Interactive BIOS simulator

HP Engage One Pro AIO System

Welcome to the interactive BIOS simulator for the
HP Engage One Pro AIO System

Here's how to use it...

BIOS Utility Menus: (Click the link to navigate to the individual menus)
On this page you will find thumbnail images of each of the product's BIOS utility menus. To view a specific menu in greater detail, simply click that thumbnail. Just as in the live BIOS, on each menu, you can select the tab of each of the other utility menus to navigate directly to that menu.

Menu options:
While the menu options cannot be toggled, many of them offer item specific information about that option. To view this information, use the cursor to rollover the option and the information will present in a pane on the right of the BIOS screen.

That's it!

On every page there is a link that brings you back to either this Welcome page or the BIOS Utility Menus page enabling you to navigate to whatever BIOS option you wish to review.

BIOS Utility Menus

Main　　　　Security　　　　Advanced　　　　UEFI Drivers

Item Specific Help

Suppress POST Errors

BASIC SYSTEM INFORMATION

Item Specific Help

Product Name	HP Engage One Pro AIO System
Processor 1	Intel(R) Pentium(R) Gold G6400E CPU @ 3.80GHz
Memory Size	16384 MB
System BIOS	S30 Ver. 80.30.00 08/06/2020

SERVICE --

Born On Date	09/22/2020
Serial Number	8CN07600GZ
SKU Number	9UK26AV
Universally Unique Identifier (UUID)	E214D0C0E12EAD4F96E37E26D7B9C5F9
UUID (standard format)	C0D014E2-2EE1-4FAD-96E3-7E26D7B9C5F9
Asset Tracking Number	

Help

Product Name   HP Engage One Pro AIO System
Memory Size   16384 MB
Storage Devices   SK hynix PC601 HFS256GD9TNG-L2A0A-NJ06Q630010107D5I (256 GB)

PROCESSOR 1 ---

ProcessorType   Intel(R) Pentium(R) Gold G6400E CPU @ 3.80GHz
Cache Size (L1/L2/L3)   128 KB / 512 KB / 4 MB
Processor Speed   3800 MHz
Processor Cores   2
MicroCode Revision   BE
Processor Stepping   0
Memory Speed   2400 MHz
DIMM 1   8 GB Samsung
DIMM 3   8 GB Samsung

Help

Main

Item Specific Help

FIRMWARE ---

System BIOS	S30 Ver. 80.30.00 08/06/2020
ME Firmware Version	14.0.39.1339
ME Firmware Mode	Enable
Audio Controller	Realtek ALC3247
Video BIOS Version	Intel(R) GOP Driver [9.0.1107]
Reference Code Revision	9.0.3F.20
Super I/O Firmware Version	9.8.12
USB Type-C Controller(s) Firmware Version:	
	Head PD : 5.6.0

SERVICE ---

Born On Date	09/22/2020
Serial Number	8CN07600GZ
SKU Number	9UK26AV

Help

Item Specific Help

Universally Unique Identifier (UUID)   E214D0C0E12EAD4F96E37E26D7B9C5F9
UUID (standard format)   C0D014E2-2EE1-4FAD-96E3-7E26D7B9C5F9
Asset Tracking Number
Feature Byte   3E3X476J6S6b7N7R7S7V7W7m8yapaq

                                              aub8bhcAdUdpdqfPhKjhk8mDmf.Af
Build ID   20WWTSAT6ay#SABA#DABA
Product Family   103C_5330US HP Engage One Pro
System Board ID   874F
System Board CT Number   10E7C6752B8EXX

COMMUNICATION --

Integrated MAC Address 1   10-E7-C6-75-2B-8E

Help

HP PC Hardware Diagnostics UEFI

Please select a Language.

English

Cestina

Dansk

Deutsch

Nederlands

Espanol

eesti keel

Suomi

Francais

Hrvatski

Magyar

Main

BIOS Event Log

Clear BIOS Event Log on Next Boot

Item Specific Help

Help

Item Specific Help

View BIOS Event Log

Date	Time	Description

No event have been logged

Help

Export to USB Key

The file cannot be accessed. Please insert a USB storage device and try again.

HP Computer Setup

Update System BIOS

Current System BIOS Version: S30 Ver. 80.30.00
Current BIOS Release Date: 06/06/2020
Installation Date of Current BIOS: 09/19/2020
Most Recent Update Check: Never Checked

----

(1)

Lock BIOS Version **(2)**

Native OS Firmware Update Service

BIOS Rollback Policy   **(3)**

Allow BIOS Updates Using a Network **(4)**

(5)

(6)

Help

Item Specific Help

1. Check HP.com for BIOS Updates
  Checks for the latest BIOS release revision on the network, and lets the user decide whether to download the BIOS image and update System.

