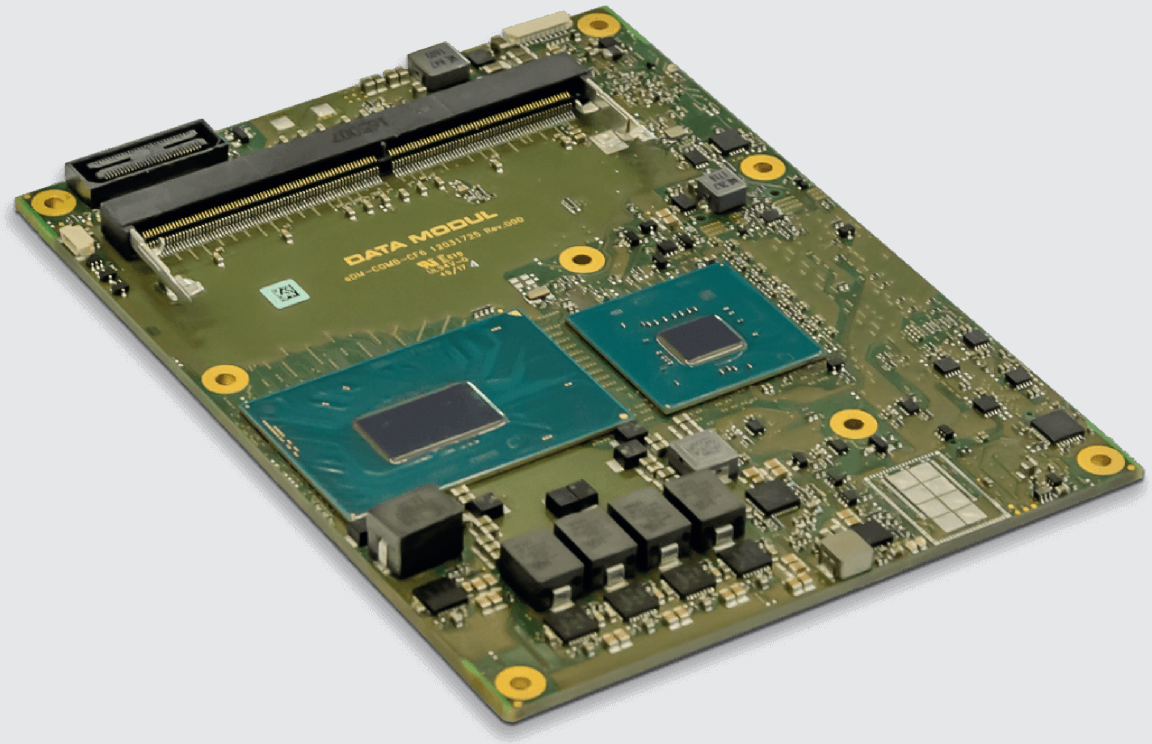
DATA MODUL

eDM-COMB-CR6



Revision History

Revision	Revision History	Date
00	First release	10.10.2019

Reference to this Document

The purpose of all the figures and illustrations in this document is merely to provide a better explanation and can differ to the actual appearance of the board. They are to be understood as schematic representations.

12044128 Rev. 00

Contents

Preface

Using this Document

- In this Document, the eDM-COMB-CR6 is also referred to as „board“.
- Please read this Document before using this board.
- This Document contains information about the hardware, software and configuration of the board.
- Awareness of the safety instructions and instructions for use in this Document will ensure the safe and correct use of the board.
- In addition to the information given here, you should comply with the local regulations for the prevention of accidents and generally applicable safety regulations.

Purpose of this Document

The purpose of this document is the definition of the technical parameters, the electrical connections and the mechanical dimensions of the eDM-COMB-CR6.

Danger Symbols & Levels

In this Document, symbols are used to highlight important safety instructions and any advice relating to the board. The instructions should be followed very carefully to avoid any risk of accident, personal injury or property damage.

Danger Symbols

	Dangerous Voltage, danger of electric shock
	Hazard point
	All DATA MODUL AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a DATA MODUL AG product except at an electrostatic-free workstation. Additionally, do not ship or store DATA MODUL AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the DATA MODUL AG Limited Warranty.

Danger Levels

DANGER	Indicates a hazardous situation, which will result in death or serious injury.
WARNING	Indicates a hazardous situation, which could result in death or serious injury.
CAUTION	Indicates a hazardous situation, which may result in minor or moderate injury.
NOTICE	Indicates a property damage.

General Symbols

	Additional support or useful information.
	The crossed-out refuse bin indicates that the products have to be properly recycled or disposed of in accordance with national legislation in the respective EU countries. If you wish to dispose of used electrical and electronic products outside the European Union, please contact your local authority so as to comply with the local regulations.

Technical Support

DATA MODUL's technicians and engineers are committed to provide the best possible technical support for our customers to enable an easy use and implementation of our products. We recommend to visit our website at www.data-modul.com first for the latest documentation, utilities and drivers, which have been made available to assist you. If you need further assistance after visiting our website please contact our technical support department by email at support@data-modul.com.

List of Abbreviations

Abbreviation	Description
COM	Computer On Module
DDC	Display Data Channel
EMI	Electro Magnetic Interference
EN	European Norm
FFC	Flat Foil Cable
HDMI	High Definition Multimedia Interface
I2C	Inter-Integrated Circuit Bus
LCD	Liquid Crystal Display
LVDS	Low Voltage Differential Signal
NA	Not Available
NC	Not Connected
PCB	Printed Circuit Board
PVM	Pulse Width Modulation
SB	Standby
SSP	Synchronous Serial Protocol
TBD	To Be Defined
TCON	Timing Controller
TMDS	Transition Minimized Differential Signaling
TTL	Transistor Transistor Logic
UL	Underwriter Lab
USB	Universal Serial Bus

Technical Data

Supported Operating Systems

- Microsoft® Windows® 10 (64 bit)
- Linux

EFI / BIOS

- UEFI based Firmware using AMI Aptio V core
- Darkboot / Bootlogo support
- Legacy Free Operation
- Boot from external SPI as defined by COM Express specification
- Memory-initialization according to SPD, X.M.P. profiles supported
- LID and Sleep signals supported
- ACPI Wake Events (WOL S3-S5, USB S3-S4, LID S3, PwrBtn S3-S5)
- AC Power Loss configurable by setup
- Spread Spectrum configurable by setup, default ON
- ACPI 6.1
- DATA MODUL family feature: Embedded Controller specification

API

- eAPI as defined by COM Express
- Data Modul specific extension to eAPI

Tools

- BIOS update tool
- FPGA update tool
- API test tool

Standards & Certifications

Environmentalism

- 2011/65/EU (of 8. June 2011 directive of the European parliament and of the council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS))
- 2006/1907/EU (of 18. December 2006 of the European parliament and of the council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH))
- 2012/19/EC (of 04. July 2012 directive of the European parliament and of the council on waste electrical and electronic equipment (WEEE))
- The board is designed and manufactured to meet ISO 14001.
- The packing complies with directive 1994/62/EU.

