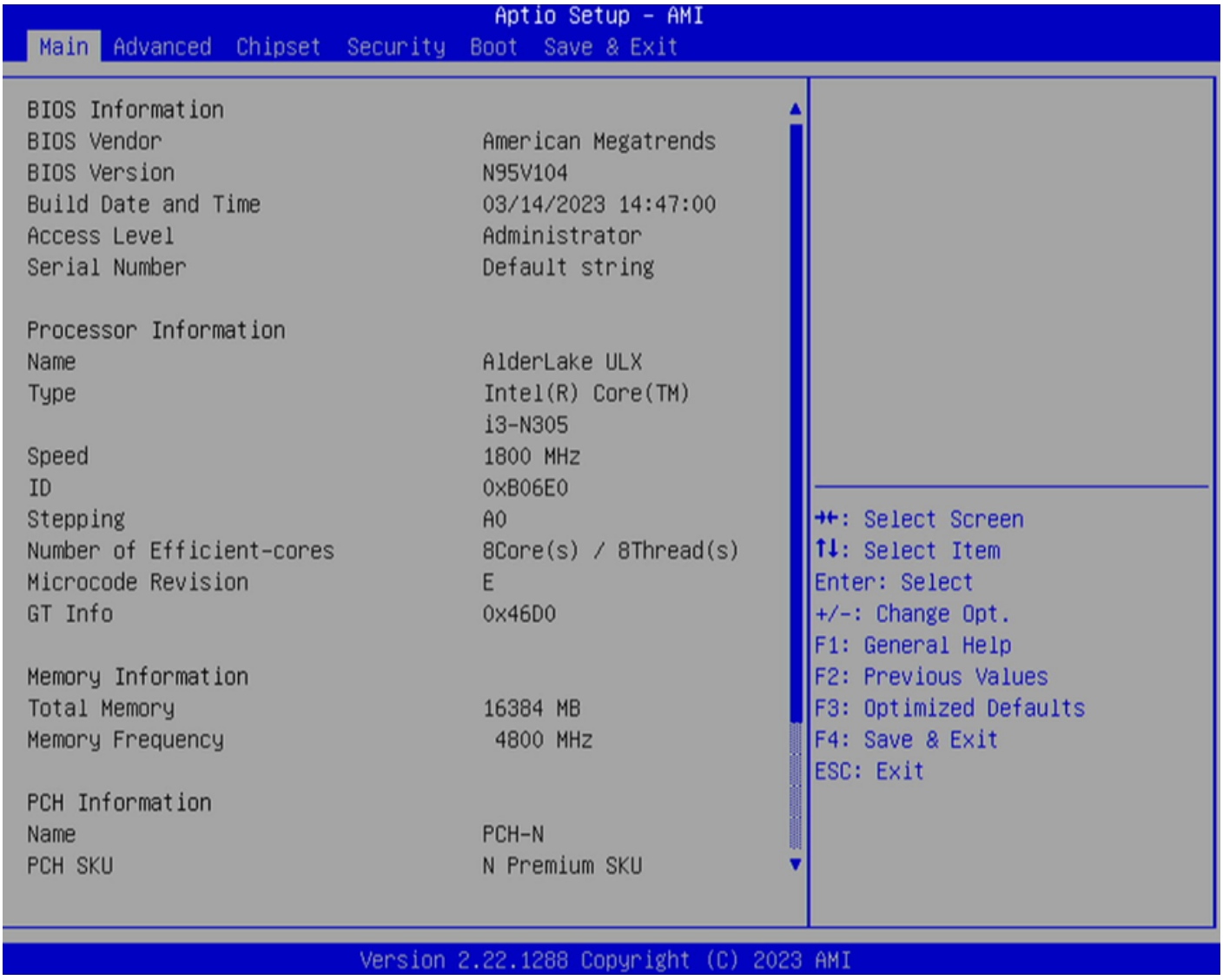
ESXI??TMP??

