When you handle components fitted with ESDs, you must observe the following points under all circumstances:

- Make sure that the device is de-energized before connecting, removing or installing components with ESD.
- Always use the antistatic equipment.
- Unplug the power before inserting or removing components containing ESDs.
- While working with ESDs you must discharge yourself by using an ESD wrist strap or grounding cable to connect yourself at all times to the earth connector of power socket or a grounded object.
- Place all components containing ESDs on a static-safe base.
- The equipment and tools you use must be free of static charges.
- Always hold boards with ESDs by their edges. Do not touch the components.
- Never touch pins or conductors on boards fitted with ESDs.

4 Specifications R1-Motherboard

CPU	LGA1151 socket for 8th/9th Generation Intel® Core™ i5/ i3, Pentium®, and Celeron® processors Supports Intel® 14nm CPU * CPU only supports up to 65W.
Chipset	Intel® Q370 Chipset
Memory	2 x SO-DIMM, max.32GB, DDR4 2666*/2400/2133 MHz, non-ECC, unbuffered memory Dual-channel memory architecture * DDR4 2666MHz and higher memory modules will run at max. 2666MHz on Intel® 8th Gen. 6-core or higher processors.
Display	Integrated graphics processor - Intel® HD Graphics support Multi-VGA output support: 2x PanelLink 2.0 (DVI-D)/VGA ports Supports up to 3 displays simultaneously
Expansion Slots	1 x M.2 Socket 3 with M key, type 2260/2280 (SATA/PCIe mode) storage devices support 1 x PCIe x16 slot 2 x PCIe x1 slots 1 x slot for USB Type-C card
LAN	1 x Intel® I219LM PCIe Gigabit LAN
Audio	Realtek® ALC887-VD2 2-channel High Definition Audio CODEC
USB	2 x USB 3.1 Gen 2 connectors (@back I/O) 4 x USB 2.0 headers support additional 6 USB 2.0 connectors (@mid-board, 1 from USB1_hub, 2 from USB2_Front, 2 from USB3, 1 from USB4) 2 x USB 2.0 connectors (@back I/O)
Serial Port	1 x COM connector (RS232) @back I/O 5 x COM headers (RS232)* * The five on-board COM headers are powered by +12V/+5V.
SIO	NCT6116D
Rear Panel I/O Ports	1 x PS/2 keyboard/mouse combo port 1 x COM connector 1x LAN (RJ45) port 1 x VGA port 2x DVI-D/PanelLink 2 x USB 2.0 connectors 2 x USB 3.1 Gen 2 connectors 3 x Audio jacks

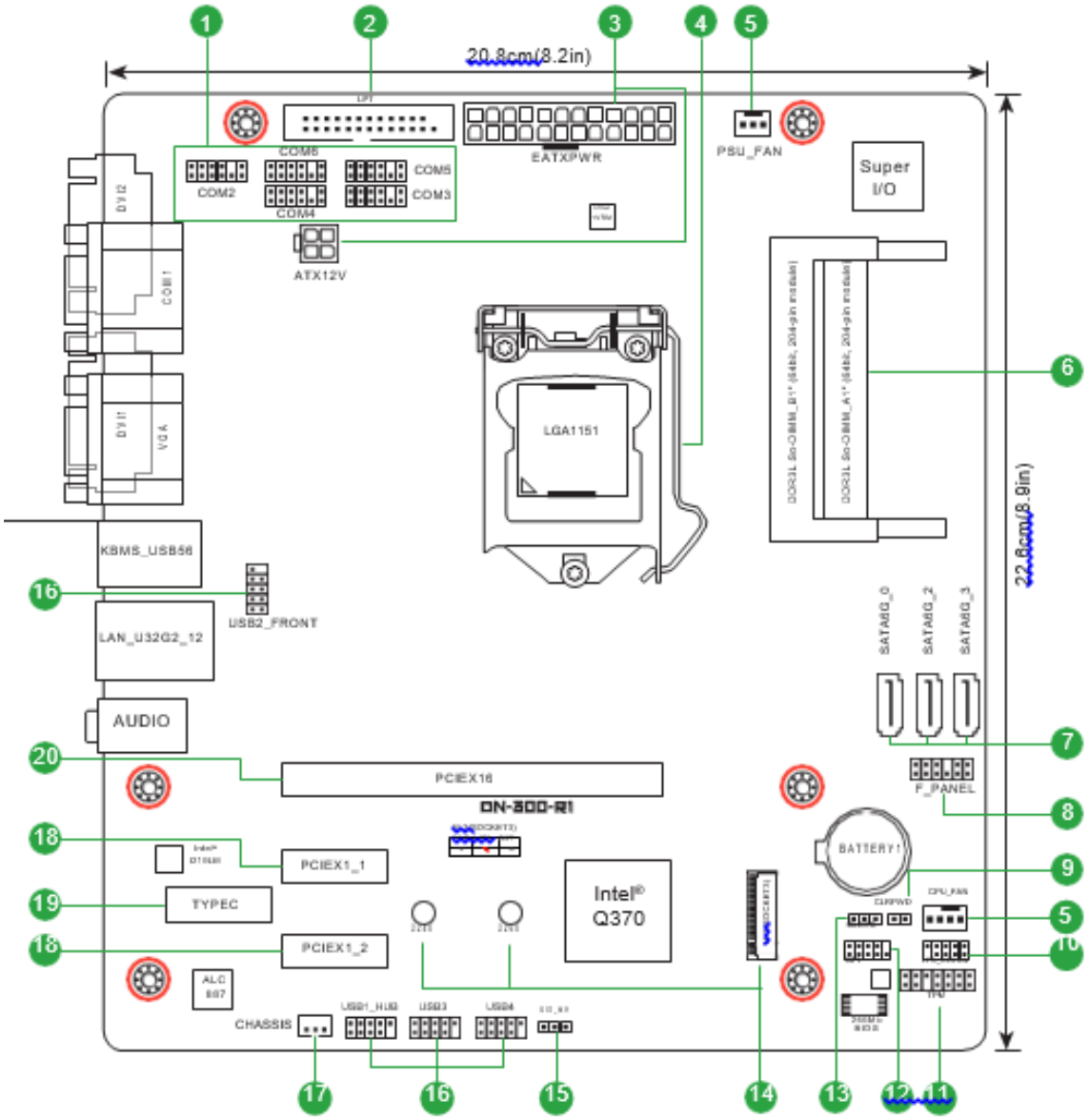
Front Panel I/O Ports	3 x SATA 6.0 Gb/s connectors 1 x CPU fan connector 1 x PSU fan connector 1 x Front panel header 1 x 3-pin Clear RTC jumper 1 x Clear Password jumper 1 x 24-pin EATX power connector 1 x 4-pin ATX power connector 1 x 3-pin Chassis Intrusion connector 4 x USB 2.0 headers 5 x COM connectors 1 x TPM 14-1 pin header 1 x LPT header 1 x SPI header 1 x LPC debug header 1 x Disable ME jumper
BIOS	256 Mb Flash ROM, UEFI AMI BIOS
Watch dog timer	Yes
Possible wake-up sources	Wake on Time Wake on LAN Wake on USB Wake on PS/2 Wake on PCIe Wake on Ring Wake on PLink1 Wake on PLink2
Operation Temperature	0~60°C
Non-operation Temperature	-40~85°C
Relative Humidity	0%~85%
Certification	CE, FCC, CB
OS Support	Windows® 10 (64-bit), Linux 64-bit (WNLPOS, CentOS 7 based)
Form Factor	Micro-ATX form factor, 8.9” x 8.2” (22.6cm x 20.8cm)

5 Specifications R2-Motherboard

CPU	LGA1151 socket for 8th/9th Generation Intel® Core™ i5/ i3, Pentium®, and Celeron® processors Supports Intel® 14nm CPU * CPU only supports up to 65W.
Chipset	Intel® H310 Chipset
Memory	2 x SO-DIMM, max.32GB, DDR4 2666*/2400/2133 MHz, non-ECC, unbuffered memory Dual-channel memory architecture * DDR4 2666MHz and higher memory modules will run at max. 2666MHz on Intel® 8th Gen. 6-core or higher processors. ** Refer to www.asus.com for the latest Memory QVL (Qualified Vendors List).
Display	Integrated graphics processor - Intel® HD Graphics support Multi-VGA output support: 2x PanelLink 2.0 (DVI-D)/VGA ports Supports up to 2 displays simultaneously
Expansion Slots	1 x M.2 Socket 3 with M key, type 2260/2280 (SATA mode) storage devices support 1 x PCIe x16 slot 2 x PCIe x1 slots 1 x slot for USB Type-C card
LAN	1 x Intel® I219V PCIe Gigabit LAN
Audio	Realtek® ALC887-VD2 2-channel High Definition Audio CODEC
USB	2 x USB 3.1 Gen 1 connectors (@back I/O) 4 x USB 2.0 headers support additional 5 USB 2.0 connectors (@midboard, 1 from USB1_hub, 2 from USB2_Front, 1 from USB3, 1 from USB4) 2 x USB 2.0 connectors (@back I/O)
Serial Port	1 x COM connector (RS232) @back I/O 5 x COM headers (RS232)* * The five on-board COM headers are powered by +12V/+5V.
SIO	NCT6116D
Rear Panel I/O Ports	1 x PS/2 keyboard/mouse combo port 1 x COM connector 2 x LAN (RJ45) port 1 x VGA port 2 x DVI-D/PanelLink 2 x USB 2.0 connectors 2 x USB 3.1 Gen 1 connectors 3 x Audio jacks

Front Panel I/O Ports	3 x SATA 6.0 Gb/s connectors 1 x CPU fan connector 1 x PSU fan connector 1 x Front panel header 1 x 3-pin Clear RTC jumper 1 x Clear Password jumper 1 x 24-pin EATX power connector 1 x 4-pin ATX power connector 1 x 3-pin Chassis Intrusion connector 4 x USB 2.0 headers 5 x COM connectors 1 x TPM 14-1 pin header 1 x LPT header 1 x SPI header 1 x LPC debug header 1 x Disable ME jumper
BIOS	128 Mb Flash ROM, UEFI AMI BIOS
Watch dog timer	Yes
Possible wake-up sources	Wake on Time Wake on LAN Wake on USB Wake on PS/2 Wake on PCIe Wake on Ring Wake on PLink1 Wake on PLink2
Operation Temperature	0~60°C
Non-operation Tempera-ture	-40~85°C
Relative Humidity	0%~85%
Certification	CE, FCC, CB
OS Support	Windows® 10 (64-bit), Linux 64-bit (WNLPOS, CentOS 7 based)
Form Factor	Micro-ATX form factor, 8.9” x 8.2” (22.6cm x 20.8cm)

