ООО «ТЕХНОЛИД»

БАЗОВАЯ СИСТЕМА ВВОДА-ВЫВОДА ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ НА БАЗЕ ПРОЦЕССОРОВ x86

Руководство пользователя

Версия 1.0.1

2025 г.

NIMBUS

Содержание

1. Main (Главное меню) 6
2. Advanced (Расширенное меню) 8
2.1 Trusted Computing 10
2.2 Redfish Host Interface Settings 11
2.3 ACPI Settings 12
2.4 UEFI Variables Protection 13
2.5 Serial Port Console Redirection 14
2.6 SIO Common Setting 15
2.7 SIO Configuration 16
2.8 Option ROM Dispatch Policy 17
2.9 PCI Subsystem Settings 18
2.10 USB Configuration 19
2.11 Network Stack Configuration 21
2.12 CSM Configuration 22
2.13 NVMe Configuration 23
2.14 Emulation Configuration 24
2.15 Tls Auth Configuration 25
2.16 All Cpu Information 26
2.17 RAM Disk Configuration 27
3. Platform Configuration 28
3.1 PCH-IO Configuration 29
3.2 PCH-IO Expander Configuration 32
3.3 Miscellaneous Configuration 33
3.4 Server ME Configuration 34
3.5 Server ME Debug Configuration 35
3.6 Runtime Error Logging 36
3.7 Reserve Memory 37
4. Socket Configuration 38
4.1 Processor Configuration 39
4.2 Common RefCode Configuration 41

4.3 Uncore Configuration 42
4.4 Memory Configuration 43
4.5 IIO Configuration 46
4.6 Advanced Power Management Configuration 47
5. Server Mgmt 47
5.1 System Event Log 49
5.2 BMC self test log 50
5.3 BMC network configuration 51
6. Security 52
6.1 Secure Boot 53
7. Boot 54
8. Save & Exit 56

Базовая система ввода-вывода для систем хранения данных на базе процессоров x86 записывает аппаратные параметры системы в EFI на материнской плате. Его основные функции включают проведение самотестирования при включении питания (POST) во время запуска системы, сохранение системных параметров, загрузку операционной системы и т. д.

Базовая система ввода-вывода для систем хранения данных на базе процессоров x86 включает программу настройки BIOS, которая позволяет пользователю изменять основные параметры конфигурации системы или активировать определенные системные функции. Когда питание выключено, батарея на материнской плате подает необходимое питание на CMOS для сохранения значений конфигурации в CMOS.

Чтобы получить доступ к программе настройки BIOS, нажать клавишу <DEL> во время POST при включении питания.

Перепрошивка BIOS потенциально рискованная процедура, если у вас не возникло никаких проблем при использовании текущей версии BIOS, рекомендуется не перепрошивать BIOS. Перепрошивать BIOS следует с осторожностью. Неправильная перепрошивка BIOS может привести к сбою в работе системы.

Рекомендуется не изменять настройки по умолчанию (если это не требуется), чтобы предотвратить нестабильность системы или другие неожиданные результаты. Неправильное изменение настроек может привести к сбою загрузки системы. Если это произошло, необходимо очистить значения CMOS и сбросить плату до значений по умолчанию. (См. раздел «Выход» в этой главе или введение в перемычку батареи/очистки CMOS в Главе 1, чтобы узнать, как очистить значения CMOS.)

Функциональные клавиши программы настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86

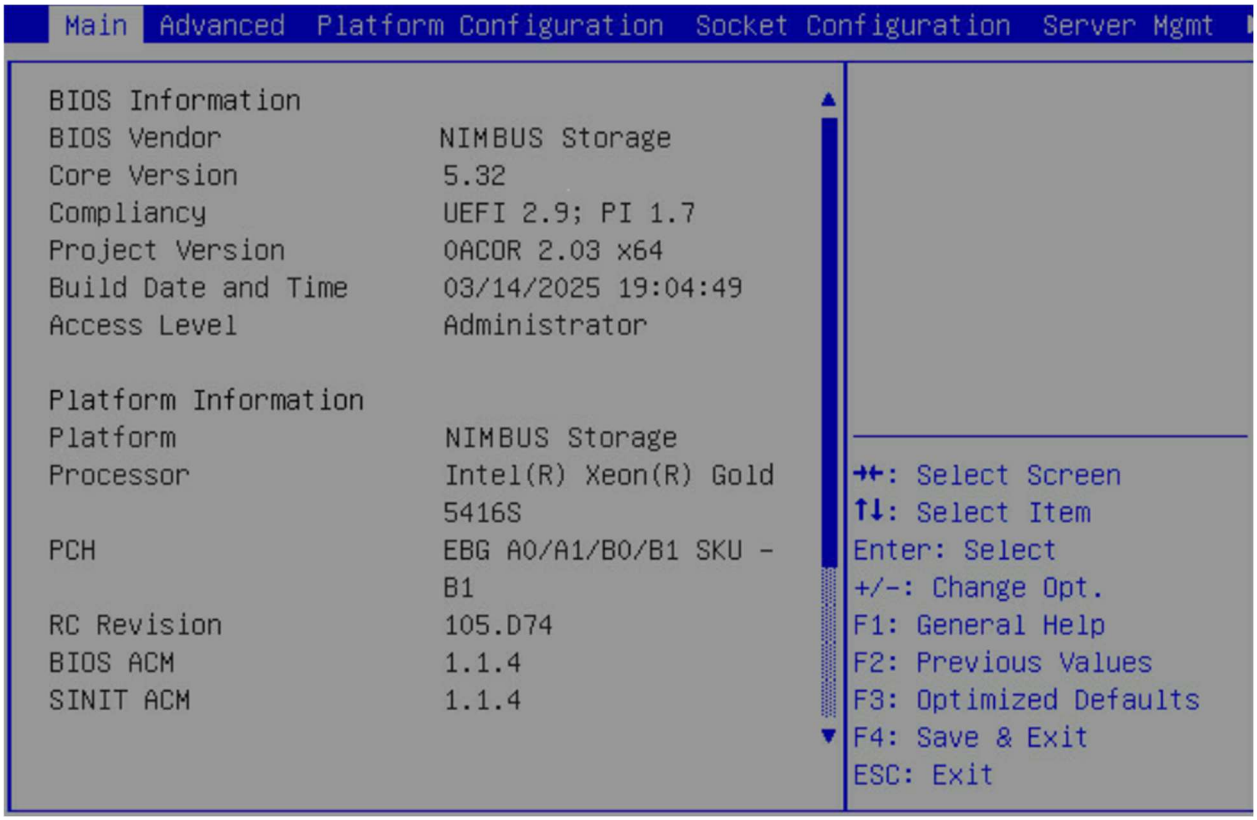
Функциональные клавиши	Назначение
<⇦><⇨>	Переместить полосу выбора, чтобы выбрать экран
<⇧>< ⇩>	Переместить полосу выбора, чтобы выбрать элемент
<+>	Увеличить числовое значение или внести изменения
<->	Уменьшить числовое значение или внести изменения
<Enter>	Выполнить команду или войти в подменю
<Esc>	Главное меню: Выход из программы настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86 Подменю: Выход из текущего подменю
<F1>	Отобразить экран справки
<F3>	Восстановить предыдущие настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86 для текущих подменю
<F9>	Загрузить оптимизированные настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86 по умолчанию для текущих подменю
<F10>	Сохранить все изменения и выйти из программы настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86
<k>, <m>	Переместить полосу выбора для справки

1. Main (Главное меню)

После входа в программу настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86 на экране отобразится Главное меню (как показано ниже). Использовать клавиши со стрелками для перемещения между элементами и нажать <Enter>, чтобы принять или войти в другое подменю.

Описание выделенного параметра настройки на экране отображается в нижней строке Главного меню. Справка по подменю.

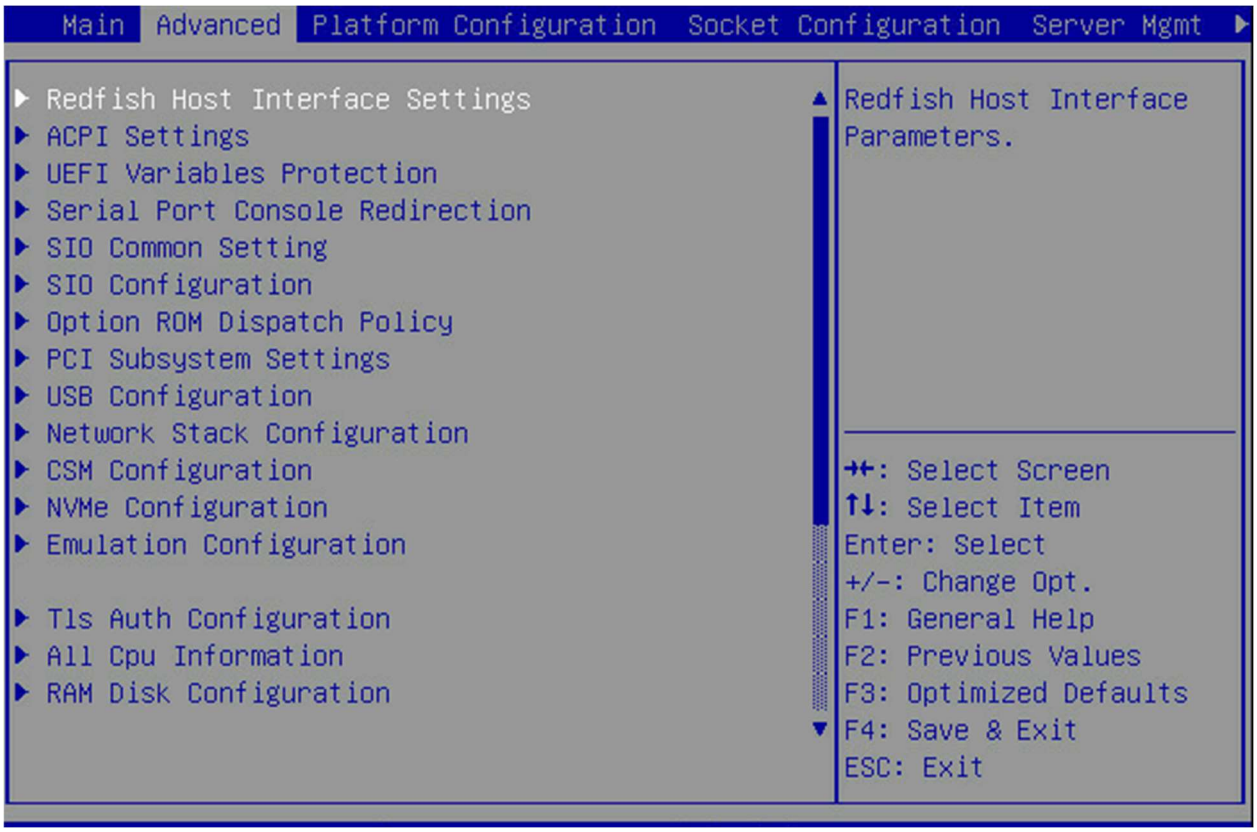
Находясь в подменю, нажать <F1>, чтобы отобразить экран справки (общая справка) функциональных клавиш, доступных для меню. Нажать <Esc>, чтобы выйти из экрана справки. Справка по каждому элементу находится в блоке справки по элементам в правой части подменю.



Элемент меню	Опция/Описание
BIOS Information	
BIOS Vendor	Отображение информации об имени вендора
Core Version	Отображение информации о версии ПО
Compliancy	Отображение информации о версии UEFI
Project Version	Отображение информации о версии проекта
Build Date and Time	Отображение информации о дате создания ПО
Access Level	Отображение информации об уровне пользователя
Platform Information	
Platform	Отображение информации об имени системы
Processor	Отображение информации об установленном процессоре
PCH	Отображение информации о PCH
RC Revision	Отображение информации о RC версии
BIOS ACM	Отображение информации о версии BIOS ACM
SINIT ACM	Отображение информации о версии SINIT ACM
Memory Information	
Total Memory	Отображение информации об установленной памяти
System Language	Выбор языка
System Date	Установка даты
System Time	Установка времени

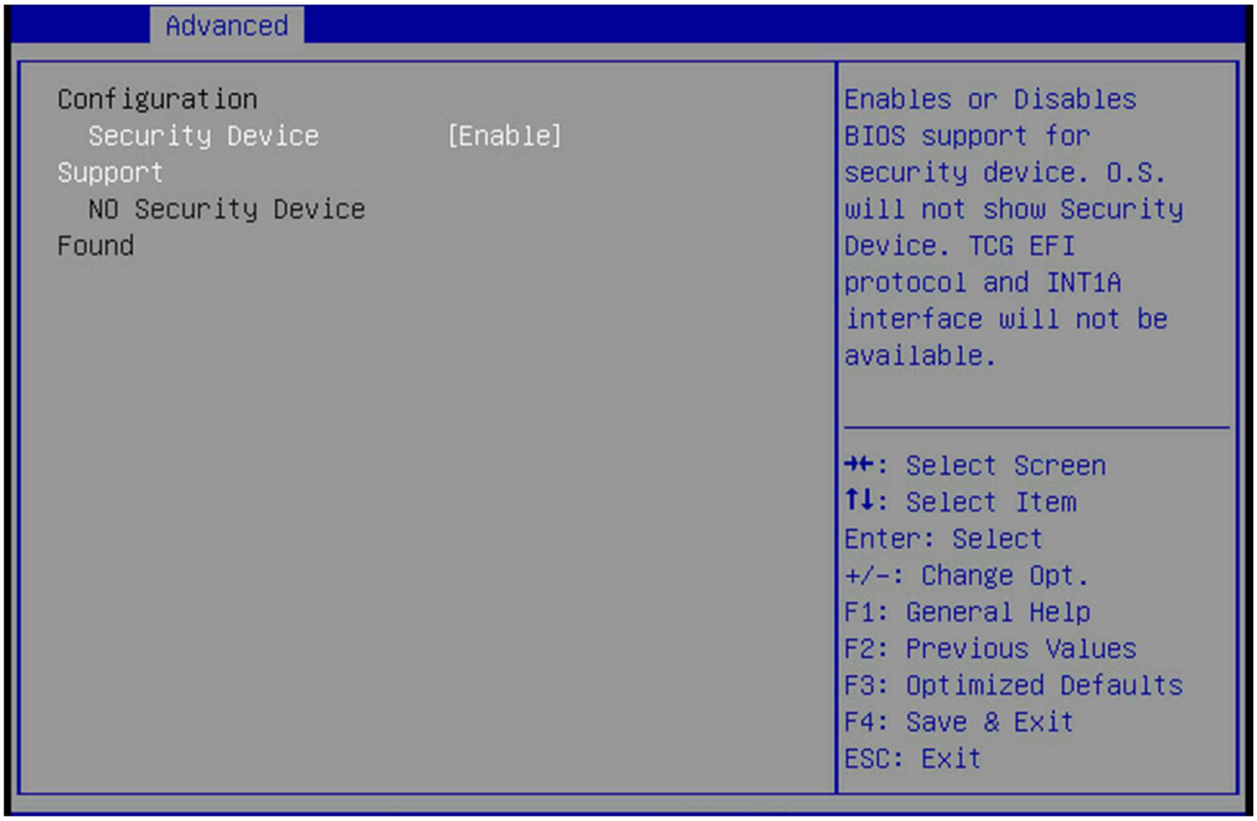
2. Advanced (Расширенное меню)

Расширенное меню отображает параметры подменю для настройки функций различных аппаратных компонентов. Выбрать элемент подменю, затем нажать <Enter>, чтобы получить доступ к соответствующему экрану подменю.



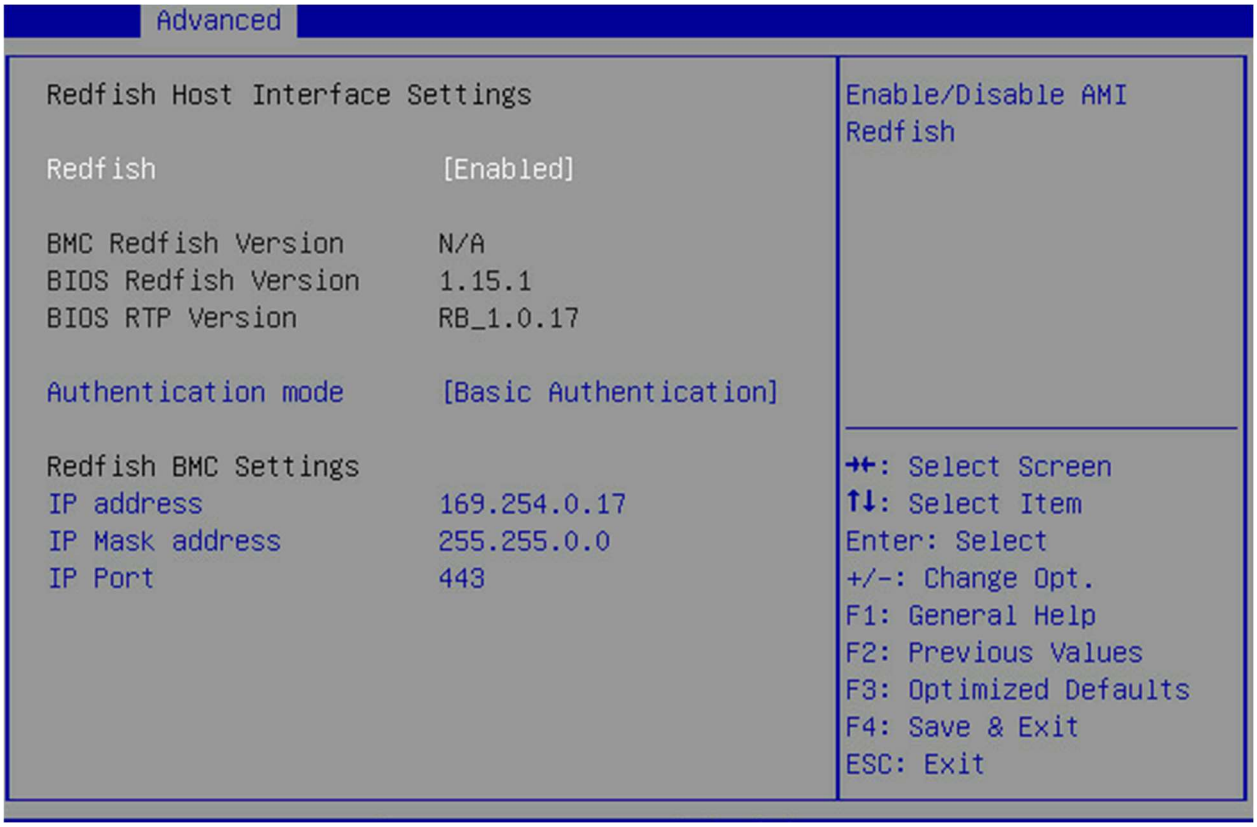
Элемент меню	Опция/Описание
Trusted Computing	Смотреть подменю > **Trusted Computing**
Redfish Host Interface Settings	Смотреть подменю > **Redfish Host Interface Settings**
ACPI Settings	Смотреть подменю > ACPI Settings
UEFI Variables Protection	Смотреть подменю > UEFI Variables Protection
Serial Port Console Redirection	Смотреть подменю > Serial Port Console Redirection
SIO Common Setting	Смотреть подменю > SIO Common Setting
SIO Configuration	Смотреть подменю > SIO Configuration
Option ROM Dispatch Policy	Смотреть подменю > Option ROM Dispatch Policy
PCI Subsystem Settings	Смотреть подменю > PCI Subsystem Settings
USB Configuration	Смотреть подменю > USB Configuration
Network Stack Configuration	Смотреть подменю > Network Stack Configuration
CSM Configuration	Смотреть подменю > CSM Configuration
NVMe Configuration	Смотреть подменю > NVMe Configuration
Emulation Configuration	Смотреть подменю > Emulation Configuration
Tls Auth Configuration	Смотреть подменю > Tls Auth Configuration
All Cpu Information	Информационная строка
RAM Disk Configuration	Смотреть подменю > RAM Disk Configuration
Qlogic QLE2692 16Gb FC Adapter 210034800D77ACB7	Смотреть подменю > Qlogic QLE2692 16Gb FC Adapter 210034800D77ACB7
Qlogic QLE2692 16GB FC Adapter 210034800D77ACB7	Смотреть подменю > Qlogic QLE2692 16GB FC Adapter 210034800D77ACB7
Broadcom <eHBA 9600-24i Tri-Mode Storage Adapter> Configuration Utility – 08.11.10.00	Смотреть подменю > Broadcom <eHBA 9600-24i Tri-Mode Storage Adapter> Configuration Utility – 08.11.10.00
Driver Health	Смотреть подменю > Driver Health

2.1 Trusted Computing



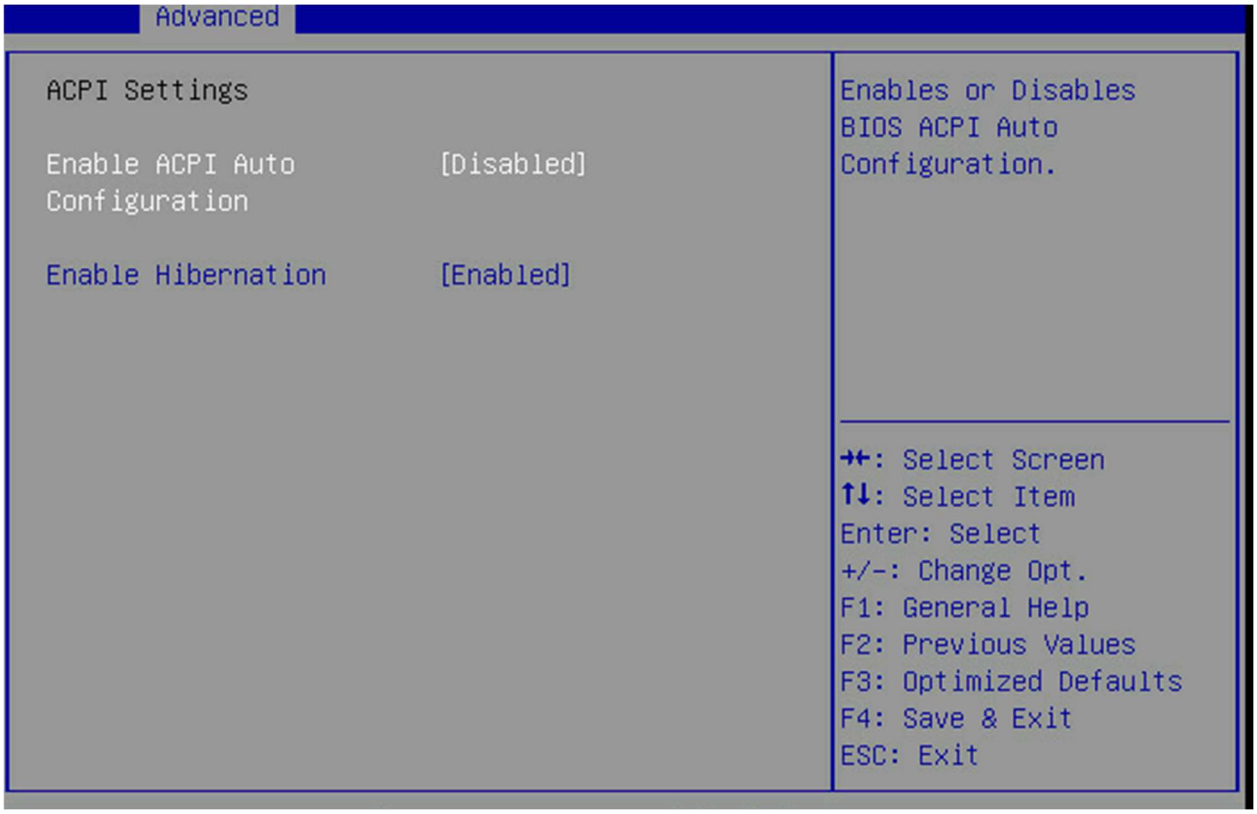
Элемент меню	Опция/Описание
Security Device Support	Enable/Disable Включает или отключает устройство поддержки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86. ОС не будет отображать устройство безопасности.