EMC Standards

EMI/EMC: according to EN55022

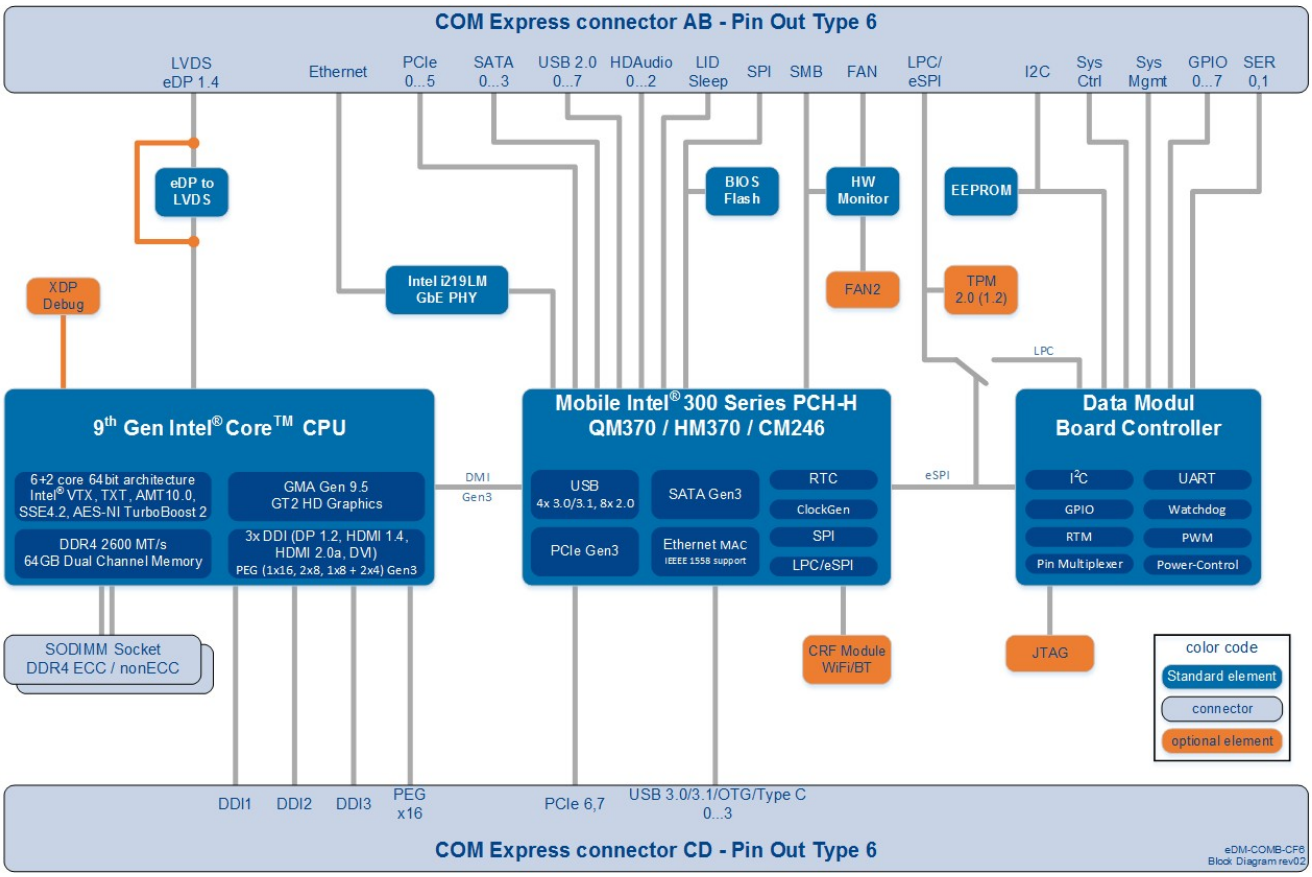
Electrical Safety

Designed to meet EN60950 and UL60950.

Shock & Vibration

Shock and Vibration according to IEC/EN60068-2-6 and IEC/EN60068-2-27.

Block Diagram



Ordering Information

Model Name	Part No.	Description
eDM-COMB-CR6-E-2276ME	12040447	COM Express Type 6 Basic with Intel® Xeon®, CM246 chipset, ECC
eDM-COMB-CR6-i7-9850HE	12040448	COM Express Type 6 Basic with Intel® Core® i7, QM370chipset
eDM-COMB-CR6-i3-9100HL	12040449	COM Express Type 6 Basic with Intel® Core® i5, QM370chipset
eDM-COMB-CF6-CF	12029280	Active cooling solution, with fan
eDM-COMB-CF6-CP	12029281	Passive cooling solution, without fan
eDM-COMB-CF6-CH	12029282	Heatspreader, 3 mm plate with 8 mm standoffs, flat surface

Hardware Features

Platform

The 9th Generation Intel® Core™ processor family are a 64-bit, multi-core processor (up to 6 cores) built on 14-nanometer process technology (Coffee Lake Refresh-H).

CPU

The eDM-COMB-CR6 supports all available Coffee Lake Refresh CPUs in FCBGA1440 package, 14nm, up to 45W TDP.

- Package: 42 mm x 28 mm x 1.395 mm, FCBGA1440 c-states
- Supported Features:
  - C-States: CO-C10
  - Intel® Virtualization Technology (Intel® VT)
  - Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
  - Intel® Hyper-Threading Technology (Intel® HT Technology)
  - Intel® 64 Architecture
  - Execute Disable Bit
  - Intel® Turbo Boost Technology 2.0
  - Intel® Advanced Vector Extensions 2 (Intel® AVX2)
  - PCLMULQDQ (Perform Carry-Less Multiplication Quad word) Instruction
  - Intel® Transactional Synchronization Extensions (Intel® TSX-NI)
  - PAIR – Power Aware Interrupt Routing
  - GMM Scoring Accelerator
  - Intel® Processor Trace
  - High Definition Contend Protection (HDCP) 2.2
- Security Features:
  - Intel® Active Management Technology 12.0 (Intel® AMT 12.0)
  - Intel® Trusted Encryption Technology (Intel® TXT)
  - Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
  - Intel® Security Key
  - SMEP – Supervisor Mode Execution Protection
  - Intel® Boot Guard
  - Intel® Software Guard Extensions (Intel® SGX)
  - Intel® Memory Protection Extensions (Intel® MPX)

Memory

- Two SO-DIMM sockets
- Memory type: DDR4, ECC/Non-ECC (Variants with Intel® CM246 chipset support ECC memory)
- Speed: up to 2666 MT/s
- Size: up to 32 GB (2 x 16 GB)

Chipset

- Mobile Intel® 300 Series Chipset QM370, HM370 and CM246 PCH

Graphic & Media

- GFX type: Intel® Gen 9.5 Graphics Processing Unit (GT2)