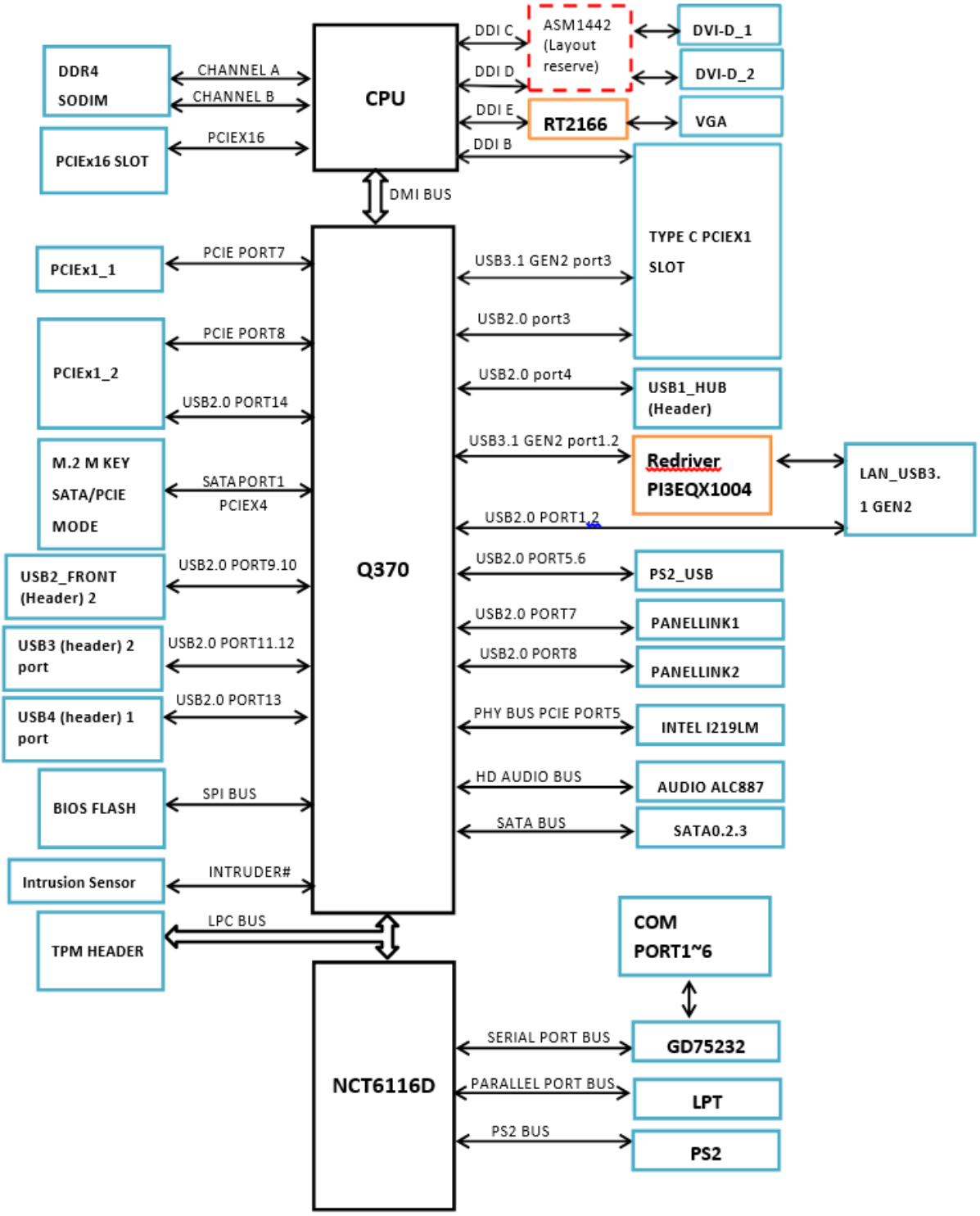
6 Motherboard Layout



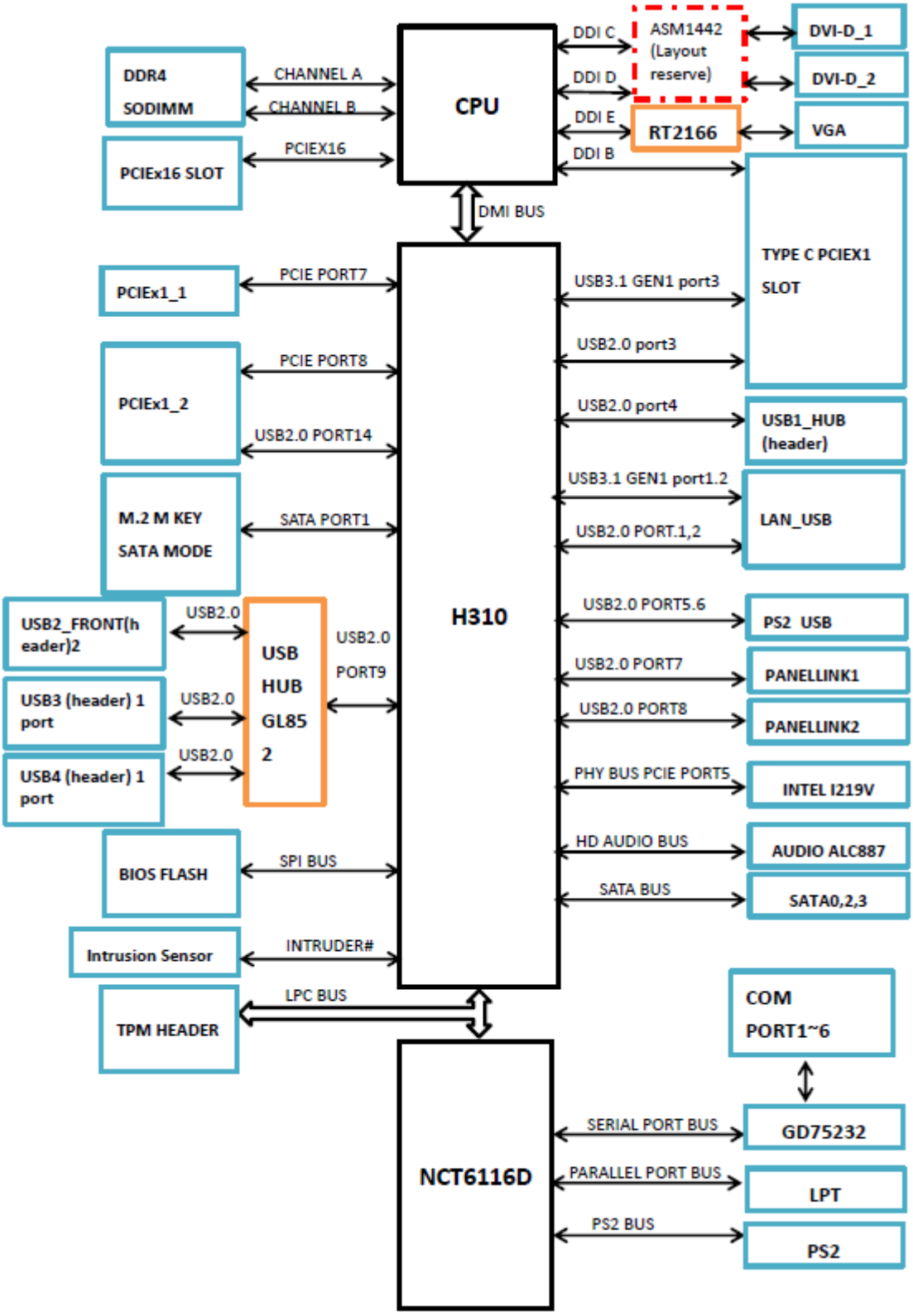
Connectors/Jumpers/Slots	
1.	Serial port connectors (12-1 pin COM2, COM3, COM4, COM5, COM6)
2.	LPT connector (26-1 pin LPT)
3.	ATX power connectors (24-pin EATXPWR, 4-pin ATX12V)
4.	Intel® LGA1151 CPU socket
5.	CPU and PSU fan connectors (3-pin PSU_FAN, 4-pin CPU_FAN)
6.	DDR4 SO-DIMM slots
7.	Serial ATA 6.0Gb/s connectors (7-pin SATA6G_0/2/3)
8.	System panel connector (12-1 pin F_PANEL)
9.	Clear password jumper (2-pin CLRPWD)
10.	LPC debug header (10-1 pin LPC_DEBUG)
11.	TPM connector (14-1 pin TPM)
12.	SPI header (10-1 pin SPI)
13.	Clear RTC RAM (3-pin CLRTC)
14.	M.2 socket 3
15.	Intel® ME Jumper (3-pin DIS_ME)
16.	USB 2.0 connectors (10-pin USB1_HUB, USB2_FRONT, USB3, USB4)
17.	Chassis intrusion jumper (3-pin CHASSIS)
18.	PCI Express x1 slots
19.	USB Type-C card slot
20.	PCI Express x16 slot

7 Block diagram

7.1 R1-Motherboard

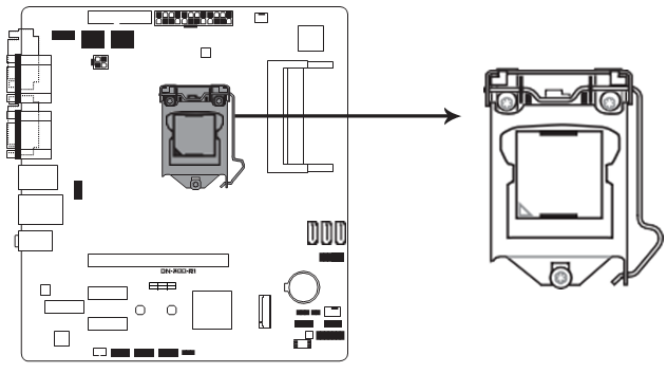


7.2 R2-Motherboard



8 Central Processing Unit

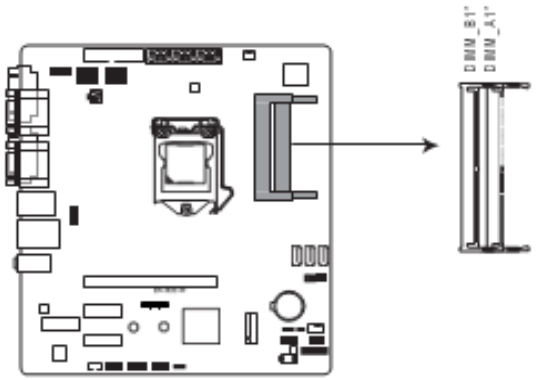
The motherboard comes with a surface mount LGA1151 socket designed for the 8th/9th Generation Intel® Core™ i5/ i3, Pentium®, and Celeron® processors.



DN-300-R1/R2 CPU socket LGA1151

8.1 System Memory

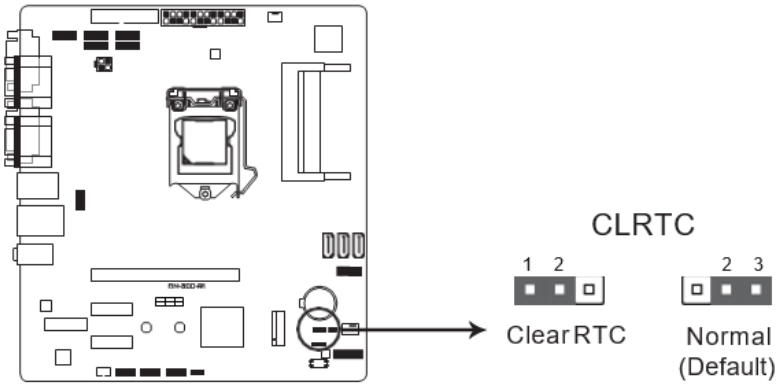
This motherboard comes with two Double Data Rate 4 (DDR4) Small Outline Dual Inline Memory Module (SO-DIMM) sockets. The figure below illustrates the location of the DDR4 SO-DIMM sockets:



Channel	Sockets
Channel A	SO-DIMM_A1*
Channel B	SO-DIMM_B1*

8.2 Jumpers

- Clear RTC RAM (3-pin CLRTC)
  This header allows you to clear the CMOS RTC RAM data.



