Chapter 5

BIOs and UEFI

Episode 5.01

Episode title: **What is BIOs?**

Objective:

- BIOS programming enables interaction with motherboard before OS loads
- BIOS is stored in nonvolatile media, thus called firmware
- POST routines are built into firmware
- The System Setup utility is also part of the firmware

Lower 3rds

Basic Input/Output System (BIOS)

Unified Extensible Firmware Interface (UEFI)

BIOS = Firmware

Main BIOS (M_BIOS)

Backup BIOS (B-BIOS)

Lower 3rds

BIOS performs the tasks that start up a PC

Power-On Self-Test (POST)

BIOS utility

UEFI interface: keyboard shortcuts, Settings app, command prompt

Lower 3rds

BIOS/UEFI configuration settings utility

Trusted Platform Module (TPM)

Fan control / Temperature monitoring settings

remove the CMOS battery

Press PC's on/off button for 10 sections

Complementary Metal-Oxide-Semiconductor (CMOS)

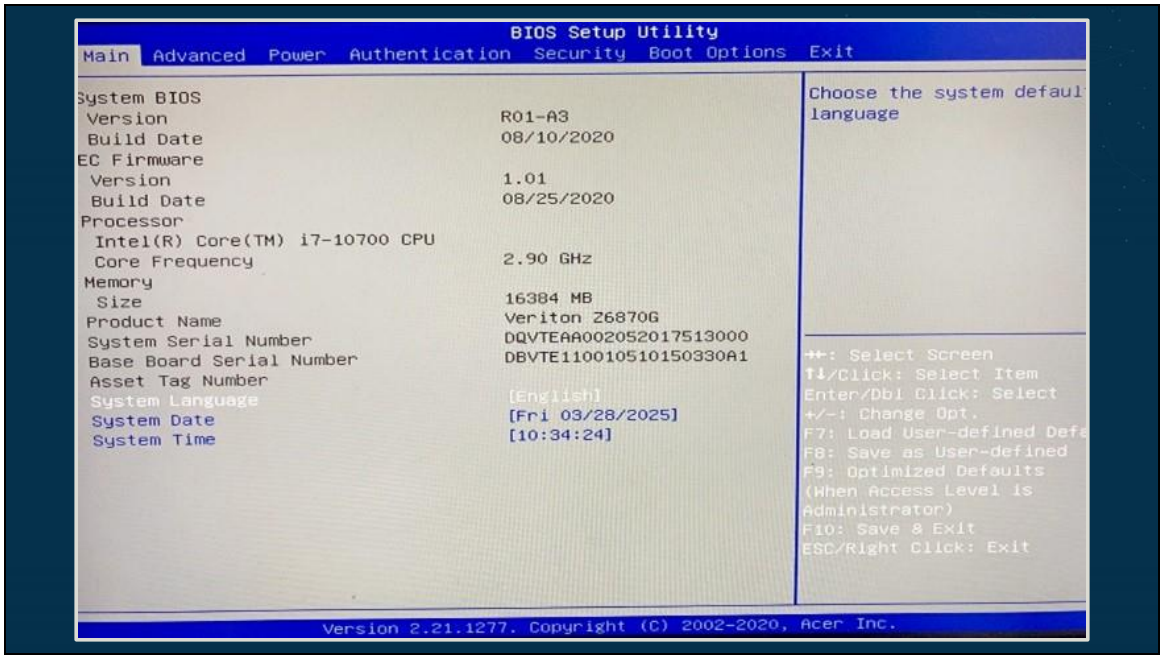
BIOS Chips

M_BIOS

- Active BIOS chip

B_BIOS

- Contains factory defaults

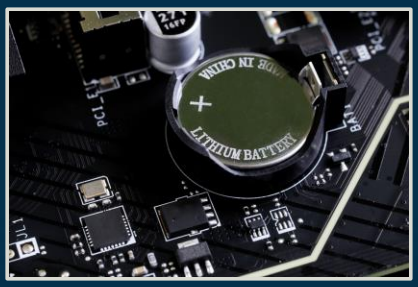

BIOS Setup Utility
Main Advanced Power Authentication Security Boot Options Exit
System BIOS
Version R01-A3
Build Date 08/10/2020
EC Firmware
Version 1.01
Build Date 08/25/2020
Processor
Intel(R) Core(TM) i7-10700 CPU
Core Frequency 2.90 GHz
Memory
Size 16384 MB
Product Name Veriton Z6870G
System Serial Number DQVTEAA002052017513000
Base Board Serial Number DBVTE1100105101503 30A1
Asset Tag Number
System Language [English]
System Date [Fri 03/28/2025]
System Time [10:34:24]
Choose the system defaul language
++: Select Screen
↑↓/Click: Select Item
Enter/Dbl Click: Select
+/-: Change Opt.
F7: Load User-defined Def
F8: Save as User-defined
F9: Optimized Defaults
(When Access Level is Administrator)
F10: Save & Exit
ESC/Right Click: Exit
Version 2.21.1277. Copyright (C) 2002-2020, Acer Inc.

