HP EliteDesk 800 G4 Mini BIOS Configuration
Document Version 1.0
09-June-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
  - 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
  - Power Button Override: 4 sec

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