To erase the RTC RAM:

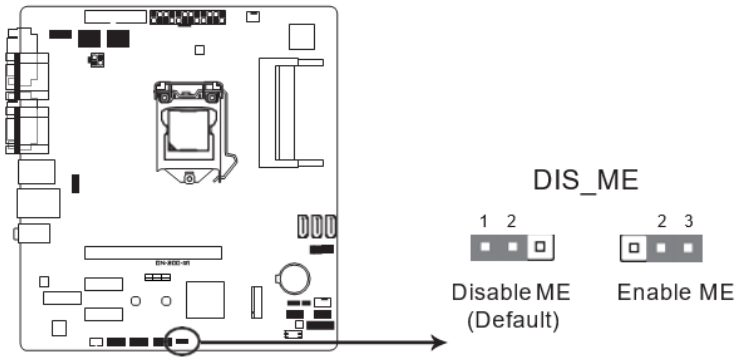
- Turn OFF the computer and unplug the power cord.
- Move the jumper cap from pins 2-3 (default) to pins 1-2. Keep the cap on pins 1-2 for about 5~10 seconds, then move the cap back to pins 2-3.
- Plug the power cord and turn ON the computer.
- Hold down the <F2> key during the boot process and enter BIOS setup to reenter data.

	NOTICE
	Except when clearing the RTC RAM, never remove the cap on CLRTC jumper default position. Removing the cap will cause system boot failure!

	NOTICE
	You do not need to clear the RTC when the system hangs due to over-clocking. For system failure due to overclocking, use the CPU Parameter Recall (C.P.R) feature. Shut down and reboot the system so the BIOS can automatically reset parameter settings to default values. This jumper will just load BIOS defaults, and will not clear BIOS password.

- Intel® ME Jumper (3-pin DIS_ME)

This jumper allows you to enable or disable the Intel® ME function. Set this jumper to pins 1-2 to enable (default) the Intel® ME function and to pins 2-3 to disable it.

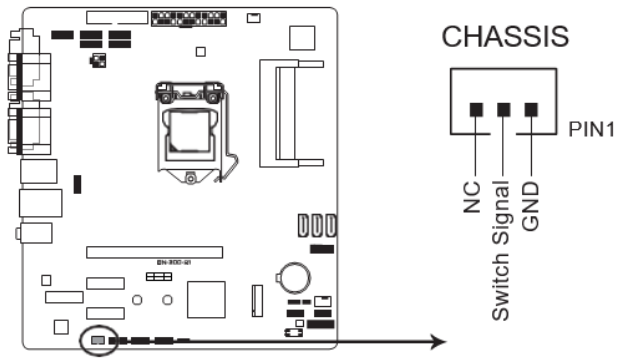


NOTICE

Disable the Intel® ME function before updating it.

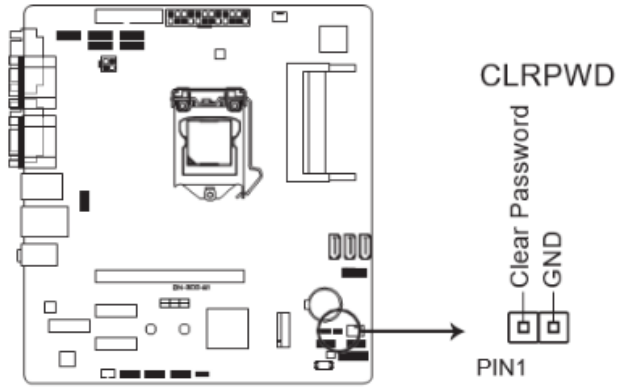
- Chassis intrusion connector (3-pin CHASSIS)

This connector is for a chassis-mounted intrusion detection sensor or switch. Connect one end of the chassis intrusion sensor or switch cable to this connector. The chassis intrusion sensor or switch sends a high-level signal to this connector when a chassis component is removed or replaced. The signal is then generated as a chassis intrusion event.



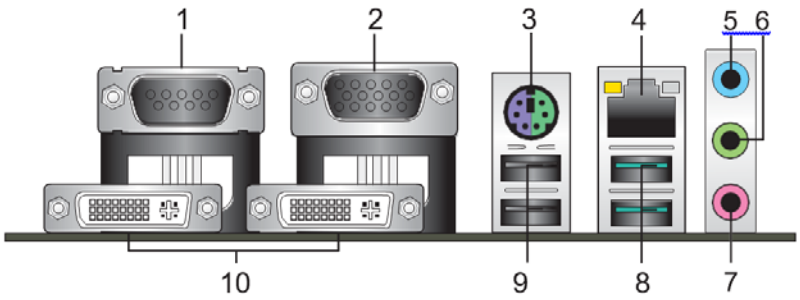
- Clear password jumper (2-pin CLRPWD)

Short the two pins, and press <F2> to enter BIOS at the next boot. The BIOS password will be removed.



8.3 Connectors

8.3.1 Rear Panel Connectors



1. Serial port connectors (COM).

These ports connect a modem, or other devices that conform with serial specification.

2. Video Graphics Adapter (VGA) port.

This 15-pin port is for a VGA monitor or other VGA-compatible devices.

3. PS/2 keyboard/mouse port.

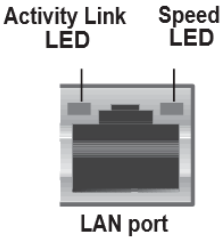
This port is for a PS/2 keyboard or mouse.

4. LAN (RJ-45) port.

This port allows Gigabit connection to a Local Area Network (LAN) through a network hub.

LAN Port LED Indications

Activity/Link LED		Speed LED	
Status	**Description**	**Status**	**Description**
Off	No link	OFF	10Mbps connection
Orange	Linked	ORANGE	100Mbps connection
Orange (Blinking)	Data activity	GREEN	1Gbps connection
Orange (Blinking then steady)	Ready to wake up from S5 mode		



5. Line In port (light blue).

This port connects to the tape, CD, DVD player, or other audio sources.

6. Line Out port (lime).

This port connects to a headphone or a speaker.

7. Microphone port (pink).

This port connects to a microphone.

8. USB 3.1 Gen 2 (up to 10Gbps) ports.

These 9-pin Universal Serial Bus (USB) ports are for USB 3.1 Gen 2 devices.

NOTICE

USB 3.1 Gen 2 devices can only be used for data storage.

We strongly recommend that you connect USB 3.1 Gen 2 devices to USB 3.1 Gen 2 ports for faster and better performance from your USB 3.1 Gen 2 devices.

Due to the design of the Intel® 300 series chipset, all USB devices connected to the USB 2.0 and USB 3.1 Gen 2 ports are controlled by the xHCI controller. Some legacy USB devices must update their firmware for better compatibility.

9. USB 2.0 ports.

These 4-pin Universal Serial Bus (USB) ports are for USB 2.0/1.1 devices.

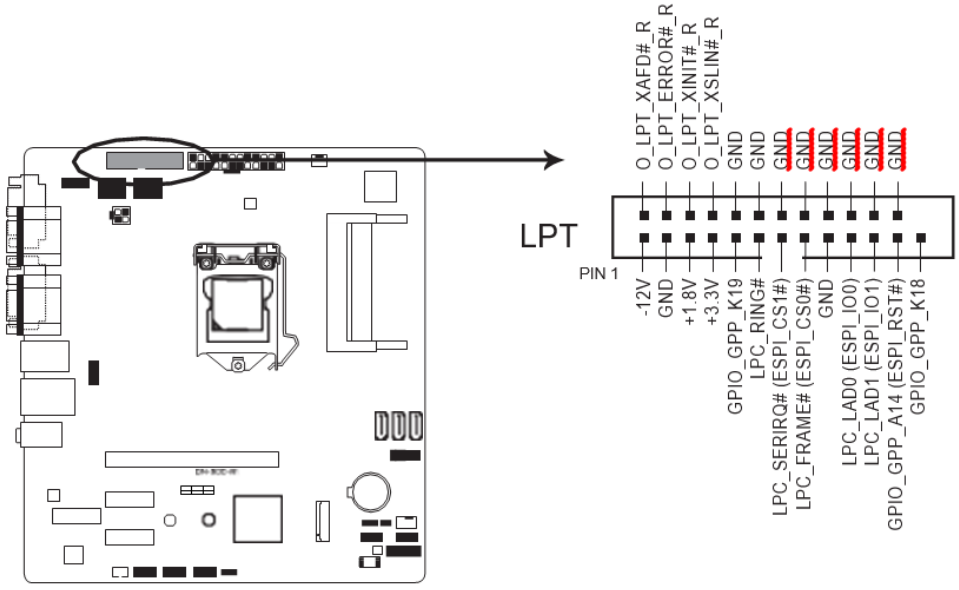
10. DVI-D and PLINK port.

This port is for DVI-D and PLINK display devices.

8.3.2 Internal Connectors

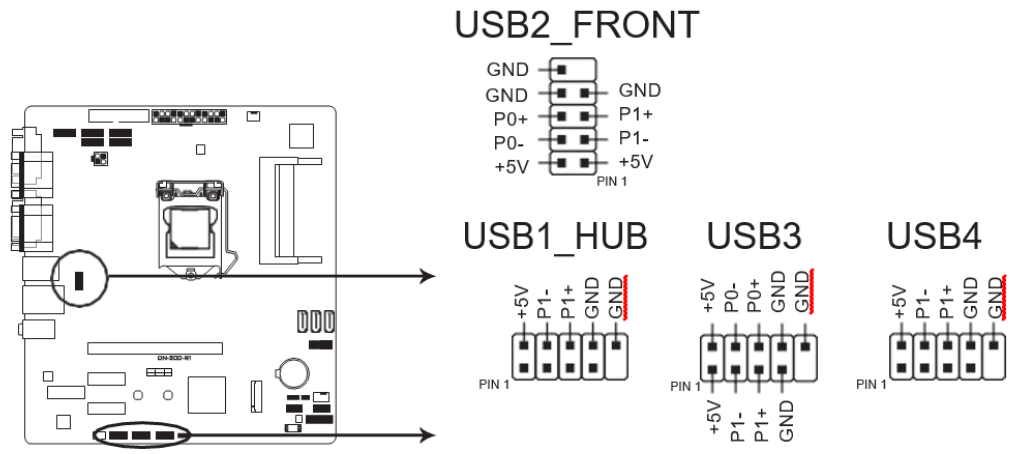
1. LPT connector (26-1 pin LPT)

The LPT (Line Printing Terminal) connector supports devices such as a printer. LPT is standardized as IEEE 1284, which is the parallel port interface on IBM PC-compatible computers.