2.2 Redfish Host Interface Settings



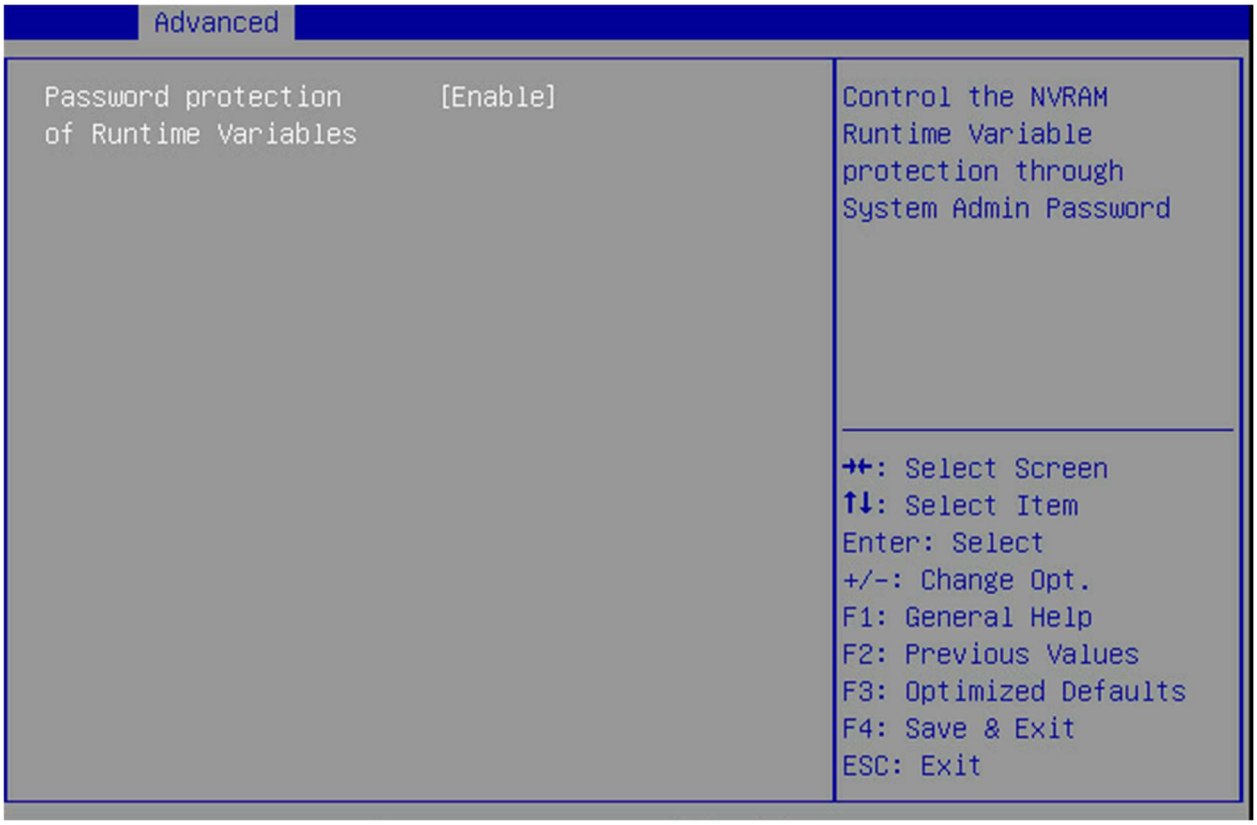
Элемент меню	Опция/Описание
Redfish	Enabled/Disabled Включает или отключает протокол Redfish
BMC Redfish Version	Версия BMC Redfish
BIOS Redfish Version	Весрия BIOS Redfish
BIOS RTP Version	Весрия BIOS RTP
Authentication mode	Basic Authentication/Session Authentication. Выбор режима аутентификации
IP address	Установка IP адреса
IP Mask address	Установка маски подсети
IP Port	Установка IP порта

2.3 ACPI Settings



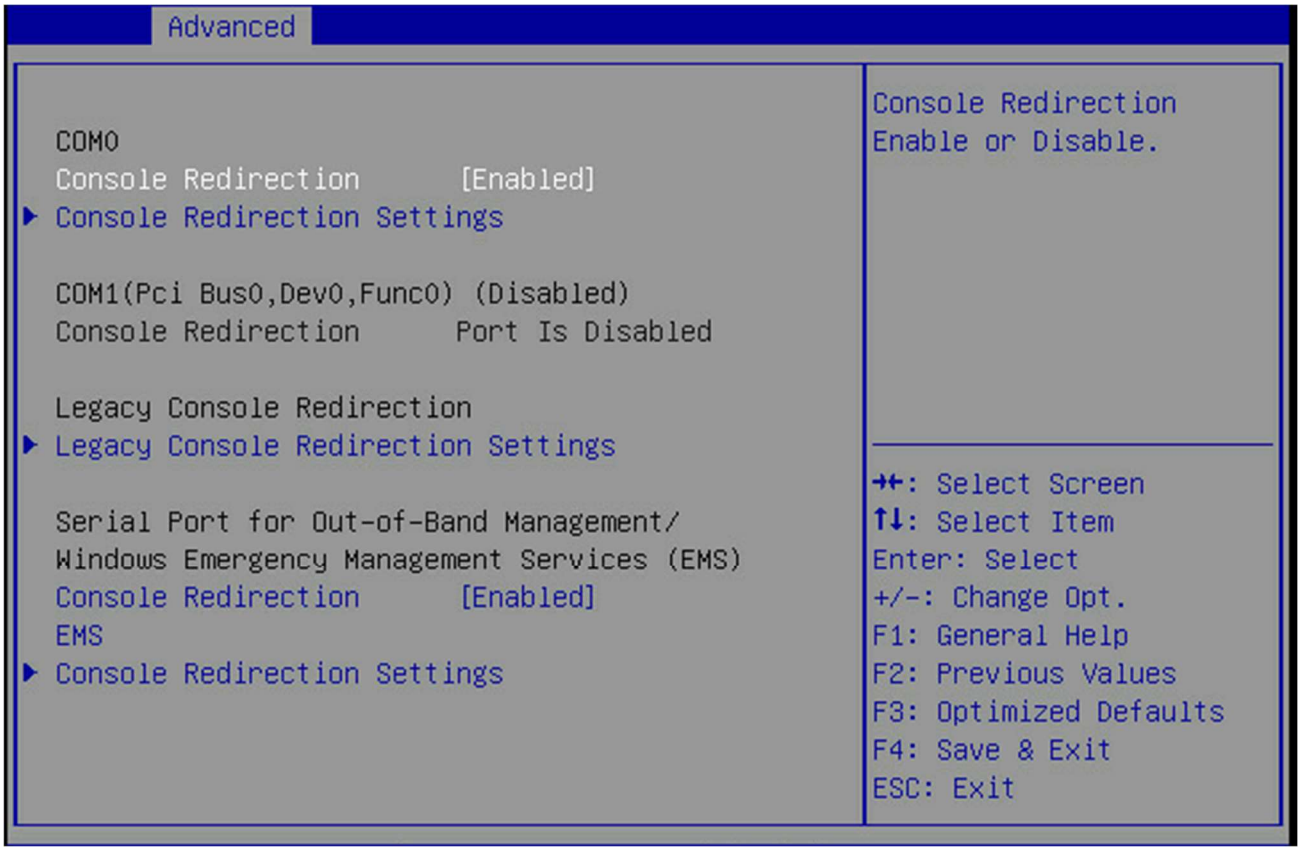
Элемент меню	Опция/Описание
Enable ACPI Auto	Enabled/Disabled Включает или отключает протокол BIOS ACPI
Enable Hibernation	Enabled/Disabled Включает или отключает Hibernation

2.4 UEFI Variables Protection



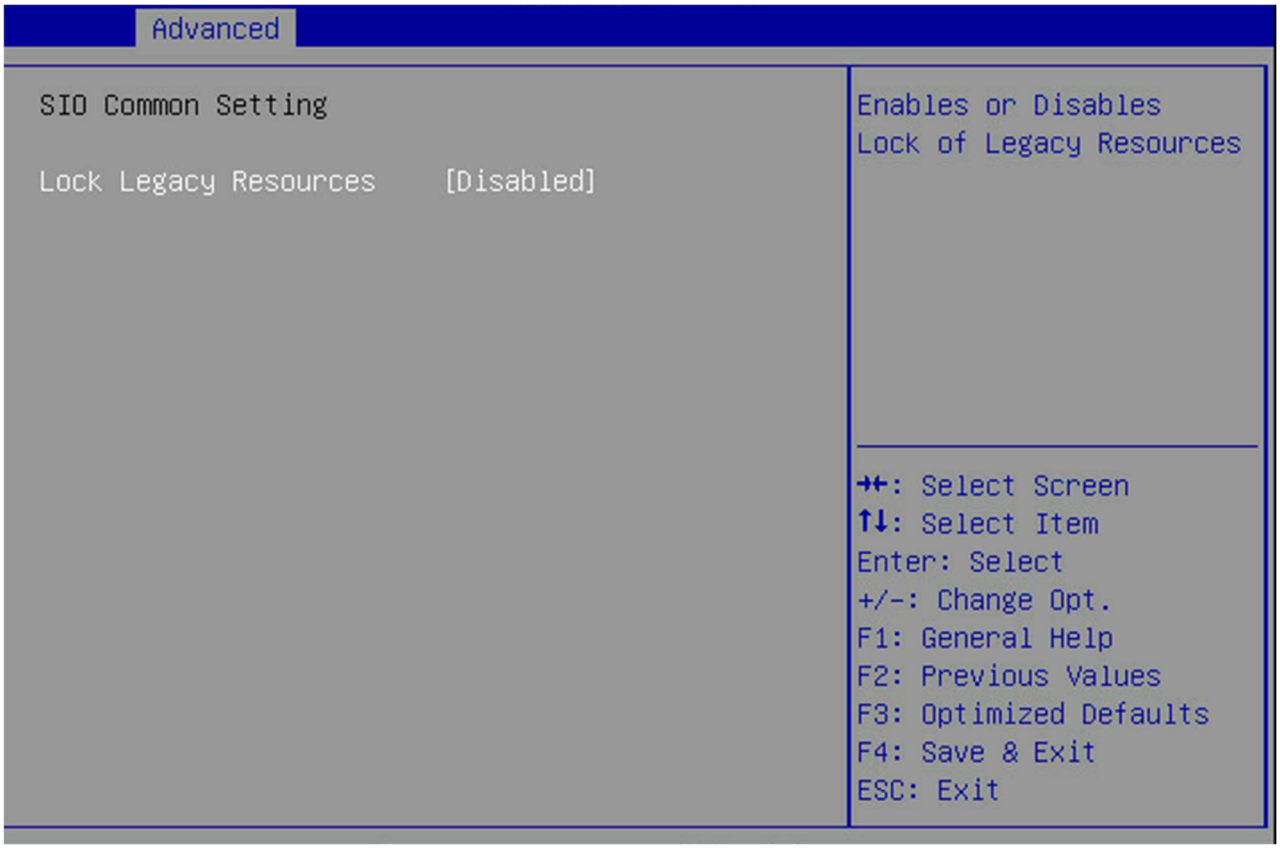
Элемент меню	Опция/Описание
Password protection of Runtime Variables	Enable/Disable. Управление защитой NVRAM Runtime Variable при помощи пароля системного администратора.

2.5 Serial Port Console Redirection



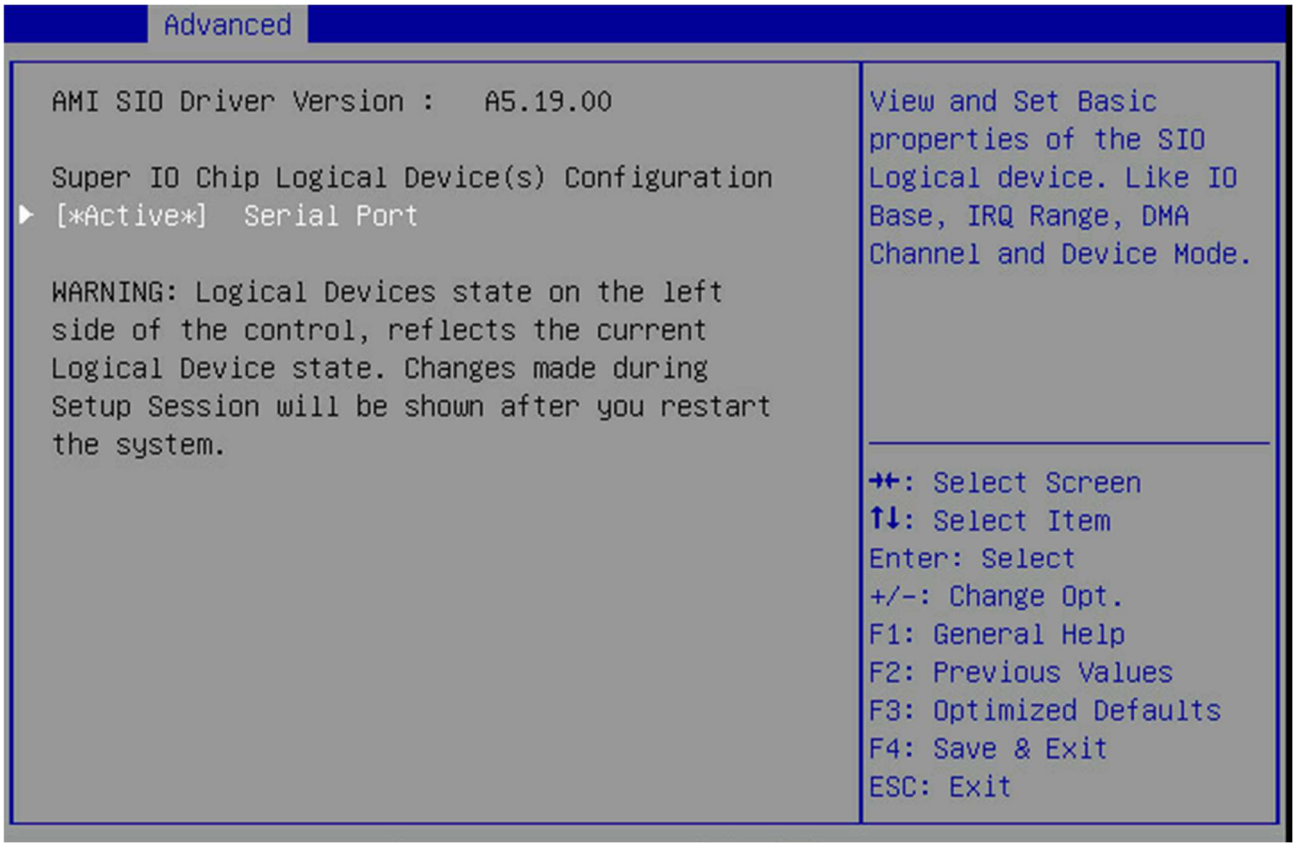
Элемент меню	Опция/Описание
Console Redirection	Enabled/Disabled. Включение или выключение Console
Console Redirection Settings	Настройки определяют, как хост-компьютер и удаленный компьютер (который использует пользователь) будут обмениваться данными. Оба компьютера должны иметь одинаковые или совместимые настройки
Legacy Console Redirection Settings	смотреть подменю > Legacy Console Redirection Settings
Console Redirection EMS	Enabled/Disabled.
Console Redirection Settings	Настройки определяют, как хост-компьютер и удаленный компьютер (который использует пользователь) будут обмениваться данными. Оба компьютера должны иметь одинаковые или совместимые настройки

2.6 SIO Common Setting



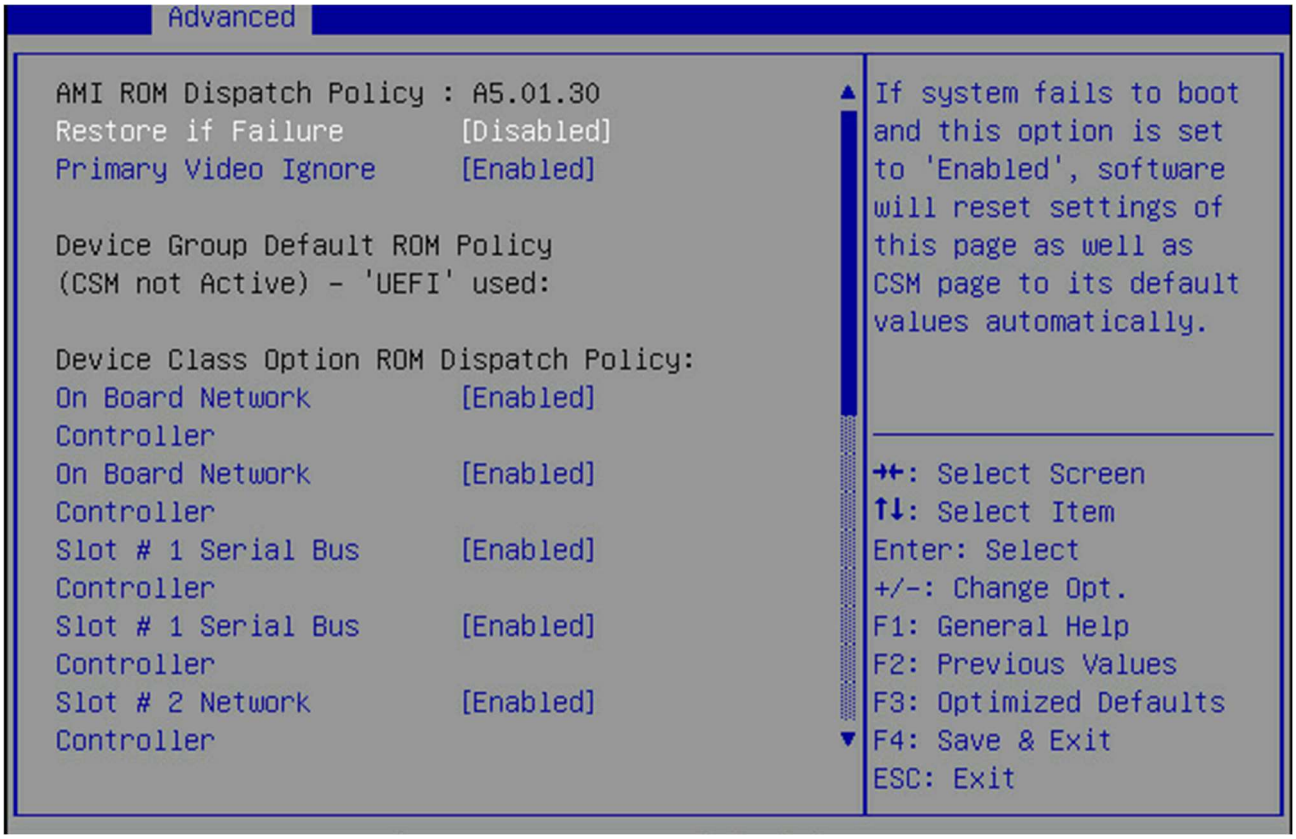
Элемент меню	Опция/Описание
Lock Legacy Resources	Enabled/Disabled. Включение или отключение Lock Legacy Resources

