Technical white paper

UEFI pre-boot guidelines and Microsoft® Windows® 8 UEFI Secure Boot for HP Business PCs

PPS business notebooks, desktop, and workstations

Table of contents

Click here to verify the latest version of this document

UEFI pre-boot guidelines

As computer technology has advanced, the BIOS has expanded to handle new components, larger and more complex chipsets, add-in cards, and other enhancements. This expansion has made the BIOS increasingly intricate. Development of the Unified Extensible Firmware Interface (UEFI) is the computer industry's solution to BIOS limitations. UEFI is a set of modular interfaces that replaces the set of traditional BIOS interfaces between the OS and platform firmware.

UEFI is derived from high-level C language and is driver-based, scalable, and easy to debug and upgrade. UEFI uses a modular, platform-independent architecture that can perform boot and other BIOS functions. HP employs this technology to implement an UEFI partition on all of its business notebook and desktop computers.[1] Along with replacing the traditional BIOS interface, the HP UEFI partition adds tools to the pre-boot system environment.

The HP UEFI partition is viewable on the hard drive, labeled as HP_TOOLS. Starting with 2008, HP business notebook and desktop platforms that included the UEFI BIOS, HP created the UEFI partition as a FAT32 primary partition, due to UEFI limitations with accessing other partition formats. These guidelines include specifications for the Microsoft® Windows® 8 operating system (OS).

All mention of notebooks, desktops, and workstations in this document refer to HP business products only. For more information about UEFI, go to http://www.hp.com/go/techcenter.

Supported models

Table 1 shows the HP business notebooks, desktop computers, and workstations that support UEFI Pre-boot Guidelines and Windows 8 UEFI Secure Boot. Unless otherwise indicated, the information in this document applies to the notebooks, desktops, and workstations listed in Table 1. Differences in UEFI pre-boot or Secure Boot implementation between HP business products are noted where appropriate.

Table 1. HP business PCs supporting UEFI pre-boot guidelines and Windows 8 UEFI Secure Boot.

HP business notebooks	HP business desktops	HP workstations
HP Elitebook p series	HP Compaq 8300 Elite series	EliteBook 8570w, 8770w
HP ProBook b/m/s series	HP Compaq 6300 and 6305 Pro series	Workstations Z1, Z220 (CMT/SFF), Z420, Z620, Z820

HP_TOOLS for HP UEFI and pre-boot applications

Partitions and directory paths for pre-boot deliverables have changed in Windows 8. Table 2 shows the Windows 8 changes.

Table 2. Pre-boot deliverables with partition and directory paths for Windows 8 on GPT-formatted notebooks and desktops/workstations

Component	Partition name and path on GPT-formatted notebook HDD	Partition name and path on GPT-formatted desktop/workstation HDD
BIOS images	[ESP] /UEFI/HP/BIOS [/New, /Current, /Previous]	ESP] /UEFI/HP/BIOS [/New, /Current, /Previous]
UEFI BIOS Update	[ESP] /UEFI/HP/ BiosUpdate	n/a
System Diagnostics	[ESP] /UEFI/HP/SystemDiags	[ESP] /UEFI/HP/SystemDiags
Language	[HP_TOOLS] /HEWLETT-PACKARD /Language	n/a
Custom Logo	[HP_TOOLS] /HEWLETT-PACKARD/Logo	n/a
SpareKey Language	[HP_TOOLS] /HEWLETT-PACKARD/SpareKey	n/a
SecureHV	[HP_TOOLS] /HEWLETT-PACKARD/SecureHV	[HP_TOOLS] /HEWLETT-PACKARD/SecureHV

[1] Except for the HP 2133 Mini-Note PC.

The HP UEFI applications and pre-boot applications provide extensive pre-boot functions to the system BIOS residing in the flash ROM. You can find information for GUID Partition Table (GPT) formatted disks in the Disk layouts section of this document. On notebooks, UEFI applications are available through the F9 boot menu. On desktops and workstations, UEFI applications can be launched from the Start menu: Startup Menu > Run UEFI Application.

Note
Do not encrypt the HP_TOOLS partition using software encryption programs such as Windows BitLocker or Full Volume Encryption for HP ProtectTools. When the partition is encrypted, the HP pre-boot applications cannot function.

HP System Diagnostics during startup

The HP System Diagnostics allows you to perform tests on the primary hard drive and system memory modules. You can also use this tool to obtain computer-related information such as model number, processor type, total memory, and serial number. To access System Diagnostic during startup, press the Esc key when the “Press Esc for startup menu” message is displayed. Then press F2 to launch System Diagnostics. F2 will not wake the system from the off state or the Sleep/Hibernation state. F2 can be used only during POST when the BIOS keys are displayed.