2. USB 2.0 connectors (10-pin USB1_HUB, USB2_FRONT, USB3, USB4)

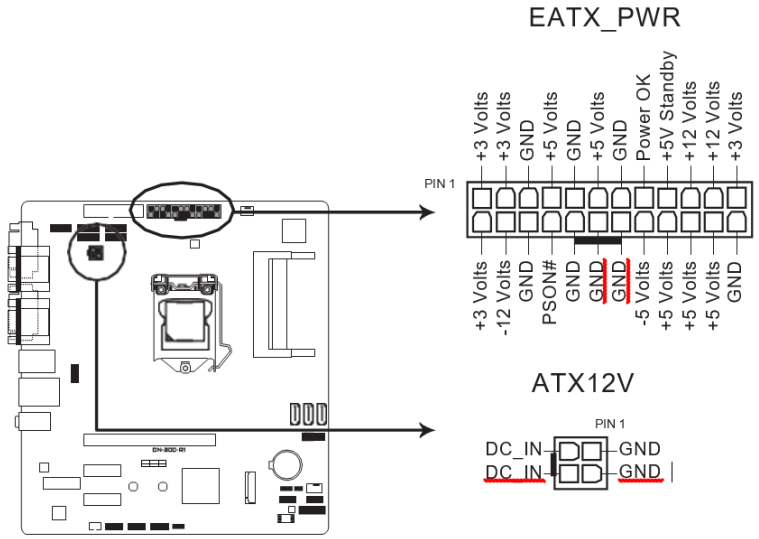
These connectors are for USB 2.0 ports. Connect the USB cable to these connectors. These USB connectors comply with USB 2.0 specification that supports up to 480 Mbps connection speed.



	NOTICE
	Never connect a 1394 cable to the USB connector. Doing so will damage the motherboard. The USB cable is purchased separately.

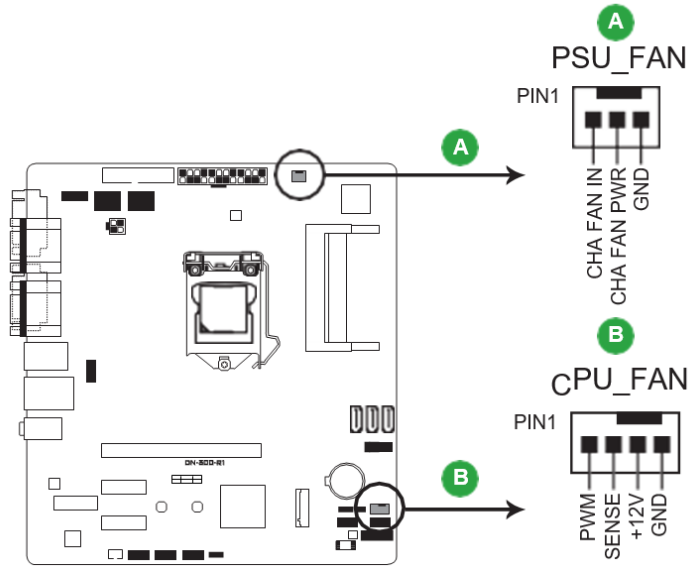
3. ATX power connectors (24-pin EATXPWR, 4-pin ATX12V)

Correctly orient the ATX power supply plugs into these connectors and push down firmly until the connectors completely fit.



4. CPU and PSU fan connectors (4-pin CPU_FAN, 3-pin PSU_FAN)

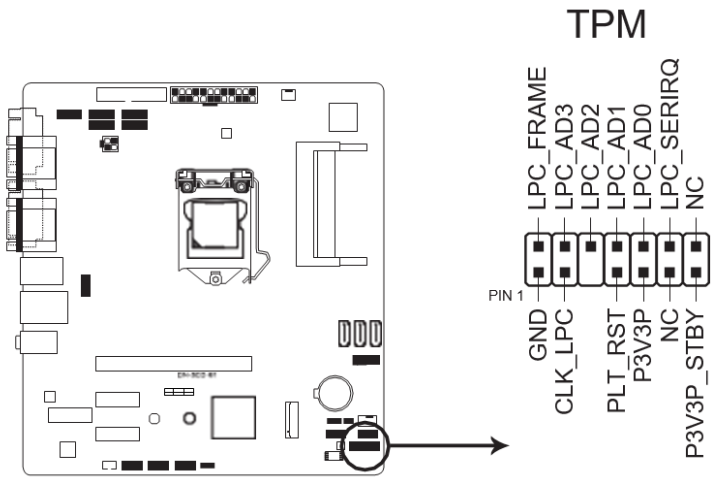
Connect the fan cables to the fan connectors on the motherboard, ensuring that the black wire of each cable matches the ground pin of the connector.



	NOTICE
	Do not forget to connect the fan cables to the fan connectors. Insufficient air flow inside the system may damage the motherboard components. These are not jumpers! Do not place jumper caps on the fan connectors!

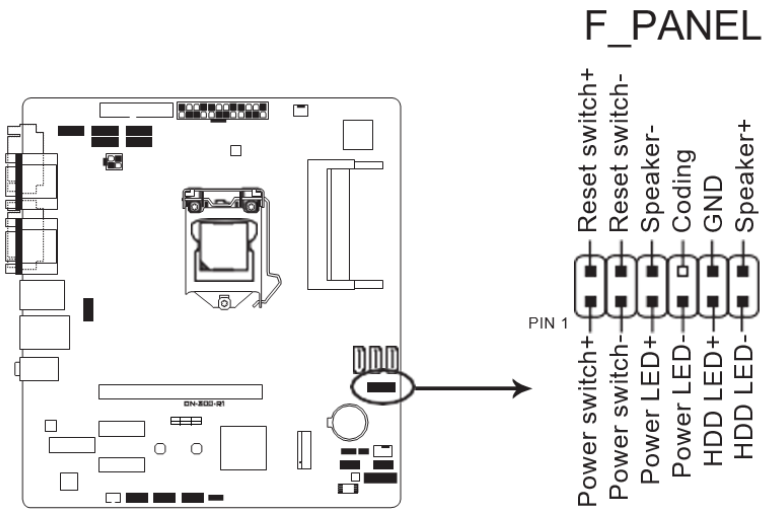
5. TPM connector (14-1 pin TPM)

This connector supports a Trusted Platform Module (TPM) system, which can securely store keys, digital certificates, passwords, and data. A TPM system also helps enhance network security, protects digital identities, and ensures platform integrity.



6. Front panel system panel connector (12-1 pin F_PANEL)

This connector supports several chassis-mounted functions.



- System power LED (2-pin Power LED)
  This 2-pin connector is for the system power LED. Connect the chassis power LED cable to this connector. The system power LED lights up when you turn on the system power, and blinks when the system is in sleep mode.

- Hard disk drive activity LED (2-pin HDD LED)
  This 2-pin connector is for the HDD Activity LED. Connect the HDD Activity LED cable to this connector. The IDE LED lights up or flashes when data is read from or written to the HDD.

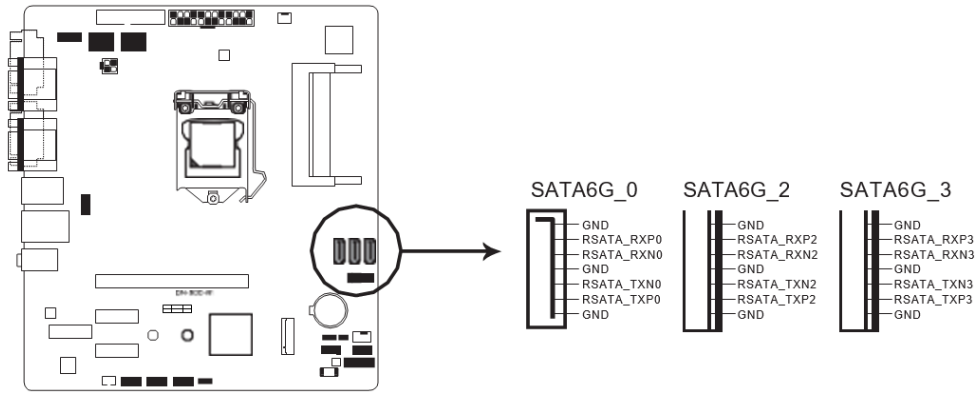
- System warning speaker (4-1 pin Speaker)
  This 4-pin connector is for the chassis-mounted system warning speaker.
  The speaker allows you to hear system beeps and warnings.

- ATX power button/soft-off button (2-pin Power switch)
  This 2-pin connector is for the system power button.

- Reset button (2-pin Reset)
  This 2-pin connector is for the chassis-mounted reset button for system reboot without turning off the system power.

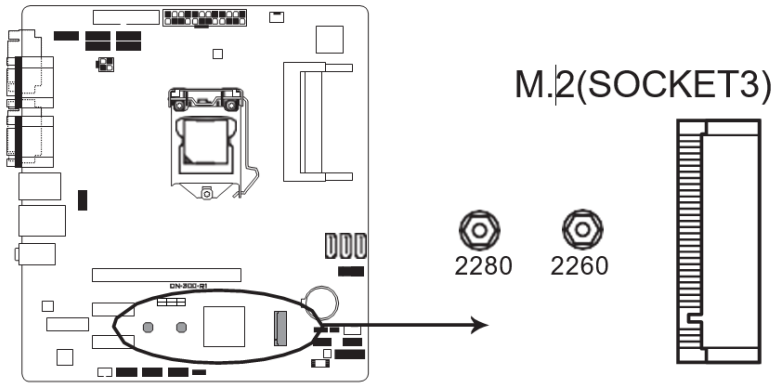
7. Serial ATA 6.0Gb/s connectors (7-pin SATA6G_0/2/3)

These connector connects to Serial ATA 6.0 Gb/s hard disk drives or an optical drive via Serial ATA 6.0 Gb/s signal cables.



8. M.2 socket 3

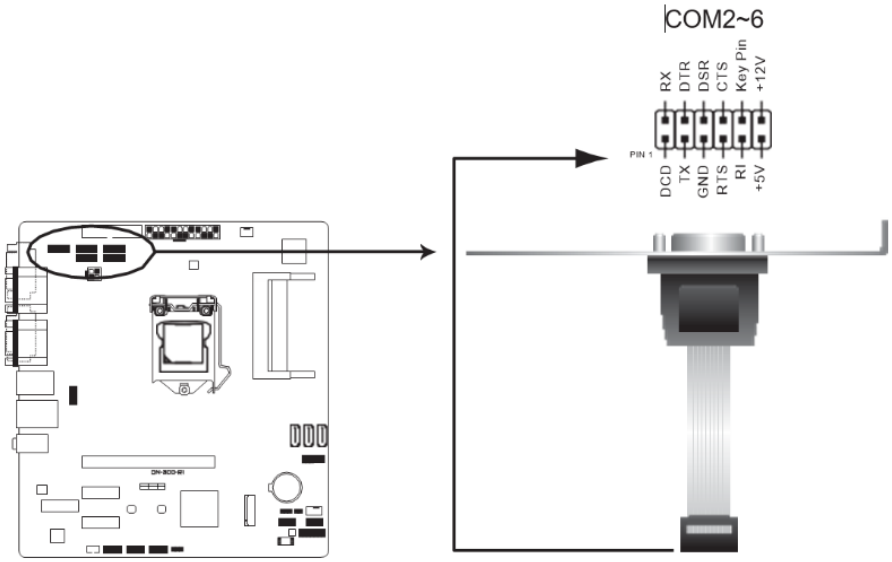
This socket allows you to install an M.2 (NGFF) SSD module.