2.7 SIO Configuration



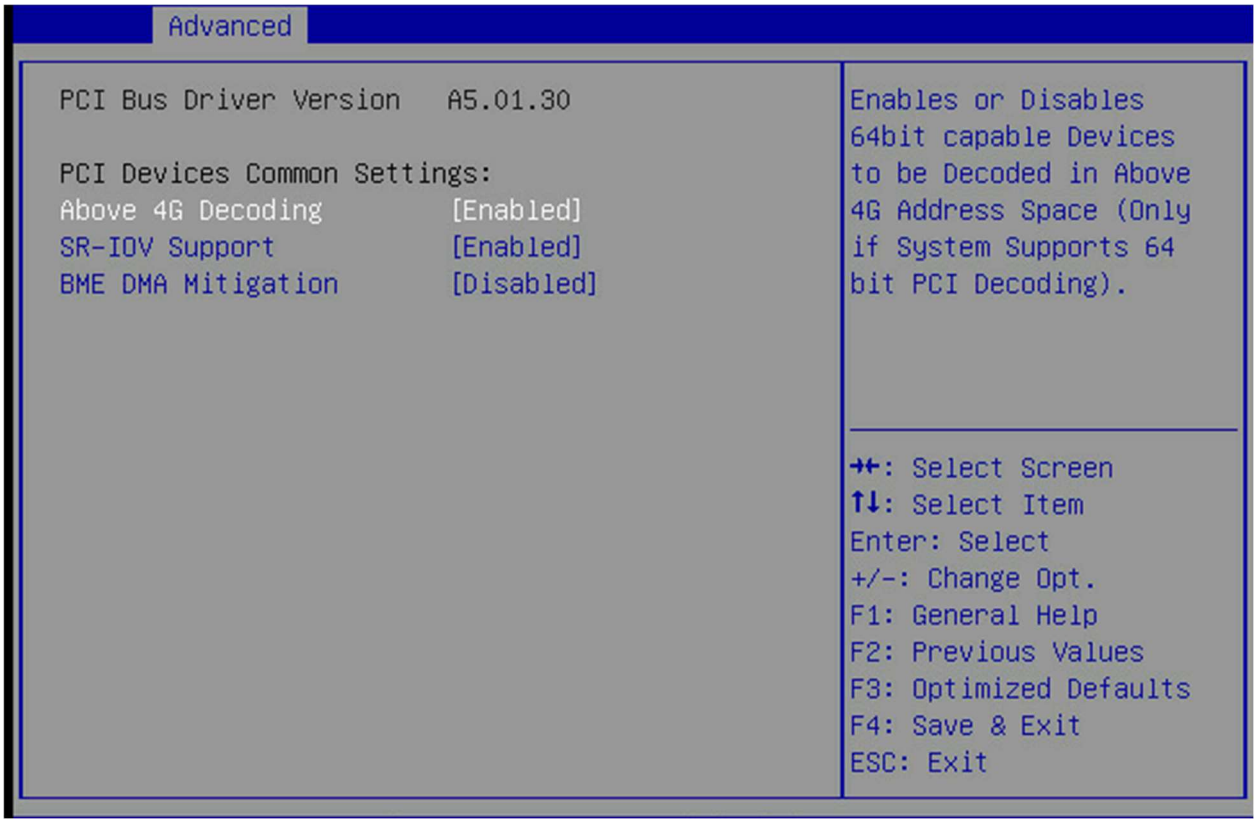
Элемент меню	Опция/Описание
[*Active*] Serial Port	Просмотр и настройка основных свойств логического устройства SIO. Например, IO Base, IRQ Range, DMA Channel и Device Mode.

2.8 Option ROM Dispatch Policy



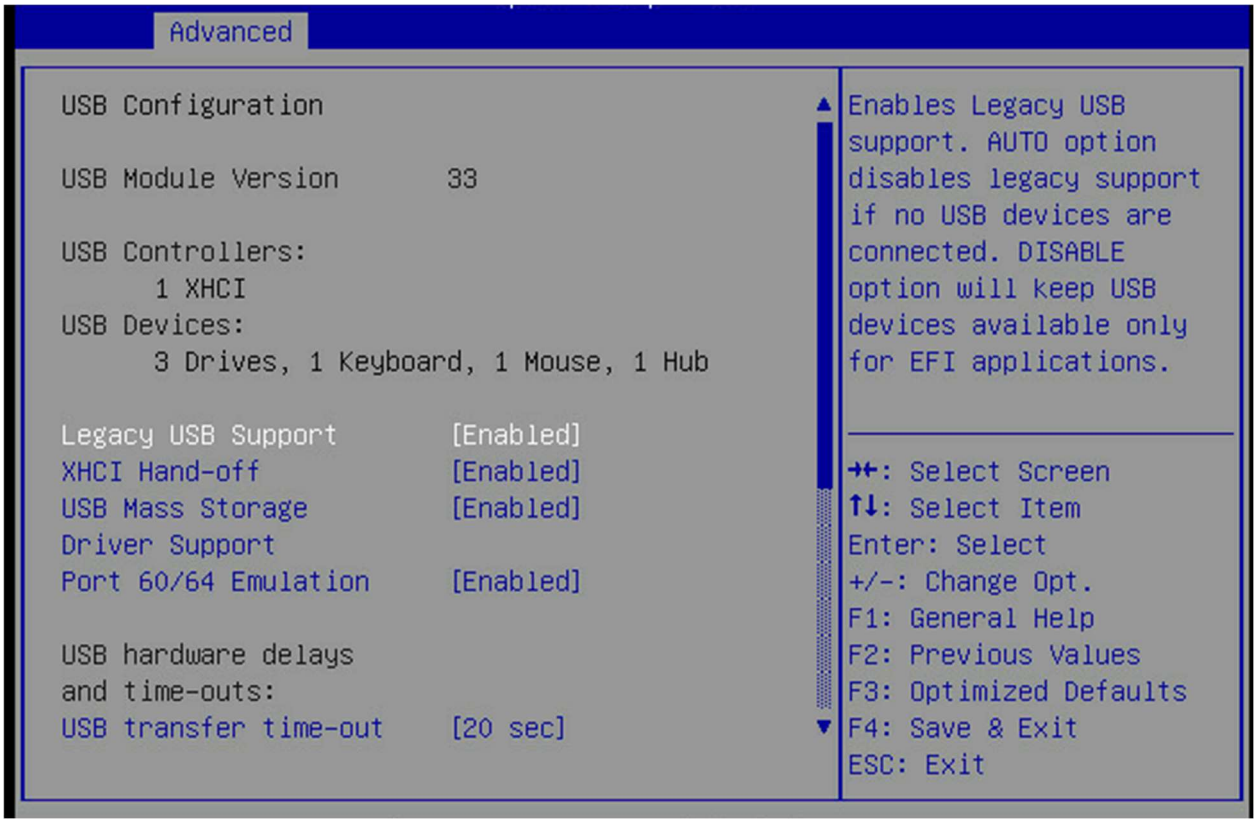
Элемент меню	Опция/Описание
Restore if Failure	Enabled/Disabled. Если система не загружается и эта опция включена, программное обеспечение автоматически сбросит настройки этой страницы, а также страницы CSM до значений по умолчанию.
Primary Video Ignore	Enabled/Disabled. Если система обнаружит, что из-за настроек политики дополнительное ПЗУ основного видеоустройства не будет отправляться, она проигнорирует настройки политики этого устройства и восстановит его в состояние «Включить».
Slot #1 / #2 / #3 / #4 / #5	Enabled/Disabled.

2.9 PCI Subsystem Settings



Элемент меню	Опция/Описание
Above 4G Decoding	Enabled/Disabled. Включает или отключает декодирование 64-битных устройств в адресном пространстве выше 4G (только если система поддерживает 64-битное декодирование PCI)
SR-IOV Support	Enabled/Disabled. Если в системе имеются устройства PCIe с поддержкой SR-IOV, этот параметр включает или отключает поддержку виртуализации Single Root IO.
BME DMA Mitifation	Enabled/Disabled. Повторное включение атрибута Bus Master, отключенного во время перечисления PCI для мостов PCI после блокировки SMM

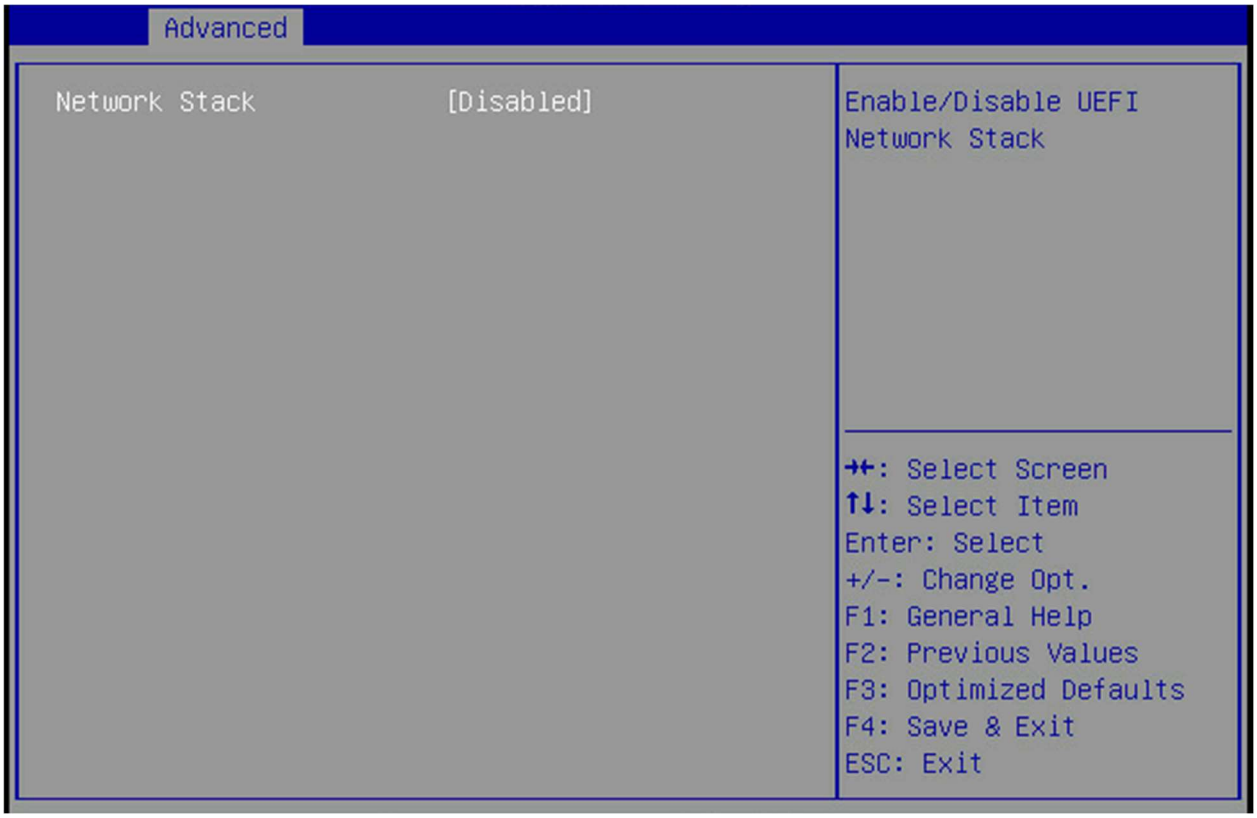
2.10 USB Configuration



Элемент меню	Опция/Описание
Legacy USB Support	Enabled/Disabled. Включение или отключение.
XHCI Hand-off	Enabled/Disabled. Включение или отключение.
USB Mass Storage Driver Support	Enabled/Disabled. Включение или отключение.
Port 60/64 Emulation	Enabled/Disabled. Включение или отключение.
USB transfer time-out	1/5/10/20 секунд. Значение тайм-аута для передач Control, Bulk и Interrupt
Device reset time-out	10/20/30/40 секунд. Истекло время ожидания команды «Запустить устройство» на USB-накопителе
Device power-up delay	Auto/Manual. Максимальное время, которое потребуется устройству, прежде чем оно сообщит о себе хост-контроллеру. «Авто» использует значение по умолчанию: для корневого порта это 100

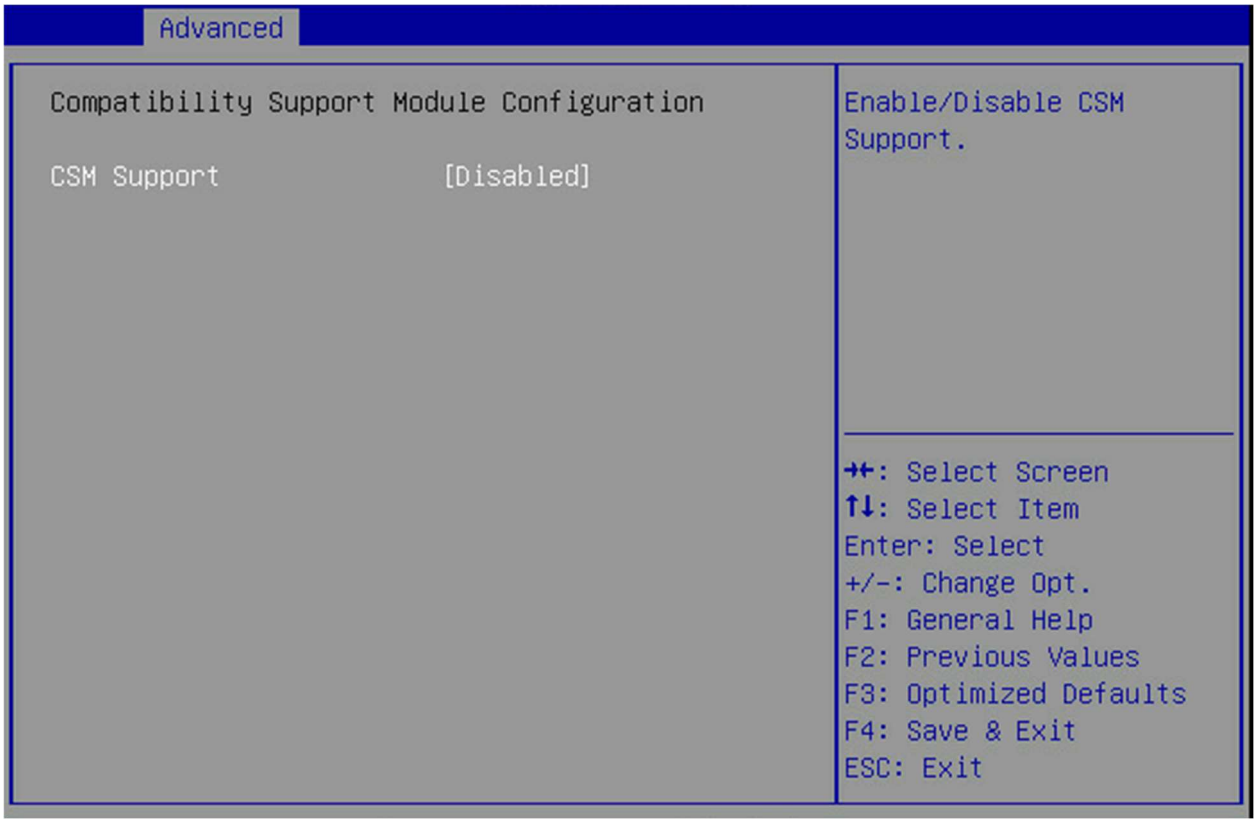
	мс, для порта концентратора задержка берется из дескриптора концентратора
Virtual CDROM0	Auto/Floppy/Forced FDD/Hard Disk/CD-ROM. Тип эмулирования. «AUTO» перечисляет устройства в соответствии с их форматом носителя. Оптические приводы эмулируются как «CDROM», приводы без носителя будут эмулироваться в соответствии с типом привода
Virtual HDisk0	Auto/Floppy/Forced FDD/Hard Disk/CD-ROM. Тип эмулирования. «AUTO» перечисляет устройства в соответствии с их форматом носителя. Оптические приводы эмулируются как «CDROM», приводы без носителя будут эмулироваться в соответствии с типом привода

2.11 Network Stack Configuration



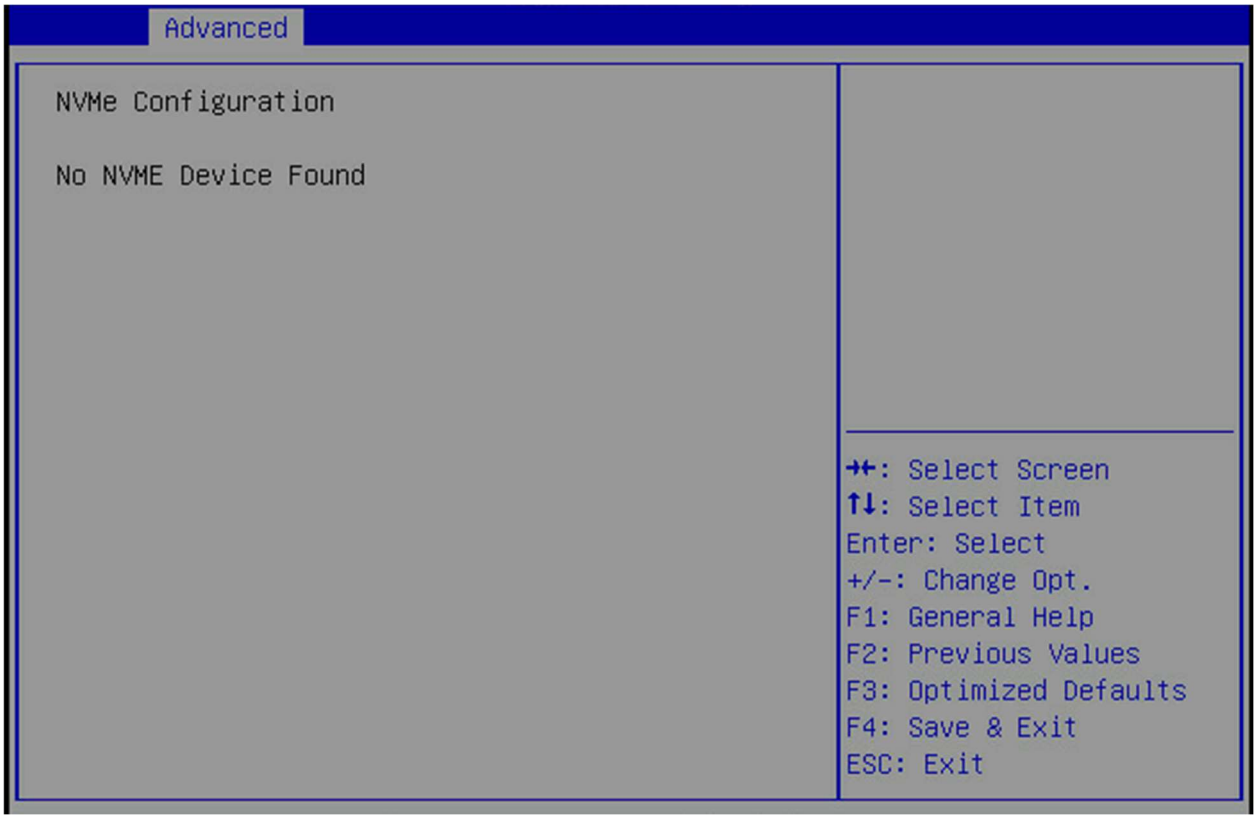
Элемент меню	Опция/Описание
Network Stack	Enabled/Disabled. Включение или отключение UEFI Сетевого стэка.

2.12 CSM Configuration



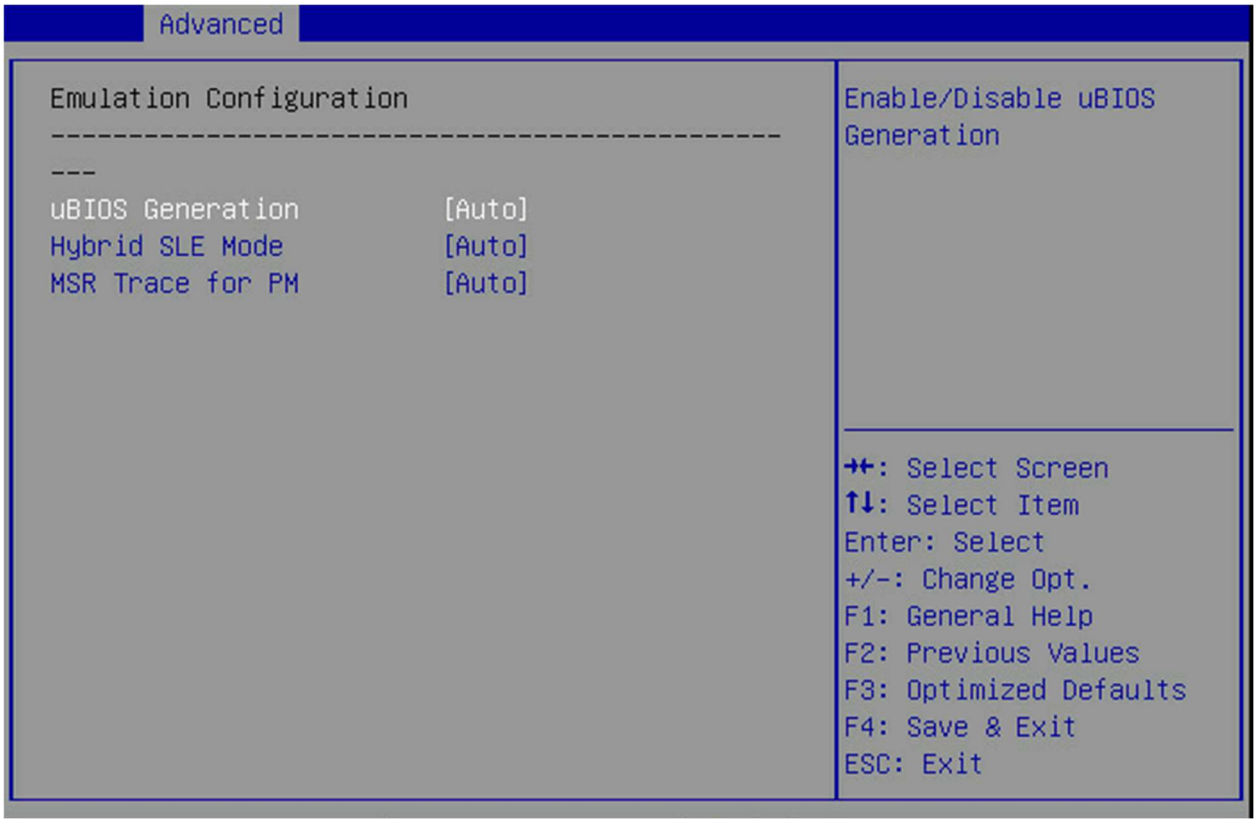
Элемент меню	Опция/Описание
CSM Support	Enabled/Disabled. Включение или отключение CSM поддержку.