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

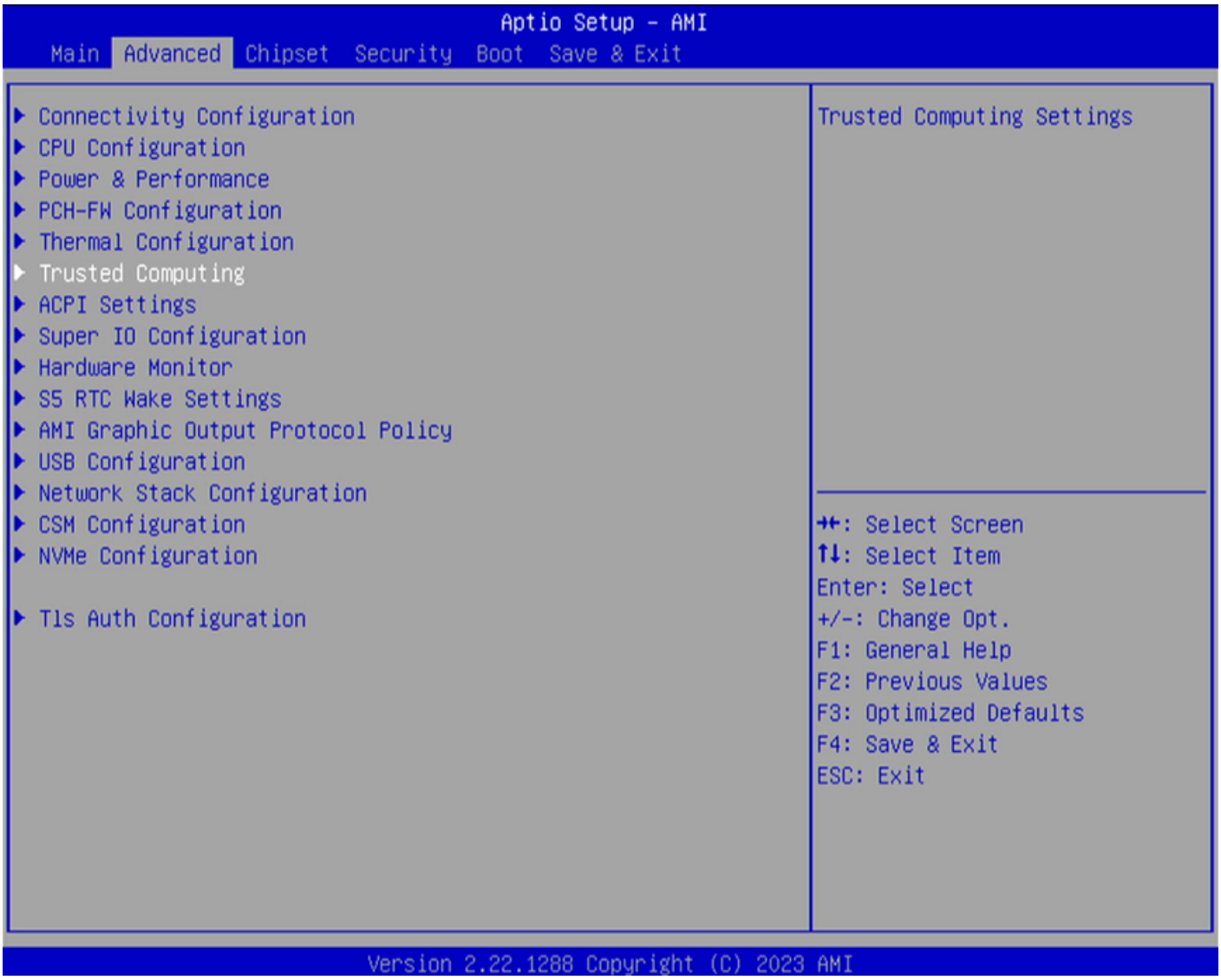
??

?????