	NOTICE
	The M.2 SSD module is purchased separately. This socket supports M Key and 2260/2280 SATA/PCIe mode storage devices.

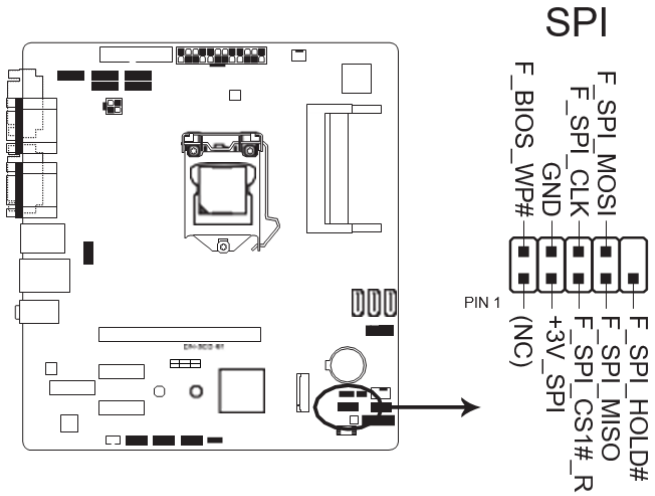
9. Serial port connectors (12-1 pin COM2, COM3, COM4, COM5, COM6)

These connectors are for serial (COM) ports. Connect the serial port cables to these connectors, then install the module to a slot opening at the back of the system chassis.



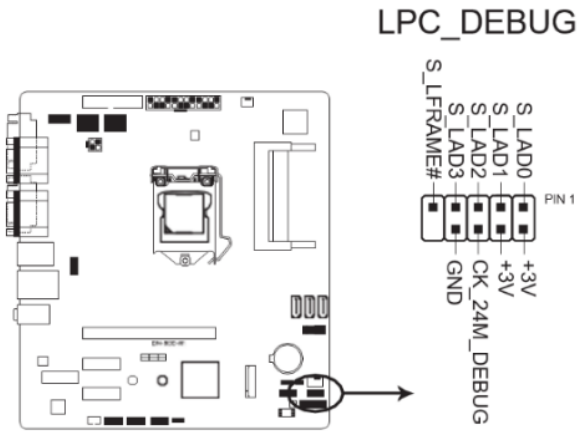
10. SPI header (10-1 pin SPI)

Use this connector to flash the BIOS ROM.



11. LPC debug header

This header allows connection to a LPC debug card.



8.4 RAID

This 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.

9 BIOS Setup Program

Use the BIOS Setup program to update the BIOS or configure its parameters. The BIOS screens include navigation keys and brief online help to guide you in using the BIOS Setup program.

9.1 Entering BIOS Setup at startup

To enter BIOS Setup at startup:

Press <F2> during the Power-On Self Test (POST). If you do not press <F2>, POST continues with its routines.

9.2 Entering BIOS Setup after POST

To enter BIOS Setup after POST:

- Press <Ctrl>+<Alt>+<Del> simultaneously.
- Press the reset button on the system chassis.
- Press the power button to turn the system off then back on. Do this option only if you failed to enter BIOS Setup using the first two options.

NOTICE

Using the power button, reset button, or the <Ctrl>+<Alt>+<Del> keys to reboot a running operating system can cause damage to your data or system. Always shut down the system properly from the operating system.

The default BIOS settings for this motherboard apply to most working conditions and ensures optimal performance. If the system becomes unstable after changing any BIOS settings, load the default settings to regain system stability. Select the option Load Optimized Defaults under the Exit Menu or press hotkey F3.

The BIOS setup screens shown in this section are for reference purposes only, and may not exactly match what you see on your screen.

9.3 Self-Recovering BIOS (after BIOS Update)

The BIOS protection technology automatically recovers the system's BIOS with a verified backup in the event of an update failure, preventing the need to replace or reinstall your hardware.

9.3.1 How works the Self-Recovering BIOS?

By using the EZFlash utility from Setup a verified backup of the BIOS (.cap) file is placed in a hidden area of your mass storage.

Once the crash happens, all you need to do is reboot. Your system will automatically activate BIOS self-recovery. EZ Flash will read the BIOS (.cap) file stored in the hidden area of your HDD, and start recovering the BIOS.

9.4 BIOS Menu Screen

Menu bar
The menu bar on top of the screen has the following main items:

Info	An overview of the basic system information
Main	For changing the basic system configuration.
Advanced	For changing the advanced system settings.
Monitor	For displaying the system temperature, power status, and changing the fan settings
Boot	For changing the system boot configuration.
Tool	For configuring options for special functions
Exit	For selecting the exit options and loading default settings.
Event Logs	For easier troubleshooting by capturing useful system information.

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

10 Main Menu

The Main menu provides you an overview of the basic system information, and allows you to set the system date, time, and security settings.

10.1 System Date [Day MM/DD/YYYY]

Allows you to set the system date.

10.2 System Time [HH:MM:SS]

Allows you to set the system time.

10.3 System Information

This menu provides you an overview of the basic system information.

10.4 Security

The Security menu items allow you to change the system security settings.

NOTICE

If you have forgotten your BIOS password, use the clear password jumper to clear the BIOS password. See section Jumpers for information on how to use the clear password jumper.

The Administrator or Boot Menu Password items on top of the screen show the default Not Installed. After you set a password, these items show Installed.

Administrator Password

If you have set an administrator password, we recommend that you enter the administrator password for accessing the system.

To set an administrator password:

1. Select the Administrator Password item and press <Enter>.
2. From the Create New Password box, key in a password, then press <Enter>.
3. From the Confirm New Password box, key in your password again to confirm the password, then click OK.

To change an administrator password:

1. Select the Administrator Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. From the Confirm New Password box, key in your password again to confirm the password, then click OK.

To clear the administrator password, follow the same steps as in changing an administrator password, but click OK when prompted to create/confirm the password. After you clear the password, the Administrator Password item on top of the screen shows Not Installed.

Boot Menu Password

If you have set a Boot Menu password, you must enter the password for accessing the Boot Menu. The Boot Menu Password item on top of the screen shows the default Not Installed. After you set a password, this item shows Installed.

To set a Boot Menu password:
1. Select the Boot Menu Password item and press <Enter>.
2. From the Create New Password box, key in a password, then press <Enter>.
3. From the Confirm New Password box, key in your password again to confirm the password, then click OK.

To change a Boot Menu password:
1. Select the Boot Menu Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. From the Confirm New Password box, key in your password again to confirm the password, then click OK.

To clear the Boot Menu password, follow the same steps as in changing a Boot Menu password, but click OK when prompted to create/confirm the password. After you clear the password, the Boot Menu Password item on top of the screen shows Not Installed.

Clear password jumper support [Enabled]
When this item is set to [Enabled], and the clear password jumper is set to clear password pins, the BIOS password will be cleared at the next boot when entering BIOS setup by pressing <F2>. Configuration options: [Disabled] [Enabled]

Chassis Intrusion [Disabled]
This item allows you to enable or disable the chassis intrusion detection function. Connect one end of the chassis intrusion sensor or switch cable to the chassis intrusion connector. The chassis intrusion sensor or switch cable sends high-level signal to the connector when a chassis component is removed or replaced. The signal is then generated as a chassis intrusion event. Configuration options: [Disabled] [Enabled]

TPM clear on intrusion [Disabled]
When this item is set to [Enabled], an intrusion event must clear the active TPM without requiring any user confirmation. Configuration options: [Disabled] [Enabled]

11 Advanced Menu

The Advanced menu items allow you to change the settings for the CPU and other system devices.

Be cautious when changing the settings of the Advanced menu items. Incorrect field values can cause the system to malfunction.

11.1 Platform Misc Configuration

The items in this menu allow you to configure the platform-related features.

PCI Express Native Power Management [Disabled]
This item allows you to enhance the power saving feature of PCI Express and perform ASPM operations in the operating system. Configuration options: [Disabled] [Enabled]

NOTICE

The following item appears only when you set the PCI Express Native Power Management to [Enabled].

Native ASPM [Disabled]

[Enabled]	Windows® Vista OS controls the ASPM (active state power management) support for devices.
[Disabled]	BIOS controls the ASPM support for the device.
[Auto]	Automatic configuration.

PCH - PCI Express options

PCH DMI ASPM [Disabled]
This item allows you to control the Active State Power Management on both NB (North-Bridge) side and SB (SouthBridge) side of the DMI Link.
Configuration options: [Disabled] [L0s] [L1] [L0sL1] [Auto]

ASPM [Disabled]
This item allows you to select the ASPM state for energy-saving conditions. Configuration options: [Disabled] [L0s] [L1] [L0sL1] [Auto]

L1 Substates [Disabled]
This item allows you to select the PCI Express L1 Substates settings. Configuration options: [Disabled] [L1.1] [L1.1 & L1.2]

PCI Express Clock Gating [Enabled]
This item allows you to enable or disable PCI Express Clock Gating for each port. Configuration options: [Disabled] [Enabled]

PCIe Speed [Auto]
Allows you to configure the PCIe speed. Configuration options: [Auto] [Gen1] [Gen2] [Gen3]

SA - PCI Express options

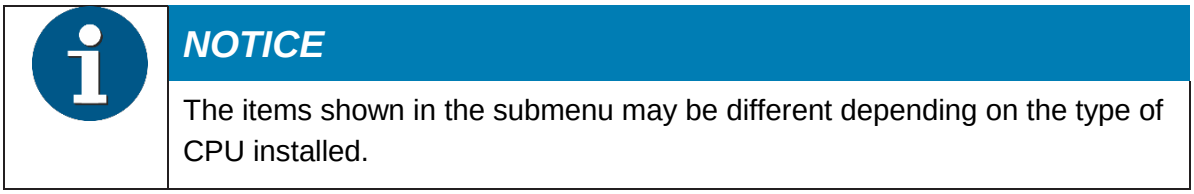
DMI Link ASPM Control [Disabled]
This item allows you to control the Active State Power Management on both CPU and PCH (platform controller hub) Both DMI link ASPM control items of the CPU and PCH sides must be enabled for the ASPM to take effect. Configuration options: [Disabled] [L0s] [L1] [L0sL1]

PEG-ASPM [Disabled]
This item allows you to select the ASPM state for energy-saving conditions, or use the optimized energy saving profile. Configuration options: [Disabled] [Auto] [ASPM L0s] [ASPM L1] [ASPM L0sL1]

SR-IOV Support [Disabled]
This option enables or disables Single Root IO Virtualization Support if the system has SR-IOV capable PCIe devices. Configuration options: [Disabled] [Enabled]

11.2 CPU Configuration

The items in this menu show CPU-related information the BIOS automatically detects.