2.13 NVMe Configuration



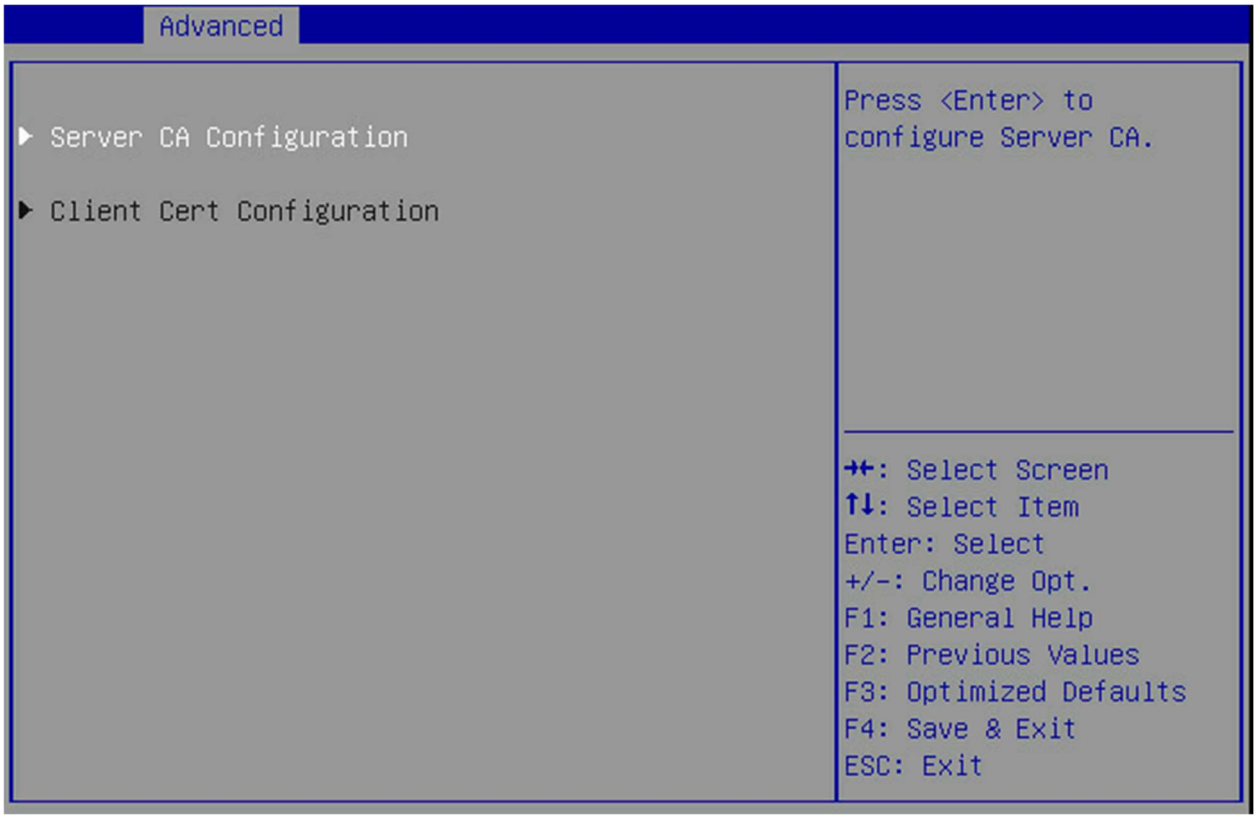
Элемент меню	Опция/Описание
NVMe Configuration	Отображение информации о NVMe устройствах

2.14 Emulation Configuration



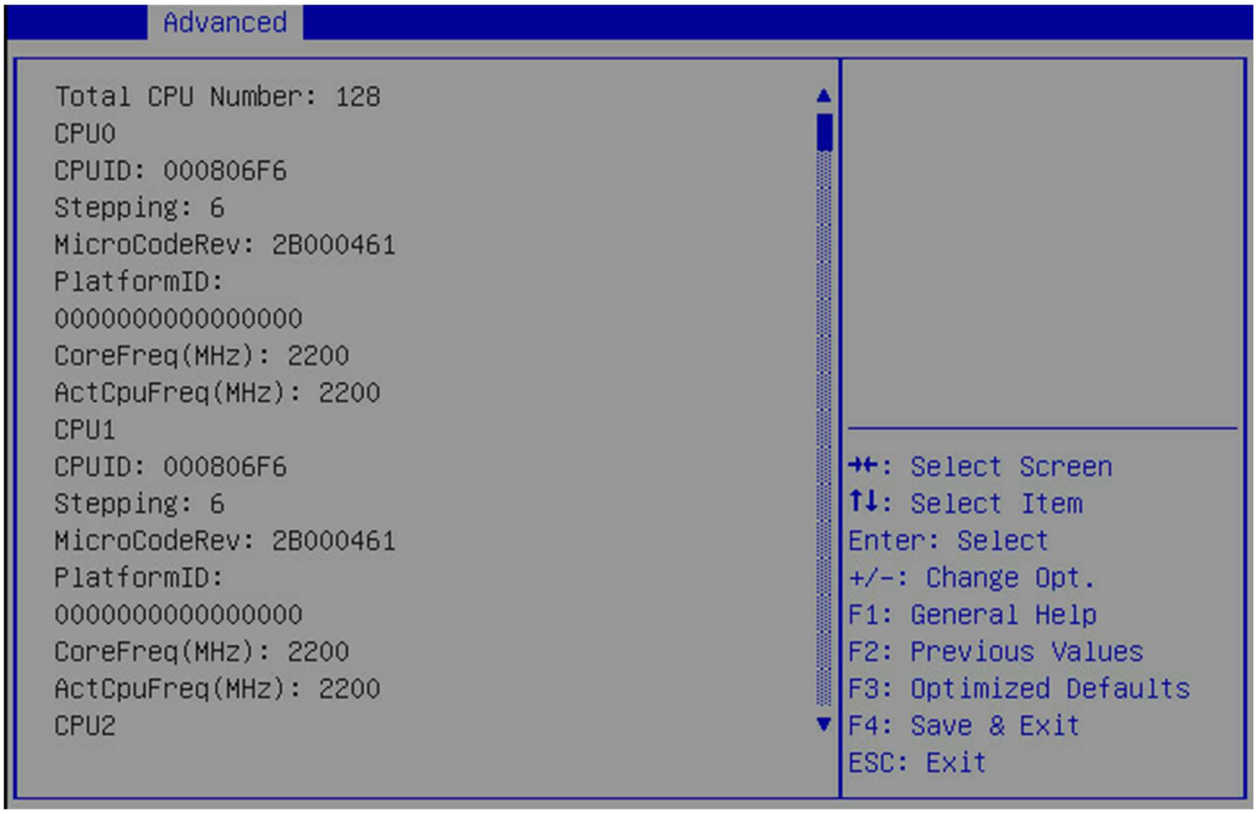
Элемент меню	Опция/Описание
uBIOS Generation	Auto/Enable/Disable. Включение или отключение uBIOS
Hybrid SLE Mode	Auto/Enable/Disable. Включение или отключение Hybrid SLE режима
MSR Trace for PB	Auto/Enable/Disable. Включение или отключение MSR Trace для PB

2.15 Tls Auth Configuration



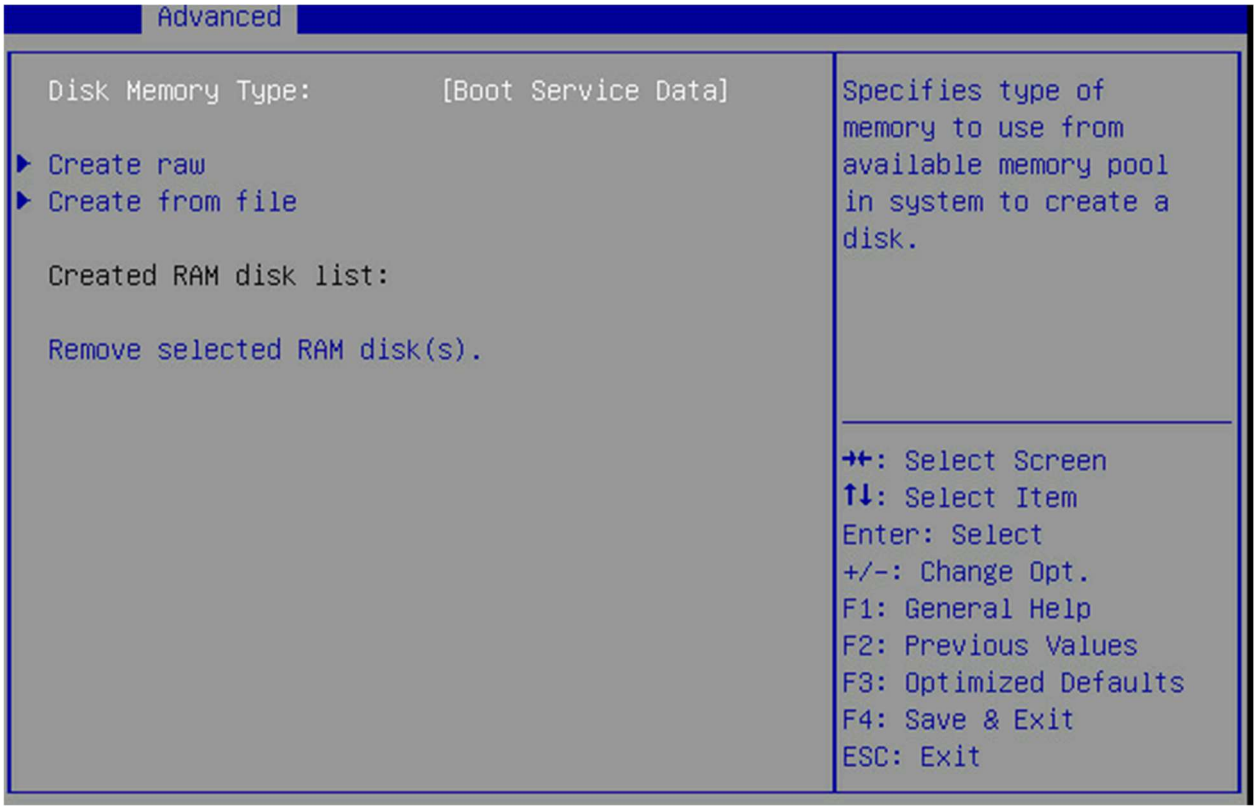
Элемент меню	Опция/Описание
Server CA Configuration	Настройка Server CA
Client Cert Configuration	Настройка Client Cert

2.16 All Cpu Information



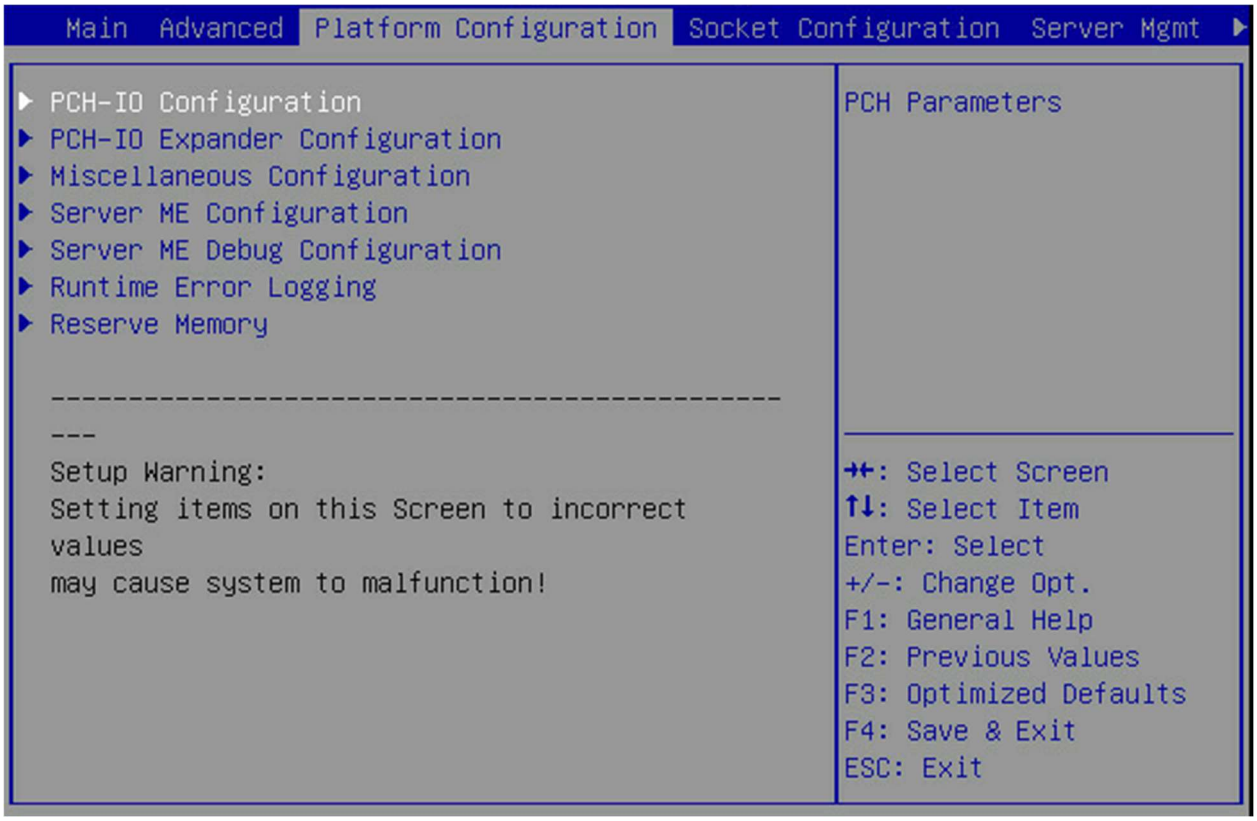
Полная информация об установленных ЦПУ.

2.17 RAM Disk Configuration



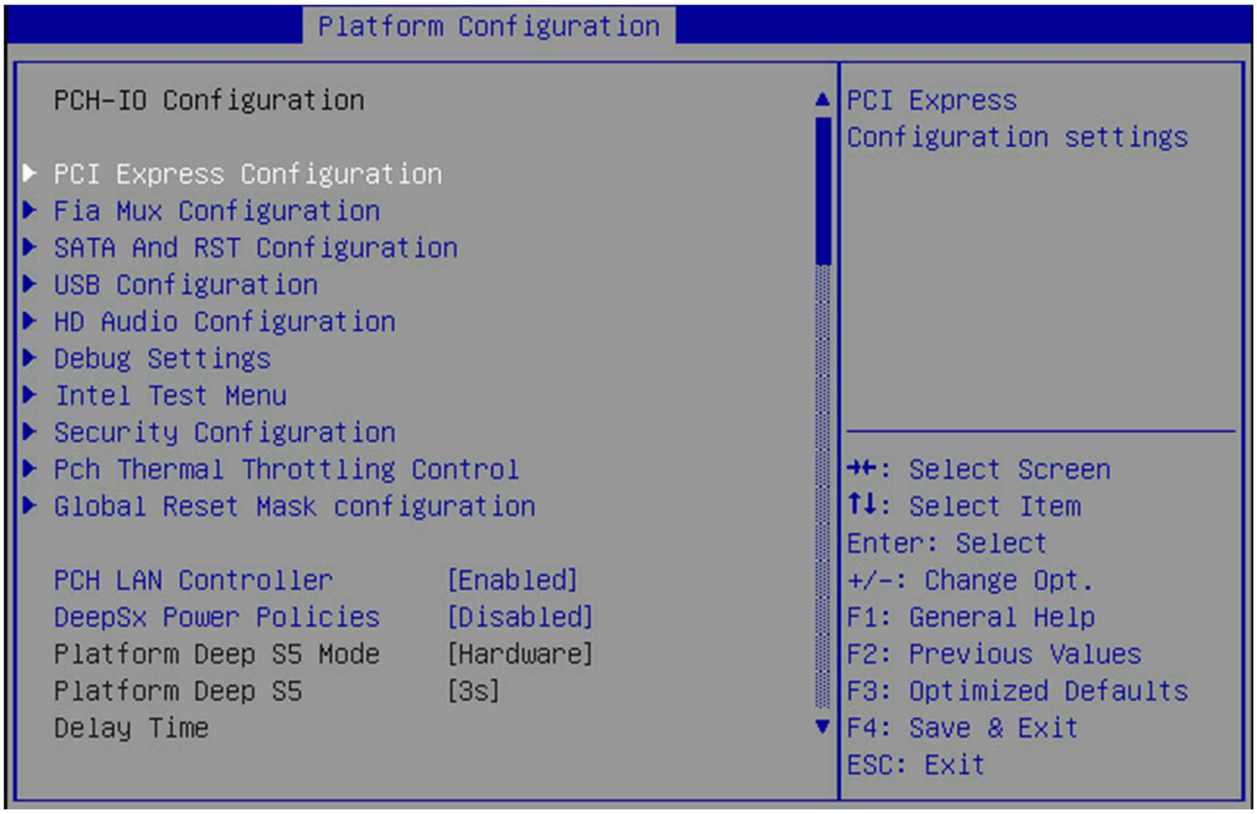
Создание RAM диска.