2. Lock BIOS Version
  If not selected, then BIOS updates are allowed, if selected then updates to BIOS are not allowed.

3. *Click on the field to see the options.*

4. Allow BIOS Updates Using a Network
  Enable/Disable automatic BIOS updates through the network in a scheduled basis.

5. BIOS Update Preferences
  Sets the configurations to perform BIOS updates through the network.

6. Network Configuration Settings
  Configure network settings to be used for download and upload.

BIOS Update Preferences

    Check for Update on Next Reboot   **1**

BIOS Source   **2**

Automatic BIOS Update Setting

  3

BIOS Update Frequency   **4**

Help

Item Specific Help

1. Check for Update on Next Reboot
   Enable/Disable an automatic BIOS check on next reboot.

2. BIOS Source
   Choose one of the available options.
   Click on the field to see the options.

Automatic BIOS Update Setting
   Choose one of the available options.
   Click on the field to see the options.

3. BIOS Update Frequency
   Choose one of the available options.

Network Configuration Settings

Proxy Server **1**

2

IPv4 Configuration **3**

DNS Configuration **4**

100 **5**

Data transfer timeout

Force HTTP no-cache **6**

Item Specific Help

1. Proxy Server
   Enable/Disable the use of a proxy server.

2. Edit Proxy Server
   Specify the Proxy Server Address and the Port Number through the common-use <server>:<port> notation.

3. Test Network Connection
   Check the network connection using current BIOS update configuration.
   Click on the field to see the options.

4. IPv4 Configuration
   Setup for static IPv4 address.
   Click on the field to see the options.

5. DNS Configuration
   Configure a list of DNS addresses.

6. Force HTTP no-cache
   Disable HTTP caching.

Help

Item Specific Help

Change Date And Time

Set Date (MM/DD/YYYY)   09 / 21 / 2020
Set Time (HH:MM):   19 : 13

Help

HP Computer Setup

System IDs

Item Specific Help

Help

Asset Tracking Number

Current Setting:

Press the space key followed by the enter key to clear current setting

Ownership Tag

Current Setting:

Press the space key followed by the enter key to clear current setting

HP Computer Setup

Replicated Setup

Item Specific Help

Help

Administrator Tools

1

Security Configuration

Physical Presence Interface **2**

Intel Software Guard Extensions (SGX) **3**

Utilities

Absolute® Persistence Module Current State

Activation Status : Inactive

Absolute® Persistence Module Permanent Disable : No

System Management Command

Item Specific Help

1. Create BIOS Administrator Password
The Administrator password controls access to the following features:
- Setup Menu (F10)
- 3rd Party Option ROM Management (F3)
- Update System ROM
- WMI Commands that change system settings
- BIOS Configuration Utility (BCU)
- Alternative Power-On Password

2. Physical Presence Interface
When this feature is set to "Enable", then the user is notified on system power up when changes are made to system security policy, and the user must manually agree to those changes before the change is confirmed

3. Intel Software Guard Extensions (SGX)
Enable/Disable Software Guard Extensions (SGX)
Click on the field to see the options.

BIOS Administrator Password

Enter BIOS Administrator Password

POST Power-On Password

Enter POST Power-On Password

TPM Embedded Security

TPM Specification Version   2.0

TPM Device   **1**

    TPM State   **2**

Clear TPM

TPM Activation Policy

Item Specific Help

1. TPM Device
   Exposes the integrated Trusted Platform
   Module (TPM) for use.
   Click on the field to see the options.

TPM State
   Enables the integrated Trusted Platform
   Module (TPM).

BIOS Sure Start

    Verify Boot Block on every boot

    Prompt on Network Controller Configuration Change

    Dynamic Runtime Scanning of Boot Block

    Sure Start BIOS Settings Protection   **1**

    Sure Start Secure Boot Keys Protection

    Enhanced HP Firmware Runtime Intrusion Prevention and Detection   **2**

Sure Start Security Even Policy   **3**

Sure Start Security Event Boot Notification

Item Specific Help

1. Sure Start BIOS Settings Protection
When enabled, HP Sure Start will lock all critical BIOS settings and provide enhanced protection for these settings via the HP Sure Start non-volatile (flash) memory

- The BIOS administrator credentials must be set to enable this setting
- See HP Sure Start documentation for details on which BIOS settings are protected

2. Enhanced HP Firmware Runtime Intrusion Prevention and Detection
Enables monitoring of HP system firmware executing out of main memory while the user Operating System is running.
Any anomalies detected in HP System firmware that is active while the user operating system is running will result in a Sure Start Security Event being generated. *Click on the field to see the options.*