DirectX 12, Direct3D 2015, OpenGL 4.5, OpenCL 2.1 APIs

- Display Pipes (3 independent)
  3 x DDIs (Digital Display Interfaces):
  - DisplayPort 1.2 with support for Multi-Stream Transport
  - HDMI 1.4 (requires external level shifter)
  - DVI port (requires external level shifter)
  - HDMI 2.0a (with converter)
    eDP 1.4, Resolutions up to 4K (UHD@60Hz)
- Video Decode: H.265/HEVC @ level 5.1 (4k), H.264/AVC @ Level 5.1(4k), VC-1, WMV9, JPEG, VP8/VP9, MPEG2
- Video Encode: H.265/HEVC @ level 5.1 (4k), H.264/AVC @ Level 5.1(4k), WMV9, JPEG, VP8/VP9, MPEG2

IO

- 4 x USB 3.0
  8 x USB 2.0, 1 x USB OTG support
- 4 x SATA 3.0 (6Gb/s) with RAID support 0/1/5/10
- 8 x PCI Express® Gen. 3 lanes (x1/x2/x4 operation)
- PEG Gen 3 port (1 x16 link (default), 2 x8 links or 1 x8 + 2 x4 links)
- SPI for onboard/external BIOS flash
- LPC bus / eSPI for Embedded Controller / TPM / external SIO (multiplexed)
- GPIOs, 1MHz SMB 2.0
- Intel HD Audio
- 2 x UART
- IEEE1588 support (Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems)

LAN

Intel® GbE support via the onboard Intel® i219-LM GbE LAN controller (with AMT 11 support).

Additional Interfaces & Functions

LVDS

The eDM-COMB-CR6 supports Dual channel LVDS 1/2x18/24bit up to 1920x1200 from an eDP2LVDS converter like NXP PTN3460. Optionally it be possible to bypass LVDS converter to redirect the eDP signals to the COM Express connector pins by 0R resistors placed stubless on the PCB.

CRF Module WiFi/BT/WiGig

Optionally the eDM-COMB-CR6 supports a soldered CRF Module (through CNVi), support for Intel Wireless-AC (Gigabit wireless speed), e.g.: Intel Wireless-AC 9560.

TPM

Optionally the eDM-COMB-CR6 supports Trusted Platform Module (Version 1.2 and 2.0).

Hardware Monitor

Hardware Monitoring supports on the eDM-COMB-CR6 design using the Nuvoton NCT7802Y.
Hardware Monitor providing following information:

- CPU DIE temperature measured through PECI interface
- PCB temperature measured inside HW Monitor (place HWM at cool spot of PCB)
- Level of VCC module input voltage
- Level of 5V_SBY input voltage
- Level of VCCRTC voltage follower OpAmp circuit.

The Hardware Monitor provides control signals to operate one a connected at the COM Express baseboard fan connector and on board connector.

Embedded Controller

An Embedded Controller providing the feature set defined in Data Modul Embedded Controller specification Rev 1.0 using an Altera MAX-10 FPGA supports by the eDM-COMB-CR6 design.

Data Modul Board Controller

The DATA MODUL Embedded Controller (DMEC) implements a set of typical embedded peripheral features in the Computer-On-Module (CoM) including devices like GPIO, I2C, Watchdog timers, UARTs etc. Depending on the DATA MODUL board type, the DMEC device is connected to the chipset either via LPC or eSPI.

The DMEC Controller on the eDM-COMB-CR6 module provides the following functionality:

- Connected to LPC on Intel 300 Series PCH-H
- Two UARTs
  - Speed up to 115200Bd
  - I/O Address/IRQ configurable via BIOS setup.
  - UART1 optionally supports RTS/CTS/DSR/DTR signals through GPIOs, configurable via BIOS setup.
- I2C controller
  - Controls up to three I2C busses via multiplexer.
  - Supports Automatic Bus Clear to prevent bus hangs.
  - Supports Multiple masters on the bus. This feature is only supported if Automatic Bus Clear is off.
  - Supports FastMode+.
  - I2C speed configurable via BIOS setup.
  - Up to 400kHz in normal mode, up to 800kHz in FastMode+.
  - IRQ configurable via BIOS setup.
- Watchdog
  - Supports up to three stages.
  - Timeout per stage: 1ms- 65sec, with a granularity of 1ms or 128ms - ~140min, with a granularity of 128ms.
  - Supports Standard and Window Mode. Window mode is an advanced watchdog feature for safety critical applications. It only allows triggering the Watchdog within a specific time window. This covers the case where software hangs in a loop within the watchdog trigger routine.
  - Stage events include NMI, Reset and IRQ (if enabled in BIOS setup).
  - Supports Auto Reload (allows to use the Watchdog as an event ticker).
  - Supports register lock to prevent the Watchdog from being disabled or its configuration being changed in safety critical applications.
  - Fully configurable via BIOS setup.
- COM Express GPIOs:
  - Supports eight bi-directional GPIOs.
  - Initial state (In/Out, High/Low, set during early POST) can be configured via BIOS setup.
  - Capable to generate IRQ events (if IRQ enabled in BIOS setup). For details on how to enable IRQ generation please refer to the DMEC Functional Specification.
  - Additional GPIO function configurable via BIOS setup:
    - GPIO2: GPIO or UART1 DSR
    - GPIO4: GPIO or UART1 CTS or PWM0
    - GPIO5: GPIO or WD Kick Input or UART1 RTS or PWM1
    - GPIO6: GPIO or I2C2 CL or UART1 DTR
    - GPIO7: GPIO or I2C2 SDA.
- PWM controller
  - Supports either two independent 8Bit channels or one 16Bit channel for higher resolution for example in DAC applications.
  - Left or center aligned PWM output
  - Programmable period and double buffered duty cycle registers
  - Configurable output polarity
  - Wide range PWM period configurable per channel via programmable pre-scaler".

Most common features are accessible through eApi function calls. eApi supports and drivers for the DMEC device are available for Windows and Linux. For details on the DMEC register layout please refer to the DMEC Functional Specification which is available from DATA MODUL on request.

OnModule Memory

An 16 MByte SPI in SO-8 package flash to store EFI and setup configuration is used on the eDM-COMB-CR6 design.
A 32kbit I2C EEPROM configured to address AE/AF is connected to the fast I2C bus of the Embedded Controller and also to the I2C interface of the COM Express connector.

Environmental Conditions

The eDM-COMB-CR6 is able to be operated and stored under the following environmental conditions:

- Temperature (operating): 0°C ... +60°C (commercial grade)
  Extended temperature ranges on request.
- Temperature (storage): -40°C ... +85°C
- Relative humidity: ‹ 80%
- Tolerable air pressure: › 708 hPa (approx. altitude 2000m)

Power Supply

Input Voltage Requirements

- VCC: 12.0 V ± 5%
- 5V_SBY: 5.0 V ± 5%
- Modes: ATX Mode or VCC only without 5V_SBY
- Voltage Ripple: max. 100mV peak to peak 0 ... 20 MHz
- Rise Time: 0.1 ... 20ms from input voltage ‹ 10% nominal VCC
- Max. Inrush Current 5V_SBY: 2A
  VCC: 10A

Power Features

- Reset Button Behavior
  Module resets immediately when reset button is pressed in S0 state.
  Module stays in reset condition when reset button is pressed and hold in any system state ‹ S0.
- Power Button Behavior
  A push of the power button power up the system to S0 if it is in S5/S3 state or shutdown to S5 if it is in S0 state. Operating system handle the power button event depending on the driver settings.
  Push and hold the power button ›4s (power button override) shutdown the system into S5 independent of the other settings.

