Technical Whitepaper

HP PC Commercial BIOS (UEFI) Setup

Administration Guide

For Commercial Platforms using HP BIOSphere Gen 3-5
2016 -2018

August 2018
919946-003

Table of contents

List of tables

1 Abstract

HP redesigned the 2015 and later generation of BIOS to support the requirements of the latest CPU and operating systems. HP took this opportunity to create a new BIOS architecture based on the UEFI specification version 2.4, with a common set of core modules and capable of supporting both notebook and desktop models. Now HP notebooks and HP desktops models using this generation of the BIOS will have a similar look and feel for the (F10) setup menu, more shared WMI strings, and more shared features.

2 Introduction

This white paper provides detailed information about features adjusted through the F10 BIOS setup menu. The section on computer notifications provides an explanation for the LED blink codes and screen messages that may occur.

For decades, HP has provided an industry leading level of built in customer value through an internally developed Read Only Memory Basic Input/Output System (ROM BIOS), a set of routines that enable a PC to load the operating system and communicate with various devices such as storage drives, keyboard, display, slots, and ports. The BIOS also exposes and provides the interfaces required to use unique firmware and hardware based HP professional innovations such as HP Sure Start, HP Sure Run, and HP Sure Recover, and HP Client Security Manager .

To help users understand the new features, the description of each feature includes a reference to the name and location of that feature from the previous year, if it is different from the current year.

This document has been updated to reflect new and updated features in the "Q" family of BIOS, introduced in 2017 & 2018. A "Q" family BIOS is a version that begins with the letter "Q". For example, "Q01 Ver. 01.02.04 12/12/2017". The new features in those platforms may not be supported in early models. Also, note that this document is the superset of BIOS setting across the product portfolio – not all current generation products support all the BIOS features described here.

2.1 Supported models

This document applies to HP commercial-grade PC products. That is products designed to meet the demanding security and manageability requirements of national, regional, and local government agencies, schools, the military, international financial institutions and retail sales companies.

This document applies to 2015 and later models only. For reference, the table below shows the year associated with models in the feature documentation below.

Table 1 Notebook Generations

Platforms		**2015 "N" Family**	**2016 "P" Family**	**2017 "Q" Family**	**2018 "Q" Family**
HP EliteBook Folio	9480m				
HP EliteBook Folio	1020				
HP ZBook	17	G3	G4		G5
HP ZBook	15	G3	G4		G5
HP ZBook	15u	G3	G4		G5
HP ZBook	14u				G5
HP EliteBook	850	G3	G4		G5
HP EliteBook	840	G3	G4		G5
HP EliteBook	830				G5
HP EliteBook	820	G3	G4		
HP EliteBook	755	G3	G4		
HP EliteBook	745	G3	G4		G5

Platforms		2015 “N” Family	2016 “P” Family	2017 “Q” Family	2018 “Q” Family
HP EliteBook	725	G3	G4		G5
HP ProBook	470	G3	G4	G5	
HP ProBook	450	G3	G4	G5	
HP ProBook	440	G3	G4	G5	
HP ProBook	430	G3	G4	G5	
HP ProBook	445	G3		G5	
HP EliteFolio	940				
HP EliteBook Folio		G3			
HP EliteBook	Revolve 810	G3			
HP ProBook		G2			
HP ZBook Studio		G3	G4		G5
HP ZBook 14u					
HP ProBook	455		G3	G4	
HP ProBook	640		G3	G4	
HP ProBook	645		G3	G4	
HP ProBook	650		G3	G4	
HP ProBook	655		G3	G4	
HP Pro	x2 612		G2		
HP EliteBook	x360 1020		G2		
HP EliteBook	x360 1030		G2	G3	
HP Elite	x2 1012		G2		
HP Elite	X2 1013			G3	

Table 2 Desktop Generations

Platforms		**2015**	**2016**	**2017**	**2018**
HP EliteDesk	1000 AiO			G1	G2
HP EliteDesk	800 TWR	G2	G3		G4
HP EliteDesk	880 TWR	G2	G3		G4
HP EliteDesk	800 SFF	G2	G3		G4
HP EliteDesk	800 DM	G2	G3		G4
HP EliteOne	800 AiO	G2	G3		G4
HP EliteDesk	705 MT	G2	G3		G4
HP EliteDesk	705 SFF	G2	G3		G4
HP EliteDesk	705 DM	G2	G3		G4
HP ProDesk	600 MT	G2	G3		G4
HP ProDesk	680 MT	G2	G3		G4
HP ProDesk	600 SFF	G2	G3		G4
HP ProDesk	600 DM	G2	G3		G4
HP ProOne	600 AiO	G2	G3		G4
HP ProDesk	400 SFF	G2.5	G4		G5
HP ProDesk	400 MT	G3	G4		G5
HP ProDesk	480 MT	G3	G4		G5
HP ProDesk	490 MT	G3			
HP ProDesk	498 MT	G3			
HP ProDesk	400 DM	G2	G3		G4
HP ProOne	400 AiO	G2	G3		G4
HP ProOne	460/480 AiO	G2	G3		
HP Retail	RP9	x			
HP Retail	RP1		x		
HP Retail	Engage Flex Pro				x
HP Elite Slice			G1		G2
HP Thin Client t530			X		

2.2 New in 2017-2018

This is a sampling of the new features and functionalities introduced in 2017-2018 with special reference to 2016 features, some of which are platform-dependent.

- HP Sure Start Secure Boot Keys Protection
- HP Sure Recover
- HP Sure Run

3 F10 Main Menu

Main	Security	Advanced	UEFI Drivers

HP Computer Setup

Organization of the F 10 section:
The hierarchy of the table of contents matches the sequence of the menus found in the F10 Setup menu, currently three levels deep.

The top-level tabs are: Main, Security, Advanced and UEFI Drivers.

The next level are the menus found under these tabs.

At the beginning of each major section is a diagram of the sub-menu items for each tab.

A table provides a list of features for each menu.

At the top of the table is a breadcrumb trail that describes the menu relationship in the hierarchy.

Advanced ->Port Options Continued...				
Feature	Type	Description	Default	Notes

The table has columns for feature, type, description, default and notes. The following is a field description or definition.

Feature
This is the name of the feature as it appears in the Setup menu. A feature prefaced with box or underlined shows how it appears in the menu.

Type
Features can be settings, actions, another menu, or display only settings. Most of the features by far are settings. A setting is system value modifiable by the user, using a check box, a drop-down menu or a text box.

Description
If the feature is a setting with a drop-down box, then all possible values are displayed. If the feature is new or has changed its name or location from the 2014 notebooks or desktops, then the description references or includes its previous name and location. The notation to describe the location indicates the menus that the user must navigate through to access the feature. For example: Menu 1->Menu 2->Feature X indicates that to access Feature X, the user navigates through Menu 1 to Menu 2.

Default
For features that are settings, this column provides the factory default setting.

Notes

Some features are not available for all types of models. The notes will describe when a feature is only available on select products.

Some actions require a reboot or physical presence. Physical presence is a menu that requires a human response to validate that a person is physically present before the action is completed. Actions that require physical presence are security sensitive changes.

Main	Security	Advanced	UEFI Drivers

HP Computer Setup

- ⇨ **System Information**
- ⇨ **System Diagnostics**
- ⇨ **Update System BIOS**
- ⇨ **Change Date and Time**
- ⇨ **System IDs**

- ⇨ **Replicated Setup**
- ⇨ **Save Custom Defaults**
- ⇨ **Apply Custom Defaults and Exit**
- ⇨ **Apply Factory Defaults and Exit**
- ⇨ **Ignore Changes and Exit**
- ⇨ **Save Changes and Exit**

3.1 Main Menu

For detailed information on the features in the main menu, see the following table.

Table 3 Main Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
System Information	Menu	System information, such as serial number, model number, Asset Tracking Number, CPU type, and memory size, UUID, SKU, and Born on Date.		
System Diagnostics	Menu	Application to run diagnostic tests on your system, such as start-up test, run-in test, memory test, and hard disk test		
Update System BIOS	Menu	Update system firmware from FAT 32 partition on the hard drive, a USB disk–on-key, or the network. Also allows you to configure if BIOS rollback is restricted or not.		
Change Date and Time	Menu	Configure the system Date and Time settings.		
System IDs	Menu	Identification strings that assigned by an enterprise to track the system including Asset Tracking Number and Ownership Tag.		
Replicated Setup	Action	Save your current BIOS settings to a file on a USB drive, and later restore your setting from this file.		
Save Custom Defaults	Action	As an alternative to factory default settings, create custom default values for all but the security settings. It is not possible to create custom default values for security settings.		Reboot required
Apply Custom Defaults and Exit	Action	Set all but the security settings to your custom default values NOTE. Now it is possible to restore to custom defaults or the factory defaults.		
Apply Factory Defaults and Exit	Action	Set all, but the security settings to factory values. See the Security menu section to set security settings to factory values		
Ignore Changes and Exit	Action	Exits F10 Setup without saving any changes made during current session		
Save Changes and Exit	Action	Exits F10 Setup and saves all changes made during current session		

3.2 Update System BIOS Menu

This sub-menu under the Main menu provides information about the current system firmware, settings; these control updates, the ability to check for updates over the internet or on the local network, and the ability to update system firmware from a FAT 32 partition on the hard drive, or a USB disk–on-key.