3. Platform Configuration



Элемент меню	Опция/Описание
PCH-IO Configuration	Смотреть подменю > PCH-IO Configuration
PCH-IO Expander Configuration	Смотреть подменю > PCH-IO Expander Configuration
Miscellaneous Configuration	Смотреть подменю > Miscellaneous Configuration
Server ME Configuration	Смотреть подменю > Server ME Configuration
Server ME Debug Configuration	Смотреть подменю > Server ME Debug Configuration
Runtime Error Logging	Смотреть подменю > Runtime Error Logging
Reserve Memory	Смотреть подменю > Reserve Memory

3.1 PCH-IO Configuration



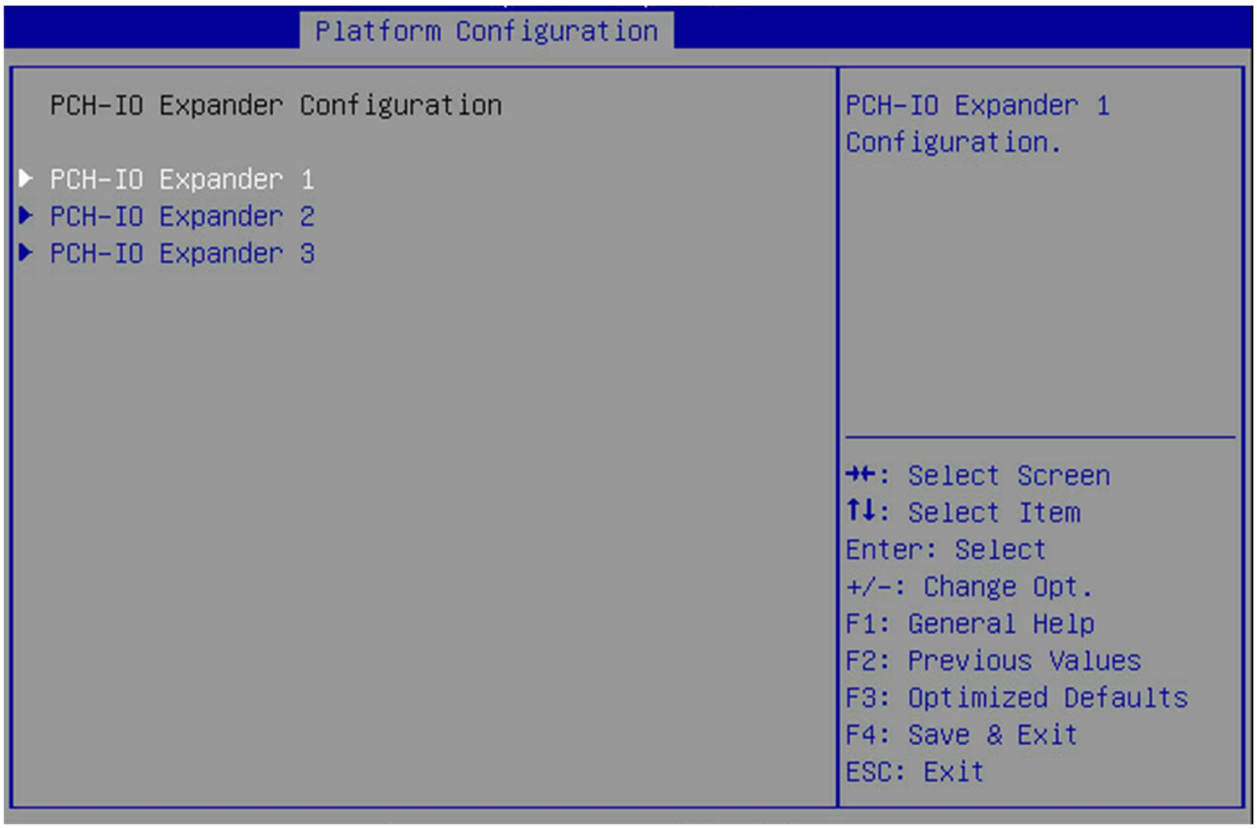
Элемент меню	Опция/Описание
PCI Express Configuration	Смотреть подменю> PCI Express Configuration
Fia Mux Configuration	Смотреть подменю> Fia Mux Configuration
SATA And RST Configuration	Смотреть подменю> SATA And RST Configuration
USB Configuration	Смотреть подменю> USB Configuration
HD Audio Configuration	Смотреть подменю> HD Audio Configuration
Debug Settings	Смотреть подменю> Debug Settings
Intel Test Menu	Смотреть подменю> Intel Test Menu
Security Configuration	Смотреть подменю> Security Configuration
Pch Thermal Throtting Control	Смотреть подменю> Pch Thermal Throtting Control
Global Reset Mask configuration	Смотреть подменю> Global Reset Mask configuration
PCH LAN Controller	Enabled/Disabled.
DeepSx Power Policies	Enabled/Disabled.
Wake on LAN Enable	Enabled/Disabled
LAN Wake From DeepSx	Enabled/Disabled

SLP_LAN# Low on DC Power	Enabled/Disabled
Wake on WLAN and BT Enable	Enabled/Disabled
Disable DSX ACPRESENT PullDown	Enabled/Disabled
Serial IRQ Mode	Continuous/Quiet
State After G3	S0 State/S5 State. Указать, в какое состояние следует перейти при повторном включении питания после сбоя питания (состояние G3). Где S0 – включение, S5 - выключение
Port 80h Redirection	LPC Bus/PCIE Bus
Enhance Port 80h LPC Decoding	Enabled/Disabled. Включение или отключение поддержки декодирования word/dword порта 80h за LPC
IOAPIC 24-119 Entries	Enabled/Disabled. Включение или выключение. Записи IOAPIC 24-119. IRQ24-119 могут использоваться устройствами PCH. Отключение этих прерываний может привести к отказу некоторых устройств
PCH Cross Throttling	Enabled/Disabled. Включение или отключение PCH Cross Throttling. Только ULT поддерживает эту опцию.
PCH Energy Reporting	Enabled/Disabled. Включение или отключение. Включить отчет по энергии ДОЛЖЕН быть установлен как ВКЛЮЧЕНО. Это только для целей тестирования
IEH Mode	Enabled/Disabled. Включение или отключение режима IEH.
Enable Timed GPIO0	Enabled/Disabled. Включение или отключение Timed GPIO0. При отключении отключает перекрестную временную синхронизацию как расширение временной синхронизации Hammock Harbor.
Enable Timed GPIO1	Enabled/Disabled. Включение или отключение Timed GPIO1. При отключении отключает перекрестную временную синхронизацию как расширение временной синхронизации Hammock Harbor
Lock PCH Sideband Access	Enabled/Disabled. Включение или отключение блокировки доступа PCH Sideband, включая блокировку интерфейса

	SideBand и маску SideBand PortID для определенной конечной точки (например, PSFx). Параметр недействителен, если установлен POSTBOOT SAI
Flash Protection Range Registers (FPRR)	Enabled/Disabled
SPD Write Disable	Enabled/Disabled. Включение или отключение SPD Write Disable
Chipset Init HECI Message	Enabled/Disabled. Включение или отключение Chipset Init HECI Message
Bypass ChipsetInit sync reset	Enabled/Disabled. Включение или отключение Bypass ChipsetInit sync reset
LGMR	Enabled/Disabled. Включение или отключение LGMR
WDT Enable	Enabled/Disabled. Включение или отключение WDT
GPIO IRQ Route	IRQ14/IRQ15. Направить все GPIO на один из маршрутов
UART0 Controller	Enabled/Disabled/Communication port. Включение или выключение SerialIo контроллера
Serial IO UART0 Settings	Смотреть подменю > Serial IO UART0 Settings
UART1 Controller	Enabled/Disabled/Communication port. Включение или выключение SerialI1 контроллера
Enable/Disable ADR	Включение или выключение Automatic DIMM Refresh (ADR)
Enable/Disable ADR Timer	Включение или выключение таймера ADR
Host Partition Reset ADR Enable	Platform-POR/Enabled/Disabled. Включение или отключение.
ADR timer 1 expire time	Ввести желаемое время истечения таймера 1 ADR , 0 - режим AUTO, допустимые значения - <1, 256>. Введенное время масштабируется по единице времени таймера ADR
ADR timer 1 time unit	1/10/100us, 1/10/100ms, 1/10 s, Auto. Выбор значения ADR таймера.1
ADR timer 2 expire time	Ввести желаемое время истечения таймера 2 ADR , 0 - режим AUTO, допустимые значения - <1, 256>. Введенное время масштабируется по единице времени таймера ADR.
ADR timer 2 time unit	1/10/100us, 1/10/100ms, 1/10 s, Auto. Выбор значения ADR таймера.2

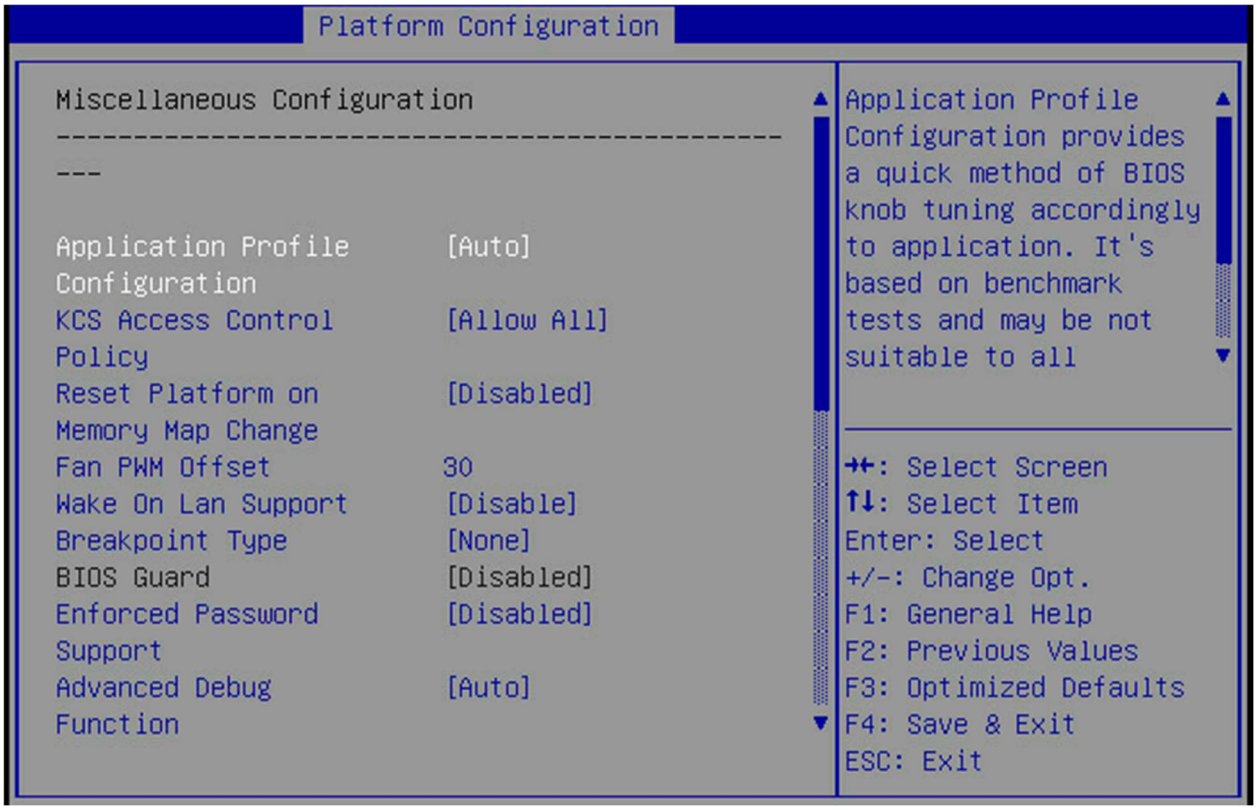
Extended BIOS Range Decode	Enabled/Disabled. Включение этой функции приведет к перенаправлению циклов памяти, попадающих в определенную область, на контроллер флэш-памяти SPI.
Thermal Trip Timer Delay	Добавление времени задержки между тепловым отключением ЦП, распространяющимся через PCH, и генерацией PCH глобального сброса
Enable I/O Margining	Enabled/Disabled. Включение или отключение инструмента I/O Margin

3.2 PCH-IO Expander Configuration



Элемент меню	Опция/Описание
PCH-IO Expander 1	Смотреть подменю> PCH-IO Expander 1
PCH-IO Expander 2	Смотреть подменю> PCH-IO Expander 2
PCH-IO Expander 3	Смотреть подменю> PCH-IO Expander 3

3.3 Miscellaneous Configuration



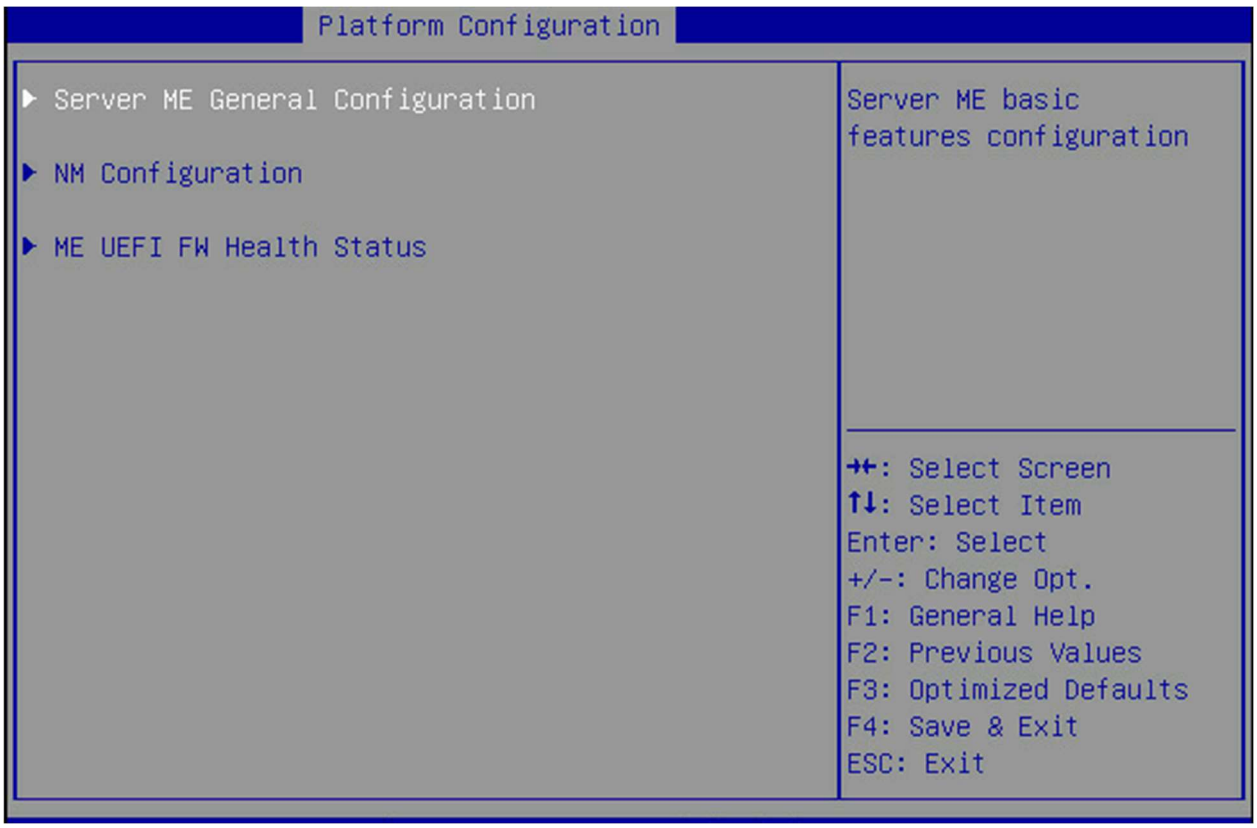
Элемент меню	Опция/Описание
Application Profile Configuration	Auto/General Computing/Memory Bandwith/Matrix Calculation/Energy Efficiency/Server Side Java/OLTP/Virtualization
KCS Access Control Policy	Allow All/Restricted/Deny All
Reset Platform on Memory Map Change	Enabled/Disabled
Fan PWM Offset	Допустимое смещение 0-100. Это число добавляется к рассчитанному значению ШИМ для увеличения скорости вентилятора
Wake On Lan Support	Enable/Disable
Breakpoint Type	None/After MRC/After KTI RC/After Resource Allocation/After PORT/After Full Speed Setup/Ready for IBIST
BIOS Guard	Disabled
Enforced Password Support	Enabled/Disabled
Advanced Debug Function	Auto/Disabled/Enabled
Serial Debug Message Level	Disable/Minimum/Normal/Maximum/Auto/Fixed PCD
Trace Messages	Enabled/Disabled/Enabled for registry writes only

Training Messages	Enabled/Disabled
Active Video	Auto/Onboard Device/PCIE Device
PS2 Port Swap	Enable/Disable
Wake On Lan from S5	Enable/Disable
Boot to Network	Enable/Disable
ARI Support	Enable/Disable
RTC Wake system from S4/S5	Disable/Enable/Enable and set wake on time
Firmware Configuration	Ignore Policy Update/Production/Test/Internal/Restricted/Restricted SV
Warm-Reset Elimination	Disable/Enable/Auto
External SSC – CK440	SSC Off/SSC=-0.3%/SSC=-0.5%/Hardware
Emulation BIOS Skip S3M Access	Auto/Disable/Enable
BMC remote setup	Enable/Disable
Force Boot With FULL Socket Number	Disable/1 Socket/2 Socket/4 Socket/8 Socket

3.4 Server ME Configuration

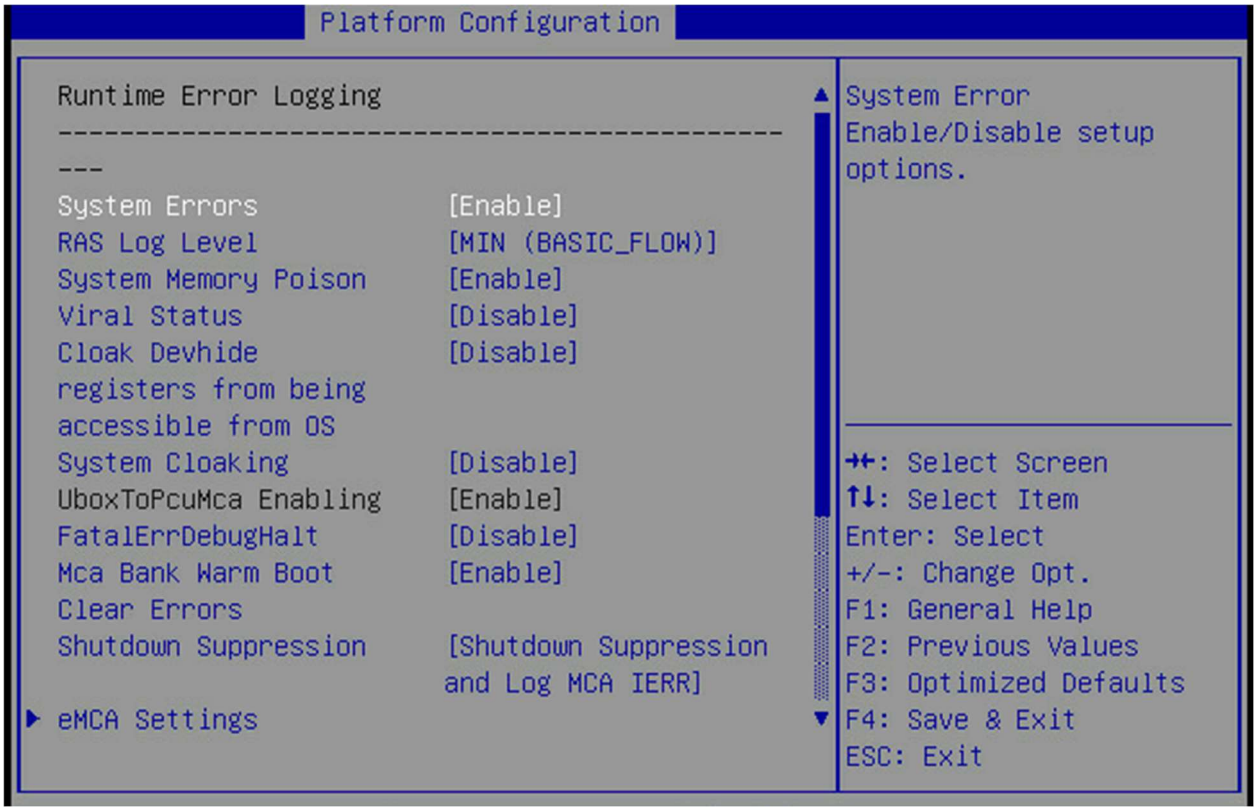
Элемент меню	Опция/Описание
Altitude	Высота расположения платформы над уровнем моря, выраженная в метрах. Шестнадцатеричное число декодируется как целое число со знаком в дополнении до 2. Укажите значение 8000 часов, если высота неизвестна
MCTP Bus Owner	Расположение владельца шины MCTP на PCIe: шина [15:8], устройство [7:3], функция [2:0]. Если все нули отправляют владельца шины, он отключается.

3.5 Server ME Debug Configuration



Элемент меню	Опция/Описание
Server ME General Configuration	Смотреть подменю > Server ME General Configuration
NM Configuration	Смотреть подменю > NM Configuration
ME UEFI FW Health Status	Смотреть подменю > ME UEFI FW Health Status

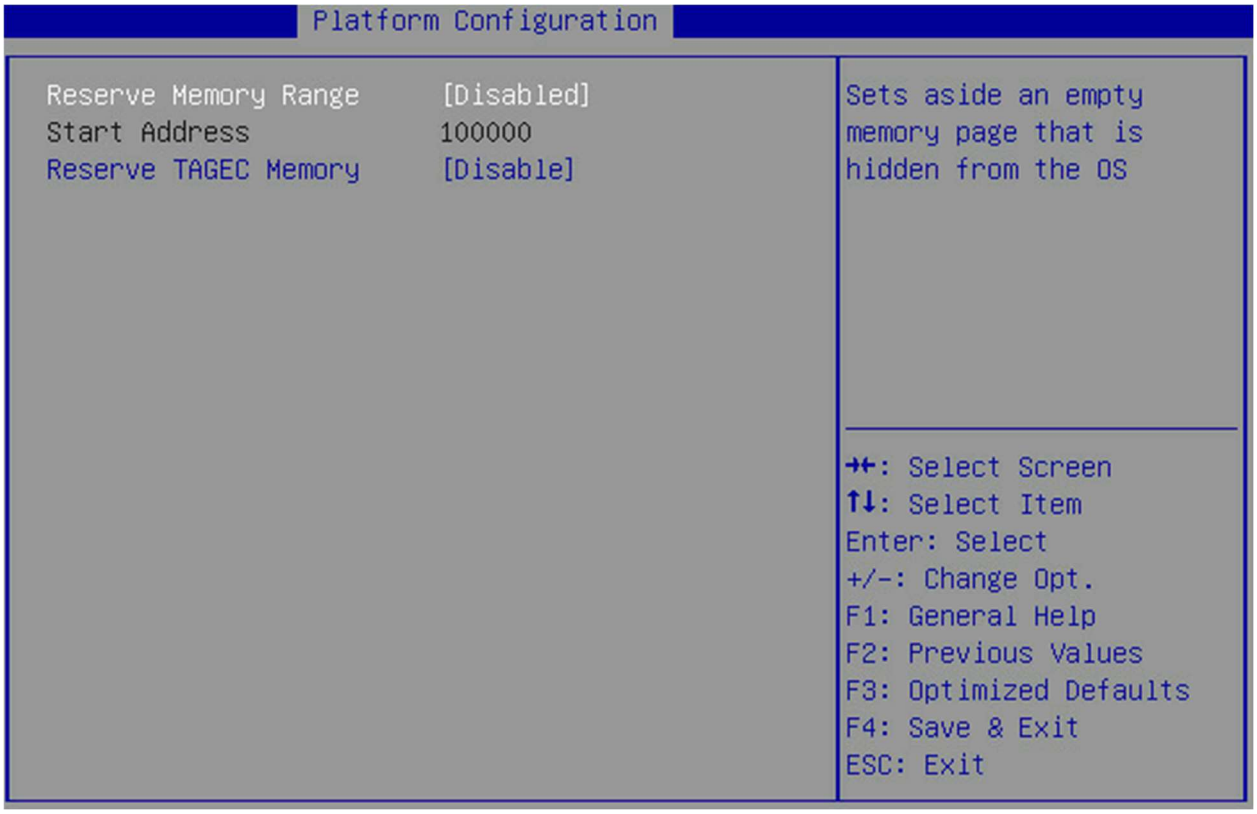
3.6 Runtime Error Logging



Элемент меню	Опция/Описание
System Errors	Enable/Disable
RAS Log Level	None/MIN/MID/MAX
System Memory Poison	Enable/Disable
Viral Status	Enable/Disable
Cloak Devhide registers from being accessible from OS	Enable/Disable
System Cloaking	Enable/Disable
UboxToPcuMca Enabling	Enable
FatalErrDebugHalt	Enable/Disable
Mca Bank Warm Boot Clear Errors	Enable/Disable
Shutdown Suppression	Disable/Shutdown Suppression and Log MCA IERR/Shutdown Log MCA IERR
eMCA Settings	Смотреть подменю > eMCA Settings
Whea Settings	Смотреть подменю > Whea Settings
Error Injection Settings	Смотреть подменю > Error Injection Settings
Memory Error Enabling	Смотреть подменю > Memory Error Enabling
IIO Error Enabling	Смотреть подменю > IIO Error Enabling

