Interactive BIOS simulator

HP EliteDesk 800 G5 DM 35W

Welcome to the interactive BIOS simulator for the
HP EliteDesk 800 G5 DM 35W

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

Main

BASIC SYSTEM INFORMATION

Item Specific Help

Product Name	HP EliteDesk 800 G5 DM 35W
Processor 1	Intel(R) Core(TM) i3-8350K CPU @ 4.00GHz
Memory Size	16384 MB
System BIOS	Q21 Ver. 80.30.12 02/01/2018

SERVICE ---

Born On Date	00/00/0000
Serial Number	5CD805D8H6
SKU Number	D83PVTB#001
Universally Unique Identifier (UUID)	6B6F91A9-2325-B106-464C-9CFBE2ACAD23
Asset Tracking Number	5CD805D8H6

Help

Main

ADVANCED SYSTEM INFORMATION

Item Specific Help

Product Name   HP EliteDesk 800 G5 DM 35W
Memory Size   16384 MB

PROCESSOR 1 --

ProcessorType   Intel(R) Core(TM) i3-8350K CPU @ 4.00GHz
Cache Size (L1/L2/L3)   256 KB / 1 MB / 8 MB
Processor Speed   4000 MHz
MicroCode Revision   80
Processor Stepping   B
Memory Speed   2133 MHz
DIMM1   16 GB Hynix/Hyundai
DIMM3   Empty

Help

Main

ADVANCED SYSTEM INFORMATION

Item Specific Help

FIRMWARE --

System BIOS	Q21 Ver. 80.30.12 02/01/2018
ME Firmware Version	12.0.0.1048
ME Firmware Mode	Enabled
Video BIOS Version	INTEL(R) VBIOS [1006.0]
Reference Code Revision	7.0.1C.58
Super I/O Firmware Version	C7.7.3
USB Type-C Controller(s) Firmware Version:	
	CCG5 : 5.13.0
	CCG5 : 5.13.0

SERVICE --

Born On Date	00/00/0000
Serial Number	5CD805D8H6
SKU Number	D83PVTB#001
Universally Unique Identifier (UUID)	6B6F91A9-2325-B106-464C-9CFBE2ACAD23

Help

Item Specific Help

Universally Unique Identifier (UUID)   6B6F91A9-2325-B106-464C-9CFBE2ACAD23
Asset Tracking Number   5CD805D8H6
Feature Byte   3E3X475K6J6S6b7B7H7M7Q7T7W7m
                                              aBaqaqaubhcAdUdpdqgdgzhK.Fq
Build ID   18WWQ6AT6az#SABA#DABA
Product Family   103C_53307F HP EliteDesk
System Board ID   8409
System Board CT Number   PGVLUX48JAE04M

COMMUNICATION ---

Integrated MAC Address   80-CE-62-49-1D-BC

Help

HP PC Hardware Diagnostics UEFI

Please select a Language.

English

Cestina

Dansk

Deutsch

Nederlands

Espanol

eesti keel

Suomi

Francais

Hrvatski

Magyar

Update System BIOS

Current System BIOS Version: Q21 Ver. 80.30.12
Current BIOS Release Date: 02/01/2018
Installation Date of Current BIOS: 02/05/2018
Most Recent Update Check: Never Checked