For the BIOS flash to succeed, do not remove power or turn off the system during any phase of the process. Below is a description of the BIOS flash phases to help you avoid interrupting the process. The BIOS flash proceeds in four phases:

1. The system displays a progress bar. When progress is 100%, the system reboots. This is the initial BIOS flash.

2. The screen is black; the system blinks one LED and makes a steady beeping sound. This is the system flashing the boot block. Video cannot display during this phase; so, the LED and the beep are the only way to let you know that the system is flashing normally.
3. (Sure Start enabled systems only) A screen indicates that the system is copying the DXE to the HP Security Device
4. The screen is black for a short period, and then the OS starts. The BIOS flash is now complete.

Table 4 Update System BIOS Menu features

Feature	Type	Description	Default	Notes
Current System BIOS Version	Display only			
Current BIOS Release Date	Display only			
Installation Date of Current BIOS	Display only			
Most Recent Update Check	Display only			
Check the Network for BIOS Updates (or) Check HP.com for BIOS Updates	Action	Updates the system BIOS by using an image stored on hp.com or another source defined in the "BIOS Update Preferences" menu. When BIOS source is HP.com, then the feature appears as "Check HP.com for BIOS Updates"		Reboot required
□ Lock BIOS version	Setting	When checked, disallows BIOS updates.	Unchecked	
BIOS Rollback Policy	Setting	Behavior when attempting to roll back to a previous BIOS version. The setting can be set to Unrestricted Rollback to older BIOS or Restricted Rollback to older BIOS.	Unrestricted Rollback to older BIOS	
Minimum BIOS version	Setting	Displays Minimum BIOS version required for optimal operation		
□ Allow BIOS Update using a Network	Setting	When checked, automatic BIOS updates through the network in a scheduled basis.	Checked	
BIOS Update Preferences	Menu	Menu with network BIOS update settings such as source, actions when and update is available and the frequency to check for updates.		
Network Configuration Settings	Menu	Configure the network connection to the server that is the host for your system firmware updates.		
Update System and Supported Device Firmware Using Local Media	Action	Updates the system BIOS by using an image stored on local media such as the hard drive or a USB drive formatted as FAT32 or EFI system partition.		Reboot required

3.3 BIOS Update Preferences Menu

The "Update System BIOS" sub-menu provides a method for initiating a check for an update to the current system firmware and settings that control where to check for system firmware updates, what to do when an update is available, and the frequency to check for system updates

Table 5 BIOS Update Preferences Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
☐ Check for Update on Next Reboot	Action	When checked, check if an updated BIOS is available during the next boot. This feature is only necessary from a WMI call. From the F10 Setup menu use the feature “Main -> Update System BIOS -> Check the Network for BIOS Updates” that will check for updates without a reboot.	Unchecked	Reboot required
BIOS Source	Setting	Select the source URL for BIOS updates • HP.com • Custom URL	HP.com	
Edit Custom URL	Setting	When not using HP.com, define the custom URL here.		
Automatic BIOS Update Setting	Setting	Defines how automatic updates behave. The following settings are possible: • Do not update • Check for BIOS updates automatically, but let me decide whether to install them • Download and install normal BIOS update automatically • Download and install important BIOS updates automatically	Do Not Update	
BIOS Update Frequency	Setting	Sets the frequency of checks to the BIOS update server. If a newer version of BIOS has been made available on the network server, the system will prompt to update the BIOS • Daily • Weekly • Monthly	Monthly	

3.4 Network Configuration Settings Menu

The “Update System BIOS” sub-menu configures the network connection to the server that is the host for the system firmware updates

Table 6 Network Configuration Settings Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
☐ Proxy Server	Setting	When checked, enables the use of a proxy server	Unchecked	
Edit Proxy Server	Setting	Specify the Proxy Server Address and the Port Number through the common-used <server>:<port> notation		
Test Network Connection	Action	Check the network connection using current BIOS update configuration		
IPv4 Configuration	Setting	The following settings are possible: • Automatic • Manual	Automatic	
IPv4 Address	Setting	When IPv4 settings are manual, setup for static IPv4 address		

Feature	Type	Description	Default	Notes
IPv4 Subnet Mask	Setting	When IPv4 settings are manual, configure a valid IPv4 address for subnet mask		
IPv4 Gateway	Setting	When IPv4 settings are manual, configure a valid IPv4 address for gateway.		
DNS Configuration	Setting	Configure a list of DNS addresses. The following settings are possible: • Automatic • Manual	Automatic	
DNS Addresses	Setting	When DNS configuration is manual, configure a comma separated list of DNS addresses		
Data Transfer Timeout	Setting	Set data transfer timeout in seconds. It is recommended not to use values under 15 seconds	30 or 100 seconds.	
□ Force HTTP No Cache	Setting	When checked, disables HTTP caching. This means that caching in upstream proxies is disabled as well, which guarantees that the BIOS goes all the way to the content source for any updated BIN files or catalog files but might slow down downloads slightly.	Unchecked	

3.5 System IDs Menu

This sub-menu provides identification strings assigned by an enterprise to track the system.

Table 7 System IDs Menu features

Level	Feature	Type	Description	Default	Notes
2	Asset Tracking Number	Setting	Allows custom configuration of an asset tag (up to 18 characters)	Blank	
2	Ownership Tag	Setting	Allows custom configuration of an ownership tag (up to 80 characters)	Blank	

3.6 Change Date and Time

Allows the system current Date and Time settings to be configured.

Feature	Type	Description	Default	Notes
Set Date (MM/DD/YYYY)	Setting	Set the current date using MM/DD/YYYY format.		
Set Time (HH:MM)	Setting	Set the current time using HH:MM (24 hour) format.		

4 Security Menu

Main | **Security** | Advanced | UEFI Drivers

HP Computer Setup

Administrator Tools

⇨ **Create/Change BIOS Administration Password**

⇨ **Create/Change POST Power-On Password**

- □ **Fingerprint Reset on Reboot** (select products only)

⇨ **Password Policies**

Security Configuration

⇨ **TPM Embedded Security**

⇨ **BIOS Sure Start**

⇨ **Smart Cover** (select products only)

⇨ **Secure Platform Management (SPM)**

- □ **Physical Presence Interface**
- □ **Trusted Execution Technology (TXT)**
  TXT cannot be enabled unless VTx, VTd and TPM are enabled first
- □ **Intel Software Guard Extensions (SGX)**

Utilities

⇨ **Hard Drive Utilities**

Absolute® Persistence Module Current State

⇨ **Activation Status:**

⇨ **Absolute® Persistence Module Permanent Disable:**

- □ **System Management Command (SMC)**

⇨ **Restore Security Settings to Factory Defaults**

4.1 Security Menu

For detailed information on the features in the security menu, see the following table.

Table 8 Security Menu features

Feature	Type	Description	Default	Notes
Create BIOS Administrator Password Or Change BIOS Administrator Password	Setting	The Administrator password controls access to the setup menu (F10), 3rd Party Option ROM Management (F3), Update System ROM, WMI commands that change system settings and the BIOS Configuration Utility (BCU). When no Administrator password is set, anyone can change the system settings, add 3rd Party Option ROM or update the system ROM. When the power-on password is set, use the administrator password as an alternative to power-on the system. Recommendation: Set an administrator password when a power-on password is set. When a power-on password is forgotten, an administrator can reset the power-on password by using "Restore Security Settings to Factory Defaults".		
Create POST Power-On Password Or Change POST Power-On Password	Setting	Password required to power on the PC, independent of the OS password. When no password is set, anyone can power-on the PC. In addition to the administrator password, there is only one power-on password. Recommendation: Set an administrator password when a power-on password is set. When a power-on password is forgotten, an administrator can reset the power-on password by using "Restore Security Settings to Factory Defaults".		
Password Policies	Menu	Allows the administrator to set password requirements for BIOS administration and power-on regarding the use of symbols, numbers, case and spaces		
☐ Fingerprint Reset on Reboot	Action	When checked, resets the fingerprint on the next reboot. After reboot, this will be unchecked again.	Unchecked	Notebook only
TPM Embedded Security	Menu	The Trusted Platform Module (TPM) is a dedicated microprocessor that provides security functions for secure communication and software and hardware integrity. The TPM hardware solution is more secure than a software only solution.		
BIOS Sure Start	Menu	Settings that control the behavior of HP Sure Start. HP Sure Start is a built-in hardware security system that protects your BIOS from accidental or malicious corruption by (1) detecting BIOS corruption and then (2) automatically restoring the BIOS to its last installed HP certified version.		
Secure Platform Management (SPM)	Menu	Options for managing HP Sure Run and HP Sure Recover		
☐Physical Presence Interface		Enable or disable the prompts that confirm that a person made the requested change		