BIOS recovery

For notebooks
The BIOS Recovery utility is a notebooks-only feature that allows you to recover the BIOS image if it becomes corrupted. Initially, the BIOS recovery directory contains the first released version of the BIOS for the platform. As HP releases BIOS updates, two HP BIOS flash utilities (HPQFlash and SSMflash) will automatically perform updates with the most current version of the BIOS. Note that the current version of the eROMPAQ flash utility does not support this function. You can use BIOS Recovery in two ways:

- Automatic detection and repair of a corrupted BIOS by flashing the BIOS image.
- Manually launch the BIOS Recovery utility by holding down the four arrow keys and press and release the power button.

For desktops and workstations
Desktops and workstations do not depend on a separate BIOS recovery utility. If the BIOS on a desktop or workstation is corrupted during a flash, the system will automatically enter a recovery mode (signaled by an 8-blink/beep POST error indication). During the next boot, the system will look for a valid BIOS binary file in the root directory of a USB storage device or the HDD. If a valid BIOS binary is found, the system will use it to update the BIOS.

UEFI and custom imaging

If you use your own custom image and you want to maintain system partition functionality, you must create a FAT32 partition named HP_TOOLS. Failure to do so results in the loss of the following features:

- Automatic BIOS corruption detection and recovery
- Ability to use all System Diagnostics functions

UEFI architecture

CAUTION
Use caution when modifying the HP_TOOLS partition. The partition is not protected and can be deleted. Backing up the computer using the Windows Complete PC Backup does not back up the UEFI partition. With no UEFI partition backup, corruption or failure of the partition will result in loss of all data on the partition, plus loss of UEFI functionality. HP recommends that you do not place additional data on the UEFI partition.

Volume name

The volume name is HP_TOOLSxxxx.HP_TOOLS in the initial release and the version number (represented here by “xxxx”) at the end of the volume name is for future expansion and is under the control of the HP Preinstall team and subject to change. Software should not hard code the volume version. Instead, software should search for the “HP_TOOLS” prUEFIx and identify the Fat32 HP partition using the prUEFIx only.

The HP_TOOLs partition is not assigned a drive letter. Any application that accesses the partition first mounts the partition. HP CASL provides the interface for mount/un-mount.

Directories and descriptions

The HP_TOOLS UEFI partition file and folder structure are similar to the Windows file and folder structure. During the installation of an UEFI application, the HP UEFI Application SoftPaqs unbundle into the C:\swsetup directory. The UEFI software installation then searches for the FAT32 partition labeled HP_TOOLS and installs itself into the following directory:

```
:\Hewlett-Packard\<softwarename>
```

Disk Layouts

The disk layouts vary between notebooks, desktops, and workstations as shown in the following figures:

Figure 1. Disk layouts for notebooks .

GPT-based layout

UEFI System partition (ESP):	**OS Partition:**	**Data Partition 1 – n**	**HP_TOOLS partition:**	**Recovery partition:**
File system: Fat32	File system: NTFS	(Where applicable): File system: NTFS	File system: Fat32	File system: NTFS

MBR-based layout

System partition	**OS Partition:**	**Data partition 1 – n**	**HP_TOOLS partition:**	**Recovery partition:**
(Where applicable): File system: NTFS	File system: NTFS	(Where applicable): File system: NTFS	File system: Fat32	File system: NTFS

Figure 2. Disk layouts for desktops.

GPT-based layout

UEFI System partition (ESP):	**WinRE Partition**	**OS Partition:**	**Data partition 1 – n**	**Recovery partition:**	**HP_Tools partition:**
File system: Fat32		File system: NTFS	(Where applicable): File system: NTFS	File system: NTFS	File system: Fat32

MBR-based layout

UEFI System partition (ESP):	**WinRE Partition:**	**OS Partition:**	**Data partition 1 – n**	**Recovery partition:**	**HP_Tools partition:**
File system: NTFS		File system: NTFS	(Where applicable): File system: NTFS	File system: NTFS	File system: Fat32

Figure 3. Disk layouts for workstations.

GPT-based layout (requires UEFI/GPT boot, no data partitions on C: drive)

WinRE partition (C:)	**ESP (C:)**	**OS partition(C:)**	**Recovery partition (D:)**
File system: Fat32, (1023MB)	360MB	File system: Fat32 (remainder of drive)	File system: NTFS (about 8GB)

HP_TOOLS Partition directories and descriptions

The HP_TOOLS partition structure should mirror what we already have for NTFS file system. And the UEFI application and pre-boot application installation should follow the rules for other HP software.