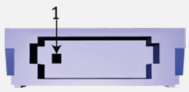
Interfaces / Connectors

COM Express connector, type 6 pin-out

- According COM Express specification Rev. 3.0

Onboard Fan

- Supported by design but not assembled in series production.
- Connector type: JST part number SM04B-SURS-TF.
- Mating cable header type: JST part number 04SUR-32S.
- Pinout

Pin assignment	Pin	Description
	1	GND
	2	VCC
	3	SENSE
	4	VCC

CPLD JTAG & debug connector

- Connector type: JST part number SM10B-SURS-TF.
- Mating cable header type: JST part number 10SUR-32S.
- Pinout

Pin assignment	Pin	Description
	1	V_3V3_S5
	2	JTAG_TCK
	3	JTAG_TDI
	4	JTAG_TMS
	5	JTAG_TDO
	6	Debug RS232 RX
	7	Debug RS232 TX
	8	JTAG EN / GPIO1
	9	Debug GPIO2
	10	GMD

BIOS Setup

The purpose of this chapter is to describe the settings in the UEFI BIOS Setup program on this Computer on Module and to explain the procedure for updating the UEFI BIOS.

Terms & Abbreviations

Term/Abbreviation	Description
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
AFU	AMI Firmware Update
ASPM	Active State Power Management
BBS	BIOS Boot Specification
COM	Computer On Module
CRID	Compatible Revision ID
CSM	Compatibility Support Module
CTDP	Configurable TDP
DMI	Direct Memory Interface
DTS	Digital Thermal Sensor
DVMT	Dynamic Video Memory Technology
ECP	Enhanced Capabilities Port
EFP	External Flat Panel
EHCI	Enhanced Host Controller Interface
EIS	Enhanced Intel Speedstep
EPP	Enhanced Parallel Port
GPIO	General Purpose Input/Output
IGFX	Intel Graphics
IPv4/IPv6	Internet Protocol Version
KEK	Key Exchange Key
LBAR	Linear Base Address Register
LFP	Local Flat Panel
MRC	Memory Reference Code
NMI	Non-Maskable Interrupt
NVRAM	Non-Volatile Random-Access Memory
OPROM	Option ROM
OS	Operating System
PK	Platform Key
PME	Power Management Event
PVM	Pulse Width Modulation
PXE	Preboot Execution Environment
RAID	Redundant Array of Independent Disk
SCI	System Control Interrupt
SMI	System Management Interrupt
SO-DIMM	Small Outline Dual Inline Memory Module
SPP	Standard Parallel Port
TDP	Thermal Design Power
TOLUD	Top Of Lower Usable Memory
TXT	Trusted Execution Technology
VT-d	Virtualization Technology for Directed I/O
WDT	Watchdog Timeout
XHCI	eXtensible Host Controller Interface

BIOS Update Description

This COM is provided with an American Megatrends, Inc. Aptio V UEFI Firmware. For updating the firmware, please use Intel® Flash Programming Tool (FPT) utility suite. This is a scriptable command line tool, utilized for factory or field BIOS updates. It is available for Microsoft Windows®, Linux, and the UEFI shell.
Please contact your DATA MODUL support for accessing the tools.

The complete UEFI Firmware image for this COM consists of several regions:

- Descriptor Region: Describes the size and location of the firmware regions and contains several configuration settings.
- BIOS Region: Responsible for main hardware initialization and feature interfaces during runtime.
- ME Region: Intel® Management Engine firmware binary.
- GBE Region: Contains Gigabit-Ethernet configuration data.

For updating the complete 16MB firmware image with the UEFI version of FPT use following command:

fpt.efi –f newbiosfile.bin

For complete command reference, please check -? command for the help screen.

BIOS Setup Description

The UEFI Setup program allows users to modify the basic system configuration and save these settings to NVRAM.

To enter UEFI Setup, press DEL or ESC during POST.

Figure POST Screen

To select a Boot Popup Menu, press F7 during POST. At End of Post a selection menu will show all available boot devices to choose from. UEFI Setup program can be entered from Boot Popup Menu as well.

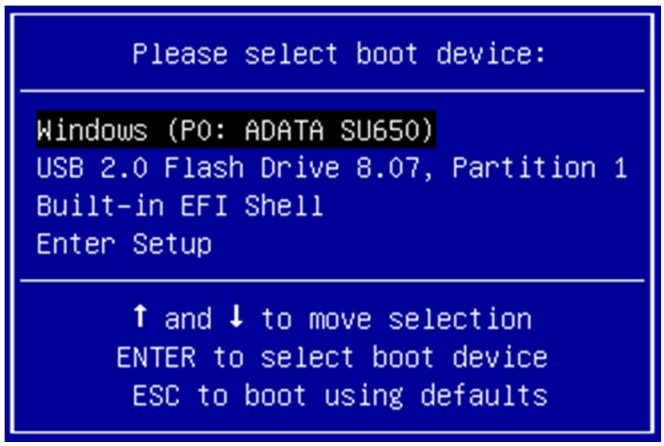


Figure Boot Popup Menu

Following is a description of the UEFI Setup pages.

Main

Parameter	Value	Comment
System Date	Day MM/DD/YYYY	Set the Date.
System Time	HH:MM:SS	Set the Time.
Module Information	Submenu	Displays Module Information.
Platform Information	Submenu	Displays Platform Information.

Advanced

Parameter	Value	Comment
CPU Configuration	Submenu	CPU Configuration Parameters
Power & Performance	Submenu	Power & Performance Options
Trusted Computing	Submenu	Trusted Computing (TPM) Settings
Serial Port Console Redirection	Submenu	Serial Port Console Redirection
Connectivity Configuration	Submenu	Connectivity Configuration Parameters
Thermal Configuration	Submenu	Thermal Configuration Parameters
SIO Configuration	Submenu	SuperIO Settings
USB Configuration	Submenu	USB Configuration Parameters
Network Stack Configuration	Submenu	Network Stack Settings
CSM Configuration	Submenu	Compatibility Support Module Settings
NVMe Configuration	Submenu	NVMe Device Options Settings
Module Peripherals Configuration	Submenu	Configure Module Peripherals
Module H/W Monitor	Submenu	Monitor hardware status
Module Watchdog Configuration	Submenu	Configure Watchdog
Module Display Configuration	Submenu	Configure Module Display options

CPU Configuration

Parameter	Value	Comment
Hardware Prefetcher	Disabled **Enabled**	Enable/Disable the Mid Level Cache (L2) streamer prefetcher.
Adjacent Cache Line Prefetch	Disabled **Enabled**	Enable/Disable the Mid Level Cache (L2) prefetching of adjacent cache lines.
Intel Virtualization Technology	Disabled **Enabled**	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Hyper-Threading	Disabled **Enabled**	Enable/Disable Hyper-Threading technology.
AES	Disabled **Enabled**	Enable/Disable CPU Advanced Encryption Standard instructions.