Feature	Type	Description	Default	Notes
Smart Cover	Menu	Controls settings for Cover Lock and Cover Sensor on a desktop models.		Desktop only with a Cover Lock
□ Trusted Execution Technology (TXT)	Setting	When checked, enables Trusted Execution Technology on select Intel-based systems NOTE: Enabling this feature disables OS management of Embedded Security Device, prevents a reset of the Embedded Security Device, and prevents the configuration of VTx, VTd, and Embedded Security Device.	Unchecked	Intel only Reboot Required
Intel Software Guard Extensions (SGX)	Setting	Enables Intel Software Guard Extensions. The following settings are possible: • Enabled • Disabled NOTE: This feature is only available for systems with Intel vPro.	Disable	Intel only
Hard Drive Utilities	Menu	Utilities to protect private information on individual hard drives: Drive Lock and Secure Erase.		
Absolute® Persistence Module	Label	A subscription service that provides PC theft recovery, tracking and data delete solutions		
Activation Status	Display only	The subscription status can be inactive, active, or permanently disabled	Inactive	
Absolute® Persistence Module Permanent Disable	Display only		No	
□ System Management Command	Setting	When checked, allows authorized HP service personnel in possession of the PC to reset security settings in case of a customer service event. For customers that require more BIOS security, uncheck this to prevent this type of HP service command. NOTE: In the event BIOS password is lost and this option is disabled, HP authorized personnel will not be able to remove a lost password.	Checked	Reboot Required
Restore Security Settings to Factory Defaults	Action	Apply factory defaults to all security settings.		Reboot Required

4.2 Password Policies Menu

This sub-menu allows the administrator to set text requirements controlling the use of symbols, numbers, case and spaces for the BIOS administration password and the power-on password. To set these requirements an administration password must be already set.

Table 9 Password Policies Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
Password Minimum Length	Setting	Allows the administrator to specify the minimum number of characters required for a password. • Minimum: 4 • Maximum: 32 2014 Desktop: New	8	
□ At least one symbol required in Administrator and User passwords	Setting	When checked, passwords require at least one symbol, such as $, %, ^, &, or #	Unchecked	
□ At least one number required in Administrator and User passwords	Setting	When checked, passwords require at least one number	Unchecked	
□ At least one upper-case character required in Administrator and User passwords	Setting	When checked, passwords require at least one upper case character	Unchecked	
□ At least one lower-case character required in Administrator and User passwords	Setting	When checked, passwords require at least one lowercase character	Unchecked	
□ Are spaces allowed in Admin and User passwords?	Setting	When checked, passwords can have one or more spaces	Unchecked	
Clear Password Jumper	Setting	On Desktops, a jumper is available that when removed, will clear the administrator and power on passwords. Set this to ignore, to prevent someone from clearing your passwords with the jumper. The following settings are possible: • Honor • Ignore	Honor	Desktop only
□ Prompt for Administrator password on F9 (Boot Menu)	Setting	When checked, the administrator password is required to enter the boot menu	Checked	
□ Prompt for Admin password on F11 (System Recovery)	Setting	When checked, the administrator password is required to enter system recovery	Checked	
□ Prompt for Admin password on F12 (Network Boot)	Setting	When checked, the administrator password is required to enter the network boot	Checked	
□ Prompt for Admin password on Capsule Update	Setting	When checked, the administrator password is required to process a firmware capsule update		

4.3 Trusted Platform Module (TPM) Embedded Security Menu

This sub-menu for the Trusted Platform Module (TPM.) is a dedicated microprocessor that provides security functions for secure communication and software and hardware integrity. The built in TPM hardware solution is more secure than a software only solution.

Table 10 TPM Embedded Security Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
TPM Specification Version	Display only	The Trusted Computing Group (TCG) is an industry group that defines specifications for a TPM. As of this writing, possible TPM specification versions are 1.2 or 2.0.		
TPM Device	Setting	Makes the TPM available. The following settings are possible: • Available • Hidden	Available	Reboot, Physical Presence Required
□ TPM State	Setting	When checked, enables the ability for the OS to take ownership of the TPM	Checked	Reboot, Physical Presence Required
Clear TPM	Action	When selected, clears the TPM on the next boot. After clearing the TPM, this resets to No. The following settings are possible: • No • On next boot	No	Reboot Required
TPM Activation Policy	Setting	This setting allows an administrator to choose between convenience and extra security. The extra security is to ensure that the user of the system will at least see that the TPM device upgraded its firmware (F1 to Boot), or at most the user has the ability to reject the upgrade of the TPM device (Allow user to reject.) These user prompts limit the impact of remote attacks on the system by requiring a user to be physically present for the upgrade. When security of the system is of less concern, the third option (No prompts) removes any requirement for a user to acknowledge the upgrade. This last option is the most convenient for remotely upgrading many systems at once. The following settings are possible: • F1 to Boot • Allow user to reject No prompts	Allow user to reject	HP recommends an option that requires the physical presence of the user

4.4 BIOS Sure Start Menu

Settings menu for Enhanced hardware based assurance that only HP approved Embedded Controller firmware will run on the HP Embedded Controller and that only HP approved BIOS will run on the host CPU.

Table 11 BIOS Sure Start Menu features

Feature	Type	Description	Default	Notes
□ Verify Boot Block on Every Boot	Setting	When not checked, HP Sure Start© will verify the integrity of HP firmware in the non-volatile (flash) memory before resume from Sleep, Hibernate, or Off. When checked, HP Sure Start© will verify the integrity of HP firmware in the non-volatile (flash) memory across operating system restart (warm reset) in addition to resume from Sleep, Hibernate Off. This setting provides higher security assurance, but could increase the time required to restart operating system.	Unchecked	Reboot Required
BIOS Data Recovery Policy	Setting	The following settings are possible for HP Sure Start – Recovery Policy: • Automatic • Manual Automatic: HP Sure Start will automatically repair any HP firmware integrity issues in the non-volatile (flash) memory Manual: HP Sure Start will not repair any HP firmware integrity issues in the non-volatile (flash) memory until the Windows +Up Arrow+ Down Arrow keys are pressed. NOTE: Manual recovery is intended for use by the system administrator in the event forensic investigation is desired before HP Sure Start repairs the issue. It is not recommended for the typical user.	Automatic	Reboot Required
Network Controller Configuration Restore	Action	HP Sure Start – Network Controller Configuration Restore This action will restore the network controller parameters to the factory state saved in the HP Sure Start Private non-volatile (flash) memory. NOTE: This process can take up to 30 seconds. You only need to restore this when the Network Controller Configuration mismatch warning is set.		Reboot Required
□ Prompt on Network Controller Configuration Change	Setting	When enabled, HP Sure Start will monitor the network controller configuration and prompt the local user if any changes are detected compared to the factory configuration. The local user has the option to ignore the prompt, or restore the network controller to the factory configuration when prompted.	Checked	Intel only Reboot Physical Presence Required
□ Dynamic Runtime Scanning of Boot Block	Setting	When checked, allows HP Sure Start will verify the integrity of the HP firmware in the non-volatile (flash) memory every 15 minutes while the system in the On state with the user operating system active	Checked	

Feature	Type	Description	Default	Notes
□ Sure Start BIOS Settings Protection	Setting	Protects critical BIOS Settings by saving a backup copy and restoring them if altered.	Unchecked	Greyed out until admin password is set.
□ Sure Start Secure Boot Keys Protection	Setting	Saves backup copy of Secure Boot Keys on private ROM, so that they can be recovered if someone attempts to alter them in an unauthorized manner.		
□ Enhanced HP Firmware Runtime Intrusion Prevention and Detection	Setting	Monitors key areas of memory for corruption or attack, notifies user of attack (based on the settings in "Sure Start Security Event Policy"), and prevents the attack from taking place. **NOTE:** Only available on certain Intel systems	Checked	
□ HP Firmware Runtime Intrusion Detection	Setting	Monitors key areas of memory for corruption or attack and notifies user of attack (based on the settings in "Sure Start Security Event Policy"). **NOTE:** Only available on certain AMD chipset systems 2016 or later.	Checked	
Sure Start Security Event Policy	Setting	Determines how a Sure Start Intrusion Detection event should be handled. • Log the event in the audit log. • Log the event in the audit log and prompt the user to acknowledge the event. • Log the event in the audit log and power off the system. Prior to 2016: Not available	Log Event and notify user	
Sure Start Security Event Boot Notification		Enable a warning message at boot screen if there is a Sure Start event (BIOS recovery, Memory intrusion, etc)	Require Acknowledgment	

4.5 Smart Cover Menu (select products only)

This sub-menu controls settings for Cover Lock and Cover Sensor.

Table 12 Smart Cover Menu features

Feature	Type	Description	Default	Notes
Cover Lock	Setting	The Smart Cover Lock is a software-controllable cover lock. This lock prevents unauthorized access to the internal components. The following settings are possible: • Lock • Unlock	Unlock	Desktop only with Cover Lock Reboot Required
Cover Removal Sensor	Setting	The Cover Removal Sensor has the following settings: • Disabled • Notify the User: (Used by individuals managing their desktop) Administrator Password: (Used to alert desktop administrators of a cover removal, by blocking use of the desktop without an administrator password. This setting is only visible when an administrator password set)	Disable	Desktop only with Cover Sensor Reboot Required

4.6 Secure Platform Management (SPM)

This sub-menu controls settings for Secure Platform Management that are used for secure enablement and management of the HP Sure Run and Sure Recover capabilities.

