HP EliteDesk 800 G4 Mini BIOS Configuration
Document Version 1.1
02-October-2020

Security
- TPM Embedded Security
    - TPM Device: Hidden
    - TPM Activation Policy: No prompts
- BIOS Sure Start
    - All options unchecked
- Intel SGX: Disable

Advanced
- Boot Options
    - Startup Delay: 5. (useful during testing to give time for Function key presses)
    - Fast Boot: unchecked
    - USB Storage Boot: **checked**
    - Network (PXE) Boot: unchecked
    - Audio Alerts During Boot: unchecked (to disable beep after pressing F9 at boot)
    - UEFI Boot Order
        - USB
        - Other boot drives as desired
    - Legacy Boot Order
        - Unchecked
- HP Sure Recover
    - Unchecked
- Secure Boot Configuration
    - Legacy Support **Disable** and Secure Boot **Disable**
    - Secure Boot Key Management
        - All options unchecked
- System Options
    - Configure Storage Controller for RAID: unchecked
    - Configure Storage Controller for Intel Optane: unchecked
    - Turbo-boost: checked
    - Hyperthreading: checked
    - Multi-processor: checked
    - Virtualization Technolgy (VTx): checked
    - Virtualization Technology for Directed I/O (VTd): unchecked
    - M.2 SSD 1: checked
    - M.2 SSD 2: checked
    - M.2 WLAN BT (unchecked if you have Intel WLAN / BT device or don't have WLAN / BT)
    - Allow PCIe/PCI SERR# Interrupt: checked

- o Power Button Override: 4 sec
- o USB Type-C Connector System Software Interface (USCI): unchecked
- o HP Application Driver: unchecked
- Built-In Device Options
  - o Embedded LAN Controller: checked
  - o Wake On LAN: Disabled
  - o Dust Filter: Unchecked
  - o Video Memory Size: ~~64MB~~ **512MB**
  - o Audio Device: checked
  - o Microphone: Enable
  - o Internal Speakers: checked
  - o Increase Idle Fan Speed (%): 0
  - o M.2 USB / Bluetooth: Unchecked (disabled in System Options)
- Port Options
  - o Front USB Ports: checked
  - o Front USB Port 1: checked
  - o Front USB Port 2: checked
  - o Front USB Port 3: checked
  - o Rear USB Port 1: checked
  - o Rear USB Port 2: checked
  - o Rear USB Port 3: checked
  - o Rear USB Port 4: checked
  - o USB Legacy Port Charging: unchecked
  - o Front USB Type-C Downstream Charging: unchecked
  - o SATA 0: checked
  - o Restrict USB Devices: Allow all USB Devices
- Option ROM Launch Policy
  - o This is grayed out for me (probably as a result of another selection)
- Power Management Options
  - o Runtime Power Management: checked
  - o Extended Idle Power States: checked
  - o S5 Maximum Power Savings: checked
  - o SATA Power Management: checked
  - o PCI Express Power Management: checked
  - o Power On from Keyboard Ports: this option is grayed out for me
  - o Unique Sleep State Blink Rates: unchecked
- Remote Management Options
  - o Intel Management Engine (ME): checked (required for proper UHD 630 Sleep / Wake)
  - o Intel Active Management Technology (AMT): unchecked