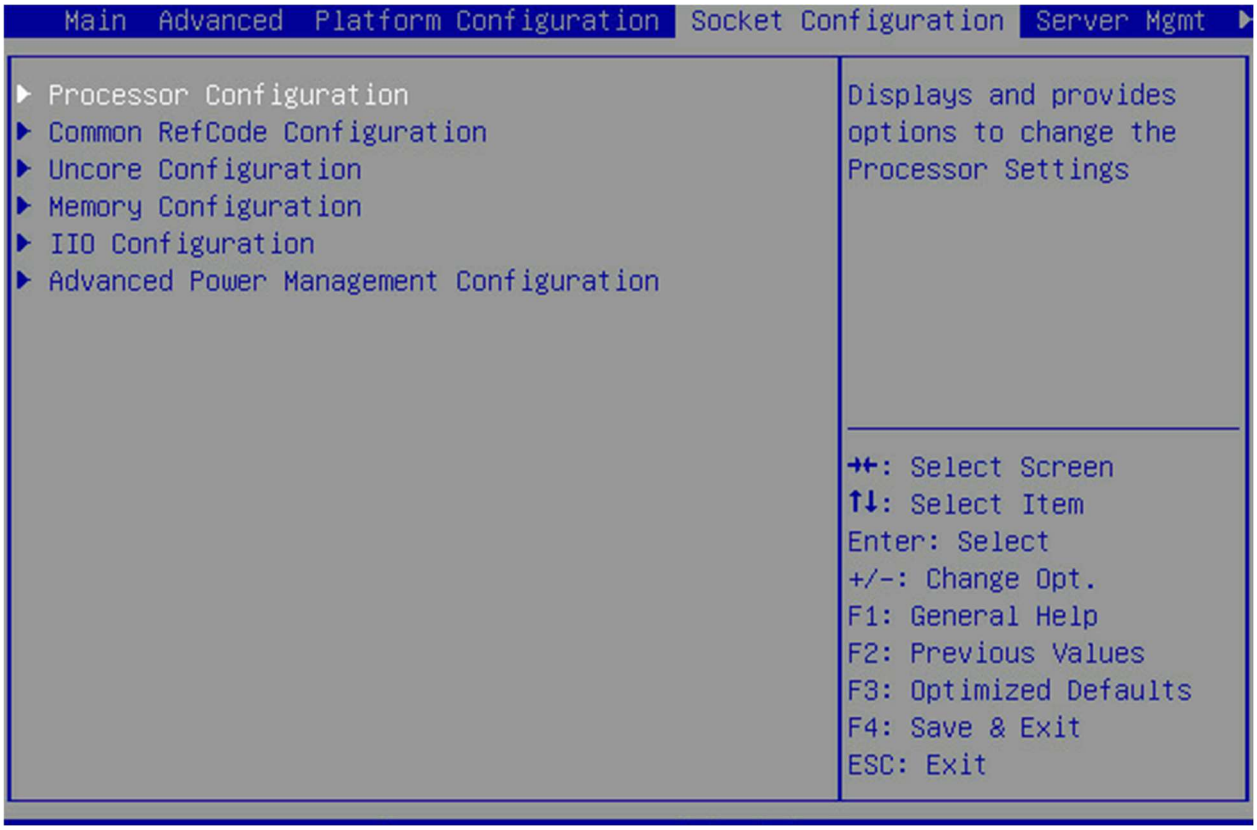
PCIe Error Enabling	Смотреть полдменю > PCIe Error Enabling
Error Control Setting	Смотреть подменю > Error Control Setting
Crash Log Enabling	Смотреть подменю > Crash Log Enabling
DWR Configuration	Смотреть подменю > DWR Configuration

3.7 Reserve Memory



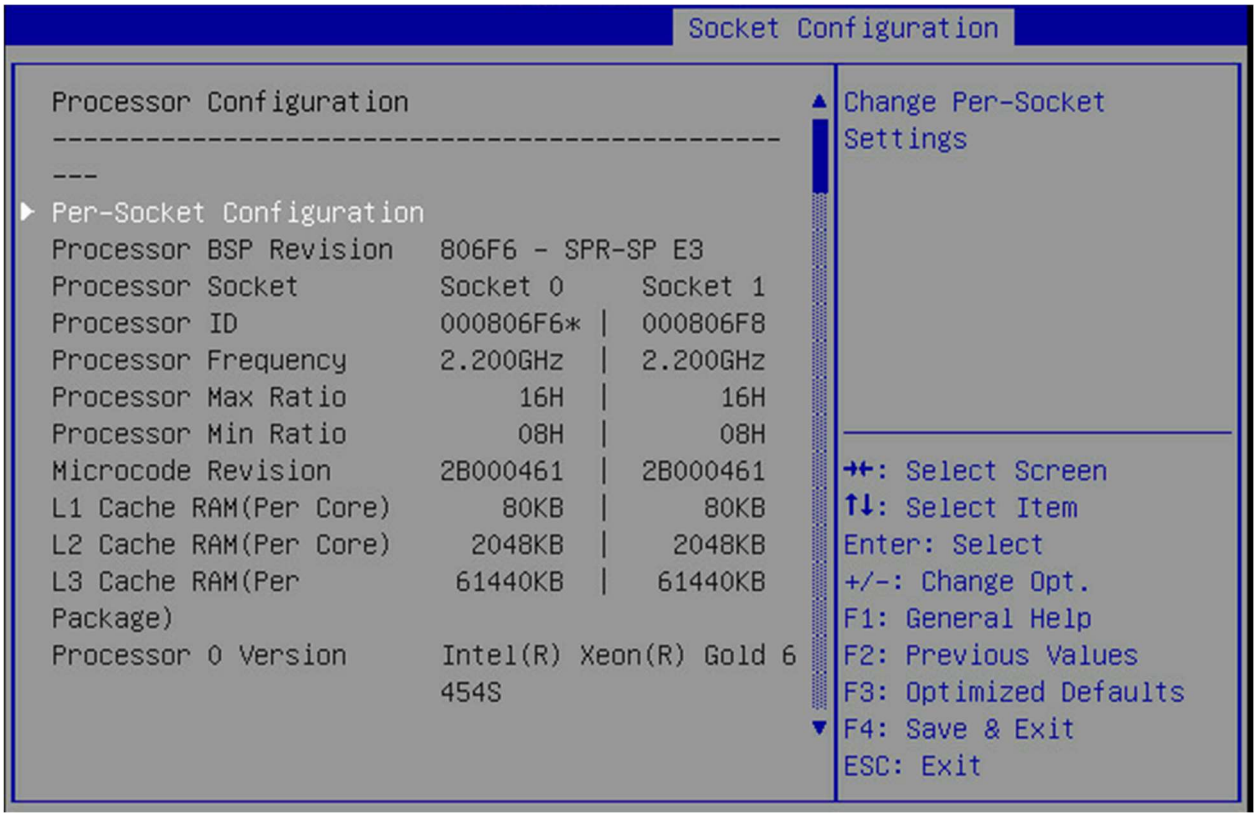
Элемент меню	Опция/Описание
Reserve Memory Range	Enabled/Disabled
Start Address	Адрес, с которого начинается зарезервированная страница памяти
Reserve TAGEC Memory	Enable/Disable

4. Socket Configuration



Элемент меню	Опция/Описание
Processor Configuration	Смотреть подменю > Processor Configuration
Common RefCode Configuration	Смотреть подменю > Common RefCode Configuration
Uncore Configuration	Смотреть подменю > Uncore Configuration
Memory Configuration	Смотреть подменю > Memory Configuration
IIO Configuration	Смотреть подменю > IIO Configuration
Advanced Power Management Configuration	Смотреть подменю > Advanced Power Management Configuration

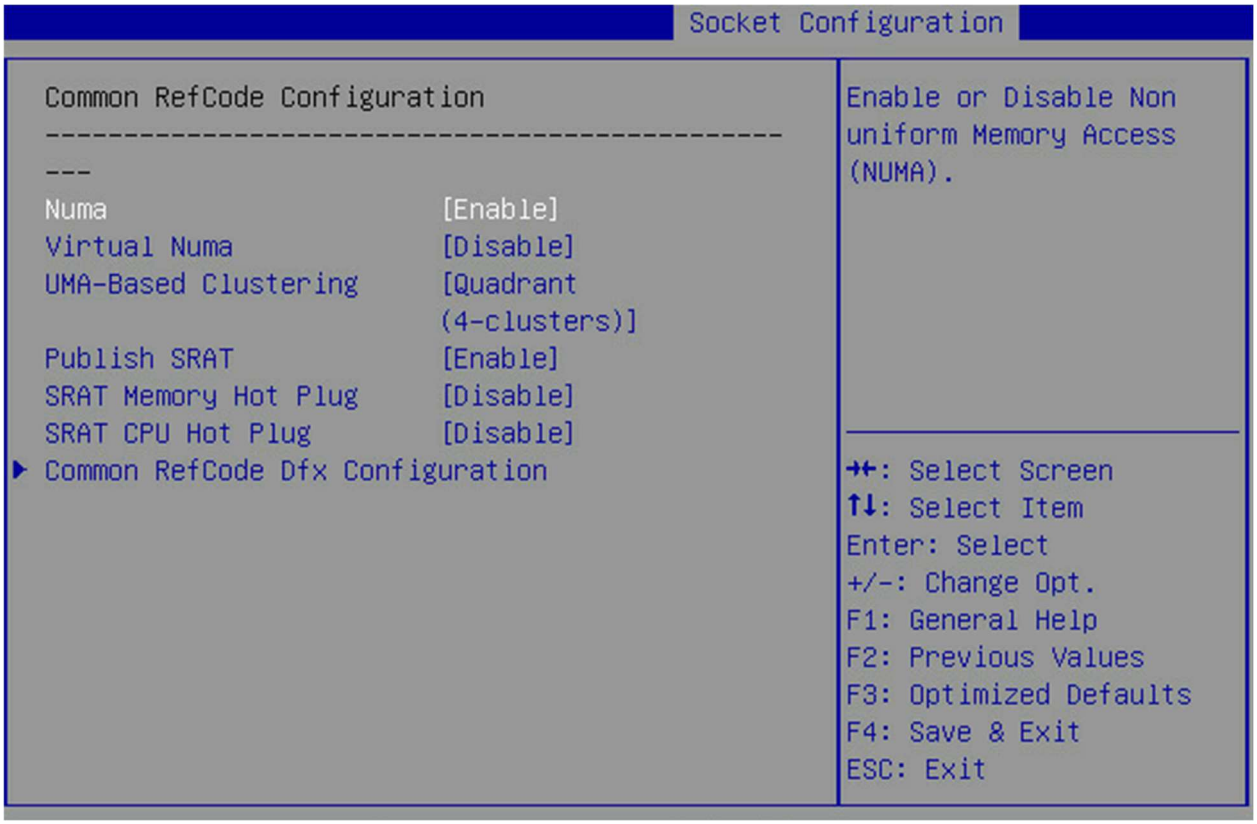
4.1 Processor Configuration



Элемент меню	Опция/Описание
Enable LP [Global]	ALL LPs/Single LP
Skip Flex Ratio Override	Enable/Disable
Check CPU BIST Result	Enable/Disable
3StrikeTimer	Enable/Disable
Fast String	Enable/Disable
Machine Check	Enable/Disable
Hardware Prefetcher	Enable/Disable
L2 RFO Prefetch Disable	Enable/Disable
Adjacent Cache Prefetch	Enable/Disable
DCU Streamer Prefetcher	Enable/Disable
DCU IP Prefetcher	Enable/Disable
LLC Prefetcher	Enable/Disable
Homeless Prefetch	Auto/Enable/Disable
FB Thread Slicing	Enable/Disable
AMP Prefetch	Auto/Enable/Disable
Bsp Selection	Auto/Socket 0/Socket 1
Extended APIC	Enable/Disable
APIC Physical Mode	Enable/Disable

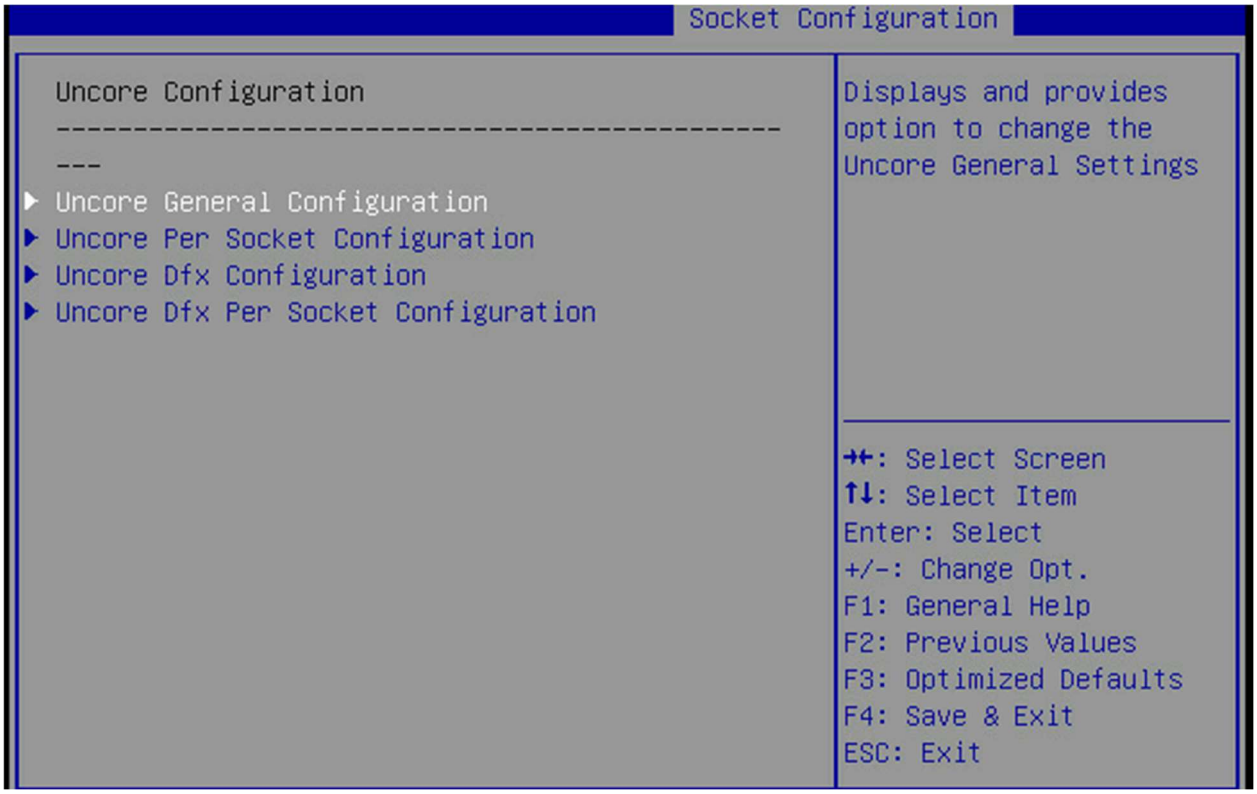
PECI Trust Mode	All PECI Agents untrusted/All PECI Agents trusted/Use per-PECI agent trust mode
Legacy Agent	Enable/Disable
SMBus Agent	Enable/Disable
IE Agent	Enable/Disable
Generic Agent	Enable/Disable
eSPI Agent	Enable/Disable
DfxRedManu Agent	Enable/Disable
DfxOrange Agent	Enable/Disable
DBP-F	Enable/Disable
IIO LLC Ways [14:0] (Hex)	MSR_IIO_LLC_WAYS bitmasdk (Все биты, установленные в маске, должны быть смежными друг с другом)
SMM Blocked and Delayed	Enable/Disable
eSMM Save State	Enable/Disable
Smbus Error Recovery	Enable/Disable
Enable Intel ® TXT	Enable/Disable
VMX	Enable/Disable
Enable SMX	Enable/Disable
Lock Chipset	Enable/Disable
MSR Lock Control	Enable/Disable
PPIN Control	Enable/Disable
AES-NI	Enable/Disable
Memory Encryption (TME)	Enable/Disable
Total Memory Encryption (TME) Bypass	Auto/Enabled/Disabled
Multi-Tenant (TME-MT) memory Integrity	Enabled/Disabled
Memory Integrity	Enabled/Disabled

4.2 Common RefCode Configuration



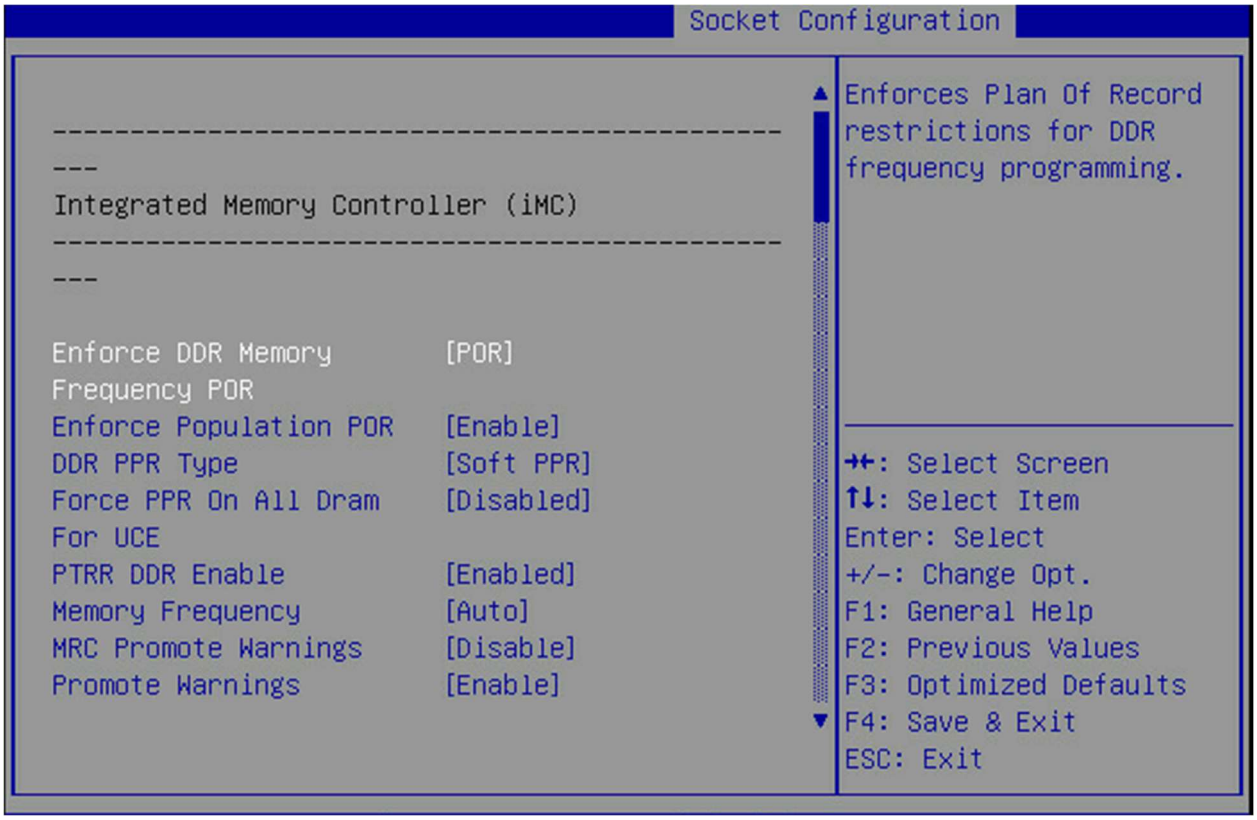
Элемент меню	Опция/Описание
Numa	Enable/Disable
Virtual Numa	Enable/Disable
UMA-Based Clustering	Hemisphere (2-clusters)/Quardrant (4-clusters)
Publish SRAT	Enable/Disable
SRAT CPU Hot Plug	Enable/Disable
Common RefCode Dfx Configuration	Смотреть подменю> Common RefCode Dfx Configuration

4.3 Uncore Configuration



Элемент меню	Опция/Описание
Uncore General Configuration	Смотреть подменю > Uncore General Configuration
Uncore Per Socket Configuration	Смотреть подменю > Uncore Per Socket Configuration
Uncore Dfx Configuration	Смотреть подменю > Uncore Dfx Configuration
Uncore Dfx Per Socket Configuration	Смотреть подменю > Uncore Dfx Per Socket Configuration