Power & Performance

Parameter	Value	Comment
CPU – Power Management Control	Submenu	CPU – Power Management Control Options
GT – Power Management Control	Submenu	GT – Power Management Control Options

CPU – Power Management Control

Parameter	Value	Comment
Intel(R) SpeedStep(tm)	Disabled **Enabled**	Enable/Disable Intel SpeedStep Technology.
Turbo Mode	Disabled **Enabled**	Enable/Disable Intel Turbo Boost Technology.
Config TDP Configurations	Submenu	Config TDP Configurations
C states	Disabled **Enabled**	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Package C State Limit	**Auto** Cpu Default C10 C9 C8 C7S C7 C6 C3 C2 C0/C1	Maximum Package C State Limit Setting. Cpu Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit.

Config TDP Configuration

Parameter	Value	Comment
Configurable TDP Boot Mode	**Nominal** Down Up Deactivated	Configurable TDP Mode as Nominal/Up/Down/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero.
Configurable TDP Lock	Enabled **Disabled**	Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When CTDP Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.
ACPI CTDP BIOS	Enabled **Disabled**	Enable/Disable ACPI Configurable TDP support (TableId CtdpB).

GT – Power Management Control

Parameter	Value	Comment
RC6 (Render Standby)	**Enabled** Disabled	Enable/Disable render standby support.
Disable Turbo GT frequency	Enabled **Disabled**	Enable: Disable Turbo GT frequency Disabled: GT frequency is not limited.

Trusted Computing

Parameter	Value	Comment
Security Device Support	Disabled **Enabled**	Enable/Disable BIOS support for security device. If disabled, OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank	Disabled **Enabled**	Enable or Disable SHA-1 PCR Bank.
SHA256 PCR Bank	Disabled **Enabled**	Enable or Disable SHA256 PCR Bank.
Pending operation	**None** TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Disabled **Enabled**	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disabled **Enabled**	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disabled **Enabled**	Enable or Disable Endorsement Hierarchy
TPM2.0 UEFI Spec Version	TCG_1_2 **TCG_2**	Select the TCG2 Spec Version Support. TCG_1_2: the Compatible mode for Win8/Win10. TCG_2: Support new TCG2 protocol and event format for Win10 or later.

Serial Port Console Redirection

Parameter	Value	Comment
Console Redirection	**Disabled** Enabled	Enables/Disables Console Redirection.
Console Redirection Settings	Submenu	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.
Legacy Console Redirection Settings	Submenu	Configure Port for Legacy Console Redirection.

Console Redirection Settings

Parameter	Value	Comment
Terminal Type	VT100 **VT100+** VT-UTF8 ANSI	Emulation: ANSI: Extended ASCII char set. 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.
Bits per seconds	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Configures the number of data bis. 8 is recommended to easily use the link for file transfer and non-English text transfer.
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. 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. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	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.
Flow Control	**None** Hardware RTS/CTS	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.
VT-UTF8 Combo Key Support	Disabled **Enabled**	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	**Disabled** Enabled	With this mode enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled **Enabled**	Enables/Disables extended terminal resolution.
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

Legacy Console Redirection Settings

Parameter	Value	Comment
Redirection COM Port	**COM0** COM1 COM2 COM3	Select a COM Port to use for Legacy OS and Legacy OPROM Console Redirection.
Resolution	80x24 **80x25**	On Legacy OS, the Number of Rows and Columns supported by redirection.
Redirection After POST	**Enabled** Disabled	Enabled: Console Redirection is available for Legacy OS. Disabled: Legacy console redirection is disabled before booting to Legacy OS.

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

Parameter	Value	Comment
Out-of-Band Mgmt Port	**COM0** COM1 COM2 COM3	Select a COM Port to use for Microsoft Windows Emergency Management Services (EMS). EMS allows for remote management of a Windows Server OS through a serial port.
Terminal Type	VT100 VT100+ **VT-UTF8** ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per seconds	9600 19200 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	**None** Hardware RTS/CTS Software Xon/Xoff	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.

Connectivity Configuration

Parameter	Value	Comment
CNVi Module	Disable **Enable**	Enable/Disable integrated CNVi module.
Advanced settings	**Disable** Enable	Configure ACPI objects for wireless devices.

Thermal Configuration

Parameter	Value	Comment
DTS SMM	**Disabled** Enabled	Disabled: ACPI thermal management uses HWMonitor reported temperature values. Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values.
Critical Trip Point	127 C **119 C (POR)** 111 C 103 C 100 C 95 C 87 C 79 C 71 C 63 C	This value controls the temperature of the ACPI Critical Trip Point - the point at which the OS will shut the system off. NOTE: 119C is the Plan Of Record (POR) for all Intel mobile processors.
Passive Trip Point	**95 C** 87 C 79 C 71 C 63 C 55 C 47 C 39 C Disabled	This value controls the temperature of the ACPI Passive Trip Point - the point at which the OS will begin throttling the processor.

SIO Configuration

Parameter	Value	Comment
Serial Port 1	Submenu	View and set basic properties of the SIO logical device. Like IO base, IRQ range, DMA channel and device mode.
Serial Port 2	Submenu	View and set basic properties of the SIO logical device. Like IO base, IRQ range, DMA channel and device mode.
Parallel Port	Submenu	View and set basic properties of the SIO logical device. Like IO base, IRQ range, DMA channel and device mode.
PS2 Controller (KB&MS)	Submenu	View and set basic properties of the SIO logical device. Like IO base, IRQ range, DMA channel and device mode.

Serial Port 1 Configuration

Parameter	Value	Comment
Use This Device	Disabled **Enabled**	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=3F8h; IRQ=4 IO=2F8h IO=3E8h IO=2E8h IRQ=3,4,5,7,9,10,11,12	Configure device's resource settings. New settings will be reflected on this setup page after system restarts.

Serial Port 2 Configuration

Parameter	Value	Comment
Use This Device	Disabled **Enabled**	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=2F8h; IRQ=3 IO=3F8h IO=3E8h IO=2E8h IRQ=3,4,5,7,9,10,11,12	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.
Mode	**Standard Serial Port Mode** IrDA Active pulse 1.6 uS IrDA Active pulse 3/16 bit time ASKIR Mode	Configure Standard or IrDA Mode of the Serial Port.

Parallel Port Configuration

Parameter	Value	Comment
Use This Device	Disabled **Enabled**	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=378h; IRQ=5 IO=278h IO=3BCh IRQ=5,6,7,9,10,11,12	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.
Mode	**STD Printer Mode** SPP Mode EPP-1.9 and SPP Mode EPP-1.7 and SPP Mode ECP Mode ECP and EPP 1.9 Mode ECP and EPP 1.7 Mode	Change Parallel Port mode. Some of the Modes required a DMA resource. After Mode changing, Reset the System to reflect actual device settings.

PS2 Controller (KB&MS) Configuration

Parameter	Value	Comment
Use This Device	Disabled **Enabled**	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=60h; IO=64h; IRQ=1	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.