Software Guard Extensions (SGX) [Software Controlled]
This item allows you to enable or disable Software Guard Extensions (SGX). Configuration options: [Disabled] [Enabled] [Software Controlled]

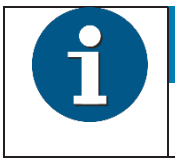
Tcc Offset Time Window [Auto]
This item allows you to set the TCC Offset Time Window for Running Average Temperature Limit (RATL) feature. RATL allows setting an average max thermal temperature. Temperatures within the time window can get higher than the temperature threshold but only the average is used to cause frequency clipping. Configuration options: [Auto] [Disabled] [5 ms] - [448 sec]

Hardware Prefetcher [Enabled]
This item allows you to turn on/off the MLC streamer prefetcher. Configuration options: [Disabled] [Enabled]

Adjacent Cache Line Prefetcher [Enabled]
This item allows you to turn on/off prefetching adjacent cache lines. Configuration options: [Disabled] [Enabled]

Intel (VMX) Virtualization Technology [Disabled]
When set to [Enabled], a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology. Configuration options: [Disabled] [Enabled]

Active Processor Cores [All]
This item allows you to select the number of CPU cores to activate in each processor package. Configuration options: [All] [1] [2] [3] [4] [5]



NOTICE

For some CPU types, only [All] and [1] appear.

Hyper-threading [Enabled]
The Intel Hyper-Threading Technology allows a hyper-threading processor to appear as two logical processors to the operating system, allowing the operating system to schedule two threads or processes simultaneously.

[Enabled] Two threads per activated core are enabled.
[Disabled] Only one thread per activated core is enabled.

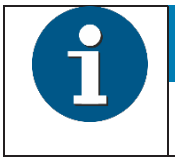
Thermal Monitor [Enabled]
This item allows you to enable or disable the Thermal Monitor. Configuration options: [Disabled] [Enabled]

CPU Power Management Control
This item allows you to manage and configure the CPU's power.

Intel(R) SpeedStep(tm) [Auto]
This item allows your system to support more than two frequency ranges. Configuration options: [Auto] [Disabled] [Enabled]

Intel(R) Speed Shift Technology [Auto]
This item allows you to enable or disable Intel(R) Speed Shift Technology support. When enabled, CPPC v2 interface allows hardware controlled
P-states. Configuration options: [Auto] [Disabled] [Enabled]

Turbo Mode [Enabled]
This item allows you to automatically set the CPU cores to run faster than the base operating frequency when it is below the operating power, current and temperature specification limit. Configuration options: [Enabled] [Disabled]



NOTICE

Turbo Mode is only available on selected CPU models only.

CPU C-states [Auto]
This item allows you to set the power saving of the CPU states. Configuration options: [Auto] [Disabled] [Enabled]

NOTICE

The following items appear only when you set the CPU C-States to [Enabled].

Enhanced C-states [Enabled]
[Enabled] Enables enhanced C1 state. [Disabled] Disables enhanced C1 state.

CPU C3 Report [Enabled]
Allows you to disable or enable the CPU C3 report to OS. Configuration options: [Enabled] [Disabled]

CPU C6 Report [Enabled]
Allows you to disable or enable the CPU C6 report to OS. Configuration options: [Enabled] [Disabled]

CPU C7 Report [CPU C7s]
Allows you to disable or enable the CPU C7 report to OS. Configuration options: [Disabled] [CPU C7] [CPU C7s]

CPU C8 Report [Enabled]
Allows you to disable or enable the CPU C8 report to OS. Configuration options: [Enabled] [Disabled]

CPU C9 Report
This item allows you to disable or enable the CPU C9 report to the operating system. Configuration options: [Enabled] [Disabled]

CPU C10 Report
This item allows you to disable or enable the CPU C10 report to the operating system. Configuration options: [Enabled] [Disabled]
Package C State Limit
This item allows you to set the C-state limit for the CPU package. Configuration options: [C0/C1] [C2] [C3] [C6] [C7] [C7s] [C8] [C9] [C10] [CPU
Default] [Auto]

CFG Lock [Disabled]
This item allows you to enable or disable the CFG lock. Configuration options: [Disabled] [Enabled]

11.3 System Agent (SA) Configuration

VT-d [Disabled]
Allows you to enable or disable VT-d function on MCH. Configuration options: [Enabled] [Disabled]

Above 4G Decoding [Disabled]
Allows you to enable or disable the 4G decoding for 64-bit devices when the system supports the 64-bit PCI decoding. Configuration options: [Enabled] [Disabled]

Memory Configuration
Memory Remap [Enabled]
Allows you to enable or disable remapping the memory above 4GB. Configuration options: [Disabled] [Enabled]

Graphics Configuration
Allows you to select a primary display from iGPU, and PCIe graphical devices.

Primary IGFX Boot Display [BIOS Default]
Select the Video Device to be activated during POST. Your selection does not take effect if you have installed an external graphics device. Secondary boot display selection will appear based on your selection. VGA modes can be supported only on the primary display. Configuration options: [BIOS Default] [USB-C] [Disp.2] [Disp.1] [VGA]

Primary Display [Auto]
Allows you to select which of the iGPU/PCIE Graphics device should be the Primary Display. Configuration options: [Auto] [CPU Graphics] [PCIE] [PEG]

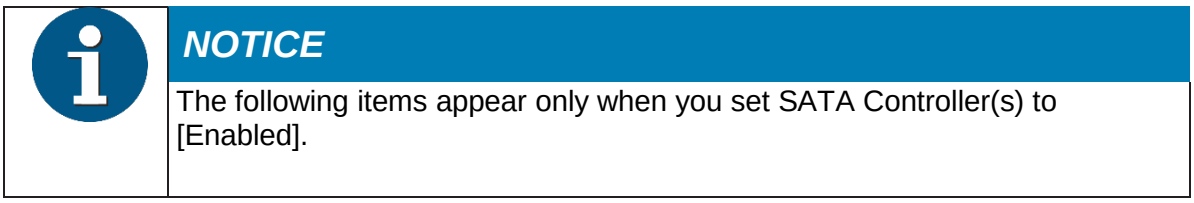
DVMT Pre-Allocated [64M]
Allows you to select DVMT 5.0 Pre_Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device. Configuration options: [32M] [64M] [96M] ~ [1024M]
RC6(Render Standby) [Auto]
Allows you to enable or disable render standby support. Configuration options: [Disabled] [Auto]

PEG Port Configuration
Allows you to configure the PEG Port settings.
PCIEX16_1 Link Speed [Auto]
Allows you to configure the PCIEX16_1 speed. Configuration options: [Auto] [Gen1] [Gen2] [Gen3]

11.4 PCH Storage Configuration

While entering Setup, the BIOS automatically detects the presence of SATA devices. The SATA Port items show Empty if no SATA device is installed to the corresponding SATA port.

SATA Controller(s) [Enabled]
Enables or disables onboard the SATA device. Configuration options: [Disabled] [Enabled]



SATA Mode Selection
This item allows you to set the SATA configuration.

[AHCI]
Set to [AHCI] when you want the SATA hard disk drives to use the AHCI (Advanced Host-Controller Interface). The AHCI allows the onboard storage driver to enable advanced Serial ATA features that increases storage performance on random workloads by allowing the drive to internally optimize the order of commands.

[Intel RST Premium With Intel Optane System Acceleration (RAID)] (R1 only)
Set to [Intel RST Premium With Intel Optane System Acceleration (RAID)] when you want to create a RAID configuration from the SATA hard disk drives.

Aggressive LPM Support [Disabled]
This item is designed for LPM (link power management) support with a better energy saving conditions. When disabled, the hot plug function of SATA ports are disabled. Configuration options: [Disabled] [Enabled]

Smart Self Test [Disabled]
This item allows you to enable or disable the SMART Self Test on all HDDs during POST. Configuration options: [Disabled] [Enabled]

SATA6G_0(White), SATA6G_2(Blue), SATA6G_3(Black) [Enabled]
Allows you to enable/disable the SATA6G ports. Configuration options: [Disabled] [Enabled]

SATA6G_0, SATA6G_2, SATA6G_3 Hot Plug [Disabled]
These items allow you to enable/disable SATA Hot Plug Support. Configuration options: [Disabled] [Enabled]

SATA6G_1(M.2) [Enabled]
Allows you to enable/disable the M.2(SOCKET3). Configuration options: [Disabled] [Enabled]

11.5 AMT Configuration (R1 only)

The items in this menu allow you to change the Intel® Active Management Technology (AMT) feature.

End of POST Message [Send in DXE]
Allows you to set whether to send the End of POST Message to ME. Configuration options: [Send in DXE] [Disabled]

USB Provisioning of AMT [Disabled]
Allows you to enable/disable AMT USB Provisioning. Configuration options: [Enabled] [Disabled]

ME Unconfig on RTC Clear [Disabled]
When this item is set to [Disabled], ME will not be unconfigured on RTC clear. Configuration options: [Disabled] [Enabled]

Secure Erase Configuration

Secure Erase mode [Simulated]
[Simulated] Clean your SSD without erasing it.
[Real] Erase your SSD.

Force Secure Erase [Disabled]
Allows you to enable/disable Secure Erase. Configuration options: [Disabled] [Enabled]

OEM Flags Settings

MEBx Hotkey Pressed [Disabled]
This item allows you to enable or disable this function. Configuration options: [Disabled] [Enabled]

MEBx Selection Screen [Disabled]
This item allows you to enable or disable this function. Configuration options: [Disabled] [Enabled]

Un-Configure ME [Disabled]
Sets this item to [Disabled] to unconfigure ME without using a password or set it to [Enabled] to use a password. Configuration options: [Disabled] [Enabled]

11.6 Trusting Computing

TPM Device Selection [Firmware TPM]
This item allows you to select the TPM device. Configuration options: [Discrete TPM] [Firmware TPM]

Security Device Support [Enable]
Allows you to enable or disable BIOS support for security devices. Configuration options: [Disable] [Enable]

SHA-1 PCR Bank [Enabled]
Allows you to enable or disable SHA-1 PCR Bank. Configuration options: [Enabled] [Disabled]

SHA256 PCR Bank [Enabled]
Allows you to enable or disable SHA256 PCR Bank. Configuration options: [Enabled] [Disabled]

Pending operation [None]
Allows you to schedule an operation for security devices. Reboot your system for the changes to take effect. Configuration options: [None] [TPM Clear]

Platform Hierarchy [Enabled]
Allows you to enable or disable Platform Hierarchy. Configuration options: [Enabled] [Disabled]

Storage Hierarchy [Enabled]
Allows you to enable or disable Storage Hierarchy. Configuration options: [Enabled] [Disabled]

Endorsement Hierarchy [Enabled]
Allows you to enable or disable Endorsement Hierarchy. Configuration options: [Enabled] [Disabled]

TPM2.0 UEFI Spec Version [TCG_2]
Allows you to select the TCG2 spec version support.
[TCG_1_2] Compatible mode for Windows® 8 / Windows® 10.
[TCG_2] Newer TCG2 protocol and event format for Windows® 10 or later.

Physical Presence Spec Version [1.3]
Allows you to select which TCG Physical Presence Interface Specification Version is supported by the OS. Configuration options: [1.2] [1.3]

11.7 Onboard Devices Configuration

Setup Mouse Support [Enabled]
Configuration options: [Disabled] [Enabled]

HD Audio [Enabled]
[Enabled] Enables the HD Audio Device. [Disabled] Disables the HD Audio Device.