----

(1)
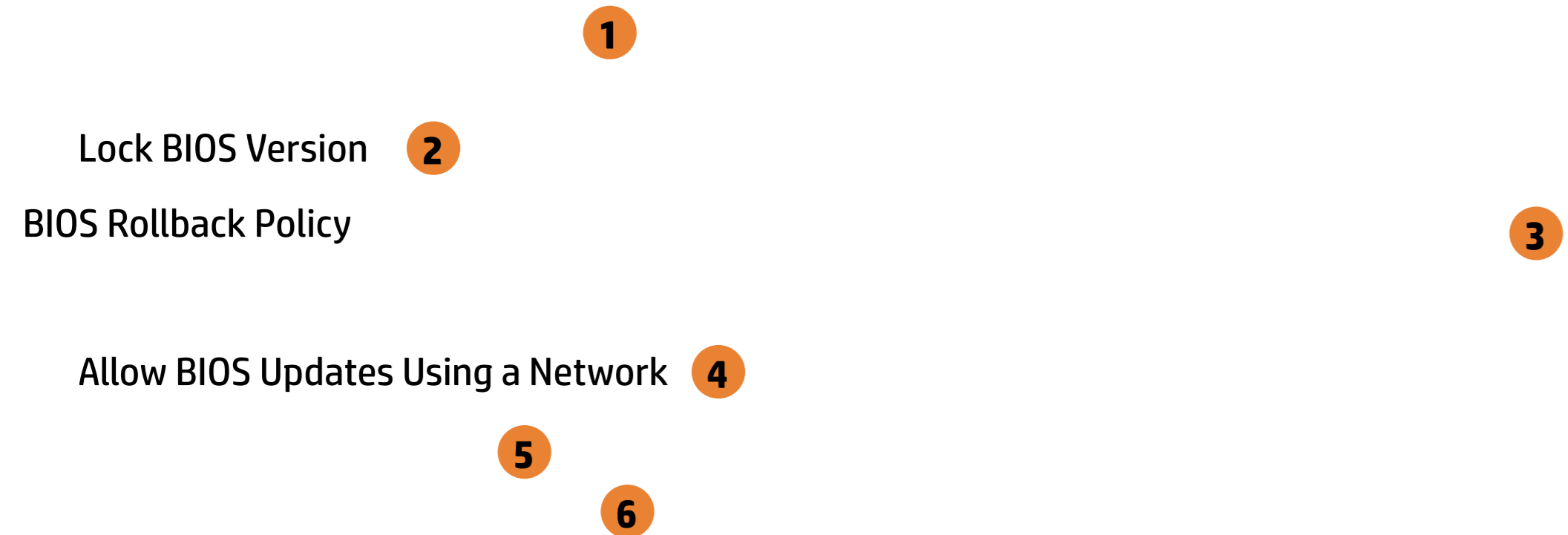
Lock BIOS Version   **(2)**

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.

Network BIOS Update

MS Windows Bitlocker Drive Encryption (BDE) may be enabled on your system.
HP requires that BDE be suspended temporarily before the BIOS is flashed and
that you obtain your BDE recovery password or recovery PIN before suspending BDE.
After the BIOS is updated, BDE can be resumed.

Minimum BIOS Version

Current Minimum BIOS Version: 00.00.00

Minimum BIOS Version:

Main

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.

HP Computer Setup

Network Configuration Settings

Proxy Server **1**

2

IPv4 Configuration **3**

DNS Configuration **4**

100 **5**

Data transfer timeout
Force HTTP no-cache **6**

Help

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.

Item Specific Help

Change Date And Time

Set Date (MM/DD/YYYY)   06 / 15 / 2018
Set Time (HH:MM):   04 : 02

Help

HP Computer Setup

Item Specific Help

Help

Feature Byte

Current Setting: 3E3X475K6J6S6b7B7H7M7Q7T7W7maBapaqaubhcAdUdpdqgdgzhK.Fq

Build ID

Current Setting: 18WWQ6AT6az#SABA#DABA

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

Serial Number

Current Setting: 5CD805D8H6

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

SKU Number

Current Setting: D83PVTB#001

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

Product Family

Current Setting: 103C_53307F HP EliteDesk

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

System Board CT Number

Current Setting: PGVLUX48JAE04M

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

Product Name

Current Setting: HP EliteDesk 800 G4 DM 95W

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

Item Specific Help

System IDs

Help

Asset Tracking Number

Current Setting: 5CD805D8H6

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

Security

Administrator Tools

1

Security Configuration

Physical Presence Interface **2**

Intel Software Guard Extension (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)
Intel Software Guard Extensions (SGX)
Enable/Disable Software Guard Extensions (SGX)

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

BIOS Data Recovery Policy

    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.