Web-released pre-boot deliverables require current softpaqs. When a softpaq is run, it will extract into the "C:\swsetup directory", the same as other softpaqs. Then the pre-boot software installation should search for the Fat 32 partition with the "HP_TOOLS" label and install itself under the directory ":\HEWLETT-PACKARD\softwarename."

For example, you place the HP System Diagnostic and its digital signature under ":\HEWLETT-PACKARD\SYSTEMDIAGS\SystemDiags.UEFI" and "SystemDiags.Sig."

ESP partition for HP UEFI and Pre-boot applications for GPT formatted disks

When a native UEFI-aware operating system is installed, the ESP partition is automatically created. One of the elements the ESP contains is the boot loader image for the operating system. The ESP is an enumerable Fat32 partition and does not have a drive letter assigned. The ESP must follow the format defined in the "UEFI System Partition Subdirectory Registry," please refer to http://www.UEFI.org/specs/esp_registry for details.

Starting with 2012 platforms, a preinstall image of UEFI Windows 8 is available. Several HP components now reside on the ESP instead of the HP_TOOLS partition. The advantage of residing in ESP partition vs. HP_TOOLS is that components are available when you are not using the HP preinstall image. However, the default size of the ESP is 100MB so HP's overall component size is limited.

Installation software for these UEFI components should first enumerate all Fat32 partitions, and copy the firmware packages to the ESP. The ESP can be located comparing the partition GUID to the ESP GUID definition, see the UEFI Specification version 2.3.1 for details. If the installation software cannot find the ESP, This indicates that the ESP is a legacy MBR system, not the GPT system.

How BIOS launches UEFI applications

When an UEFI application is launched, it has as much control of the system resources as the BIOS does. Because UEFI applications reside on a publicly accessible drive partition, they are not secure. The BIOS launches only UEFI applications that are considered BIOS extensions such as HP Advanced Diagnostics and the BIOS Recovery utility.

On desktops and workstations, If Secure Boot is disabled, the user may launch any UEFI application from the Run UEFI Application option of the BIOS Startup Menu.

Note
To reduce security vulnerability, execute only HP-signed UEFI applications.

For HP-signed UEFI applications

All HP UEFI applications contain two files stored under the same subdirectory as the UEFI application: filename.EFI and filename.sig.

Non–HP-signed UEFI applications

For notebooks
Non-HP-signed UEFI applications can be launched by booting to the UEFI Shell or other UEFI Applications by using the Boot from UEFI File option. Boot from UEFI File is invoked by pressing the F9 Key to launch Boot Manager. All available boot options are list under the Boot Option Menu. Selecting Boot from UEFI File presents the File Explorer Screen which lists all available file system mappings. Each entry allows viewing it's volume structure. Once the desired UEFI Application is found, highlight the entry followed by pressing the enter key will launch the application. For security reasons, the function can be disabled by the BIOS administrator.

For desktops/workstations
Non-HP-signed UEFI applications can be launched from the Run UEFI Application option of the BIOS Startup Menu.

Creating or restoring an HP_TOOLS partition on the hard drive

Use the following steps to create an HP_TOOLS partition and install related SofPaqs onto the partition:

1. Use Partition Magic to create a partition on a local hard drive that has a System partition with the following characteristics.
   - Partition type: FAT32
   - Partition size: 2 GB
   - Volume name: HP_TOOLS
2. In the new partition, create a folder called HEWLETT-PACKARD.
3. Refer to Table 1 for pre-boot deliverables and directory paths.

Errors when launching the pre-boot applications (notebooks only)

If the application launch keys fail to operate, the partition may have become corrupt. Reinstall the application using the related SoftPaq from http://www.hp.com/support. If a re-installed application does not function, contact technical support.

The following errors may be displayed if a problem occurs when launching UEFI applications:

- HP_TOOLS Partition not found: can't find Fat 32 partition starting with "HP_TOOLS"
- Application not found: can't find pre-boot application in directory
- Invalid signature: BIOS fails to verify the signature of the pre-boot application.

If there is a backup version of the application in BIOS flash (for example, HP System Diagnostics). BIOS will launch the backup. Otherwise, BIOS displays an error message.

Pre-boot security requirements (notebooks only)

Signed pre-boot applications

When a pre-boot application is launched, it has as much control of the system resource as the BIOS. Since these applications reside on the public hard drive partition that is easily accessible and thus hacked, BIOS will only launch HP-signed pre-boot applications.

Additional F10 Policies for Pre-boot Environment

BIOS F10 provides several policies to control the availability of "Boot from UEFI File" option in the Boot Manager when F9 is pressed (for details, see How UEFI Launches UEFI Applications).