Intel LAN Controller [Enabled]
[Enabled] Enables the Intel LAN controller.
[Disabled] Disables the controller.

Serial Port Configuration
The sub-items in this menu allow you to set the serial port configuration.

Serial Port 1~6 Configuration
Serial Port [Enabled]
Allows you to enable or disable the serial port (COM). Configuration options: [Disabled] [Enabled]

Parallel Port Configuration
The sub-items in this menu allow you to set the parallel port configuration.

Parallel Port [Enabled]
Allows you to enable or disable the parallel port (LPT/LPTE).Configuration options: [Disabled] [Enabled]

11.8 APM Configuration

ErP Ready [Disabled]
Allows BIOS to switch off some power at S4/S5 to get the system ready for ErP requirement. When set to [Enabled], all other PME options will be switched off. Configuration options: [Enabled] [Disabled]

Restore AC Power Loss [Power Off]

[Follow AC Power]	The system goes into on state once the AC power is restored from a power loss.
[Power Off]	The system goes into off state after an AC power loss.
[Last State]	The system goes into the last state (on or off state) once the AC power is restored from a power loss.

Power Button in S0 [Enabled]
This item allows you to enable or disable the power button in the S0 state. Configuration options: [Enabled] [Disabled]

Wake on LAN/PCIe [Disabled]
Enables or disables the wake-on-LAN function of the onboard LAN controller or the PCIe LAN devices. Configuration options: [Disabled] [S3] [S3/S4/S5]

Wake on Ring [Disabled]
Enables or disables Wake on Ring support. Configuration options: [Disabled] [S3] [S3/S4/S5]

Wake on Time [Disabled]
Enables or disables Wake on Time support. Configuration options: [Disabled] [S3] [S3/S4/S5]

Wake on USB [Disabled]
Enables or disables USB S5 wakeup support. Configuration options: [Disabled] [S3] [S3/S4/S5]

Wake on PLink1 [S3/S4/S5]
Enables or disables Wake on PLink1 support. Configuration options: [Disabled] [S3] [S3/S4/S5]

Wake on PLink2 [S3/S4/S5]
Enables or disables Wake on PLink2 support. Configuration options: [Disabled] [S3] [S3/S4/S5]

11.9 Serial Port Console Redirection (R1 only)

COM0
Console Redirection [Disabled]
Allows you to enable or disable the console redirection feature. Configuration options: [Disabled] [Enabled]

NOTICE

The following item appears only when you set Console Redirection to [Enabled].

Console Redirection Settings
These items become configurable only when you enable the Console Redirection item. The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

Terminal Type [ANSI]
Allows you to set the terminal type. [VT100] ASCII char set.
[VT100+] Extends VT100 to support color, function keys, etc.
[VT-UTF8] Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. [ANSI] Extended ASCII char set.

Bits per second [115200]
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. Configuration options: [9600] [19200] [38400] [57600] [115200]

Data Bits [8]
Configuration options: [7] [8]

Parity [None]
A parity bit can be sent with the data bits to detect some transmission errors. [Mark] and [Space] parity do not allow for error detection.
[None] None
[Even] parity bit is 0 if the num of 1's in the data bits is even
[Odd] parity bit is 0 if num of 1's in the data bits is odd
[Mark] parity bit is always 1
[Space] parity bit is always 0

Stop Bits [1]
Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning.) The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. Configuration options: [1] [2]

Flow Control [None]
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. Configuration options: [None] [Hardware RTS/CTS]

VT -UTF8 Combo Key Support [Enabled]
This allows you to enable the VT -UTF8 Combination Key Support for ANSI/VT100 terminals. Configuration options: [Disabled] [Enabled]

Recorder Mode [Disabled]
With this mode enabled only text will be sent. This is to capture Terminal data. Configuration options: [Disabled] [Enabled]

Resolution 100x31 [Disabled]
This allows you to set whether to use the resolution 100x31. Configuration options: [Disabled] [Enabled]

Putty Keypad [VT100]
This allows you to select the FunctionKey and Keypad on Putty. Configuration options: [VT100] [LINUX] [XTERMR6] [SCO] [ESCN] [VT400]

Legacy Console Redirection Settings
Redirection COM Port [COM0]
Allows you to select a COM port to display redirection of Legacy OS and Legacy OPROM Messages. Configuration options: [COM0] [COM1(PCI Bus0, Dev0, Func0) (Disabled)]
Resolution [80x24]
This allows you to set the number of rows and columns supported on the Legacy OS. Configuration options: [80x24] [80x25]
Redirection After POST [Always Enable]
This setting allows you to specify if Bootloader is selected than Legacy console redirection. Configuration options: [Always Enable] [Bootloader]

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

Console Redirection [Disabled]
Allows you to enable or disable the console redirection feature. Configuration options: [Disabled] [Enabled]

NOTICE

The following item appears only when you set Console Redirection to [Enabled].

Console Redirection Settings
Out-of-Band Mgmt Port [COM0]
Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port. Configuration options: [COM0] [COM1(PCI Bus0, Dev0, Func0) (Disabled)]
Terminal Type [VT-UTF8]
Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port. Configuration options: [VT100] [VT100+] [VT-UTF8] [ANSI]
Bits per second [115200]
Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port. Configuration options: [9600] [19200] [57600] [115200]
Flow Control [None]
Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port. Configuration options: [None] [Hardware RTS/CTS] [Software Xon/Xoff]

11.10 Intel® TXT Information (R1 only)

This menu displays Intel® Trusted Execution Technology (TXT) related information.

11.11 USB Configuration

NOTICE

The USB Devices item lists auto-detected values. If no USB device is detected, the item shows None.

XHCI Hand-off [Disabled]

NOTICE

This item is set to [Disabled] by default for the EHCI (enhanced host controller interface) support by XHCI drivers in operating systems.

[Disabled] Support XHCI by XHCI drivers for operating systems with XHCI support.
[Enabled] Support XHCI by BIOS for operating systems without XHCI support.

USB hardware delays and time-outs

USB transfer time-out [20 sec]
Allows you to select the USB transfer time-out value. Configuration options: [1 sec] [5 sec] [10 sec] [20 sec]

Device reset time-out [20 sec]
Allows you to select the USB device reset time-out value. Configuration options: [10 sec] [20 sec] [30 sec] [40 sec]

Device power-up delay [Auto]
This allows you to set the maximum time the device will take before it properly reports itself to the Host Controller. Configuration options: [Auto] [Manual]

USB Single Port Control
This item allows you to enable or disable the individual USB ports.

NOTICE

Refer to the manual for the location of the USB ports.

11.12 Network Stack Configuration

Network Stack [Enabled]
This item allows user to disable or enable the UEFI network stack. Configuration options: [Disabled] [Enabled]

NOTICE

The following two items appear only when you set the previous item to [Enabled].

Ipv4 PXE Support [Enabled]
This item allows user to disable or enable the Ipv4 PXE Boot support. Configuration options: [Disabled] [Enabled]

Ipv6 PXE Support [Enabled]
This item allows user to disable or enable the Ipv6 PXE Boot support. Configuration options: [Disabled] [Enabled]

11.13 NVMe Configuration

This menu displays the NVMe controller and drive information of the connected devices.

11.14 HDD/SSD SMART Information

This menu displays the SMART information of the connected devices.

NOTICE

NVM Express devices do not support SMART information.

11.15 Intel(R) Rapid Storage Technology

This menu allows you to configure the RAID settings.

NOTICE

This menu appears only when you set the SATA Mode Selection item to [Intel RST Premium With Intel Optane System Acceleration (RAID)].
See section **PCH Storage Configuration** for details.

RAID Volumes:
Displays all RAID volumes. Select one and change it's settings.

Volume1, RAID0 (Stripe), xxxGB
Delete
Select Yes to delete the RAID volume. All hard drives under this RAID volume will be reset to non-RAID disks. Configuration options: [Yes] [No]
SATA xx, xxx (HDD name), xxxGB
Reset to non-RAID
Select Yes to remove the selected hard drive from the RAID structure. Configuration options: [Yes] [No]

11.16 Intel(R) Ethernet Connection (7) I219LM

This menu allows you to configure the Ethernet settings.

NIC Configuration
Link Speed [Auto Negotiated]
Specifies the port speed for the selected boot device. Configuration options:
[Auto Negotiated] [10 Mbps Half] [10 Mbps Full] [100 Mbps Half] [100 Mbps Full]
Wake On LAN [Enabled]
Allows you to enable or disable the server powered on using an magic packet. Configuration options: [Disabled] [Enabled]

Blink LEDs
Identify the physical port by blinking the associated LED.

Link Status [Disconnected]
Displays the Ethernet connection status.

Monitor menu
The Monitor menu displays the system temperature/power status, and allows you to change the fan settings.

CPU / MotherBoard Temperature [xxxºC/xxxºF]
The onboard hardware monitor automatically detects and displays the CPU/ motherboard temperatures.

CPU / PSU Fan Speed [xxxx RPM]
The onboard hardware monitor automatically detects and displays the CPU / PSU fan speeds in rotations per minute (RPM). If the fan is not connected to the motherboard, the field shows N/A.

CPU Core Voltage, 3.3V Voltage, 5V Voltage, 12V Voltage, VBAT 3.0V
The onboard hardware monitor automatically detects the voltage output through the onboard voltage regulators.

Sensor configuration

HW info	SIO Pin	Register	Calculation
+3V	3VCC	Bank0, Index03	3V Voltage = Reading*0.008*2V
+12V	VIN2	Bank0, Index05	12V Voltage = Reading*0.008*12V
+5V	VIN1	Bank0, Index04	5V Voltage = Reading*0.008*5.02V
Vcore	CPU-VCORE	Bank0, Index00	Vcore = Reading*0.008*2V
Battery	VBAT	Bank0, Index08	Vbat = Reading*0.008*2V
MB Temperature	SYSTIN	Bank3, Index0C	Compared to 80H, when <80H, the temperature is positive. The value shown on the UI will be temperature.
CPU Temperature	CPUTIN	Bank3, Index0D	
PECI	PECI	Bank0, Index19	
PSU FAN Speed	SYSFANIN	Bank0, Index30[bit 15:8], Index31[bit 7:0]	Conversion to decimal is the speed value.
CPU FAN Speed	CPUFANIN	Bank0, Index32[bit 15:8], Index33[bit 7:0]	Conversion to decimal is the speed value.

CPU Fan Speed Low Limit [Ignore]
This item appears only when you enable the CPU Q-Fan Control feature and allows you to disable or set the CPU fan warning speed. Configuration options: [Ignore] [200RPM] [300 RPM] [400 RPM] [500 RPM] [600RPM]

PSU Fan Speed Low Limit [400 RPM]
This item appears only when you enable the PSU Fan Q-Fan Control feature and allows you to disable or set the PSU Fan warning speed. Configuration options: [Ignore] [200RPM] [300 RPM] [400 RPM] [500 RPM] [600RPM]

BAT Voltage Low Warning [Enabled]
Allows you to set whether to show a warning message when the BAT voltage is getting low. Configuration options: [Disabled] [Enabled]

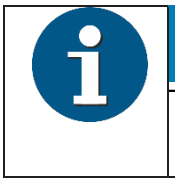
12 Boot Menu

The Boot menu items allow you to change the system boot options.