The provisioning of SPM and activation of HP Sure Run can not be performed directly from the BIOS Setup interface. It can be provisioned using HP Client Security Manager Software or the HP Manageability Integration Kit. Once provisioned, the controls in this menu can be used to deprovision the system or deactivate HP Sure Run.

Table 13 Secure Platform Management Menu features

Feature	Type	Description	Default	Notes
HP Sure Run Current State	Setting (Display only)	• Inactive • Active	Inactive	
Deactivate HP Sure Run	Action	This action will deactivate HP Sure Run without deprovisioning SPM.		
SPM Current State	Setting (Display only)	• Provisioned • Unprovisioned	Unprovisioned	
Unprovision SPM	Action	This action will deprovision SPM which will cause HP Sure Run to revert to the Inactive state and return HP Sure Recover to default settings		

4.7 Hard Drive Utilities Menu

This sub-menu provides features that protect the data on individual hard drives, such as: recovering the master boot record, preventing unauthorized access and erasing data.

Table 14 Hard Drive Utilities Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
□ Save/Restore MBR of the system hard drive	Setting	When checked, saves a baseline MBR that can be restored if a change is detected NOTE: Not applicable for UEFI boot modes	Unchecked	Reboot Required
□ Save/Restore GPT of System Hard Drive	Setting	When checked, saves a baseline GUID Partition Table that can be restored if a change is detected. NOTE: Not applicable for Legacy boot modes Prior to 2016: Did not exist	Unchecked	Reboot Required
Boot Sector (MBR/GPT) Recovery Policy	Setting	Allows selection of the default action when an MBR/GPT event occurs	Local User Control	
DriveLock/Automatic DriveLock	Menu	DriveLock prevents unauthorized access to the contents of a selected hard drive.		
Secure Erase Select a Drive…	Action	Uses hardware based methods to erase safely all data and personal information from a selected Hard Drive.		Reboot Required
□ Allow OPAL Hard Drive SID Authentication	Setting	Allows for higher security on self-encrypting drives that support SID Authentication. If enabled 3rd parties (including some encryption software) are not allowed to perform certain drive activities.	Unchecked	Reboot Required

4.8 DriveLock/Automatic DriveLock Menu

DriveLock prevents unauthorized access to the contents of a selected hard drive. Enter a password to access the drive and the drive is accessible only when attached to a PC.

NOTE: DriveLock states cannot change after a warm reboot. Power off the system then boot directly to the setup menu, then to this menu. The DriveLock Master and User passwords cannot be changed if you enable Automatic DriveLock.

Table 15 DriveLock Menu features

Feature	Type	Description	Default	Notes
□ Automatic DriveLock	Setting	This feature is intended to prevent someone from accessing data on your drive after they have physically removed it from your system. A BIOS administrator password is required for this feature. When this feature is enabled, the BIOS sets a randomly-generated user password, sets the master password with the BIOS administrator password, and marks the drive as a member of an Automatic DriveLock group. Thereafter, the BIOS will automatically unlock the drive while it is attached to the its host system. If the drive is physically removed from its host system and attached to another system, the user will be prompted for the DriveLock password. The user must provide the BIOS administrator password from the original host system to access the drive. NOTE: Drivelock is not supported on NVMe drives.	Disable	Reboot Required
Set DriveLock Master Password	Setting	Password to disable or access a hard drive with DriveLock protection.		Reboot Required
Enable DriveLock	Setting	Enables DriveLock protection and creates a user password distinct from the master password that allows access to the hard drive	Disable	Reboot Required
Change DriveLock User Password	Action	Displayed only if DriveLock is enabled and a valid password was supplied at the DriveLock POST prompt. Allows the user password to be changed when selected		
Change DriveLock Master Password	Action	Displayed only if DriveLock is enabled and a valid password was supplied at the DriveLock POST prompt. Allows the master password to be changed when selected.		
Disable DriveLock	Setting	Displayed only if DriveLock is enabled and a valid password was supplied at the DriveLock POST prompt. Allows DriveLock to be disabled when it is enabled.		

5 Advanced Menu

Main | Security | **Advanced** | UEFI Drivers

HP Computer Setup

⇨ **Display Language**

⇨ **Scheduled Power-On**

⇨ **Boot Options**

⇨ **HP Sure Recover**

⇨ **Secure Boot Configuration**

⇨ **System Options**

⇨ **Built-In Device Options**

⇨ **Port Options**

⇨ **Option ROM Launch Policy**

⇨ **Power Management Options**

⇨ **Remote Management Options** (select products only)

⇨ **Electronic Labels** (select products only)

⇨ **MAC Address Pass Through** (select products only)

Remote HP PC Hardware Diagnostics

⇨ **Settings**

⇨ **Remote HP PC Hardware Diagnostics**

5.1 Advanced Menu

For detailed information on the features in the advanced menu, see the following table.

Table 16 Advanced Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
Display Language	Menu	Select the display language and the keyboard language. Choose between 14 languages. You can display the menu in English, French, German, Spanish, Italian, Dutch, Danish, Japanese, Norwegian, Portuguese, Swedish, Finnish, Chinese Traditional, or Chinese Simplified. NOTE: Affects the BIOS menus, not the OS nor the WMI commands.		
Scheduled Power On	Menu	Choose days of the week and a single time of day for the system to power-on. This feature wakes the system up from a powered off state.		
Boot Options	Menu	Settings that control the behavior of the system during boot up		
HP Sure Recover	Menu	Settings that control when and how the BIOS should attempt to reinstall the operating system.		
Secure Boot Configuration	Menu	Starting with Windows 8, Secure Boot is a UEFI feature that helps resist attacks and infection from malware. From the factory, your system came with a list of keys that identify trusted hardware, firmware, and operating system loader code. Your system also has a list of keys to identify known malware.		
System Options	Menu	Settings that control the CPU, PCI, PCIe, the power button and function keys.		
Built in Device Options	Menu	Settings of devices built-in to the PC		
Port Options	Menu	Settings that enable or disable ports and interrupts on the system.		
Option ROM Launch Policy	Menu	Configure the Device Option ROMs that load at boot time.		
Power Management Options	Menu	Settings that control power saving features and the behavior of the system in low power modes		
Remote Management Options	Menu	Settings that controls Intel Active Management technology that provides out-of-band remote management of the system.		Intel only
Electronic Labels	Display only	Mandatory certification marks, for example: the Federal Communication Commission (FCC) Declaration of Conformity (Doc) and the CE marking for Europe		Notebook only
MAC Address Pass Through	Menu	Configure a custom Host Based MAC Address (HBMA) for the system as well as define the priority of Network Interface Cards (NIC).	Disable	Notebook only
Remote HP PC Hardware diagnostics	Label	Remote HP PC Hardware diagnostics		
Settings	Menu	Settings for Remote HP PC Hardware diagnostics		

Feature	Type	Description	Default	Notes
Execute Remote HP PC Hardware Diagnostics	Action	When selected, will download and run HP Remote Diagnostics		

5.2 Display Language Menu

This sub-menu allows for selection of the display language and the keyboard language. For each setting, choose from the following languages:

- English
- Deutsch
- Español
- Italiano
- Français
- 日本語
- Português
- Danske
- Svenska
- Nederlands
- Norsk
- Suomi
- 简体中文
- 繁體中文

NOTE: Affects the BIOS menus, not the OS nor the WMI commands.

Table 17 Display Language Menu features

Feature	Type	Description	Default	Notes
Select Language	Setting	Language used by BIOS setup menus	English	
Select Keyboard Layout	Setting	Language of the keyboard layout used by BIOS setup menus	English	

5.3 Scheduled Power-On Menu

This sub-menu controls the days of the week and a single time of day for the system to power-on. This feature wakes the system up from a powered off state.

Table 18 Scheduled Power On Menu features

Feature	Type	Description	Default	Notes
□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday	Setting	Days of the week selection		Reboot Required
Hour	Setting	Time selection	0	Reboot Required
Minute	Setting	Hour: 0 – 23, Minute: 0 – 59	0	Reboot Required

5.4 Boot Options Menu

Sub-menu controls the behavior of the system during boot up

Table 19 Boot Options Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
Startup Menu Delay	Setting	Select the number of seconds (0 – 60) to pause the boot before starting the OS. Increasing the delay, gives more time to press a key that opens one of the BIOS menus. Set this to 0 if you have excellent twitch reflexes honed from a lifetime of video games. Increase the delay, if you need a little more time to respond during the boot up.	0	
□ Fast Boot	Setting	When checked, reduces boot up time by bypassing boot to USB, CD-ROM, and PXE. NOTE: When a power on password, other security features, or default boot order have been modified, Fast Boot is ignored	Checked	
□ CD-ROM Boot	Setting	When checked, allows system to boot from CD-ROM Only available on systems with a CD drive.	Checked	
□ USB Storage Boot	Setting	When checked, allows system to boot from USB	Checked	
□ Network PXE Boot	Setting	When checked, allows system to boot from a network card	Checked	
After Power Loss	Setting	Specifies the desktop state after power loss. The following settings are possible: • Power Off • Power On • Previous State	Power Off	Desktop only
□ Power On When AC Detected	Setting	When checked, the notebook will power on when it is off, AC power has not been available and then becomes available.	Unchecked	Notebook only
□ Power On When Lid is Open	Setting	When checked, the system will power on when the lid opens	Unchecked	Notebook only
□ Prompt on Battery Errors	Setting	When checked, the system will pause during system boot to warn about battery errors	Checked	Notebook only
□ Audio Alerts during boot	Setting	When checked, errors trigger audible beeps during POST	Checked	
□ Prompt on Memory Size Change	Setting	When checked, notify the user during the boot process when a memory size change has been detected	Checked	
□ Prompt on Fixed Storage Change	Setting	When checked, notify the user during the boot process when a fixed storage change has been detected.	Unchecked	
Audio Alerts During Boot	Setting	When checked, errors trigger audible beeps during POST	Checked	