4.4 Memory Configuration

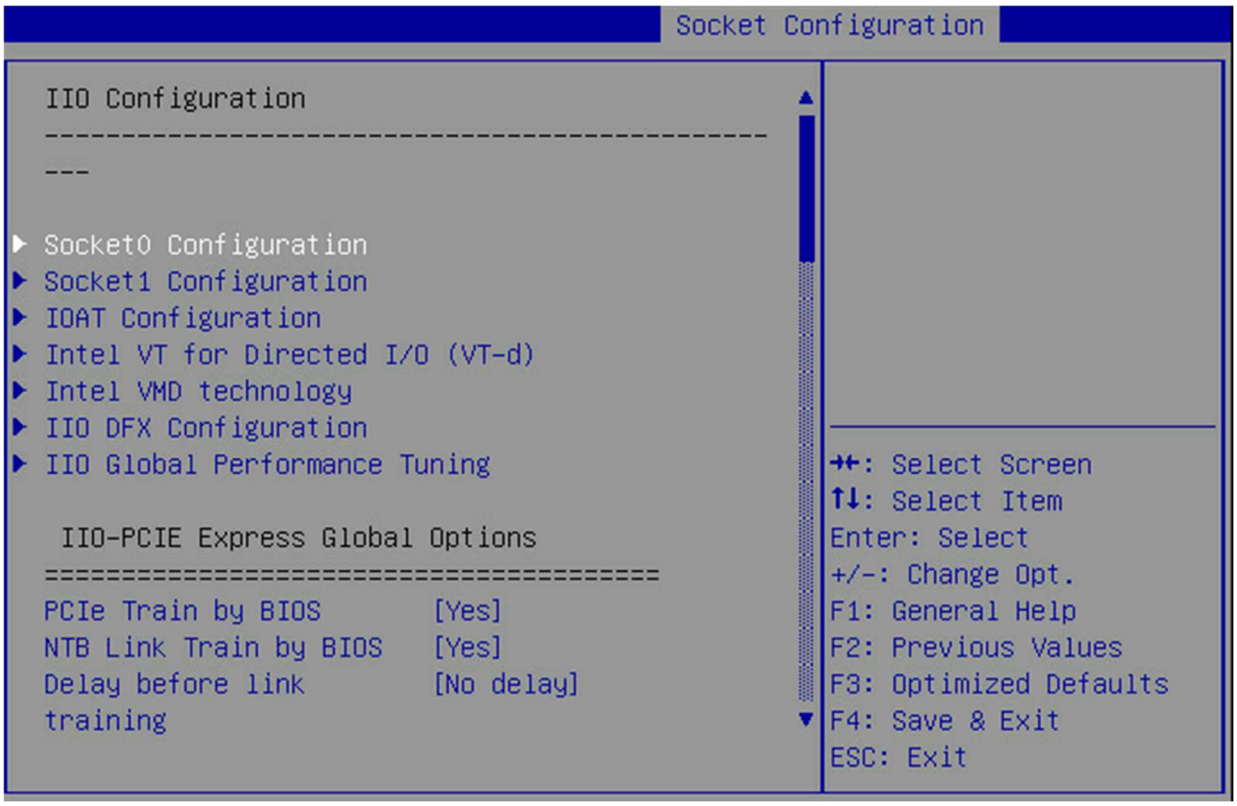


Элемент меню	Опция/Описание
Enforce DDR Memory Frequency POR	POR/Disable
Enforce Population POR	Enable/Disable
DDR PPR Type	PPR Disabled/Hard PPR/Soft PPR
Force PPR On All Dram For UCE	Enabled/Disabled
PTRR DDR Enable	Enabled/Disabled
Memory Frequency	Auto/3200/3600/4000/4400/4800/5200/5600
MRC Promote Warning	Enabled/Disabled
Promote Warning	Enable/Disable
Auto Reset on Mem Training Error	Enable/Disable
100 series Pmem Not Supported Exception	Enable/Disable
PMem MediaStatus Exception	Enable/Disable
Socket in parallel	All/1/2/4
SPD Lock Check	Enable/Disable
SPD CRC Check	Auto/Enable/Disable
Enhanced Log Parsing	Enable/Disable
LRDIMM Module Delay	Auto/Disable
Allow Untested Memory for DXE Drivers	Enable/Disable

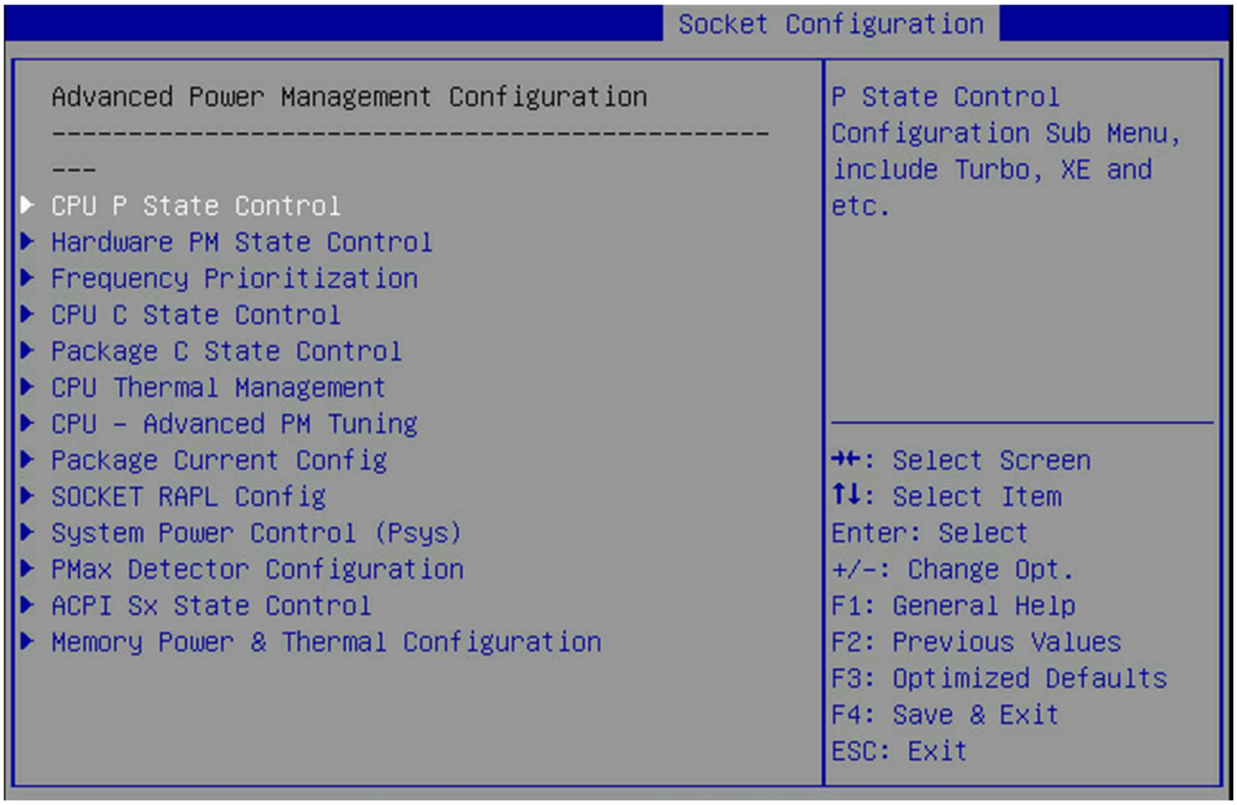
Memtest	Enable/Disable
MemTest Loops	Количество циклов тестирования памяти во время обычной загрузки. Установить значение 0, чтобы запустить memtest бесконечно.
SK Hynix SmarttestKey	Конфиденциальный ключ для использования в SK Hynix Smart Test
Adv Memtest Options	Эта опция представляет собой битовую маску [19:0]: все 0 = отключено: бит-0 = XMATS8, бит-1 = XMATS16, бит-2 = зарезервировано, бит-3 = зарезервировано, бит-4 = WCMATS8, бит-5 = WCMCH8, бит-6 = зарезервировано, бит-7 = MARCHCM64, бит-8 = зарезервировано, бит-9 = зарезервировано, бит-10 = зарезервировано, бит-11 = TWR, бит-12 = DATARED, бит-13 = MATS8TC1, бит-14 = MATS8TC3, бит-15 = MATS8TC3, бит-16 = SK-HYNIX, бит-17 = SAMSUNG, бит-18 = MICRON-RMW, бит-19 = SCRAM_X2
Avd Memtest Rank Selection	Смотреть подменю > Avd Memtest Rank Selection
Adv MemTest PPR	Enable/Disable
Adv MemTest Retry After Repair	Enable/Disable
Adv MemTest Reset Failure Tracking List	Enable/Disable
Adv MemTest Conditions	Auto/Enable/Disable
Training Result Offset	Enable/Disable
Memory Type	UDIMMs and RDIMMs/RDIMMs only/UDIMMs only
Attempt Fast Boot	Enable/Disable
Attempt Fast Cold Boot	Enable/Disable
MemTest On Cold Fast Boot	Enable/Disable
BDAT	Enable/Disable
Data Scrambling for PMem	Auto/Enable/Disable
Data Scrambling for DDR4/5	Enable/Disable
Allow Memory Test Correctable Error	Enable/Disable
Scrambling Seed Low	Нижние 32 бита скремблирующего начального числа
Scrambling Seed High	Верхние 32 бита скремблирующего начального числа
Enable fADR	Enable/Disable
Enable ADR	Enable/Disable
NVDIMM Energy Policy	Device-Managed/Host-Managed
Custom Refresh Enable	Enable/Disable

DDR 2x Refresh Enable	Auto/Disable/Enable
Adaptive Refresh Management Level	Default/Level A/Level B/Level C
Opp read during WMM	Enable/Disable
Normal Operation Duration	Установить интервал длительности нормальной работы (0-65535)
I3C Clock Frequency	Auto/4 MHz in I3C mode/6 MHz in I3C mode/8 MHz in I3C mode
SPD Print	Enable/Disable
SPD Print Length	Auto/256 Bytes/512 Bytes
DDR Cycling	Enable/Disable
Mem Flows	Enable (1)/Disable (0)
Mem FlowsExt	Enable (1)/Disable (0)
Mem FlowsExt2	Enable (1)/Disable (0)
Mem FlowsExt3	Enable (1)/Disable (0)
BLOCK GNT2CMD1CYC	POR/PO Safe Value
Disable DDRT DIMM OPPRD	POR/PO Safe Value
Cmd Setup % Offset	Cmd setup / hold процент смещения для результата обучения позднего cmd. Возможные значения от 0 до 100
Periodic Rcomp	Auto/Enable/Disable
Periodic Rcomp Interval	Выбор интервала
Training Compensation Options Values	Only on PHY Init/after every JEDEC Init/right before every training step
Outlier Check Mapout	Enable/Disable
Outlier Threshold Modifier	Насколько изменить базовый порог выброса (например, -17), чтобы изменить -1, введите 101 (порог будет -18), чтобы изменить +1, введите 1 (порог будет -16)
Memory Topology	Смотреть подменю > Memory Topology
Page Policy	Смотреть подменю > Page Policy
Memory Training	Смотреть подменю > Memory Training
Memory I/O Health Check	Смотреть подменю > Memory I/O Health Check
Memory Map	Смотреть подменю > Memory Map
Memory RAS Configuration	Смотреть подменю > Memory RAS Configuration
PMem Configuration	Смотреть подменю > PMem Configuration
Memory Dfx Configuration	Смотреть подменю > Memory Dfx Configuration
RMT Configuration Menu	Смотреть подменю > RMT Configuration Menu
CMI Init Configuration	Смотреть подменю > CMI Init Configuration

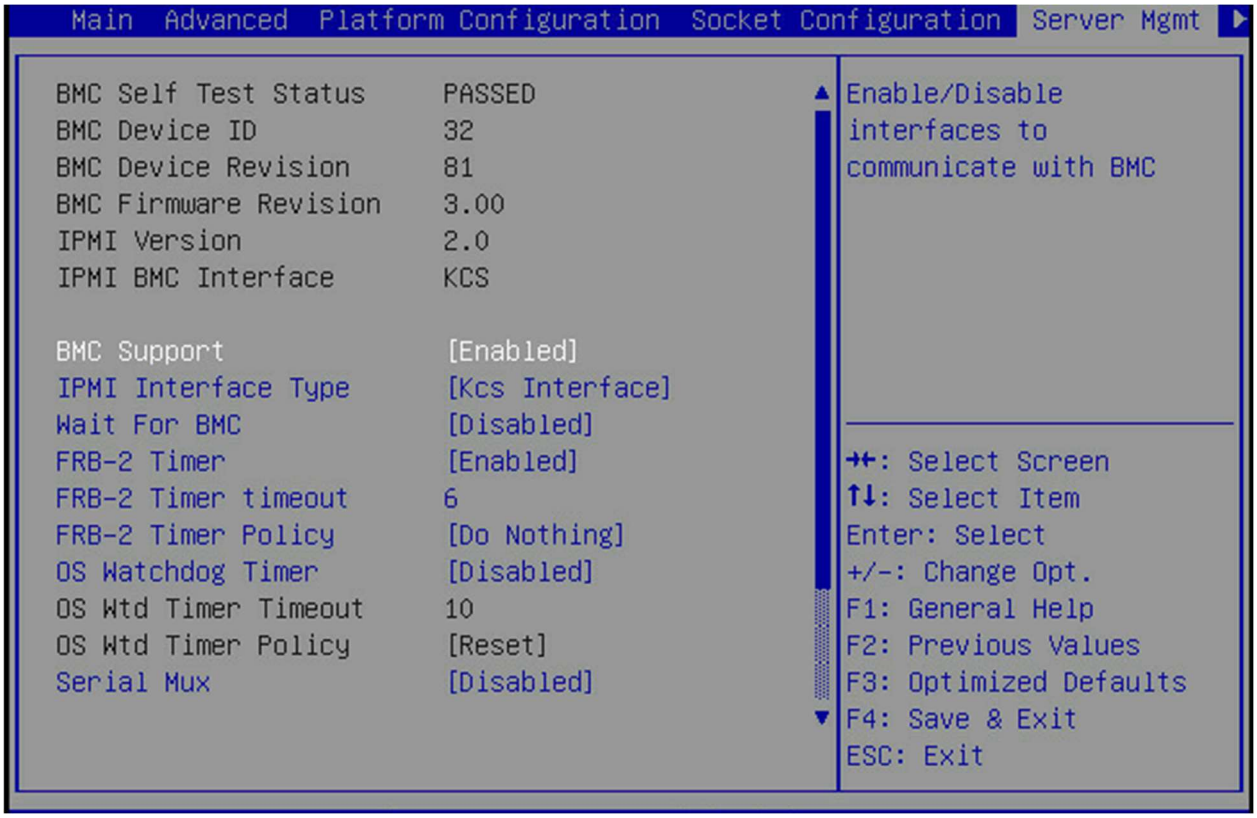
4.5 IIO Configuration



4.6 Advanced Power Management Configuration

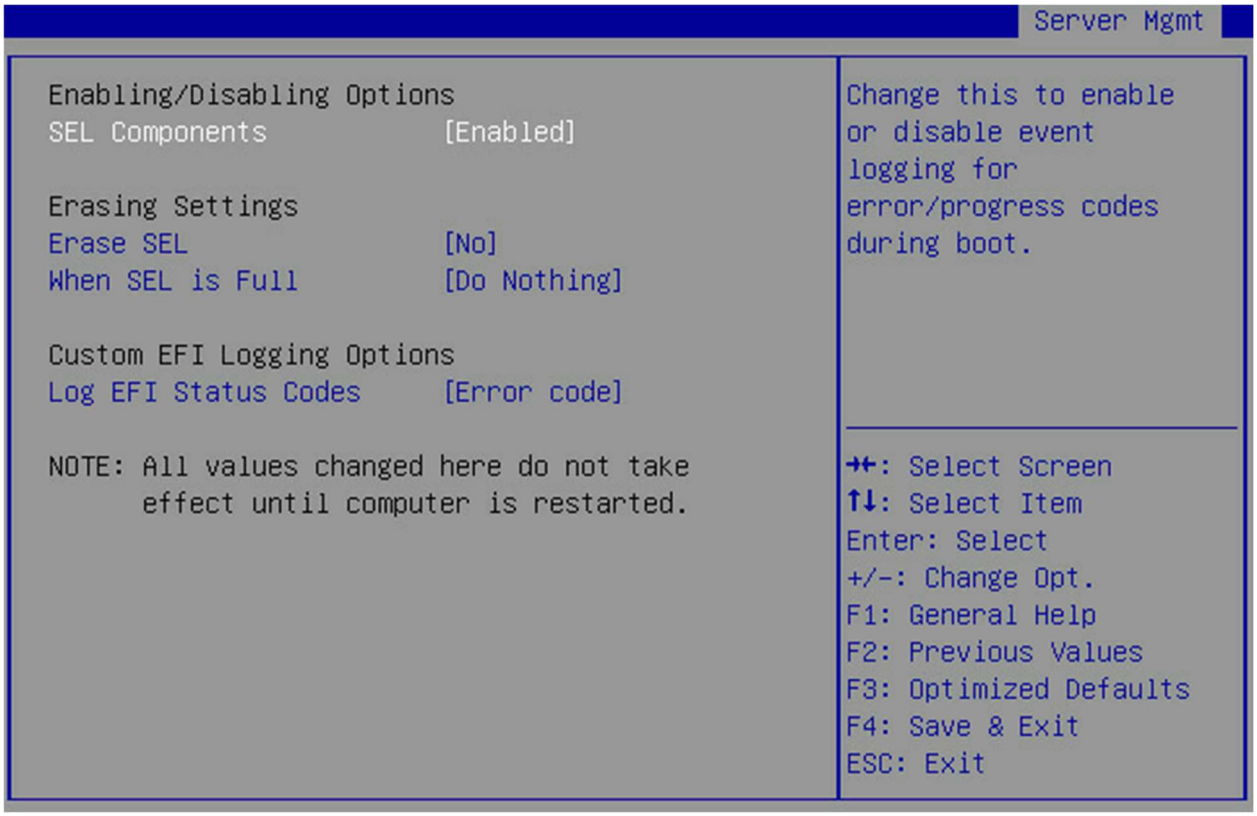


5. Server Mgmt

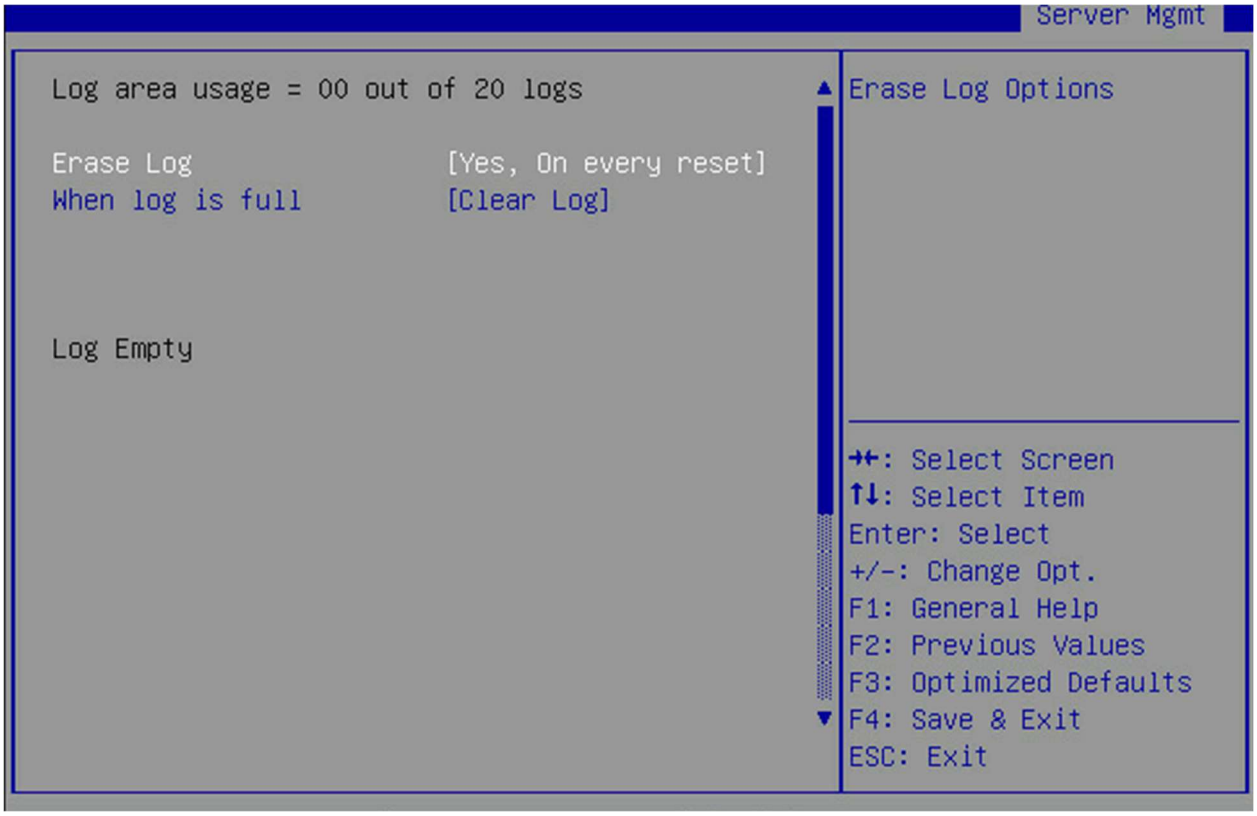


Элемент меню	Опция/Описание
BMC support	Enabled/Disabled. Включение или выключение интерфейса BMC
IPMI Interface Type	Kcs Interface/Bt Interface. Выбор типа интерфейса для подключения к BMC из хоста.
Wait For BMC	Enabled/Disabled. Ожидать ответа BMC в течение указанного времени ожидания. Инициализация хоста для BMC занимает около 30 секунд
FRB-2 Timer	Enabled/Disabled. Включение или отключение FBR-2 таймера (POST таймер)
FRB-2 Timer timeout	Значение таймера в минутах от 1 до 30
FBR-2 Timer Policy	Do Nothing/Reset/Power Down/Power Cycle. Настраивает политику таймера FRB2
OS Wathdog Timer	Enabled/Disabled. Если включено, запускает таймер Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86, который может быть отключен только программным обеспечением управления после загрузки ОС. Помогает определить, что ОС успешно загрузилась или следует политике OS Boot Watchdog Timer
OS Wtd Timer Timeout	Значение таймера в минутах от 1 до 30
OS Wtd Timer Policy	Do Nothing/Reset/Power Down/Power Cycle. Настраивает политику таймера.
Serial Mux	Enabled/Disabled. Включение или отключение Serial Mux
System Event Log	Смотреть подменю> System Event Log
Bmc self test log	Смотреть подменю> Bmc self test log
BMC network configuration	Смотреть подменю> BMC network configuration
View System Event Log	Просмотр журнала событий.
BMC Warm Reset	Сброс конфигурации BMC