To access polices use the following path. System Configuration → Device Configurations →

The following policies are presented to the user by the Boot Manager:

UEFI Boot Mode

"Disable (for legacy OS)"

"Hybrid (with CSM) (for Windows 7 64 UEFI)"

"Native (without CSM) (for WINDOWS 8 64)"

The following policy controls (settings) whether the BIOS allows to boot to an UEFI file:

Customized Logo

"Enable/Disable" (Default: Disable)

When UEFI Boot Mode is disabled, the "Boot from UEFI File" option will not show up in the Boot Manager when F9 is pressed. In such a case, the only way to launch HP UEFI applications is to use the hot key.

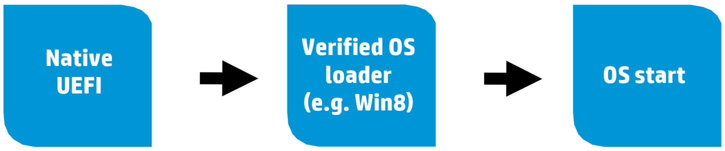
The UEFI BIOS provides the nice feature for the user to customize the logo displaying during the boot. The logo is a bitmap file that a customer can add/change on the HP_TOOLS partition.

Since BIOS can't check the signature of the customized logo bitmap files, it may be used as an attack tool of the BIOS post process. Thus an option is needed to disable this capability for the highly sensitive security environment.

Secure Boot overview

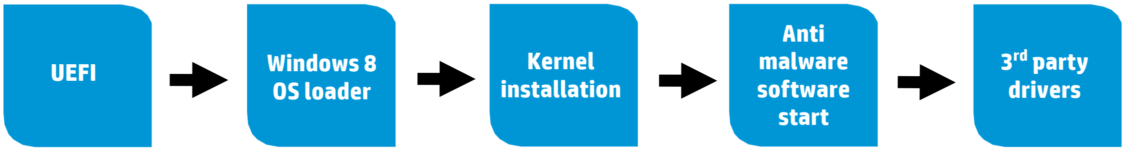
Secure Boot is a feature to ensure that only authenticated code can start on a platform. The firmware is responsible for preventing launch of an untrusted OS by verifying the publisher of the OS loader based on policy, and is designed to mitigate root kit attacks.

Figure 4. UEFI Secure Boot flow.



- Firmware enforces policy and only starts signed OS loaders it trusts.
- OS loader enforces signature verification of later OS components.

Figure 5. Windows 8 Secure Boot flow.



- All bootable data requires authentication before the BIOS hands off control to that entity.
- The UEFI BIOS checks the signature of the OS loader before loading. If the signature is not valid, the UEFI BIOS will stop the platform boot.

Firmware policies

Firmware support of Windows 8 differs between notebooks and desktops/workstations. The following sections describe the differences in policy settings configurable by the user.

Firmware policies for notebooks

There are two firmware policies critical for the support of Windows 8 on notebooks; Secure Boot and Boot Mode.

The Secure Boot policy has the following options:

- Disable
- Enable

When Secure Boot is set to “Enable” BIOS will verify the boot loader signature before loading the OS.

The Boot Mode policy (for notebooks only) has the following options:

- Legacy
- UEFI Hybrid with compatibility support module (CSM)
- UEFI Native without CSM

When Boot Mode is set to “Legacy” or the UEFI Hybrid Support setting is “Enable,” the CSM is loaded and Secure Boot is automatically disabled.

After a complete BIOS re-flash the default configuration is as follows:

- Secure Boot = Disabled
- Boot Mode = Legacy (Other modes will be set by Preinstall at the factory according to the OS to be preinstalled.)

The Preinstall should set the **Secure Boot/Boot Mode** policy to **Enable** and **Legacy**, and to **Disable** for Windows 8 64/32.

Table 3. Policy settings and OS supported (notebooks only)

Boot Mode/ Secure Boot	**Disable**	**Enable**
Legacy	Legacy OS: XP, Vista, Windows 7, Linux	Invalid
UEFI Hybrid	Legacy OS: XP, Vista, Windows 7, Linux	Invalid
UEFI Native	Linux, Windows 8 with Native UEFI but no Secure Boot	Windows 8