Feature	Type	Description	Default	Notes
□ UEFI Boot Order		When checked, allows the system to boot from UEFI devices. When Legacy Boot is Disabled, the check boxes for UEFI Boot Order and Legacy Boot Order will grayed out and not functional, because only UEFI devices can boot in this mode. When enabling the UEFI Boot Order, the system attempts to boot from all UEFI devices before any non-UEFI devices. Arrange the boot order from the UEFI devices found. By default, the system will arrange the boot order by device type using the following precedence: 1. USB 2. SATA DVD (select products only) 3. SATA Hard Drives 4. M.2 devices 5. Network Boot	Checked	
Numlock on at Boot	Setting	Set the keyboard Num Lock control to be on or off when system is booted.		
□ Legacy Boot Order	Setting	When checked, allows the system to boot from non-UEFI devices. Requires “Legacy Boot Enable and Secure Boot Disable.” See “Secure Boot Configuration” -> “Configure Legacy Support and Secure Boot” When Legacy Boot is Disabled, the check boxes for UEFI Boot Order and Legacy Boot Order will grayed out and not functional, because only UEFI devices can boot in this mode. When enabling the UEFI Boot Order, the system attempts to boot from all UEFI devices before any non-UEFI devices. Arrange the boot order from the non-UEFI devices found. By default, the system will arrange the boot order by device type using the following precedence: 1. USB 2. SATA DVD (select products only) 3. SATA Hard Drives 4. M.2 devices 5. Network Boot	Checked	

5.5 HP Sure Recover

Table 20 HP Sure Recover

Feature	Type	Description	Default	Notes
HP Sure Recover	Setting	If this setting is enabled and HP Sure Recover is launched, the system firmware will honor local and remote requests to reinstall the OS. If it is disabled, all requests to reinstall the OS will be ignored	Enable	
Recover from Network	Setting	If this is enabled, the system firmware will obtain the recovery agent from the network. Otherwise, the system firmware will obtain the recovery agent from a local drive	Enable	Assuming Windows 10 is preinstalled
Recover after Boot Failure	Setting	If this setting is enabled and at least one enabled, disk-based entry in the UEFI boot order fails to boot, the system firmware will launch HP Sure Recover.	Enable	Assuming Windows 10 is preinstalled
Prompt before Boot Failure Recovery	Setting	If this setting is enabled and HP Sure Recover is launched due to a boot failure, the user is notified of the boot failure and asked to choose whether to start or cancel HP Sure Recover.	Enable	
Recovery Agent	Label			
URL:		Location of the current recovery agent URL		
Username:		Username (optional) to access the recovery agent		
Provisioning Version:		Version of the recovery agent's provisioning data		
Recovery Image	Label			
URL:		Location of the current recovery image URL		
Username:		Username (optional) to access the recovery image		
Provisioning Version:		Version of the recovery image's provisioning data		

5.6 Secure Boot Configuration Menu

Submenu to configure Secure Boot. Starting with Windows 8, Secure Boot is a UEFI feature that helps resist attacks and infection from malware. From the factory, your system came with a list of keys that identify trusted hardware, firmware, and an operating system loader code. It also created a list of keys to identify known malware.

Table 21 Secure Boot Configurations Menu features

Feature	Type	Description	Default	Notes
Configure Legacy Support and Secure Boot	Setting	Legacy Support is the ability to boot from a non-UEFI device. Only UEFI devices can support Secure Boot. The following settings are possible: • Legacy Support Enable and Secure Boot Disable • Legacy Support Disable and Secure Boot Enable • Legacy Support Disable and Secure Boot Disable	OS Dependent	
□ Import Custom Secure Boot keys	Setting	When checked and system is rebooted, custom secure boot keys are imported from the EFI\HP directory from the Hard drive or USB device. The custom keys consist of PK, KEK, DB, and Dbx .bin files. When import succeeds or fails, a pre-boot prompt will appear showing the results of each key bin file.	Unchecked	Reboot Required
□ Clear Secure Boot Keys	One Time Action	When checked, clears the Secure Boot keys one time on next save and exit. This setting will be unchecked again, when you return from exit. This action is not available with Legacy Support enabled or when no keys are present, possibly from a previous clear command.	Unchecked	
□ Reset Secure Boot Keys to Factory Defaults	One Time Action	When checked, restores secure boot keys to factory defaults one time on next save and exit. This setting will be unchecked again, when you return from exit.	Unchecked	
□ Enable MS UEFI CA key	Setting	When checked, the Microsoft (MS) UEFI Certificate Authority (CA) key is trusted by Secure Boot **NOTE:** Uncheck this to support Windows 10 Device Guard feature	Checked	

Ready BIOS for Device Guard Use	Action	"Ready BIOS for Device Guard Use" includes a drop down that will allow the user to set up the BIOS configuration Windows requires to enable Device Guard, or change the configuration back to the configuration before Device Guard was enabled. Device Guard is a Windows feature that enables higher security around drivers and BIOS behavior. The following settings are possible: • Configure on Next Boot • Clear Configuration on Next Boot When set to "Configure on Next Boot", the BIOS will change the features listed below to their suggested Device Guard states, on the boot after saving changes and exit. Virtualization features will be enabled. Removable and network boot devices will be disabled (for example, USB boot, CD-ROM boot, Thunderbolt boot, etc.). MS UEFI CA Key will be disabled. When set to "Clear Configuration on Next Boot", the BIOS will set the listed features to their Custom Default state if custom defaults have been saved. If custom defaults have not been saved, the BIOS will restore the listed features to their factory default states.		

5.7 System Options Menu

Table 22 System Options Menu features

Feature	**Type**	**Description**	**Default**	**Notes**
□ Configure Storage Controller for RAID	Setting	When checked, configures SATA Controller for RAID mode	Unchecked	Desktop only
PCIE GEN Support Speed	Setting	Allows you to restrict the maximum speed of the PCI Express devices to previous generations. The following settings are possible: • Auto • Gen 1 • Gen 2 • Gen 3	Auto	Available on select products only.
□ POST Prompt for RAID Configuration	Setting	When checked, prompts for RAID Configuration utility	Checked	Desktop only
□Configure Storage Controller for Intel Optane	Setting	UEFI only. Enables driver support for NVMe Intel Optane storage module. Requires additional configuration by Intel Rapid Storage Technology software application.	Unchecked	
□ Turbo Boost	Setting	When checked, enables Intel® Turbo Boost Technology to improve performance when operation conditions allow	Checked	Intel only

Feature	Type	Description	Default	Notes
□ Hyper-threading (Intel® HT)	Setting	When checked, enables Hyper-threading capability on Intel processors Intel HT Technology (HT) is designed to improve performance of multi-threaded software products and requires a computer system with a processor supporting HT and an HT-enabled chipset, BIOS and OS. Please contact your software provider to determine compatibility. Not all customers or software applications will benefit from the use of HT. See http://www.intel.com/info/hyperthreading for more information.	Checked	Intel CPU with hyper-threading only (Core i7)
□ Multi-processor	Setting	When checked, enables BIOS to report multiple processor cores to the OS.	Checked	
□ Launch Hotkeys without Fn keypress	Setting	When checked, allows the Fn-Fx hotkey combinations to be activated by just pressing the Fx key (for instance, F4 instead of Fn-F4). Desktop: Does not exist.	Unchecked	
□ Virtualization Technology (VTx)	Setting	When checked, enables VT on Intel-based systems.	Unchecked	Intel only
□ Virtualization Technology for Directed I/O (VTd)	Setting	When checked, grants virtual machines direct access to peripheral devices on select Intel-based systems.	Unchecked	Intel only
□ SVM CPU Virtualization	Setting	When checked, enables Virtualization on AMD-based systems.	Unchecked	AMD only
□ Swap Fn and Ctrl (Keys)	Setting	When checked, switches functionality between Fn and Ctrl keys.	Unchecked	Notebook only
□ Enable Turbo Boost on DC	Setting	When checked, allows Intel® Turbo Boost Technology to activate when a power adapter is not connected.	Unchecked	Intel notebook only
□Force enable HP Sure View	Setting	When check it enables HP Sure View's privacy panel by changing the screen brightness.	Unchecked	Notebook with HP Sure View only
□ PCI Express x16 Slot 1	Setting	When checked, PCI Express x16 slot is available.	Checked	Desktop only
□ PCI Express x1 Slot 1	Setting	When checked, PCI Express x1 slot is available.	Checked	Desktop only
□ PCI Express x1 Slot 2	Setting	When checked, PCI Express x1 slot is available.	Checked	Desktop only
□ PCI Express x1 Slot 3	Setting	When checked, PCI Express x1 slot is available.	Checked	Desktop only
□ PCI Express x4 Slot 1	Setting	When checked, PCI Express x4 slot is available.	Checked	Desktop only