3. Sure Start Security Event Policy
This setting controls HP Sure Start behavior upon identifying a critical security event (any modification to HP firmware) during OS runtime.
- Log event only - HP Sure Start will log all critical security events m the HP Sure Start Audit log within the HP Sure Start non-volatile (flash) memory
- Log Event and notify user: In addition to logging all critical security events. HP Sure Start will notify the user within thr operating system that a critical event has occurred
- Log Event and power off system: In addition to logging all critical events. HP Sure Start will power off the system upon detecting a HP Sure Start Security Event. Due to the potential for data loss, use of this setting is only recommended in situations where security integrity of the system is a higher priority than the risk of potential data loss

Secure Boot Configuration

    Secure Boot

Secure Boot Key Management

    Import Custom Secure Boot Keys

    Clear Secure Boot keys

    Reset Secure Boot keys to factory defaults

    Enable MS UEFI CA key

    Access to the above settings requires Sure Start Secure Boot Keys Protection to be disabled

Ready BIOS for Device Guard Use

Requires BIOS Administrator credentials to be configured and Secure Boot to be enabled.

Item Specific Help

Secure Platform Management (SPM)

NOTE: Some actions may not be selectable due to a pending password change.

SPM

    SPM Current State: Not provisioned

HP Sure run

    HP Sure Run Current State: Inactive

HP Sure Admin

Enhanced BIOS Authentication Mode (EBAM)

    EBAM Current State: Disabled

Local Access Key: Not Present

Item Specific Help

1. Create BIOS Administrator Password

The Administrator password controls access to the following features:

- Setup Menu (F10)
- 3rd Party Option ROM Management (F3)
- Update System ROM
- WMI Commands that change system settings
- BIOS Configuration Utility (BCU)
- Alternative Power-On Password

2. Physical Presence Interface

When this feature is set to "Enable", then the user is notified on system power up when changes are made to system security policy, and the user must manually agree to those changes before the change is confirmed

3. Intel Software Guard Extensions (SGX)

Enable/Disable Software Guard Extensions (SGX)

Smart Cover

Cover Removal Sensor

Item Specific Help

Hard Drive Utilities

Save/Restore GPT of System Hard Drive **(1)**

Boot Sector (MBR/GPT) Recovery Policy **(2)**

Allow OPAL Hard Drive SID Authentication

Disable Drivelock on NVMe drives before using applications for hardware-based encryption

Item Specific Help

1. **Save/Restore GPT of System Hard Drive**
   Enabling this feature will save the GUID Partition table (GPT) of the system Hard Drive. If the GPT is subsequently changed, the user will be prompted to whether to restore GPT.

2. **Boot Sector (MBR/GPT) Recovery Policy**
   Click on the field to see the options.

Help

HP Computer Setup

Select a Drive

1

Item Specific Help

1. <u>M.2 SSD 1:</u> SK hynix PC601 HFS256GD9T-NG-L2A0A-NJ06Q630010107D5I
Set HDD Password

Help

Item Specific Help

DriveLock Security Options

The hard drive's security state cannot be changed.
Cycle power to manage DriveLock on this drive.

Help

HP Computer Setup

Item Specific Help

Select a Drive

M.2 SSD 1: SK hynix PC601 HFS256GD9TNG-L2A0A-NJ06Q630010107D5I (Drive is locked)

Help

1

Remote HP PC Hardware Diagnostics

2

3

Item Specific Help

1. Port Options
   Enable/Disable Port Settings

2. Settings
   Set the configuration for Remote HP PC
   Hardware Diagnostics, including the URLs
   used for download and upload, the
   scheduled execution frequency, etc.

**3. Execute Remote HP PC Harware
   Diagnostics**
   Immediate execution of Remote HP PC Hard-
   ware Diagnostics based on the configura-
   tions in Settings option. Note that any un-
   saved BIOS settings are lost.

Advanced

HP Computer Setup

Display Language

Select Language

Select Keyboard Layout

Item Specific Help

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Hour   0
Minute   0

Boot Options

Startup Delay (sec.)

    Fast Boot
    USB Storage Boot
    Network (PXE) Boot

After Power Loss

    Prompt on Memory Size Change

    Prompt on Fixed Storage Change

    Audio Alerts During Boot

☐ NumLock on at boot

UEFI Boot Order

        M.2 SSD 1: Windows Boot Manager
        USB:
        NETWORK BOOT: IPV4 Network - Intel(R) Ethernet Connection (11) 1219-LM
        NETWORK BOOT: IPV6 Network - Intel(R) Ethernet Connection (11) 1219-LM

Item Specific Help

HP Sure Recover

HP Sure Recover **1**

Recover from Network **2**

Recover after Boot Failure **3**

Prompt before Boot Failure Recovery **4**

Recovery Agent
URL: http://ftp.hp.com/pub/pcbios/CPR
Username:
Provisioning Version: 0

Recovery Image
URL:
Username:
Provisioning Version: 0

System Options

    Configure Storage Controller for RAID

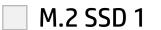   Configure Storage Controller for Intel Optane

