

ESXI??TMP??

???Esxi????????? TPM 2.0 ????????????

??



??????

1.?????????????logo???Del?????????BIOS

Aptio Setup - AMI

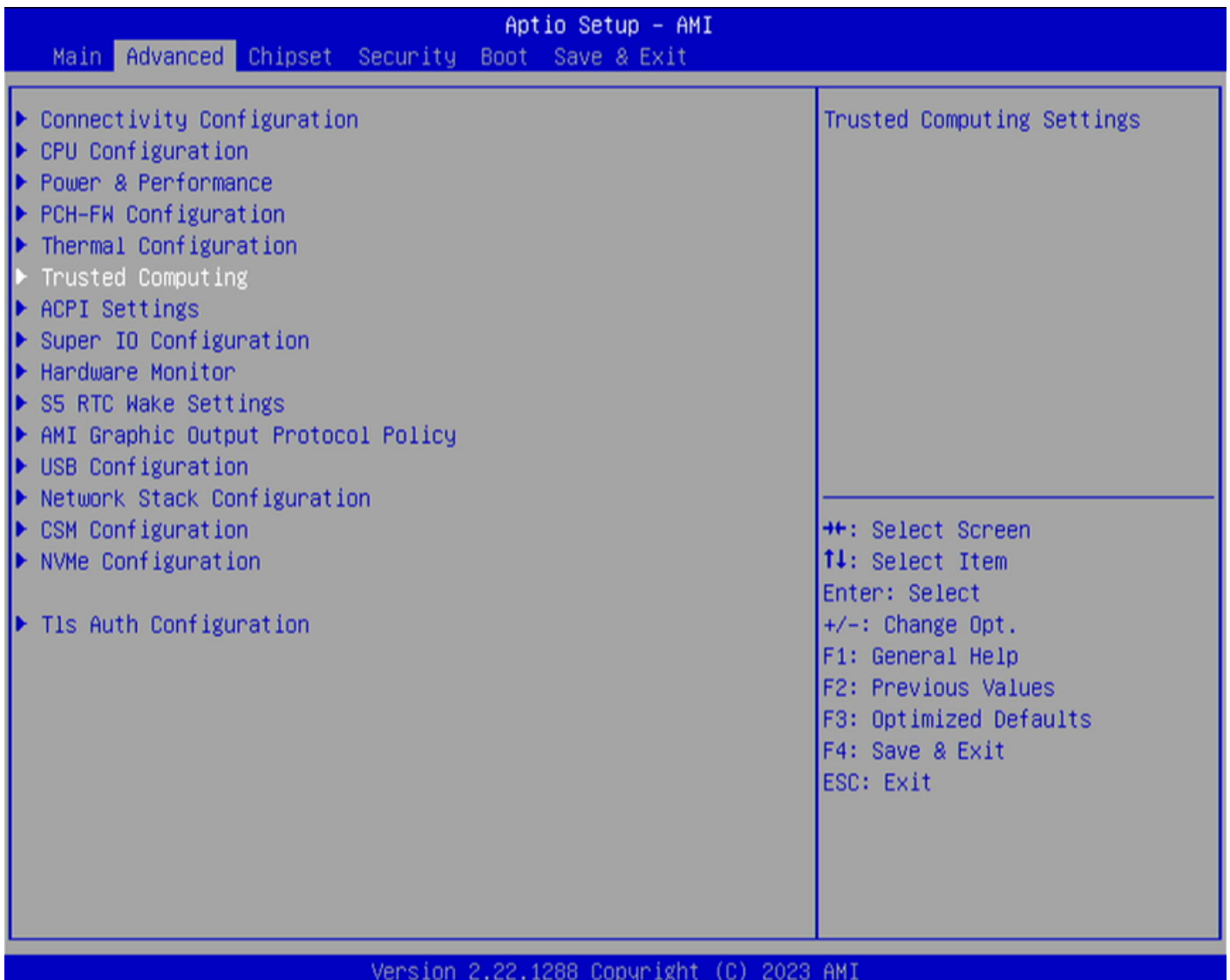
Main Advanced Chipset Security Boot Save & Exit

BIOS Information	
BIOS Vendor	American Megatrends
BIOS Version	N95V104
Build Date and Time	03/14/2023 14:47:00
Access Level	Administrator
Serial Number	Default string
Processor Information	
Name	AlderLake ULX
Type	Intel(R) Core(TM) i3-N305
Speed	1800 MHz
ID	0xB06E0
Stepping	A0
Number of Efficient-cores	8Core(s) / 8Thread(s)
Microcode Revision	E
GT Info	0x46D0
Memory Information	
Total Memory	16384 MB
Memory Frequency	4800 MHz
PCH Information	
Name	PCH-N
PCH SKU	N Premium SKU

⇐: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI

2.????Advanced?????Trusted Computing?