Feature	Type	Description	Default	Notes
□ Allow PCIe/PCI SERR# Interrupt	Setting	When checked, enables PCI device to generate SERR# (System Error), as defined by the PCI specification.	Checked	Desktop only
Power Button Override	Setting	Sets the time required to hold the power button down for the desktop to turn off, overriding the power button behavior defined by the operating system. The following settings are possible: • Disable • 4 sec • 15 sec	4 sec	Desktop only
□ AMD DASH	Setting	AMD Remote system management capability.	Unchecked	AMD only
□ Fast Charge	Setting	Batteries charge more quickly.	Checked	Notebook only
□ Power Button Protection		When selected the power button will not function while the lid is closed.	On Battery only	On supported tablets and convertibles only.
USB Type-C Connector System Software Interface (UCSI)	Setting	When checked, allows UCSI to be activated.	Enable	
Dynamic Platform and Thermal Framework	Setting	Manages power and thermal conditions to keep system from overheating.	Enable	Intel notebook only
Top Cover Function	Setting	Menu to enable or disable the top cover functionality for HP Elite Slice.	Enable	HP Elite Slice only

5.8 Built-in Device Options Menu

This menu provides settings built-in devices on the system.

Table 23 Built-in Device Options Menu features

Feature	Type	Description	Default	Notes
□ Embedded LAN Controller	Setting	When checked, enables integrated network interface controller (NIC) device	Checked	
Wake on LAN	Setting	Allows the system to wake via Local Area Network (LAN). The following settings are possible: • Disabled • Boot to Network • Boot to Hard Drive • Boot to Normal Boot Order	Boot to Hard Drive	

Feature	**Type**	**Description**	**Default**	**Notes**
Wake on WLAN	Setting	Allows the system to wake via Wireless Local Area Network (WLAN), provided the system is equipped with this device. The following settings are possible: • Disabled • Boot to Hard Drive	Unchecked	
□ Dust Filter	Setting	When checked, enables the dust filter reminder. This will prompt you after a period of days specified by the setting below.	Unchecked	Desktop only
Dust Filter Reminder (Days)		Number of days for a reminder to replace the dust filter • 15 • 30 • 60 • 90 • 120 • 180	60	Desktop only
□ Integrated Video	Setting	When checked, enables the integrated video device. When not using the integrated video, disable the integrated video to save system memory.	Checked	Desktop with add-in graphics card only
VGA Boot Device		The firmware can only support one graphic device when booting up; so, when a graphics card is added, this feature selects the graphics system to use as the primary VGA device during boot-up • The integrated graphics • Add-in graphics card	Add-in graphics is set as primary	Desktop with add-in graphics card only
Video Memory Size	Setting	System memory reserved for video memory. The following settings are possible: Intel: • 32 MB • 64 MB • 128 MB • 256 MB • 512 MB AMD: • 128 MB • 256 MB • 512 MB • Auto	Intel: 32 MB AMD: Auto	

Feature	**Type**	**Description**	**Default**	**Notes**
Graphics	Setting	Set the graphics adapter. The following settings are possible and depend on the model of notebook to determine which are present along with what the default is set to: • Hybrid Graphics • UMA Graphic • Discrete Graphics • Auto (Let OS Decide if hybrid graphics is enabled or disabled).	Hybrid Graphics OR Auto (select products only)	Multiple Graphic Card Notebook only
□ Audio Device	Setting	This setting provides a single point of control for the integrated microphone, the internal speakers, and the headphone out. When checked, the operating system visibility of each audio device below is controlled independently When unchecked, hides all audio devices from the operating systems. The individual audio device settings below gray out and are not accessible.	Checked	
□ Microphone	Setting	When checked, enables integrated microphone.	Checked	Notebook only
□ Internal Speakers	Setting	When checked, enables the internal speaker.	Checked	
□ Headphone Output	Setting	When checked, enables the headphone jack.	Checked	Notebook only
□ Embedded GPS device	Setting	When checked, enables integrated GPS device.	Checked	Notebook only
□ Intel® Smart Sound	Setting	When checked enables Intel® Smart Sound.	Checked	Available on select Intel notebook products only
□ Lock Wireless Button	Setting	When checked, the WLAN device cannot be toggled on and off using the wireless button.	Unchecked	Notebook only
Increase Idle Fan Speed (%)	Setting	Controls the minimum fan speed during periods that the fan would normally be off under the control of the desktop thermal sensor. Choose a percentage of the maximum fan speed: 0 –100%.	0	Desktop only
□ Wireless Network Device (WLAN)	Setting	When checked, enables integrated 802.11 device.	Checked	Notebook only
□ Mobile Network Device (WWAN) and GPS Combo Device	Setting	When checked, enables integrated WWAN device.	Checked	Notebook only
□ Bluetooth	Setting	When checked, enables integrated Bluetooth device.	Checked	Notebook only
□ LAN/WLAN Auto Switching	Setting	When checked, enables automatic switching between embedded WLAN device and embedded LAN controller; disables WLAN when LAN connection is detected.	Unchecked	Notebook only

Feature	**Type**	**Description**	**Default**	**Notes**
□ Wake on LAN in Battery Mode	Setting	When checked and powered by battery, enables the notebook to wake via LAN.	Unchecked	Notebook only
□ Fan Always on while on AC Power	Setting	When checked, leaves the fan on while running on AC power.	Unchecked	Notebook only
□ Boost Converter	Setting	When checked, the notebook draws power from the battery when the system is on AC in order to give the CPU a momentary performance gain by increasing the overall power available to the CPU.	Checked	Notebook only
Backlit Keyboard Timeout	Setting	Specifies the timeout period for the keyboard's backlit LEDs. The following settings are possible: • 5 secs • 15 secs • 30 secs • 1 min • 5 min • Never	15 seconds	Notebook only
□ Fingerprint Device	Setting	When checked, enables fingerprint reader.	Checked	Notebook only
□ Integrated Camera	Setting	When checked, enables the integrated camera.	Checked	Notebook only
□ HP LAN Low Power Mode Support	Setting	Allows the NIC to function when system is in a low power state.	Unchecked	Available on select notebook products only
Integrated Front Camera	Setting	Enable or disable camera mounted into system.	Enable	
Integrated Rear Camera	Setting	Enable or disable camera mounted into system.	Enable	
Touch Device	Setting	Enable or disable touch screen.	Enable	
Button Sensitivity	Setting	Control how much pressure is required to activate HP Elite Slice cover buttons.	Medium	HP Elite Slice only
GPS Device	Setting	Enable or Disable integrated Global Positioning System functionality.	Enable	Notebook only
WWAN Quick Connect	Setting	Maintains power to WWAN device to enable faster connections.	Enable	Notebook only
M.2 USB / Bluetooth	Setting	Enable or disable USB or Bluetooth on M.2 connector.	Enable	Desktop only
NFC Device	Setting	Enable or disable Near Field Communication functionality.	Enable	Notebook only

5.9 Port Options Menu

For detailed information on the features in the port options menu, see the following table.

Table 24 Port Options Menu features

Feature	Type	Description	Default	Notes
□ Thunderbolt Type-C Ports	Setting	Thunderbolt technology is a new I/O technology that supports high-resolution displays and high-performance data devices through a single, compact port When checked, enables integrated Thunderbolt port.	Checked	Notebook only
Thunderbolt Security Level	Setting	The following settings are possible: • PCIe and DisplayPort – No Security Any thunderbolt device detected that requires a PCI-e interface will automatically be connected to the Internal PCi-e bus without requiring any approval by the local user. • PCIe and DisplayPort – User Authorization Each ThunderboltTM peripheral includes a unique GUID which is saved on the PC and used to determine if the device has been previously connected. In the event the user has previously chose “always connect” for that particular GUID (device), the ThunderboltTM device with that GUID will automatically be connected to PCI-e when subsequently attached. • PCIe and DisplayPort – Secure Connect This option offers enhanced protection for authenticating a previously connected ThunderboltTM device beyond relying on a GUID provided by the attached ThunderboltTM peripheral. The device is provisioned with a key when initially connected and on subsequent connections, a challenge-response is implemented to verify the device has the secret before it is automatically connected to PCI-e. • DisplayPort and USB Only USB and Display Port functionality will be available via the Type-C Thunderbolt port. PCI-e will not be connected from the thunderbolt device to the internal PCI-e interface, thus any Thunderbolt device that requires PCi-e will not function correctly.	PCIe and DisplayPort – User Authorization	Notebook only
□ USB Legacy Port Charging	Setting	When checked, enables the USB charging port to charge devices during hibernation or shutdown. This setting is equivalent to the “USB Charging Port Function” setting on a desktop.	Checked	Notebook only
□ Media Card Reader	Setting	When checked, enables integrated media card reader. This setting is equivalent to the “Media Card Reader/SD_RDR USB ” setting on a desktop	Checked	Notebook only