CMOS Chip

Constantly powered by its battery

Retains data even when the PC is powered off

Saves configuration settings of the PC



Episode 5.02

Episode title:

Objective:

Episode 5.03

Episode title: **System Setup**

Objective: See Next Page

Objectives

•220-1201 – Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

- BIOS/Unified Extensible Firmware Interface (UEFI) settings
  - Boot options
  - USB permissions
  - Trusted Platform Module (TPM) security features
  - Fan considerations
  - Secure Boot
  - Boot password
  - BIOS password

·220-1202 – 2.7 Given a scenario, apply workstation security options and hardening techniques.

- Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords

Lower 3rds

New BIOS called UEFI

We call it UEFI BIOS

Press Del key to enter Setup Menu

F12 to enter Boot Menu

Boot options

Lower 3rds

USB permissions

Trusted Platform Module (TPM) security features

Fan considerations

Secure Boot

Boot password

BIOS password

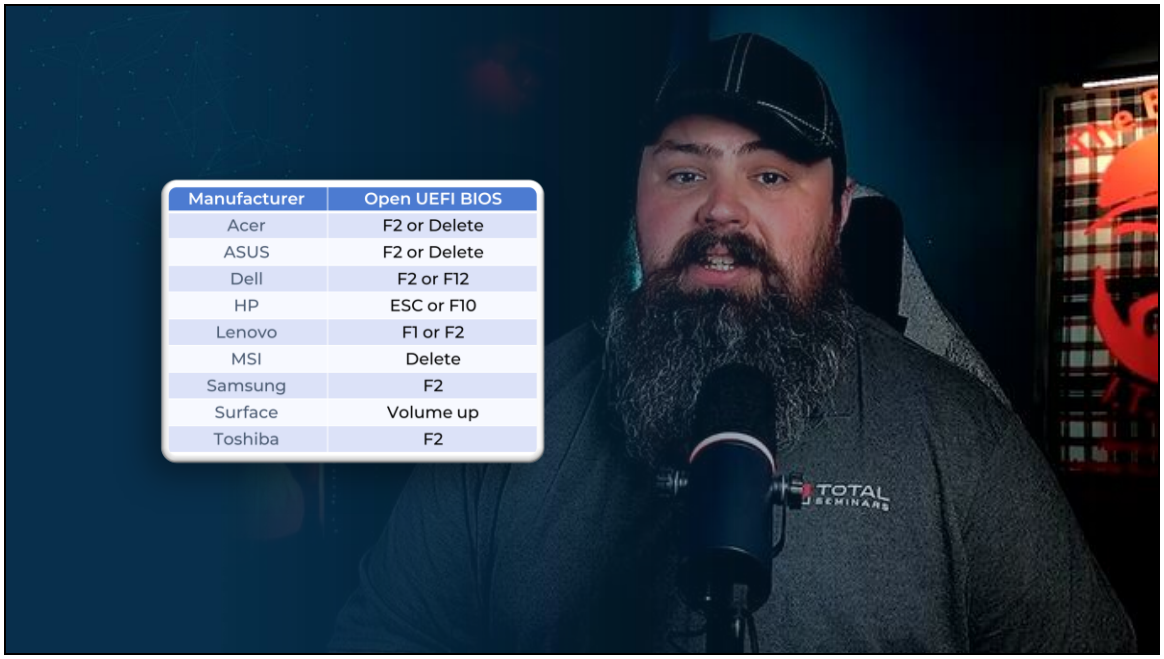
Lower 3rds

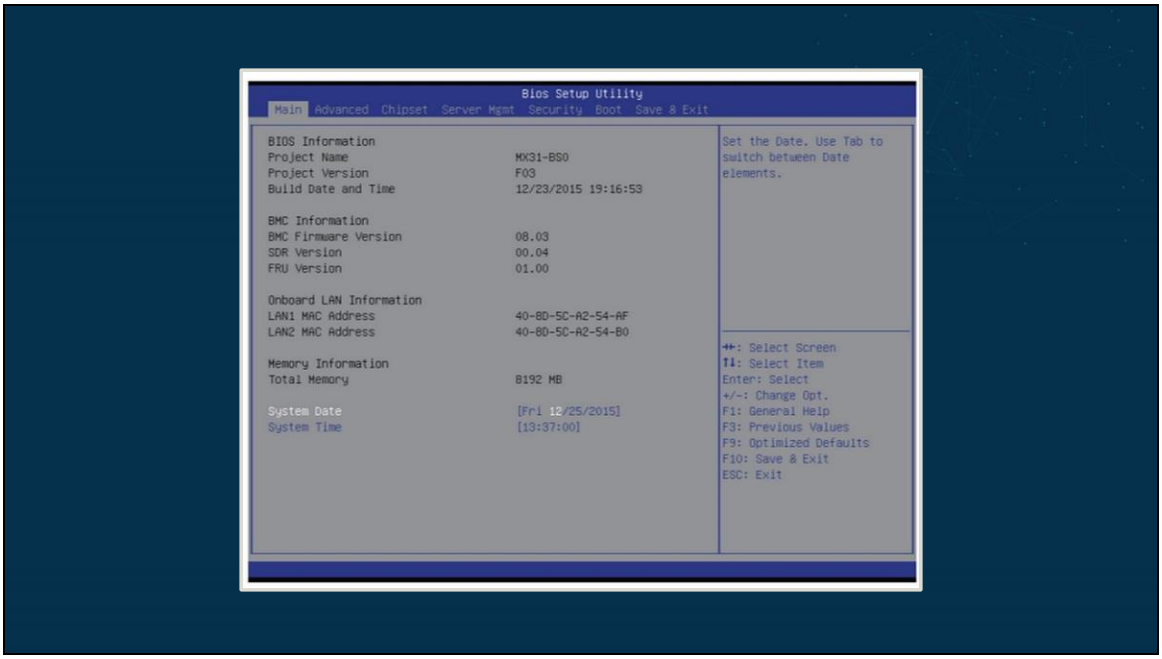
Administrator password / User password

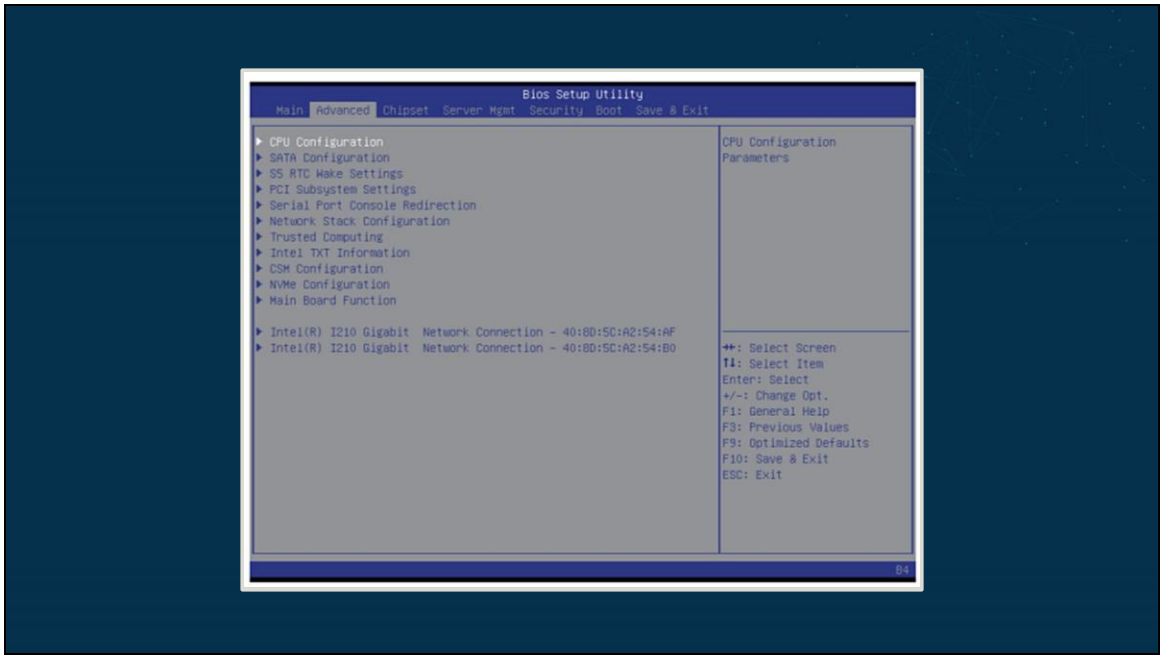
F2 or Delete

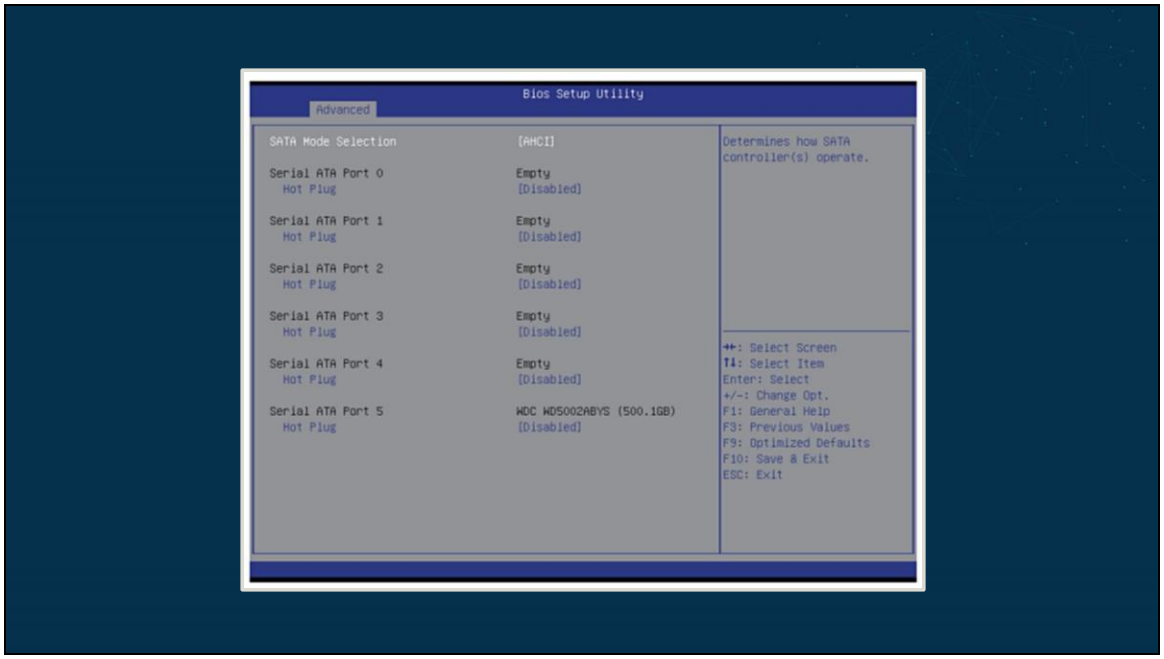
we can control all of this

Make sure that you're aware of it


Manufacturer
Open UEFI BIOS
Acer
F2 or Delete
ASUS
F2 or Delete
Dell
F2 or F12
HP
ESC or F10
Lenovo
F1 or F2
MSI
Delete
Samsung
F2
Surface
Volume up
Toshiba
F2
TOTAL
SEMINARS


Bios Setup Utility
Main Advanced Chipset Server Mgmt Security Boot Save & Exit
BIOS Information
Project Name MX31-BS0
Project Version F03
Build Date and Time 12/23/2015 19:16:53
BMC Information
BMC Firmware Version 08.03
SDR Version 00.04
FRU Version 01.00
Onboard LAN Information
LAN1 MAC Address 40-8D-5C-A2-54-AF
LAN2 MAC Address 40-8D-5C-A2-54-B0
Memory Information
Total Memory 8192 MB
System Date [Fri 12/25/2015]
System Time [13:37:00]
Set the Date. Use Tab to switch between Date elements.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit


Bios Setup Utility
Main Advanced Chipset Server Mgmt Security Boot Save & Exit
CPU Configuration
SATA Configuration
SS RTC Wake Settings
PCI Subsystem Settings
Serial Port Console Redirection
Network Stack Configuration
Trusted Computing
Intel TXT Information
CSM Configuration
NVMe Configuration
Main Board Function
Intel(R) I210 Gigabit Network Connection - 40:8D:5C:A2:54:AF
Intel(R) I210 Gigabit Network Connection - 40:8D:5C:A2:54:B0
CPU Configuration
Parameters
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit
84