USB Configuration

Parameter	Value	Comment
USB Mass Storage Driver Support	Disabled **Enabled**	Enable/Disable USB Mass Storage Driver Support.
USB Beep	**Disabled** Enabled	Enable/Disable Beep on USB events.
Mass Storage Devices	**Auto** Floppy Forced FDD Hard Disk CD-ROM	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CD-ROM', drives with no media information will be emulated according to a drive type.

Network Stack Configuration

Parameter	Value	Comment
Network Stack	**Disabled** Enabled	Enable/Disable UEFI Network Stack.
Ipv4 PXE Support	**Disabled** Enabled	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created.
Ipv6 PXE Support	**Disabled** Enabled	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created.
PXE boot wait time	**0** – 5 **(0 default)**	Wait time to press ESC key to abort the PXE boot.
Media detect count	**1** – 50 **(1 default)**	Number of times presence of media will be checked.

CSM Configuration

Parameter	Value	Comment
CSM Support	**Disabled** Enabled	Enable/Disable CSM Support.
Option ROM Messages	**Force BIOS** Keep Current	Force BIOS: Change display to text mode and show OpROM messages. Keep Current: Don't change display mode and suppress legacy OpROM messages.
Boot Option Filter	UEFI and Legacy Legacy only **UEFI only**	Configure available boot options.
Network	**Do not launch** UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM.
Storage	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy Storage OpROM.
Video	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy Video OpROM.
Other PCI Devices	Do not launch **UEFI** Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video.

Module Peripherals Configuration

Parameter	Value	Comment
LBAR	Disabled **Enabled**	Configure and use Linear Base Address (LBAR) if supported in FPGA.
ACPI Devices	**Disabled** Enabled	Select how resources are reported to the OS via ACPI. Enabled: Separate device, may require Driver. Disabled: Motherboard Resource.
UART Configuration	Submenu	Configure integrated UARTs.
I2C Configuration	Submenu	Configure integrated I2C controllers.
GPIO Bank A Configuration	Submenu	Configure GPIO Bank A pins.
Misc. Configuration	Submenu	Miscellaneous Configuration

UART Configuration

Parameter	Value	Comment
Base Address	**Disabled** 3F8h 2F8h 3E8h 2E8h	Select the Base address for the device.
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.

I2C Configuration

Parameter	Value	Comment
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.
I2C Clock	1kHz 10kHz 50kHz **100kHz** 200kHz 400kHz 625kHz 800kHz	Select I2C Speed (OS driver may use different speed). Note: Depending on I2C controller, actual speed may be slightly below selected values.
Auto-BusClear	**Disabled** Automatic	If enabled, the I2C controller monitors the SDA line for conditions where the slave device blocks it and tries to recover the bus by pulsing the SCL line. Note: If enabled, the multi-master capability is no longer guaranteed!
FastMode+	**Disabled** Enabled	If enabled, the SCL line is switched from open drain to push-pull to allow for higher speeds. Note: If enabled, multi-master capability and Clock stretching functionality is no longer guaranteed!!
MultiMaster	Disabled **Enabled**	If disabled, the I2C master will omit bus arbitration.

GPIO Configuration

Parameter	Value	Comment
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.
GPIO0 (COMe GPI0)	Submenu	Configure GPIO Bank A pins.
GPIO1 (COMe GPI1)	Submenu	Configure GPIO Bank A pins.
GPIO2 (COMe GPI2)	Submenu	Configure GPIO Bank A pins.
GPIO3 (COMe GPI3)	Submenu	Configure GPIO Bank A pins.
GPIO4 (COMe GPO0)	Submenu	Configure GPIO Bank A pins.
GPIO5 (COMe GPO1)	Submenu	Configure GPIO Bank A pins.
GPIO6 (COMe GPO2)	Submenu	Configure GPIO Bank A pins.
GPIO7 (COMe GPO3)	Submenu	Configure GPIO Bank A pins.

GPIO0, GPIO1, GPIO3

Parameter	Value	Comment
Usage	**GPIO**	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO2

Parameter	Value	Comment
Usage	**GPIO** UART1 DSR	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO4

Parameter	Value	Comment
Usage	**GPIO** PWM0 UART1 CTS	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO5

Parameter	Value	Comment
Usage	**GPIO** WD Kick PWM1 UART1 RTS	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO6

Parameter	Value	Comment
Usage	**GPIO** I2C2 SCL UART1 DTR	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO7

Parameter	Value	Comment
Usage	**GPIO** I2C2 SDA	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

Misc. Configuration

Parameter	Value	Comment
Watchdog IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the Watchdog device. IRQ selection will be available in the Watchdog menu after reboot.

Module HW Monitor

Parameter	Value	Comment
Temperature Unit	**Celsius** Fahrenheit	Select temperature scale: Celsius or Fahrenheit.
Configure Fan Sensors	Submenu	Configure Fan parameters.

Fan Configuration

Parameter	Value	Comment
Ticks/Rev	1 – 16 **(2 default)**	Number of ticks per Fan revolution.
Fan Mode	Off Manual **SmartFan(TM)**	Select Fan mode of operation.
Fan Speed	10 – 100 **(40 default)**	Select fixed Fan Speed in %.
Trigger Temperature	Celsius: 20 – 80 **(40 default)** Fahrenheit: 68 – 176 **(104 default)**	Select the temperature at which the Fan starts spinning.
Initial Speed	10 – 80 **(50 default)**	Initial Fan Speed in %.
Control Temperature	**CPU Temperature** PCH Temperature Module Temperature	Temperature to use.

Module Watchdog Configuration

Standard Mode

Parameter	Value	Comment
Watchdog	**Disabled** Standard Mode Window Mode	Enable/Disable Watchdog and select Mode.
Auto Reload	**Disabled** Enablede	Enable Auto Reload. If enabled, Timeout registers will be reloaded automatically after expiration.
Lock	**Disabled** Enablede	If enabled, the Watchdog registers will be locked and become read only after initialisation.
Stage	Submenu	Configure Watchdog Stage.

Stage Configuration

Parameter	Value	Comment
Stage Action	**Disabled** Delay None Reset IRQ	Select Stage Action on timeout. For choosing IRQ, enable Interrupt within Menu 'Module Peripherals Configuration' – 'Misc. Configuration' – Watchdog IRQ' first, then Save and Reboot to Setup.
Timeout	**1** - 65535	Select the timeout value for the stage.
WDT#	**Disabled** Enablede	Assert WDT# signal to Baseboard.

Window Mode

Parameter	Value	Comment
Watchdog	**Disabled** Standard Mode Window Mode	Enable/Disable Watchdog and select Mode.
Lock	**Disabled** Enabled	If enabled, the Watchdog registers will be locked and become read only after initialisation.
Delay	Submenu	Enable/Disable Watchdog and select Mode.
Window Closed Period	Submenu	Trigger events during this period will be treated as error and cause the timeout event selected in the Window Open Stage.
Window Opened Period	Submenu	Trigger events during this period will reload the watchdog timer and transition the internal state machine to the Window Closed Stage.