Boot Configuration
Boot Logo Display [Disabled]

[Auto]	Adjusts logo automatically based on Windows® display requirements.
[Full Screen]	Maximize the boot logo size.
[Disabled]	Hide the logo during POST.

POST Delay Time [3 sec]
This item appears only when you set Boot Logo Display to [Auto] and [Full Screen] This item allows you to select the desired additional POST waiting time to easily enter the BIOS setup. You can only execute the POST delay time during Normal Boot. The values range from 0 to 10 seconds.



NOTICE

This feature will only work under normal boot.

POST Report Delay Time [3 sec]
This item appears only when you set Boot Logo Display to [Disabled]. This item allows you to select a desired post report waiting time. Configuration options: [1 sec] ~ [10 sec] [Until Press ESC].

Bootup NumLock State [On]
This item allows you to enable or disable power-on state of the NumLock. Configuration options: [On] [Off]

POST Warnings [Just Warning]
Configuration options: [Just Warning] [Warning and Stop Booting]

AMI Native NVMe Driver Support [Enabled]
Configuration options: [Disabled] [Enabled]

F10 Boot Menu [Enabled]
Configuration options: [Disabled] [Enabled]

USB Boot [Enabled]
Configuration options: [Disabled] [Enabled]

Watch Dog [Disabled]
Enables/disables the watchdog feature. Configuration options: [Disabled] [Enabled]

POST End Beep [Enabled]
When this item is enabled, there will be a short beep at the end of the POST phase. Configuration options: [Disabled] [Enabled]

LED Error Codes

Error	Frequency
RAM Error	2Hz
CPU Error	1Hz
Chipset Initialization Error	
UEFI/NVRAM error	0.5Hz
GFX Error	0.25Hz
CPU temperature too high	0.125Hz
FAN speed below 400rpm	0.0625Hz
Disabled	Drive low

The items below allow you to select whether to show the LED error codes.

RAM Error LED [Enabled]
Configuration options: [Disabled] [Enabled]

CPU/Chipset Init Error LED [Enabled]
Configuration options: [Disabled] [Enabled]

NVRAM Error LED [Enabled]
Configuration options: [Disabled] [Enabled]

GFX Error LED [Enabled]
Configuration options: [Disabled] [Enabled]

CPU temperature Error LED [Enabled]
Configuration options: [Disabled] [Enabled]

FAN Speed Error LED [Disabled]
Configuration options: [Disabled] [Enabled]

Secure Boot
Allows you to configure the Windows® Secure Boot settings and manage its keys to protect the system from unauthorized access and malwares during POST.

OS Type [Other OS]
Allows you to select your installed operating system.

[Windows UEFI mode]	This item allows you to select your installed operating system. Execute the Microsoft® Secure Boot check. Only select this option when booting on Windows® UEFI mode or other Microsoft® Secure Boot compliant OS.
[Other OS]	Get the optimized function when booting on Windows® non- UEFI mode. Microsoft® Secure Boot only supports Windows® UEFI mode.

Key Management
This allows you to manage the Secure Boot keys.

Install Default Secure Boot keys
This item allows you to immediately load the default Security Boot keys, Platform key (PK), Key-exchange Key (KEK), Signature database (db), and Revoked Signatures (dbx). When the default Secure boot keys are loaded, the PK state will change from Unloaded mode to loaded mode.

Clear Secure Boot keys
This item appears only when you load the default Secure Boot keys. This item allows you to clear all the previously applied Secure Boot keys.

Save all Secure Boot variables
This item allows you to save all the Secure Boot keys to a USB storage device.

PK Management
The Platform Key (PK) locks and secures the firmware from any non-permissible changes. The system verifies the PK before your system enters the OS.

Save to File
This item allows you to save the downloaded PK to a USB storage device.

Set New Key
This item allows you to load the downloaded PK from a USB storage device.

NOTICE

The PK file must be formatted as a UEFI variable structure with time-based authenticated variable.

Delete Key
This item allows you to delete the PK from your system. Once the PK is deleted, all the system's Secure Boot keys will not be active.

KEK Management
The KEK (Key-exchange Key or Key Enrollment Key) manages the Signature database (db) and Revoked Signature database (dbx).

NOTICE

Key-exchange Key (KEK) refers to Microsoft® Secure Boot Key-Enrollment Key (KEK).

Save to File
Allows you to save the downloaded KEK to a USB storage device.

Set New Key
Allows you to load the downloaded KEK from a USB storage device.

Append Key
Allows you to load the additional KEK from a storage device for an additional db and dbx loaded management.

NOTICE

The KEK file must be formatted as a public key certificate or UEFI variable structure with time-based authenticated variable.

Delete key
Allows you to delete the Key from your system. Configuration options: [Yes] [No]

DB Management
The db (Authorized Signature database) lists the signers or images of UEFI applications, operating system loaders, and UEFI drivers that you can load on the single computer.

Save to File
Allows you to save the downloaded db to a USB storage device.

Set New Key
Allows you to load the downloaded db from a USB storage device.

Append Key
Allows you to load the additional KEK from a storage device for an additional db and dbx loaded management.

NOTICE

The db file must be formatted as a UEFI variable structure with time-based authenticated variable.

Delete Key
Allows you to delete the db file from your system. Configuration options: [Yes] [No]

DBX Management
The DBX (Revoked Signature database) lists the forbidden images of db items that are no longer trusted and cannot be loaded.

Save to File
Allows you to load the downloaded dbx to a USB storage device.

Set New Key
Allows you to load the downloaded dbx from a USB storage device.

Append Key
Allows you to load the additional KEK from a storage device for an additional db and dbx loaded management.

NOTICE

The dbx file must be formatted as a UEFI variable structure with time-based authenticated variable.

Delete key
Allows you to delete the Key from your system. Configuration options: [Yes] [No]

Boot Option Priorities
These items specify the boot device priority sequence from the available devices. The number of device items that appears on the screen depends on the number of devices installed in the system.

NOTICE

To select the boot device during system startup, press <F8> when DN Logo appears.

UEFI Network Device Priorities
This item allows you to set the booting order of the UEFI Network devices.

Boot Override
These items displays the available devices. The number of device items that appears on the screen depends on the number of devices installed in the system. Click an item to start booting from the selected device.

13 Tool Menu

The Tool menu items allow you to configure options for special functions. Select an item then press <Enter> to display the submenu.

EZ Flash 3 Utility
This item allows you to run EZ Flash 3 utility. When you press <Enter>, a confirmation message appears. Use the left/right arrow key to select between [Yes] or [No], then press <Enter> to confirm your choice.

Start Quick Memory Diagnosis
This item allows you to run quick memory diagnosis. When you press <Enter>, a confirmation message appears. Use the left/right arrow key to select between [Yes] or [No], then press <Enter> to confirm your choice.

Start Quick HDD Diagnosis
This item allows you to run quick HDD diagnosis. When you press <Enter>, a confirmation message appears. Use the left/right arrow key to select between [Yes] or [No], then press <Enter> to confirm your choice.

Start CPU Stress Diagnosis
This item allows you to run CPU stress diagnosis. When you press <Enter>, a confirmation message appears. Use the left/right arrow key to select between [Yes] or [No], then press <Enter> to confirm your choice.

14 Exit Menu

The Exit menu items allow you to load the optimal default values for the BIOS items, and save or discard your changes to the BIOS items. You can access the EZ Mode from the Exit menu.

Load Optimized Defaults
This option allows you to load the default values for each of the parameters on the Setup menus. When you select this option or if you press <F3>, a confirmation window appears. Select OK to load the default values.

Save Changes & Reset
Once you are finished making your selections, choose this option from the Exit menu to ensure the values you selected are saved. When you select this option or if you press <F10>, a confirmation window appears. Select OK to save changes and exit.

Discard Changes & Exit
This option allows you to exit the Setup program without saving your changes. When you select this option or if you press <Esc>, a confirmation window appears. Select Yes to discard changes and exit.

Launch EFI Shell from USB drives
This item allows you to attempt to launch the EFI Shell application (shellx64.efi) from one of the available filesystem devices.

15 Event Logs

A built-in event log enables easier troubleshooting by capturing useful system information.

15.1 Change Smbios Event Log Settings

Allows you to change the Smbios event log configuration.

Smbios Event Log [Enabled]
Configuration options: [Disabled] [Enabled]

Erase Event Log [No]
Allows you to choose options for erasing Smbios Event Log. Configuration options: [No] [Yes, Next reset] [Yes, Every reset]

When Log is Full [Do Nothing]
Allows you to choose options for reactions to a full Smbios Event Log. Configuration options: [Do Nothing] [Erase Immediately]

Smbios Event Log Standard Settings
Log System Boot Event [Disabled]
Allows you to enable or disable logging of System boot event. Configuration options: [Enabled] [Disabled]

15.2 View Smbios Event Log

Allows you to view all the events in the Smbios event logs.

Type	Event log
1. Flash Update	Type: 0xA0, Log: Flash Update
2. RTC Clear	Type: 0xA1, Log: RTC Clear
3. Battery Removed	Type: 0xA2, Log: Battery Removed
4. Chassis Intrusion	Type: 0xA3, Log: Chassis Intrusion
5. AC Power Loss	Type: 0xA4, Log: AC Power Loss
6. USB Over Current	Type: 0xA5, Log: USB Over Current
7. CPU Over Heating	Type: 0xA6, Log: CPU Over Heating
8. CPU Over Voltage	Type: 0xA7, Log: CPU Over Voltage
9. Fan Slow	Type: 0xA8, Log: Fan Slow
10. 4S Forced Shutdown	Type: 0xA9, Log: 4S Forced Shutdown

16 Certifications of the Manufacturer

The device complies with the requirements of the EU directives 2014/30/EU with regard to “Electromagnetic compatibility” and, if applicable, 2014/35/EU “Low Voltage Directive” and 2011/65/EU "Restriction of Hazardous Substances". Therefore, you will find the CE mark on the device or packaging.

The system is approved for the USA and Canada.

Supplier's Declaration of Conformity

47 CFR § 2.1077 Compliance Information

Responsible Party in the U. S.:	Diebold Nixdorf
Address:	5995 Mayfair Road N. Canton, OH 44720 / USA
Contact:	cynthia.williams@dieboldnixdorf.com

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference in which case the user will be required to correct the interference at his expense. Modifications not authorized by the manufacturer may void user’s authority to operate this device.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numerique de la classe A est conforme à la norme NMB-003 du Canada. (2) This device must accept any interference received, including interference that may cause undesired operation.

17 Recycling

This device was designed according to the Diebold Nixdorf standard "Environmentally Conscious Product Design and Development”.

The device is manufactured without the use of CFCs and CCHs and is manufactured to a great extent out of materials and components which are recyclable.

For recycling purposes do not attach any additional adhesive labels to the terminal.

Diebold Nixdorf disposes of old terminals in an environmentally responsible manner at a recycling center that is ISO 9001 and ISO 14001 certified, as is the entire company. Follow your local regulations on the disposal of toxic waste.

Your Diebold Nixdorf vendor will answer any questions you have concerning returns, recycling, and disposal of our products.

Diebold Nixdorf
D-33094 Paderborn
Order No.: 01750340075A