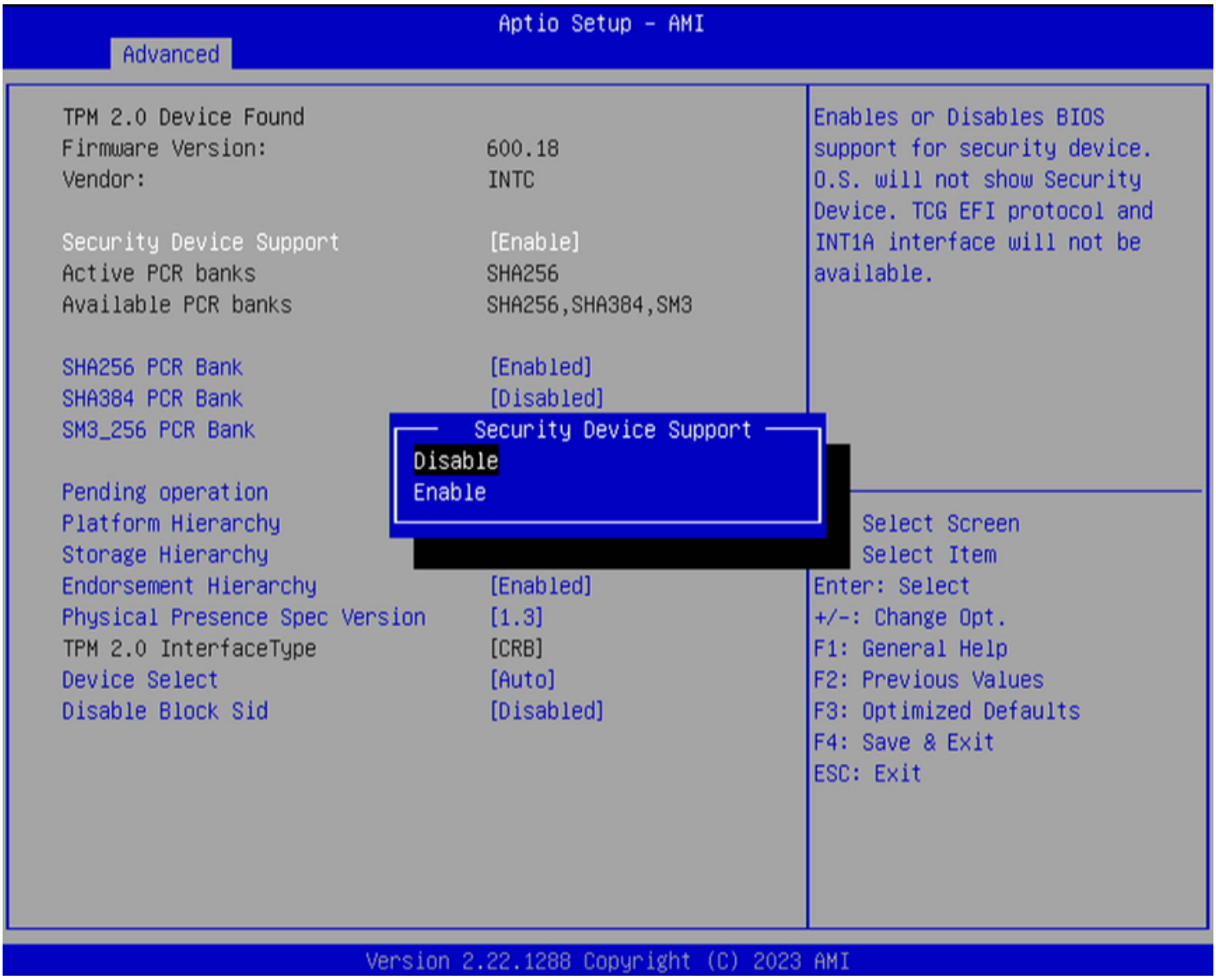
1.???????????logo???Del??????BIOS



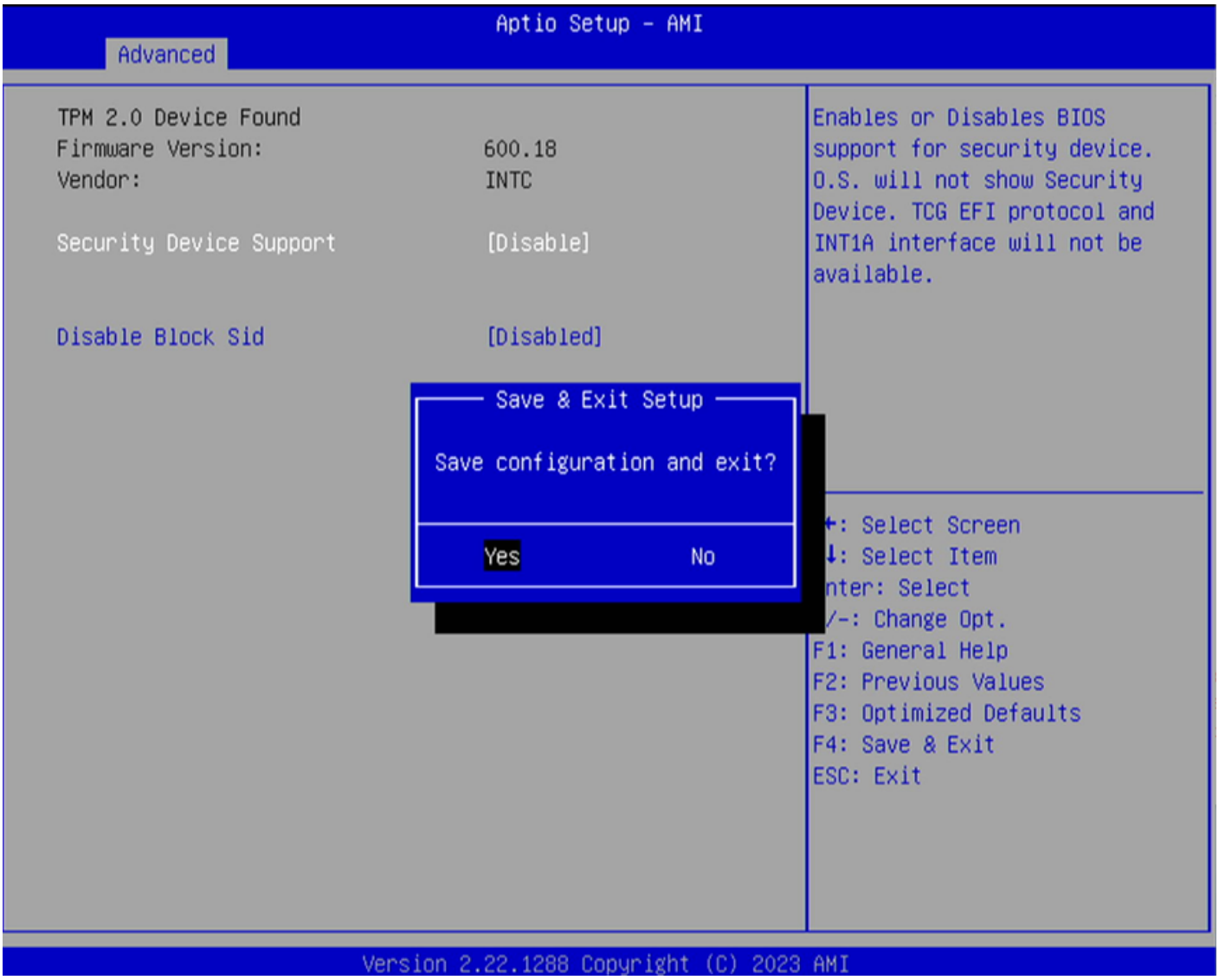
2.????Advanced?????Trusted Computing?



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
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]
Security Device Support
Disable
Enable
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.
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

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



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

Revision #1
Created 31 March 2025 10:27:21 by Admin

Updated 31 March 2025 10:29:47 by Admin