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 in 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 the 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
Click on the field to see the options.

Secure Platform Management (SPM)

HP Sure Run Current State: Inactive

SPM Current State: Not provisioned

Item Specific Help

Smart Cover

Cover Removal Sensor   **1**

Item Specific Help

1. Cover Removal Sensor
   Choose one of thve available options.
   Click on the field to see the options.

Hard Drive Utilities

Save/Restore MBR of the system hard drive is only available with drives that have a Master Boot Record.

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

Boot Sector (MBR/GPT) Recovery Policy

Allow OPAL Hard Drive SID Authentication

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 he prompted to choose whether to restore GPT.

Help

Select a Drive

Item Specific Help

Help

Secure Erase

This operation will erase all data
on the hard drive. Please make
sure the computer is connected
to AC power during this process.

Select a Drive

Item Specific Help

BIOS Administrator Password

Enter BIOS Administrator Password

Remote HP PC Hardware Diagnostics

1

2

3

Display Language

Select Language

Select Keyboard Layout

Item Specific Help

Scheduled Power-On

    Sunday

    Monday

    Tuesday

    Wednesday

    Thursday

    Friday

    Saturday

Hour   0
Minute   0

Item Specific Help

Boot Options

Startup Delay (sec.)

    Fast Boot
    USB Storage Boot
    Network (PXE) Boot
    After Power Loss   **1**
    Prompt on Memory Size Change
    Prompt on Fixed Storage Change
    Audio Alerts During Boot
    NumLock on at boot
    UEFI Boot Order

       M.2 SAMSUNG MZVLB512HAJQ-000H1-S3WTNE0JC03455
       USB:
       NETWORK BOOT: IPV4 Network - Intel(R) Ethernet Connection (7) I219-LM
       NETWORK BOOT: IPV6 Network - Intel(R) Ethernet Connection (7) I219-LM

☐ Legacy Boot Order

       USB:
       M.2: SAMSUNG MZVLB512HAJQ-000H1-S3WTNE0JC03455

Item Specific Help

1. After Power Loss
   Determine the system's state after power is lost to the unit.

HP Sure Recover

HP Sure Recover **1**
Recover from Network **2**
Recover after Boot Failure **3**

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

Recovery Image
URL:
Username:
Provisioning Version: 0

Item Specific Help

1. HP Sure Recover
   If this setting is enabled, the system firm-
   ware will honor local and remote requests to
   reinstall the OS. If it is disabled, all requests
   to reinstall the OS will be ignored.

2. Recover from Network
   If this setting is enabled, the system firm-
   ware will obtain the recovery agent from the
   network. Otherwise, the system firmware
   will obtain the recovery agent from a local
   drive.

3. Recover after Boot Failure
   If this setting is enabled and no bootable
   UEFI OS is found, the system firmware will
   launch HP Sure Recover.

Item Specific Help

Secure Boot Configuration

Configure Legacy Support and 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 Password to be configured and Secure Boot to be enabled.

System Options

Configure Storage Controller for RAID

POST Prompt for RAID Configuration

Configure Storage Controller for Intel Optane

Multi-processor

Virtualization Technology (VTx)

Virtualization Technology for Directed I/O (VT'd)

M.2 SSD 1　　　　**1**

M.2 SSD 2　　　　**2**

M.2 WLAN/BT　　**3**

Allow PCIe/PCI SERR# Interrupt

Power Button Override　　　　　　**4**

Item Specific Help

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

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

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

4. Power Button Override
 Click on the field to see the options.

Built-In Device Options

Embedded LAN Controller

Wake On LAN

Dust Filter

Dust Filter Reminter (Days)