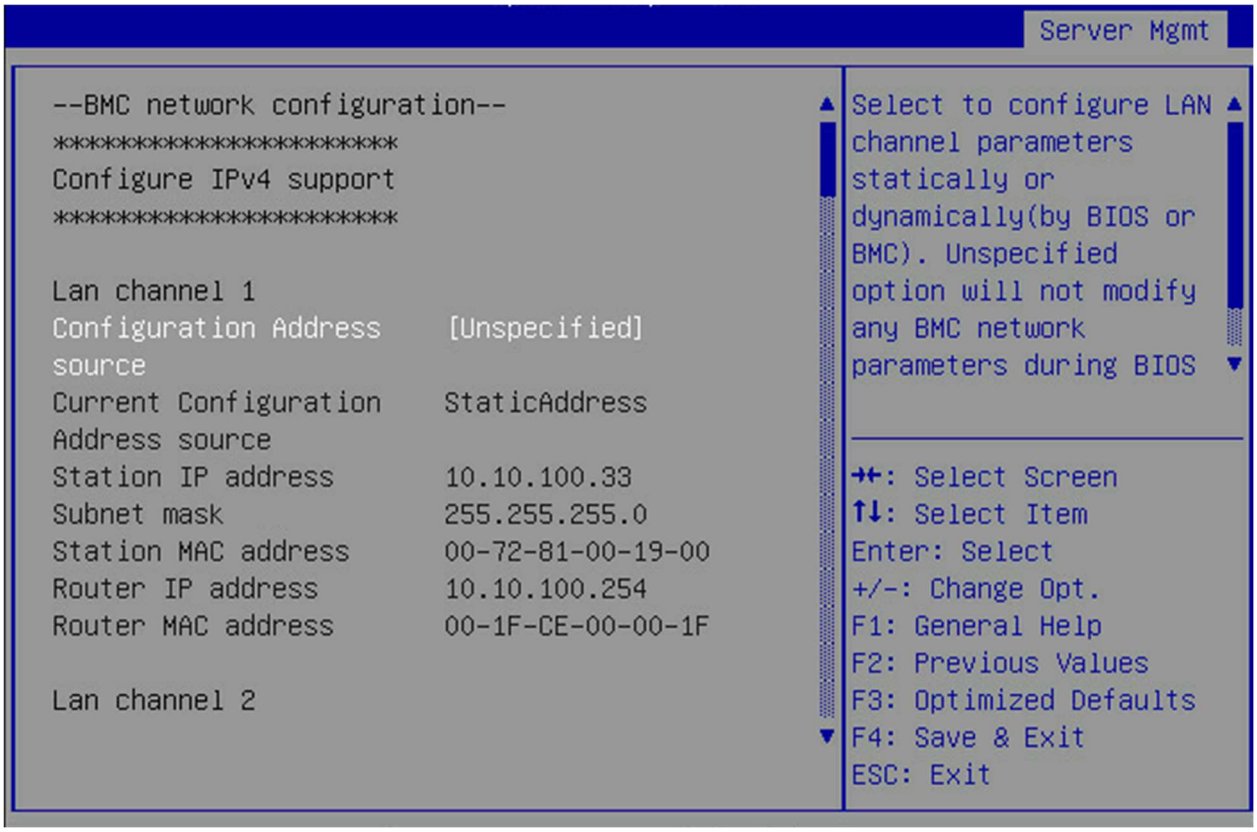
5.1 System Event Log



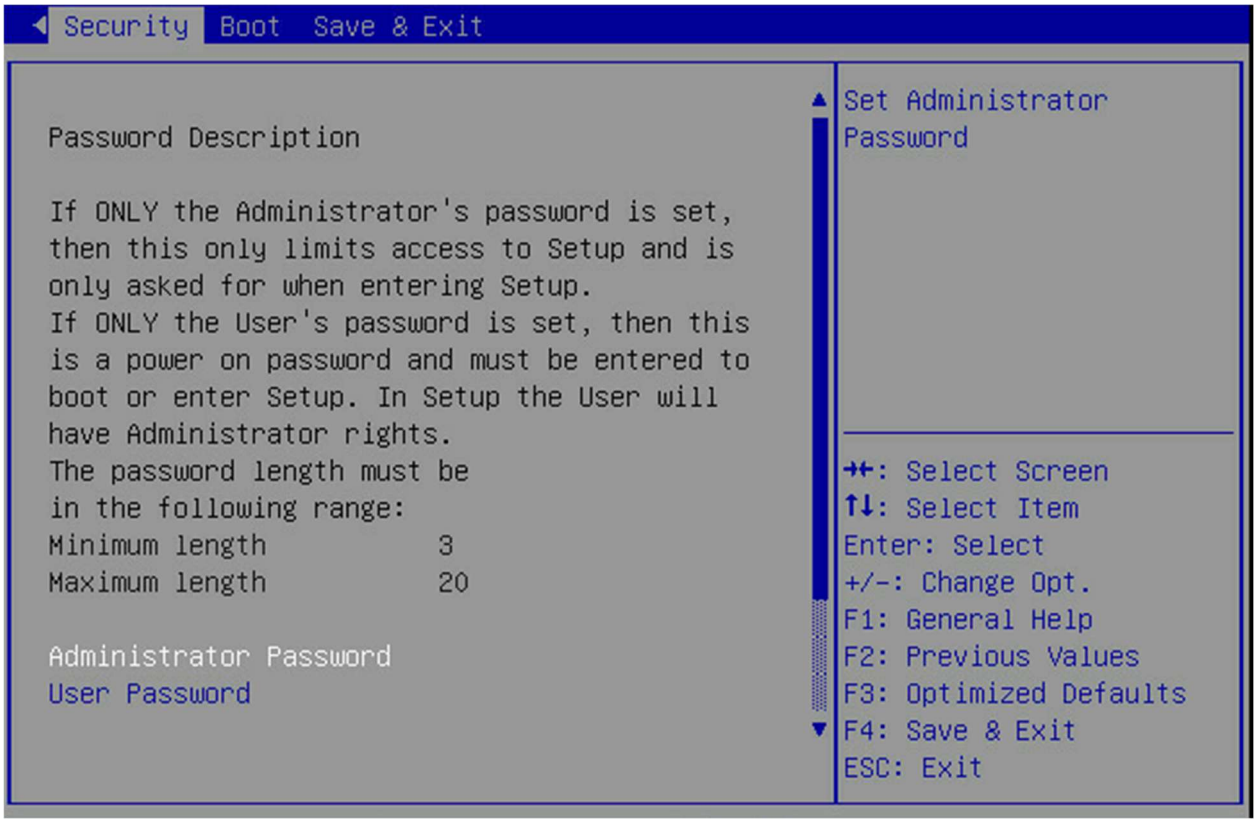
5.2 BMC self test log



5.3 BMC network configuration



6. Security

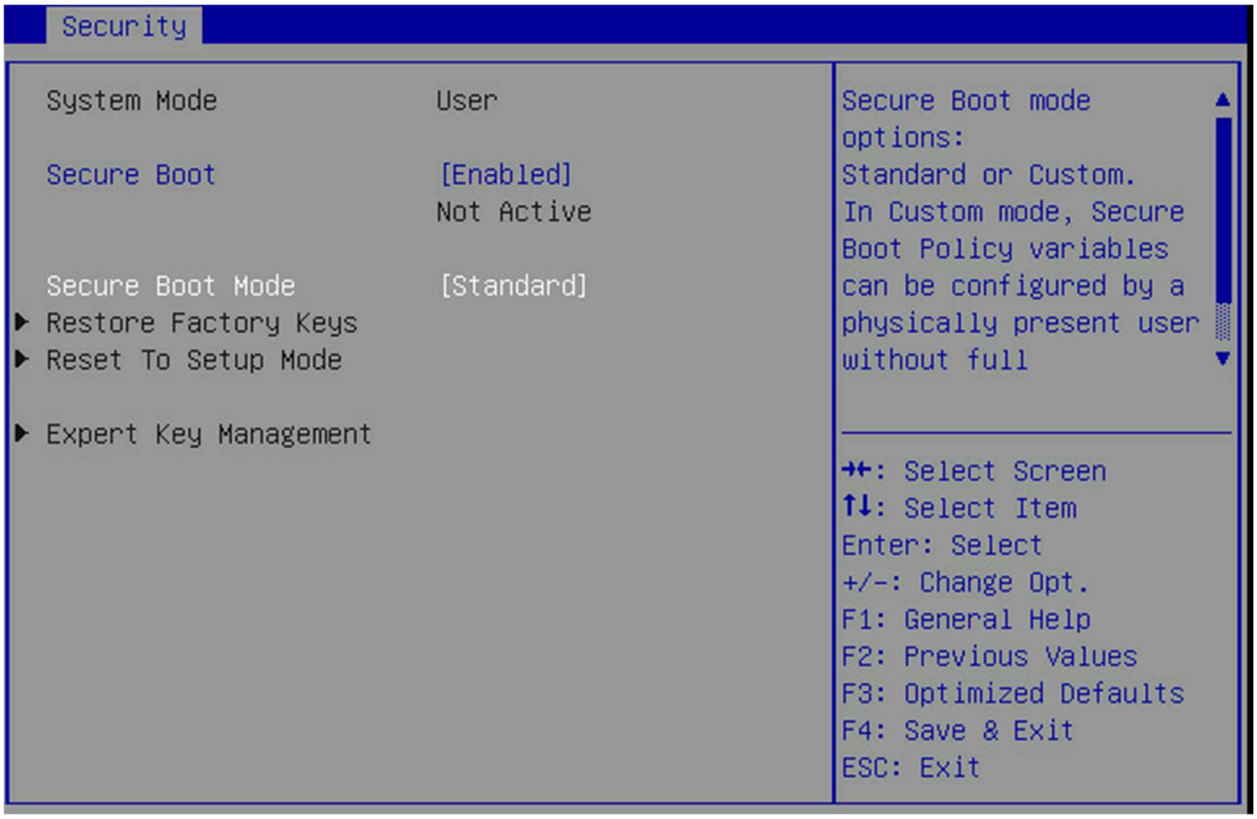


Если установлен ТОЛЬКО пароль администратора, то он ограничивает доступ только к настройке и запрашивается только при входе в настройку. Если установлен ТОЛЬКО пароль пользователя, то это пароль включения питания, который необходимо ввести для загрузки или входа в настройку. В настройке пользователь будет иметь права администратора. Длина пароля должна быть в следующем диапазоне:

- минимальная длина пароля 3;
- максимальная длина пароля 20.

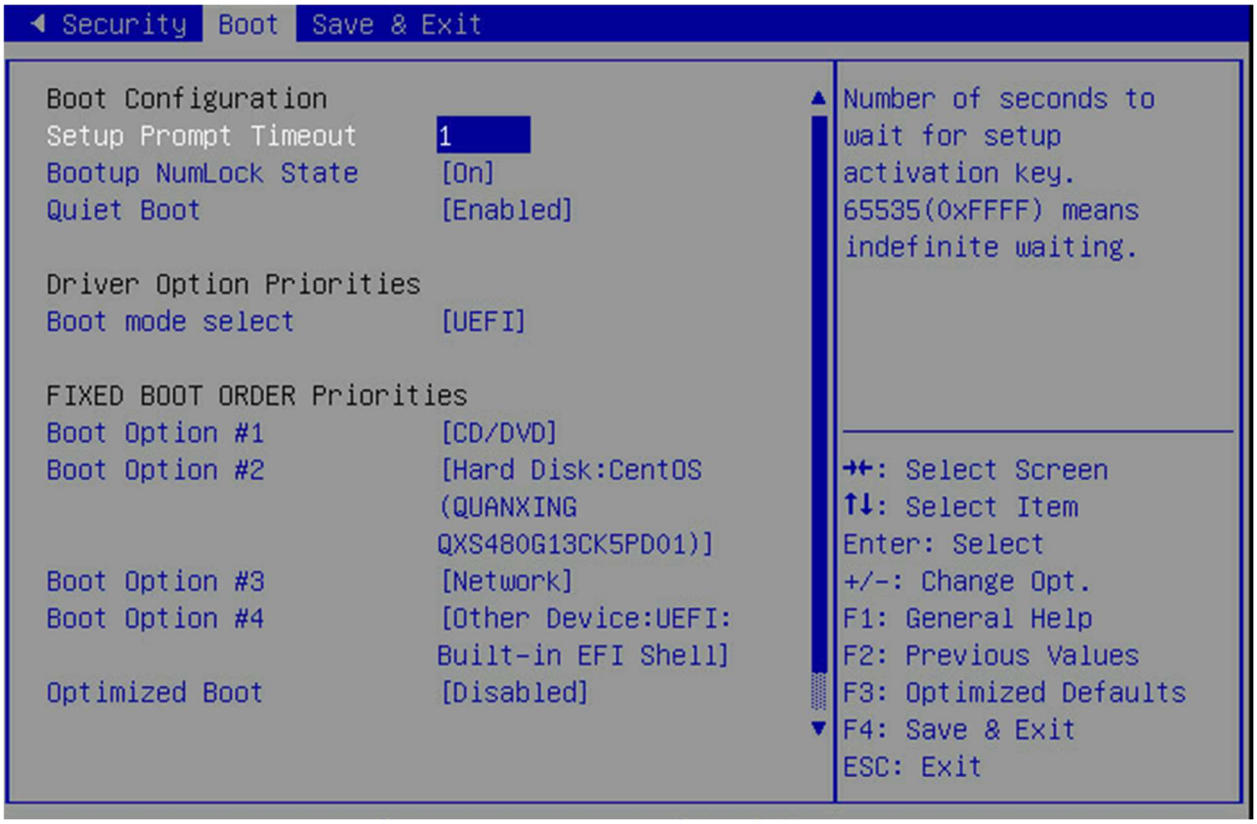
Элемент меню	Опция/Описание
Administrator Password	Установка пароля Администратора
User Password	Установка пароля Пользователя
Secure Boot	Смотреть подменю > Secure Boot

6.1 Secure Boot



Элемент меню	Опция/Описание
Secure Boot	Enabled/Disabled
Secure Boot Mode	Standart/Custom. Варианты режима безопасной загрузки: стандартный или пользовательский. В пользовательском режиме переменные политики безопасной загрузки могут быть настроены физически присутствующим пользователем без полной аутентификации.
Restore Factory Keys	Смотреть подменю > Restore Factory Keys
Reset To Setup Mode	Смотреть подменю > Reset To Setup Mode
Expert Key Management	Смотреть подменю > Expert Key Management

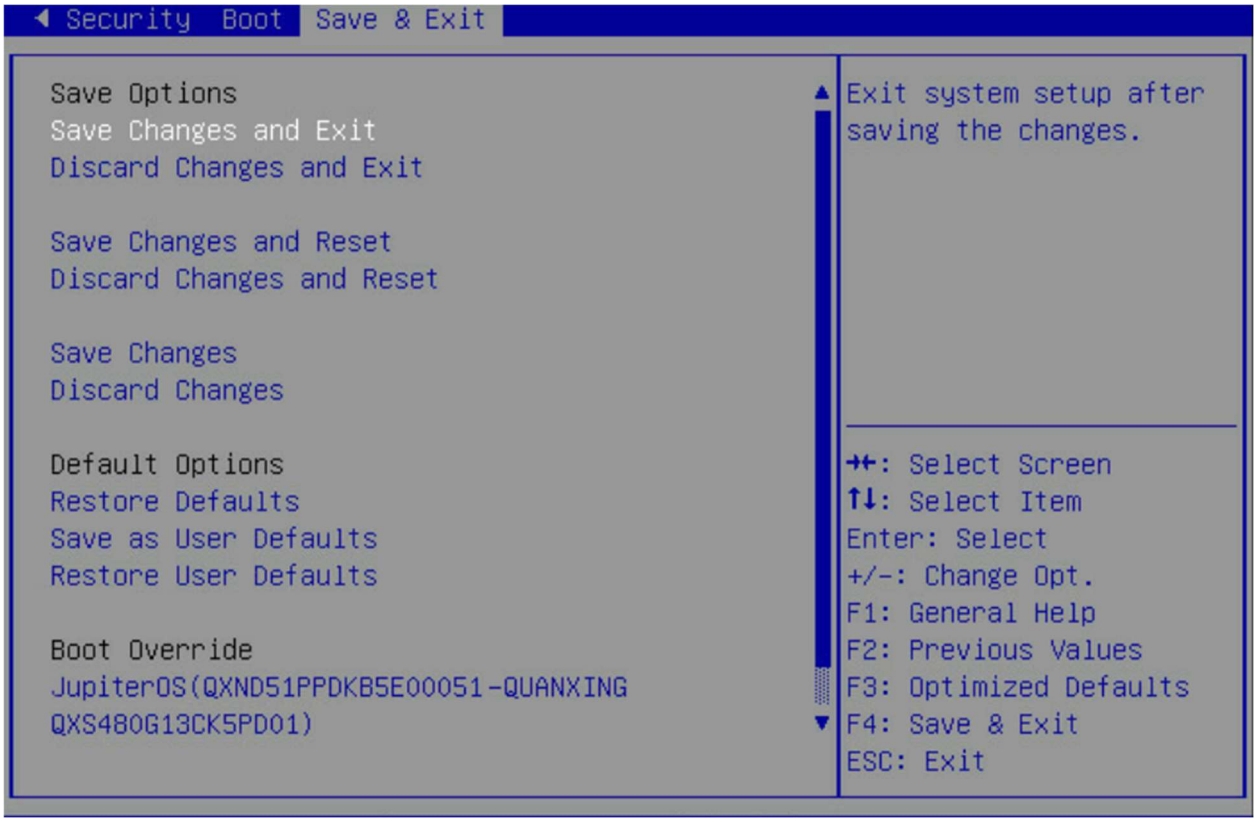
7. Boot



Элемент меню	Опция/Описание
Setup Promt Timeout	Количество секунд ожидания ключа активации настройки. 65535 (0xFFFF) означает неопределенное время ожидания.
Bootup NumLock State	On/Off. Включить или выключить NumLock
Quiet Boot	Enabled/Disabled. Включение или выключение Quiet Boot
Boot mode select	UEFI/Legacy. Выбор режима загрузки.
Boot Option #1 / #2 / #3 / #4 / #5	Press [Enter] to configure the boot order priority. By default, the server searches for boot devices in the following sequence: 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
Optimized Boot	Enabled/Disabled. Включает или отключает оптимизированную загрузку. Включение оптимизированной загрузки отключит поддержку Csm и отключит подключение сетевых устройств для уменьшения времени загрузки. При отключении оптимизированной загрузки обязательно

	восстановить предыдущее значение параметра поддержки Csm перед включением оптимизированной загрузки
UEFI Hard Disk Drive BBS Priorities	Нажмите [Enter], чтобы настроить приоритет загрузки.
UEFI Other Drive BBS Priorities	Нажмите [Enter], чтобы настроить приоритет загрузки.

8. Save & Exit



Элемент меню	Опция/Описание
Save Changes and Exit	Перезапускает систему после сохранения внесенных изменений. Доступные варианты: Да, Нет.
Discard Changes and Exit	Перезапускает систему без сохранения изменений. Доступные варианты: Да, Нет.
Save Changes and Reset	Перезапускает систему после сохранения внесенных изменений. Доступные варианты: Да, Нет.
Save Changes	Сохраняет изменения, сделанные до сих пор в любой из опций настройки. Доступные опции: Да, Нет.
Discard Changes	Отменяет внесенные изменения и закрывает настройки BIOS. Доступные варианты: Да, Нет.
Restore Defaults	Загружает настройки по умолчанию для всех параметров настройки Базовой системы ввода-вывода для систем хранения данных на базе процессоров x86. Настройки по умолчанию довольно требовательны с точки зрения потребления ресурсов. Если использовать низкоскоростные микросхемы памяти или другие виды низкопроизводительных компонентов и загрузить эти настройки, система может работать некорректно. Доступные параметры: Да, Нет.

Save as User Defaults	Сохраняет внесенные изменения как настройки пользователя по умолчанию. Доступные варианты: Да, Нет.
Restore User Defaults	Loads the user default settings for all BIOS setup parameters. Options available: Yes, No.
Boot Override	Нажмите [Enter], чтобы настроить устройство в качестве загрузочного диска.