    Hyperthreading   **(1)**

    Virtualization technology (VTx)

    Virtualization technology for Directed I/O (VTd)

    DMA Protection

Pre-Boot DMA Protection   **(2)**

☐ M.2 WLAN /BT   **(3)**

☐ M.2 SSD 1   **(4)**

☐ M.2 SSD 2   **(5)**

Power Button Override

    USB Type-C Connector System Software Interface (UCSI)   **(6)**

    HP Applicaton Driver

Item Specific Help

1. Hyperthreading
Permits the user to control the processor capability.

2. Pre-Boot DMA Protection
Selecting the device scope for Pre-Boot DMA Protection.
Click on the field to see the options.

3. M.2 WLAN/BT
Hides the slot from the OS.

4. M.2 SSD 1
Hides the slot from the OS.

5. M.2 SSD 2
Hides the slot from the OS.

6. USB Type-C Connector System Software Interface (UCSI)
The UCSI option should be disabled if booting a Microsoft Windows 10 version before 1709 to avoid system stability issues.

HP Computer Setup

Built-In Device Options

    Embedded LAN Controller

Wake On LAN

Video memory size

    Touch Device

    NFC

    Audio Device   **1**

Microphone

    Internal Speakers

Increase Idle Fan Speed (%)   **2**

    M.2 USB/Bluetooth

    LAN/WLAN Auto Switching

    Wake on WLAN

Item Specific Help

1. Audio Device

Hides the Audio device from OS.

2. Increase Idel Fan Speed (%)

Enter the percentage to increase the minimum fan speed (0 - 100).

HP Computer Setup

Port Options

Left USB Ports **1**

Right USB Ports **2**

Top USB Ports **3**

Bottom USB Ports **4**

Always Power the Stand Ports **5**

Rear USB Ports

☐ Rea USB Type-C Port

☐ Rear USB Port 1

☐ Rear USB Port 2

☐ Rear USB Port 3

☐ Rear 24V Powered USB Port

☐ Rear 12V Powered USB Port

Item Specific Help

1. Left USB Ports
  Hides the left USB ports from the OS

2. Right USB Ports
  Hides the right USB ports from the OS

3. Top USB Ports
  Hides the top USB ports from the OS

4. Bottom USB Ports
  Hides the bottom USB ports from the OS

5. Always Power the Stand Ports
  When enabled, power to the stand and base remains on to support wake events and USB charging. Requires S5 Maximum Power Savings to be off.

Advanced

Power Management Options

Runtime Power Management   **1**

Extended Idle Power States   **2**

SS Maximum Power Savings

PCI Express Power Management   **3**

Unique Sleep State Blink Rates

Item Specific Help

1. Runtime Power Management
   Enables Runtime Power Management

2. Extended Idle Power States
   Increases the OS's Idle Power Savings

3. PCI Express Power Management
   Enabling this option permits the PCI Express links to use Active State Power Management (ASPM) to enter low power states while not in use.

Remote Management Options

Intel Active Management Technology (AMT) **1**

USB Key Provisioning Support

USB Redirection Support

Unconfigure AMT on next boot **2**

SOL Terminal Emulation Mode

Show Unconfigure ME Confirmation Prompt

Verbose Boot Messages

Watchdog Timer **3**

OS Watchdog Timer (min.)

BIOS Watchdog Timer (min.)

CIRA Timeout (min.) **4**

Item Specific Help

1. Intel Active Management Technology (AMT)
This option allows for a user to enable Intel Active Management Technology, which is tied to all ME-regulated remote management functions. Disabling AMT will still allow for ME Firmware updates, which are recommended for receiving platform stability fixes.

2. Unconfigure AMT on next boot
Perform AMT/ME unconfigure without password operation.
Click on the field to see the options.

3. Watchdog Timer
Enable/Disable Watchdog Timer.

4. CIRA Timeout (min.)
Set CIRA Timeout (minutes).
Click on the field to see the options.

Electronic Labels

Item Specific Help

Remote HP PC Hardware Diagnostics

Diagnostics Download URL ①

➡ Custom Download Address

Diagnostics Logs Upload URL

②

③

④

Scheduled Execution ⑤

Frequency ⑥

Execute On Next Boot ⑦

⑧

Custom Upload URL

There is no Custom Upload URL configured.
Type a new Custom Upload URL and press ENTER to save.
Press ESC to CANCEL

Upload Server Username

There is no Username configured.
Type a new Username and press ENTER to save.
Press ESC to CANCEL

Upload Server Password

There is no Upload Server Password configured.
Type a new Upload Server Password and press ENTER to save.
Press ESC to CANCEL

This will restart the system into the 3rd Party Option ROM Management application.
You can get to this application directly by pressing F3 during startup.

Item Specific Help