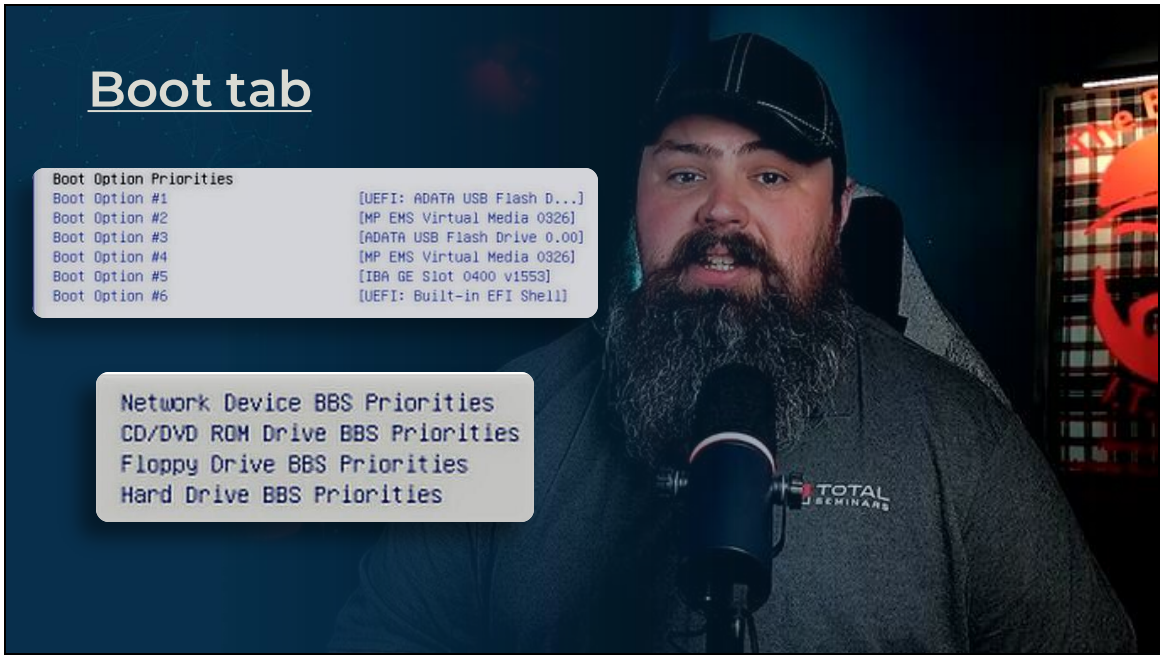

Bios Setup Utility
Advanced
SATA Mode Selection
[AHCI]
Determines how SATA controller(s) operate.
Serial ATA Port 0
Empty
Hot Plug
[Disabled]
Serial ATA Port 1
Empty
Hot Plug
[Disabled]
Serial ATA Port 2
Empty
Hot Plug
[Disabled]
Serial ATA Port 3
Empty
Hot Plug
[Disabled]
Serial ATA Port 4
Empty
Hot Plug
[Disabled]
Serial ATA Port 5
WDC WD5002ABYS (500.1GB)
Hot Plug
[Disabled]
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

Chipset tab


Bios Setup Utility
Main Advanced Chipset Server Mgmt Security Boot Save & Exit
VT-d [Enabled]
xDCI Support [Disabled]
Restore AC Power Loss [Last State]
ERP Support [Disabled]
Intel Server Platform Services
System Agent (SA) Configuration
Power Policy
VT-d capability
++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

Boot tab


Bios Setup Utility
Main Advanced Chipset Server Mgmt Security Boot Save & Exit
Boot Configuration
Bootup NumLock State [On]
Full Screen LOGO Show [Enabled]
Boot Option Priorities
Boot Option #1 [UEFI: ADATA USB Flash D...]
Boot Option #2 [MP EMS Virtual Media 0326]
Boot Option #3 [ADATA USB Flash Drive 0.00]
Boot Option #4 [MP EMS Virtual Media 0326]
Boot Option #5 [IBA GE Slot 0400 v1553]
Boot Option #6 [UEFI: Built-in EFI Shell]
Network Device BBS Priorities
CD/DVD ROM Drive BBS Priorities
Floppy Drive BBS Priorities
Hard Drive BBS Priorities
Select the keyboard NumLock state
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit


Boot tab
Boot Option Priorities
Boot Option #1 [UEFI: ADATA USB Flash D...]
Boot Option #2 [MP EMS Virtual Media 0326]
Boot Option #3 [ADATA USB Flash Drive 0.00]
Boot Option #4 [MP EMS Virtual Media 0326]
Boot Option #5 [IBA GE Slot 0400 v1553]
Boot Option #6 [UEFI: Built-in EFI Shell]
Network Device BBS Priorities
CD/DVD ROM Drive BBS Priorities
Floppy Drive BBS Priorities
Hard Drive BBS Priorities
TOTAL SEMINARS

Episode 5.04

Episode title: **Troubleshooting Firmware**

Objective:

System Setup Screen