Module Display Configuration

Parameter	Value	Comment
Primary IGFX Boot Display	**Auto** LFP EFP1 EFP2 EFP3 CRT	Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display.
Secondary IGFX Boot Display	**Disabled** LFP EFP1 EFP2 EFP3 CRT	Select Secondary Display Device.
LFP Panel Type	**Auto** LVDS EEPROM Carrier EEPROM Module EERPOM 640x480 800x600 ...	Select LFP timings used by Internal Graphics Device. LVDS, Carrier and Module EEPROM timings are available if appropriate data is found.
LFP Fallback Type	**Disabled** 640x480 800x600 ...	Enable LFP with selected timings if auto detection fails.
Panel Color Depth	**18 Bit** 24 Bit VESA 24 Bit oLDI	Panel Color Depth for EDID 1.3 detection.
Panel Channel Count	**Single Channel** Dual Channel	Panel Channel Count for EDID detection.
Backlight Type	None **PWM** PWM Inverted	Select Backlight Inverter Type and Polarity.
Backlight Value	0 – 100 **(50 default)**	Set Backlight Value in Percentage.
PWM Frequency	**200**	Set PWM Frequency (200 Hz - 40000 Hz).
Backlight On	**Enabled** At End Of Post	Configure if LVDS Backlight should be set when panel is powered, or inhibit until End Of Post.
Backlight OS Controlled	**Enabled** Disabled	Configure if PWM values can be overridden by OS Power Options.
LVDS Spread Spectrum	**Disabled** 0.5 % 1.0 % 1.5 % 2.0 % 2.5 %	Set LVDS Center Spreading.
EFP Type	HDMI/DVI **DP w. HDMI/DVI Comp.** DP only	Select the type of the EFP.

Chipset

Parameter	Value	Comment
System Agent (SA) Configuration	Submenu	System Agent (SA) Parameters (Graphics, Graphics Audio, DMI, PEG, Memory)
PCH-IO Configuration	Submenu	Platform Controller Hub Parameters

System Agent Configuration

Parameter	Value	Comment
Memory Configuration	Submenu	Configure Memory Settings
Graphics Configuration	Submenu	Config Graphics Settings
PEG Port Configuration	Submenu	Configure System Agent PCI Express Settings.
VT-d	Disabled **Enabled**	Enable/Disable VT-d function on System Agent.
Above 4GB MMIO BIOS assignment	Enabled **Disabled**	Enable/Disable above 4GB MemoryMappedIO BIOS assignment. This is disabled automatically when Aperture Size is set to 2048MB.

Memory Configuration

Parameter	Value	Comment
Max TOLUD	**Dynamic** 1 GB 1.25 GB 1.5 GB 1.75 GB 2 GB 2.25 GB 2.5 GB 2.75 GB 3 GB 3.25 GB 3.5 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.
Memory Remap	**Enabled** Disabled	Enable/Disable memory remap above 4GB.
MRC Fast Boot	Disabled **Enabled**	Enable/Disable MRC fast boot. Skips memory training if memory configuration not changed.

Graphics Configuration

Parameter	Value	Comment
Primary Display	**Auto** IGFX PEG PCIe	Select which of IGFX/PEG/PCIe Graphics Device should be Primary Display.
Internal Graphics	**Auto** Disabled Enabled	Keep IGFX enabled based on the setup options.
Aperture Size	128MB – 2048MB **(256MB default)**	Select the Aperture Size. Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Pre-Allocated	0MB – 64MB **(32MB default)**	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128MB **256MB** MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

PEG Port Configuration

Parameter	Value	Comment
PEG Configuration	**1x16** 2x8 1x8 + 2x4	Select PEG port link width configuration.
Enable Root Port	Disabled Enabled **Auto**	Enable or Disable the Root Port.
Max Link Speed	**Auto** Gen1 Gen2 Gen3	Configure PEG Max Speed.
Max Link Width	**Auto** Force X1 Force X2 Force X4 Force X8	Force PEG link to retrain to X1/2/4/8
ASPM	**Disabled** Auto ASPM L0s ASPM L1 ASPM L0sL1	Control ASPM support for the PEG Device. This has no effect if PEG is not the currently active device.
ASPM L0s	Root Port Only Endpoint Port Only **Both Root and Endpoint Ports**	Enable PCIe ASPM L0s.
De-emphasis Control	-6 dB **-3.5 dB**	Configure the De-emphasis control on PEG.
PEG Max Payload Size	**Auto** 128 256 TLP	Select PEG Max Payload Size; Choose Auto (Default Device Capability) or force to 128/256 Bytes.

PCH-IO Configuration

Parameter	Value	Comment
PCI Express Configuration	Submenu	PCI Express Configuration settings
SATA Configuration	Submenu	SATA Device Options Settings
USB Configuration	Submenu	USB Configuration settings
HD Audio	Disabled **Enabled**	Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled. Enabled = HDA will be unconditionally Enabled.
PCH LAN Controller	**Enabled** Disabled	Enable/Disable onboard NIC.
Wake on LAN	**Enabled** Disabled	Enable/Disable integrated LAN to wake the system.
Restore AC Power Loss	Power Off **Power On** Last State	Select AC power state when power is re-applied after a power failure. Power Off and Last State need a RTC battery in the system.

PCI Express Configuration

Parameter	Value	Comment
DMI Link ASPM Control	Disabled L0s L1 L0sL1 **Auto**	The control of Active State Power Management of the DMI Link.
PCIe Function Swapping	Disabled **Enabled**	Enable/Disable PCI Express Root Port Function Swapping. \nWhen disabled and any function other than 0th is enabled, 0th will become visible.
PCI Express Root Port	Submenu	PCI Express Root Port Settings.

PCI Express Lane

Parameter	Value	Comment
PCI Express Root Port	Disabled **Enabled**	Control the PCI Express Root Port.
ASPM	**Disabled** L0s L1 L0sL1 Auto	Set the ASPM Level: Force all links to appropriate ASPM state, or Auto negotiate ASPM configuration or Disable ASPM.
PME SCI	Disabled **Enabled**	Enable/Disable PCI Express Powermanagement System Control Interrupt.
Hot Plug	Enabled **Disabled**	Enable/Disable PCI Express Hot Plug.
PCIe Speed	**Auto** Gen1 Gen2	Select PCI Express Port speed.
Extra Bus Reserved	0 – 7 **(0 default)**	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	1 – 20 **(10 default)**	Reserved memory (1-20MB) for this Root Bridge.
Reserved I/O	4 – 20 **(4 default)**	Reserved I/O (4kB/8kB/12kB/16kb/20kB) Range for this Root Bridge.

SATA Configuration

Parameter	Value	Comment
SATA Controller	**Enabled** Disabled	Enable/Disable SATA Device.
SATA Mode Selection	**AHCI** Intel RST	Determines how SATA controller operate.
Aggressive LPM Support	Disabled **Enabled**	Enable PCH to aggressively enter link power state.
SATA Controller Speed	**Default** Gen1 Gen2 Gen3	Default configures controller speed to max supported speed of connected devices. Other values limit speed to according value.
SATA Port	Disabled **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled** Enabled	Designates this port as Hot Pluggable.