Video memory size

Audio Device **1**

Microphone

Internal Speakers

Increase Idel Fan Speed (%)   0

M.2 USB / Bluetooth

LAN/WWAN Auto Switching

Wake on WL

Item Specific Help

1. Audio Device
    Hides the Audio device from OS

Port Options

Front USB Ports **1**

Front USB Port 1 **2**

Front USB Port 2 **2**

Front USB Port 3 **2**

Rear USB Ports **3**

Rear USB Port 1 **4**

Rear USB Port 2 **4**

Rear USB Port 3 **4**

Rear USB Port 4 **4**

USB Option Port **5**

USB Legacy Port Charging **6**

Rear USB Type-C Downstream Charging **7**

Front USB Type-C Downstream Charging **8**

SATA 0 **9**

Restrict USB Devices

Item Specific Help

1. Front USB Ports
   Hides the front USB ports from the OS

2. Front USB Port 1-3
   Enables individual legacy or Type-C USB port.
   On Desktop platforms, ports are typically num-
   bered bottom to top, then left to right when in
   horizontal orientation. On Notebook platforms,
   Ports are typically numbered front to rear.

3. Rear USB Ports
   Hides the rear USB ports from the OS

4. Rear USB Port 1-4
   Enables individual legacy or Type-C USB port.
   On Desktop platforms, ports are typically num-
   bered bottom to top, then left to right when in
   horizontal orientation. On Notebook platforms,
   Ports are typically numbered front to rear.

5. USB Option Port
   Hides the USB option port from the OS

6. USB Legacy Port Charging
   Enable USB charging port for charging capabili-
   ty when system Hibernate/Shutdown

7. Rear USB Type-C Downstream Charging
   Enable USB Charging port for charging capabili-
   ty when system Hibernate/Shutdown

8. Front USB Type-C Downstream Charging
   Enable USB Charging port fro charging capabili-
   ty when system Hibernate/Shutdown

9. SATA 0
   Hides the SATA port from the OS

Option ROM Launch Policy

Configure Option ROM Launch Policy ① **1**

Item Specific Help
1. Configure Option ROM Launch Policy Configure the launching of the EFI versus Legacy Option ROMs

Power Management Options

Runtime Power Management **1**

Extended Idle Power States **2**

S5 Maximum Power Savings **3**

SATA Power Management

PCI Express Power Managment **4**

Power On from Keyboard Ports **5**

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. S5 Maximum Power Savings
Enabling this feature reduces the power of this system as much as possible in the S5 state. Power is removed from the wake up circuitry, the expansion slots and any management features while in S5.

4. 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.

5. Power On from Keyboard Ports
To wake up system from Hibernate/Shutdown via keyboard.

Remote Management Options

    Active Management (AMT)

    USB Key Provisioning Support

    USB Redirection Support

Unconfigure AMT on next boot   **1**

SOL Terminal Emulation Mode

    Show unconfigure ME Confirmation Prompt

    Verbose Boot Messages

    Watchdog Timer   **2**

    OS Watchdog Timer (min.)   **3**

    BIOS Watchdog Timer (min.)   **4**

CIRA Timeout (min.)   **5**

Item Specific Help

1. Unconfigure AMT on next boot
Perform AMT/ME unconfigure without password operation.

2. Watchdog Timer
Enable/Disable WatchDog Timer.

3. OS Watchdog Timer (min.)
Set OS watchdog timer (Minutes).

4. BIOS Watchdog Timer (min.)
Set BIOS watchdog timer (Minutes).

5. CIRA Timeout (min.)
Set CIRA Timeout (Minutes).

MAC Address Pass Through

Host Based MAC Address

Configure Factory/System MAC Address

Current Factory : C8-D9-D2-FF-98-C0
Current System : C8-D9-D2-FF-98-C0

Examples:
1234567890AB
12-34-56-78-90-AB
Writes blank to clear the MAC address
The Second Byte must be even digit, either 0, 2, 4, 6, 8, A, C or E

Press ESC to CANCEL
Type the System MAC Address and press ENTER to SAVE

Thunderbolt Options

Thunderbolt Mode **1**

Require BIOS PW to change Thunderbolt Security Level

Thunderbolt Security Level

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**

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