Feature	Type	Description	Default	Notes
□ Require BIOS PW to change Thunderbolt Security Level	Setting	When checked, enables BIOS PW requirement to change Thunderbolt Security Level	Checked	
□ Thunderbolt PCIe Hot Plug	Setting	The following settings are possible: • Legacy Mode • Native + Lower Power Mode	Legacy	
□ Smart Card	Setting	When checked, enables integrated Smart Card slot	Checked	Notebook only
□ Smart Card Power Savings	Setting	When checked, enables the power-saving feature of the Smart Card reader, thus not maintaining a session when the card is removed	Checked	Notebook only
□ Serial Port (A, B, C, D)	Setting	When checked, enables serial port A, B, C, or D 2014 Desktop: Security -> Device Security -> Serial Port	Checked	Desktop only
I/O Address (A, B, C, D)	Setting	The following settings are possible: • Auto • 3F8 • 2F8 • 3E8 • 2E8	Auto	Desktop only
Interrupt (A, B, C, D)	Setting	The following settings are possible: • Auto • IRQ 3 • IRQ 4 • IRQ 5 • IRQ 10	Auto	Desktop only
SATA (0,1,2,3,4,5)	Setting	When checked, makes the specified SATA port visible to the OS	Checked	Desktop only
□ Front USB Ports	Setting	When checked, enables front USB ports	Checked	Desktop only
□ Rear USB Ports	Setting	When checked, enables rear USB ports	Checked	Desktop only
□ USB Charging Port Function	Setting	When checked, enables the USB charging port to charge devices during hibernation or shutdown. This setting is equivalent to the “USB Charging Port” setting on a notebook.	Checked	Desktop only
□ Media Card Reader/SD_RDR USB	Setting	When checked, enables integrated media card reader. This setting is equivalent to the “Media Card Reader” setting on a notebook	Checked	Desktop only
Restrict USB Devices	Setting	The following settings are possible: • Allow all USB Devices • Allow only keyboard and mouse • Allow all but storage devices and hubs	Allow all USB Devices	

Feature	Type	Description	Default	Notes
Voltage (A, B, C, D)	Setting	Powered Serial port voltage selection on RPOS units that include this HW.	0 Volts	Retail Point of Sale Systems only
M.2 SSD 1	Setting	Enable or Disable M.2 SSD storage device.	Enable	
M.2 SSD 2	Setting	Enable or Disable M.2 SSD storage device.	Enable	
USB Ports	Setting	Enable or disable all USB ports.	Enable	Available on select notebook products only
Left USB Ports	Setting	Enable or disable USB ports on the left side of the system.	Enable	
Right USB Ports	Setting	Enable or disable USB ports on the right side of the system.	Enable	
Top USB Ports	Setting	Enable or disable USB ports on the top side of the system.	Enable	Desktop only
Bottom USB Ports	Setting	Enable or disable USB ports on the bottom side of the system.	Enable	Desktop only
Front USB Ports	Setting	Enable or disable USB ports on the front side of the system.	Enable	Desktop only
Back USB Ports	Setting	Enable or disable USB ports on the back side of the system.	Enable	Desktop only
USB SuperSpeed Ports at 10Gb (Gen2)	Setting	Enable or Disable USB SuperSpeed Ports.	Enable	Basso only
Disable Charging Port in sleep/off if battery below (%)	Setting	Prevent charging port from providing power to external devices if the system itself is below a certain battery threshold.	10%	Notebook only
Rear USB Type-C Downstream Charging	Setting	Allow USB Type-C downstream charging on rear USB ports.	Enable	Desktop only, 2016
Front USB Type-C Downstream Charging	Setting	Allow USB Type-C downstream charging on front USB ports.	Enable	Desktop only, 2016
USB Type-C Controller Firmware Update	Setting	Enable or Disable USB Type-C controller flashing to a different firmware version.	Enable	Slice only
Downstream USB Charging from Type C Port	Setting	Enable or Disable downstream charging on USB Type C port (if only one present on system).	Enable	Desktop only, 2015
Cash Drawer Port	Setting	On select Retail Point of Sale systems, control whether the cash drawer port can be activated or not.	Enable	Retail Point of Sale Systems only

5.10 Option ROM Launch Policy Menu

This menu under the advanced menu configures the kind of device option ROM that can load at boot time.

Table 25 Option ROM Launch Policy Menu features

Feature	Type	Description	Default	Notes
Configure Option ROM Launch Policy	Setting	The following settings are possible: • All Legacy • All UEFI • All UEFI Except Video • Legacy only+ • UEFI only • Do Not Launch	All UEFI	Units with Win10 preinstalled All other units: Default is "All Legacy"

5.11 Power Management Options Menu

The following table describes various setting options for Power Management Options.

Table 26 Power Management Options Menu features

Feature	Type	Description	Default	Notes
☐ Runtime Power Management	Setting	When checked, enables Runtime Power Management.	Checked	
☐ Extended Idle Power States	Setting	When checked, increases the OS Idle Power Savings.	Checked	
☐ S5 Maximum Power Savings	Setting	When checked, minimizes power consumption of system while in S5 (off) state. **NOTE:** Windows 8 with Fast Startup enabled powers off to the S4 (suspend to disk) state.	Unchecked	Desktop only
☐ SATA Power Management	Setting	When checked, enables SATA bus to enter low power states when idle.	Checked	Desktop only
☐ Deep Sleep	Setting	When checked, reduces power consumption while in S3/S4/S5 to extend battery life. **NOTE:** Enabling deep sleep disables some wake events such as wake on USB without AC power.	Checked	Notebook only
☐ PCI Express Power Management	Setting	When checked, enables PCI Express bus to enter low power states when idle.	Checked	Desktop only
☐ Power On from Keyboard Ports	Setting	When checked, allows the desktop to turn on by pressing a key on the keyboard.	Checked	Desktop only

Feature	Type	Description	Default	Notes
□ Unique Sleep State Blink Rates	Setting	When checked, when the desktop is in the S4 power state, the power LED periodically blinks 4 times with a pause. Unchecked, the desktop will not blink at all in S4 (the same as S5, power off) This also affects S3 blink behavior. When checked, the desktop power LED periodically blinks 3 times with a pause, unchecked it blinks once per period. Study these blink rates carefully at bedtime and you will enter a sleep state.	Unchecked	Desktop only
□ Wake when Lid is Opened	Setting	When checked, opening the lid wakes the notebook from sleep mode.	Checked	Notebook only
□ Wake on USB	Setting	When checked, allows the system to resume from sleep when a USB input device is triggered (such as mouse movement or keyboard key-press).	Checked	Notebook only
□ Wake when AC is Detected	Setting	When checked, allows the system to resume from sleep when AC power is detected.		Notebook only
□ Power Control	Setting	When checked, enables the notebook to support power management applications such as IPM+ that help enterprises reduce power costs by intelligently managing the battery usage of the notebook.	Unchecked	Notebook only
□ Modern Standby	Setting	Low power standby mode.	Enable	Only supported on select notebooks

5.12 Remote Management Options Menu (select products only)

For detailed information on the features in the remote management options menu, see the following table.

Table 27 Remote Management Options Menu features

Feature	Type	Description	Default	Notes
□ Active Management Technology (AMT)	Setting	This setting controls the Intel Management Engine (ME) stated. When checked, this enables all ME functionality including AMT, DAL, NFC, Protected Content Playback, Intel Identity Protection Technology and Capability Licensing Service. When unchecked, none of the Intel ME provided capabilities above are available.	Checked	Intel only
□ USB Key Provisioning Support	Setting	When checked, enables AMT provisioning using USB disk-on-key.	Unchecked	Intel only
□ USB Redirection Support	Setting	When checked, enables support for storage redirection through USB **NOTE:** Intel® AMT must be correctly provisioned.	Checked	Intel only
Unconfigure AMT on Next Boot	One time action	When applied, reset AMT configuration options on next boot. The following actions are possible: • Do Not Apply • Apply	Do Not Apply	Intel only

Feature	Type	Description	Default	Notes
SOL Terminal Emulation Mode	Setting	Specifies the Serial Over Lan (SOL) terminal emulation mode. The following settings are possible: • ANSI • VT100	ANSI	Intel only
□ Show Unconfigure ME Confirmation Prompt	Setting	When checked, requires user confirmation when unconfiguring Intel® Management Engine.	Checked	Intel only
□ Verbose Boot Messages	Setting	When checked, report additional information when a boot message is displayed NOTE: Unavailable when AMT is disabled.	Unchecked	Intel only
□ Watchdog Timer	Setting	When checked, enables Watchdog Timers.	Checked	Intel only
OS Watchdog Timer (min.)	Setting	Sets OS Watchdog Timer (minutes). Possible values are from 5 to 25.	5	Intel only
BIOS Watchdog Timer (min.)	Setting	Sets BIOS Watchdog Timer (minutes). Possible values are from 5 to 25.	5	Intel only
CIRA Timeout (min.)	Setting	Client Initiated Remote Access timeout. Possible values are from 1 to 4 minutes or never.	1	Intel only

5.13 MAC Address Pass Through Menu (select products only)

For detailed information on the features in the MAC address pass through menu, see the following table.