USB Configuration

Parameter	Value	Comment
USB Per-Port Disable	**Disabled** Enabled	Enable/Disable the corresponding USB port from reporting a Device Connection to the controller. If all ports are disabled, setup cannot be entered anymore with USB keyboard.
USB Port	Disabled **Enabled**	Enable/Disable USB Port.

Security

Parameter	Value	Comment
Administrator Password		Set Administrator Password
User Password		Set User Password
User Password Policy	Setup Boot Boot + Setup	Setup: Password is necessary to enter Setup. Boot: Password is needed for starting system. If Administrator Password is also active, Setup can only be entered with Administrator Password. Boot+Setup: Password needed during POST, enter setup with User Password possible.
HDD Security	Submenu	HDD Security Configuration for selected drive.
Secure Boot	Submenu	Customizable Secure Boot settings.

HDD Security Configuration

Parameter	Value	Comment
Set User Password		Set HDD User Password.

Secure Boot Configuration

Parameter	Value	Comment
Secure Boot	**Disabled** Enabled	Secure Boot can be enabled if: 1. System running in User mode with enrolled Platform Key (PK). 2. CSM function is disabled.
Secure Boot Mode	Standard **Custom**	Secure Boot mode selector: In Custom mode Secure Boot Variables can be configured without authentication.
Restore Factory Keys	Function Key	Force System to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode	Function Key	Delete all Secure Boot key databases from NVRAM.
Key Management	Submenu	Enables expert users to modify Secure Boot Policy variables without full authentication.

Key Management

Note: Default Secure Boot Keys PK and KEK should be updated by OEM PK and KEK Keys.

Parameter	Value	Comment
Factory Key Provision	**Disabled** Enabled	Install factory default Secure Boot keys when System is in Setup Mode.
Restore Factory Keys	Function Key	Force System to User Mode. Install factory default Secure Boot key databases.
Reset to Setup Mode	Function Key	Delete all Secure Boot key databases from NVRAM.
Export Secure Boot variables	Function Key	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.
Enroll Efi Image	Function Key	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).
Remove 'UEFI CA' from DB	Function Key	Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature databes (db).
Restore DB defaults	Function Key	Restore DB variable to factory defaults.
Platform Key (PK)	Function Key	**Enroll Factory Defaults or load certificates from a** file: **1. Public Key Certificate in:** a)EFI_SIGNATURE_LIST **b)EFI_CERT_X509 (DER encoded)** c)EFI_CERT_RSA2048 (bin) **d)EFI_CERT_SHA256 (bin)** 2. Authenticated UEFI Variable **3. EFI PE/COFF Image (SHA256)** Key source: Default, External, Mixed, Test
Key Exchange Keys	Function Key	
Authorized Signatures	Function Key	
Forbidden Signatures	Function Key	
Authorized TimeStamps	Function Key	
OsRecovery Signatures	Function Key	

Boot

Port Based

Parameter	Value	Comment
Setup Prompt Timeout	1 – 65535 **(1 default)**	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard NumLock state.
Quiet Boot	**Disabled** Enabled	Enables or disables Quiet Boot option.
Fast Boot	**Disabled** Enabled	Enables/disables boot with initialization of a minimal set of devices required to launch active boot option.
SATA Support	**Last Boot HDD Only** All Sata Devices	Select if only last HDD booted or all SATA HDD should be initialized.
NVMe Support	Disabled **Enabled**	If Disabled, NVMe device will be skipped.
VGA Support	Auto **EFI Driver**	If Auto, only install Legacy OpROM with Legacy OS. Logo would NOT be shown during post. Efi driver will still be installed with EFI OS.
USB Support	Disabled **Full Initial** Partial Initial	If Disabled, all USB devices will NOT be available until OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Device Support	**Disabled** Enabled	If Disabled, PS2 devices will be skipped.
Network Stack Driver Support	**Disabled** Enabled	If Disabled, Network Stack Driver will be skipped.
Redirection Support	**Disabled** Enabled	If Disabled, Redirection function will be disabled.
Popup Boot Menu	Disabled **Enabled**	Enable/Disable Popup Boot Menu.
New Boot Option Policy	Default **Place First** Place Last	Controls the placement of newly detected UEFI boot options.
Boot Menu Mode	Device Based **Port Based**	Device: Choose Boot Option by Device, Port: Choose Boot Option by Type. Need to reset and enter setup again for changes.
USB Boot Devices	**Grouped** By Port	Show all USB Boot Devices in one group or show all USB Ports.
Boot Option Priorities	Depends on recognized devise	Sets the boot order. Priority of devices from same type can be selected in BBS priority menus.
USB Priorities	Submenu	Set the order of the devices in this group. Appears if more than 1 device of this group is connected.

Device Based

Parameter	Value	Comment
Boot Option Priorities	Depends on recognized devise	Sets the boot order. Priority of devices from same type can be selected in Priority Submenus.
Hard Drive BBS Priorities	Submenu	Set the order of the legacy devices in this group. Appears if more than 1 legacy device of this group is connected.
USB Device BBS Priorities	Submenu	Set the order of the legacy devices in this group. Appears if more than 1 legacy device of this group is connected.

Save & Exit

Parameter	Value	Comment
Save Changes and Exit	Function Key	Exit system setup after saving the changes.
Discard Changes and Exit	Function Key	Exit system setup without saving any changes.
Save Changes and Reset	Function Key	Reset the system after saving the changes.
Discard Changes and Reset	Function Key	Reset system setup without saving any changes.
Save Changes	Function Key	Save Changes done so far to any of the setup options.
Discard Changes	Function Key	Discard Changes done so far to any of the setup options.
Restore Defaults	Function Key	Restore/Load Default values for all the setup options.
Save as User Defaults	Function Key	Save the changes done so far as User Defaults.
Restore User Defaults	Function Key	Restore the User Defaults to all the setup options.
Boot Override	Depends on recognized devise	Boots to selected device.
Launch EFI Shell from filesystem device	Function Key	Attempts to Launch EFI Shell application (shell.efi) from one of the available filesystem devices.

This page intentionally left blank.

DATA MODUL

Headquarters:

DATA MODUL AG
Landsberger Str. 322
DE-80687 Munich - Germany
Phone: +49-89-56017-0
Fax: +49-89-56017-119
www.data-modul.com

Logistics, Production & Services:

DATA MODUL Weikersheim GmbH
Lindenstrasse 8
DE-97990 Weikersheim - Germany
Phone: +49-7934-101-0
Fax: +49-7934-101-101

Subsidiaries & Sales Offices:

Germany – Hamburg
Germany – Duesseldorf
Denmark
Dubai
Finland/Baltic
France
Italy
Singapore
Spain
Switzerland
UK
USA

DATA MODUL's worldwide offices
can be found on our website:
www.data-modul.com/eu/sm/contact-us/offices.html

10.2013

DIN-EN-ISO 9001/14001 | www.data-modul.com