3.??Security Device Support? ???Disabled??????

Aptio Setup - AMI

Advanced

TPM 2.0 Device Found
Firmware Version: 600.18
Vendor: INTC

Security Device Support [Enable]
Active PCR banks SHA256
Available PCR banks SHA256,SHA384,SM3

SHA256 PCR Bank [Enabled]
SHA384 PCR Bank [Disabled]
SM3_256 PCR Bank

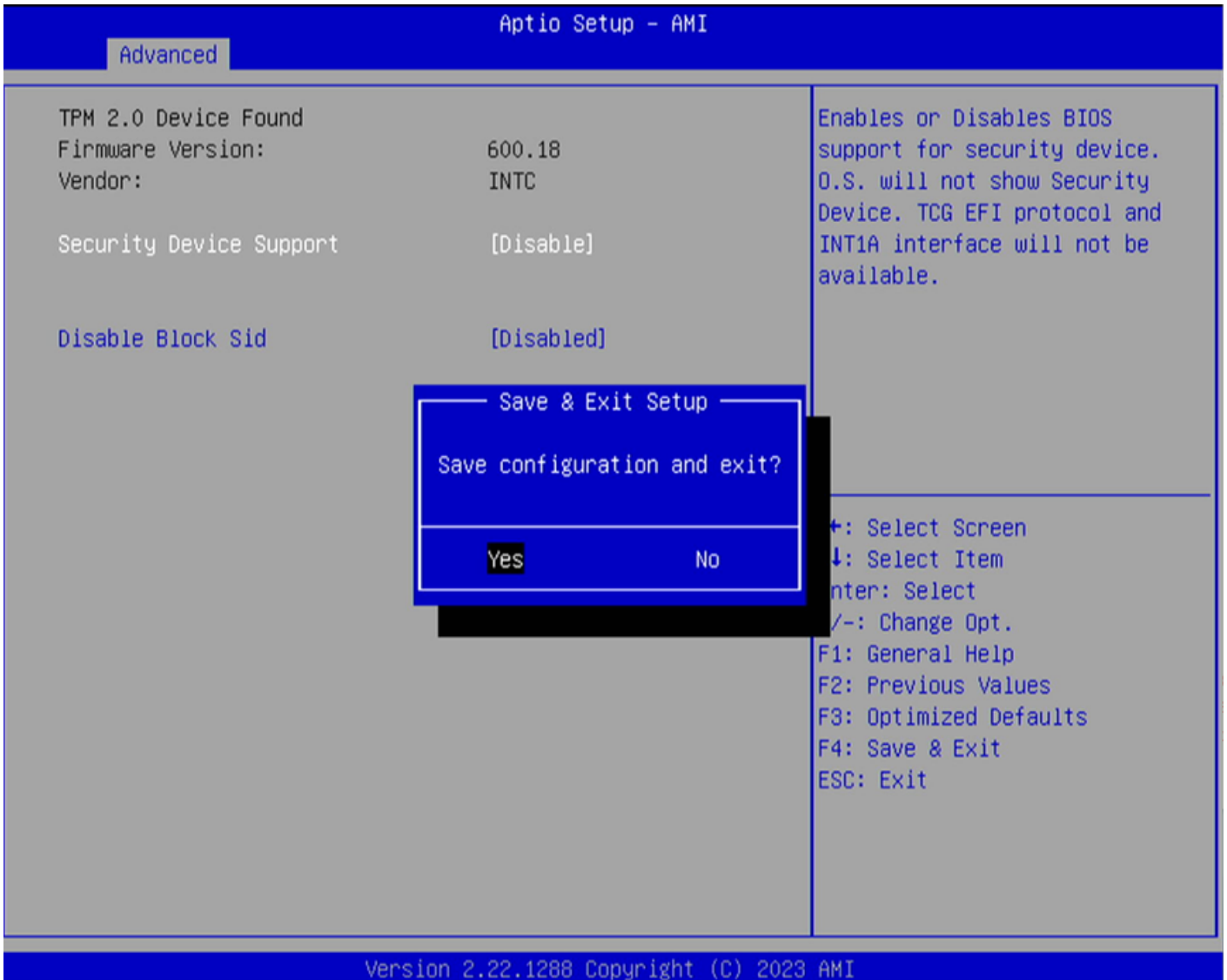
Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Security Device Support
Disable
Enable

Pending operation
Platform Hierarchy
Storage Hierarchy
Endorsement Hierarchy [Enabled]
Physical Presence Spec Version [1.3]
TPM 2.0 InterfaceType [CRB]
Device Select [Auto]
Disable Block Sid [Disabled]

Select Screen
Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

4.?????F4???????



5.????Esxi????????TPM???