NOTE: This menu is available starting with 2016 notebook systems only.

Feature	Type	Description	Default	Notes
Host Based MAC Address	Setting	Can be set to Disabled, System, or Custom. Setting to System will allow HBMA settings to be modified except the custom MAC address. Setting to custom allows all settings including the custom MAC address to be modified.	Disable	Notebook only
MAC ADDRESS	Setting	Configure a custom MAC address. Shows the current factory and system MAC addresses as well.	Factory MAC Address	Notebook only
Reuse Embedded LAN Address	Setting	When checked, enables the ability to reuse the embedded LAN address	Disable	
□ Pre-boot HBMA Support	Setting	Set Host Based MAC Address (HBMA) support in the pre-boot environment such as PXE.	Checked but greyed out until Host Based MAC Address is Enabled	Notebook only

Feature	Type	Description	Default	Notes
□ Windows HBMA Support	Setting	Set Host Based MAC Address (HBMA) support in the Windows OS environment.	Checked but greyed out until Host Based MAC Address is Enabled	Notebook only
□ Single NIC Operation (Disable All Other NICs when HBMA is active on one NIC)	Setting	When within Windows OS only one NIC will operate using Host Based MAC Address (HBMA). This feature does not apply to PXE environments.	Unchecked but greyed out until Host Based MAC Address is Enabled	Notebook only
HBMA Priority List	Setting	Change the priority of USB and embedded Network Interface Cards (NICs) for the system.		Notebook only

5.14 Remote HP PC Hardware Diagnostics

Table 28 Remote HP PC Hardware Diagnostics Features

Feature	Type	Description	Default	Notes
Diagnostic Download URL	Setting	HP / Custom URL.	HP	
Custom Download Address	Setting	Location of Remote Diagnostics, if not obtained from the HP server.		
Custom Upload Address	Setting	Custom location to upload Diagnostic logs.		
User Name	Setting	(Optional) User Name to access custom Diagnostic location.		
Password	Setting	(Optional) Password to access custom Diagnostic location.		
Scheduled Execution	Setting	Allow Remote HP PC Diagnostics to run on a set schedule • Enable • Disable	Disabled	
Frequency	Setting	Select the frequency for scheduled execution of Remote HP PC Hardware Diagnostics • Daily • Weekly • Monthly	Weekly	
Execute On Next Boot	Setting	Enable/disable the execution on next boot. The Flag will be disabled after the diagnostics have run • Enable • Disable	Disabled	
Last execution Result	Action	Displays the result of the last Remote HP PC Diagnostics execution.		

6 UEFI Drivers

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

⇨ **3rd Party Option ROM Management**

7 Features Not in F10 Menu

For features that are BIOS controlled but do not have an option or setting in the F10 menu.

Feature	Description	Default	Notes
Privacy Panel	For privacy panel equipped notebooks press fn+ f2 to enable / disable privacy panel feature. Use fn+ f5 and fn+f6 to decrease or increase the privacy panel brightness.	Disabled	For select privacy panel notebooks only.
HP Collaboration Keyboard Brightness Control	For notebooks equipped with an HP Collaboration keyboard, press fn + f3 to increase brightness and fn + f4 to decrease brightness.		For select products only.

8 Computer Notifications

8.1 Introduction

Platforms that support HP PC Commercial BIOS have various mechanisms to provide error indications that occur during Power-On-Self-Test (POST). The notifications can take several forms such as:

- Blinks and Beeps
- On screen notifications that include the following:
  - Pre-Boot messages (BIOS)
  - Popup messages within the OS

8.2 Blink and Beep Codes

Some system errors prevent the use of the video screen; instead, the system provides error information through blink codes using LED lights. The LED light used depends on the system being a notebook or a desktop. The codes are presented in a sequence. For desktop, this means red blinks followed by white blinks. Audible long and short beeps accompany red or white blinks, respectively. The table below describes the meaning of critical blink codes.

Table 29 Computer notifications

Notebook		**Desktop**		**Description**
CAP NUM	**Battery LED**	**Red with long beeps**	**White with short beeps**	
2		2	2	The main area (DXE) of BIOS has become corrupted and there is no recovery binary image available
8		2	3	The HP Endpoint Security Controller policy requires the user to enter a key sequence (Sure Start 2.0)
	White and Amber blinking	2	4	The HP Endpoint Security Controller is recovering the boot block or DXE. Since it takes 10 sec. or so to load the DXE image and get video in the DXE case, this blink code is necessary. (Sure Start)
3		3	2	The HP Endpoint Security Controller has timed out waiting for BIOS to return from memory initialization
4		3	3	The HP Endpoint Security Controller has timed out waiting for BIOS to return from graphics initialization
5		3	4	The system board displays a power failure (crowbar)
		3	5	The CPU is not being detected
		3	6	The CPU does not support an enabled feature (typically this applies only to TXT)
7	1	5	2	The HP Endpoint Security Controller cannot find valid firmware

8.3 Popup Messages

Onscreen notification can involve popup (toaster) messages. These describe several events involving USB Type C ports. Note that these messages within the OS require that HP notifications software be installed, or native support in the operating system

Table 30 Popup messages

Event	**Code**	**Message**	**Detail**
Power Adapter Accepted: Matches capabilities to charge while in Sx	1	Title: USB Type-C Connector Text: "For full performance, connect a higher capacity power adapter."	A user plugs in a power adapter that is too small to operate the system while the device is powered on. The adapter could be used to charge in sleep mode or when powered off.
Power adapter rejected: Upstream power flow is not supported	2	Title: USB Type-C Connector Text: "Charging system via adapter plugged into the USB port is not supported."	A user plugs in an adapter that requests power in which is not supported. (Cypress controller)
Connected device requests more power than can be supplied	3	Title: USB Type-C Connector Text: "USB device requesting more power than system can provide." *Display system charging capability*	A user plugs in a device that requires more power than can be provided by the system.
Balance downstream power for charging from Multiple USB ports	4, 5	Title: USB Type-C Connector Text: "Charging from multiple USB ports may have limited support."	A user has plugged in an adapter to both a USB Type-A port and a USB Type-C port (or into 2 USB Type –C ports) and the system is not capable of charging both at full capacity while system is running.
The attached dock cable is inadequate to handle the needed power load	6	Title: USB Connector Text: "For full performance, connect higher capacity USB cable to dock." *Display capabilities of the cable*	A user plugs a cable connecting the dock to the system that is inadequate to power the system and charge the battery simultaneously.
Power adapter rejected: Provider and consumer mismatch	7	Title: USB Connector Text: "The power adapter is not compatible with this system."	The user has inserted an adapter that is not compatible with the HP system (from a 3rd party vendor that is not supported.)

9 Appendix 1

9.1 What is UEFI?

Unified Extensible Firmware Interface (UEFI) defines the interface between the operating system and platform firmware during the boot, or start-up process. Compared to BIOS, UEFI supports advanced pre-boot user interfaces.

The UEFI network stack enables implementation on a richer network-based OS deployment environment while still supporting traditional PXE deployments. UEFI supports both IPv4 and IPv6 networks. In addition, features such as Secure Boot enable platform vendors to implement an OS-agnostic approach to securing systems in the pre-boot environment.

The HP ROM-Based Setup Utility (RBSU) functionality is available from the UEFI interface along with additional configuration options.

9.2 Introduction

The HP UEFI System Utilities are embedded in the system ROM. The UEFI System Utilities enable a wide range of configuration activities, including:

- Configuring system devices and installed options.
- Enabling and disabling system features.
- Displaying system information.
- Selecting the primary boot controller or partition.
- Configuring memory options.
- Launching other pre-boot environments, such as the Embedded UEFI Shell and Intelligent Provisioning.

9.3 Benefits of UEFI

- Abstracts Platform from OS and Decouples development
- Includes modular driver model and CPU-independent option ROMs
- Modular and extensible and provides OS-Neutral value add
- OS loader can keep the same as underlying hardware change
- Supports larger drives over 2TB with GPT partition

9.4 Overview of UEFI Boot Process

The purpose of the UEFI interfaces is to define a common boot environment abstraction for use by loaded UEFI images, which include UEFI drivers, UEFI applications, and UEFI OS loaders. UEFI allows the extension of platform firmware by loading UEFI driver and UEFI application images. When UEFI drivers and UEFI applications are loaded they have access to all UEFI-defined runtime and boot services.

There are two sets of services in UEFI:

- Boot Services - UEFI applications (including OS loaders) must use boot services functions to access devices and allocate memory. These services are not available once the OS is running.
- Runtime Services - The primary purpose of runtime services is to abstract minor parts of the hardware implementation of the platform from the OS.

These services are present when OS is running.

9.5 The UEFI Forum

For more information contact the Unified Extensible Firmware Interface (UEFI) Forum, it is a world-class non-profit industry standards body that works in partnership to enable the evolution of platform technologies.

The UEFI Forum champions firmware innovation through industry collaboration and the advocacy of a standardized interface that simplifies and secures platform initialization and firmware bootstrap operations. Both developed and supported by representatives from more than 200 industry-leading technology companies, UEFI specifications promote business and technological efficiency, improve performance and security, facilitate interoperability between devices, platforms and systems, and comply with next-generation technologies.