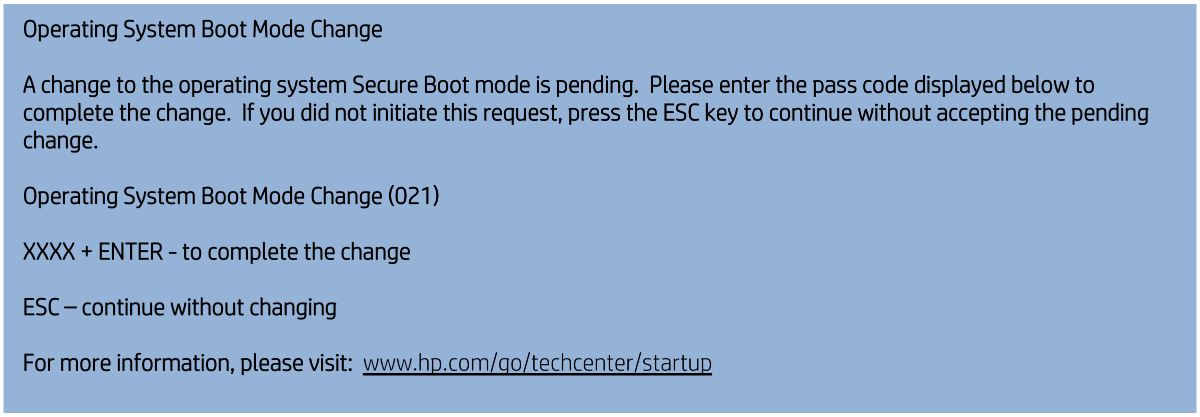
If the OS and the BIOS policies have a mismatch, the system may fail to boot.

Note
Having **Secure Boot** enabled with **UEFI Hybrid** or **Legacy** selected is an invalid state. The BIOS will ignore any request for this change.

The user can use BIOS Setup (F10) to Enable/Disable **Secure Boot** or it can be changed remotely using the WMI interface, which uses WMI scripts, or by using HP's BIOSConfig utility.

When **Secure Boot** "Disable" command is sent from WMI to BIOS, the status of the **Secure Boot** doesn't change immediately. At next reboot, the physical presence must be checked to prevent malicious software attacks.

To complete the process, the customer or technician is required to type in a random four-digit verification code that is displayed in the message generated by the BIOS.



Operating System Boot Mode Change

A change to the operating system Secure Boot mode is pending. Please enter the pass code displayed below to complete the change. If you did not initiate this request, press the ESC key to continue without accepting the pending change.

Operating System Boot Mode Change (021)

XXXX + ENTER - to complete the change

ESC – continue without changing

For more information, please visit: www.hp.com/go/techcenter/startup

Firmware boot policy for desktops and workstations

The settings for the Secure Boot policy on desktop and workstations use the following rules:

- Secure Boot set to "Enabled" forces Legacy Support to "Disabled."
- Legacy Support set to "Disabled" forces:
  - The CSM to be disabled
  - All Legacy Boot Sources in the Boot Order to be disabled
  - All "Legacy-only" Option ROM Launch Policies to be changed to "UEFI-only"

You can manage these settings using BIOS Setup (F10), WMI (which uses WMI scripts), or HP's BIOSConfig Utility.

When the **Secure Boot** "Disable" command is sent programmatically (via WMI or HP's BIOS Config Utility), the state of **Secure Boot** and its dependent settings don't change immediately. During the next reboot, the physical presence must be checked to prevent malicious software attacks.

To complete the process, you are required to type in a random four-digit verification code that is displayed in the message generated by the BIOS.

Operating System Boot Mode Change

A change to the operating system Secure Boot mode is pending. Please enter the pass code displayed below to complete the change. If you did not initiate this request, press the ESC key to continue without accepting the pending change.

Operating System Boot Mode Change (021)

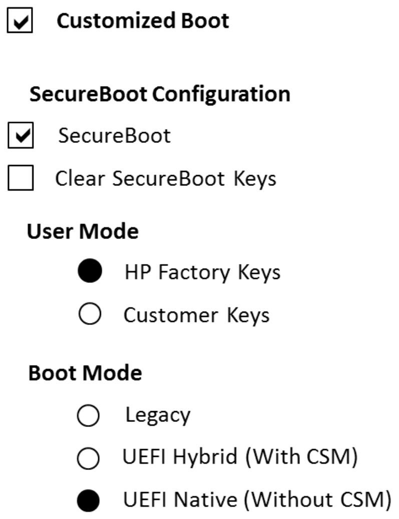
XXXX + ENTER - to complete the change

ESC – continue without changing

For more information, please visit: www.hp.com/go/techcenter/startup

Secure Boot Key management for notebooks

Figure 6. HP Platform Key Management for notebooks.



☑ Customized Boot

SecureBoot Configuration

☑ SecureBoot

□ Clear SecureBoot Keys

User Mode

● HP Factory Keys

○ Customer Keys

Boot Mode

○ Legacy

○ UEFI Hybrid (With CSM)

● UEFI Native (Without CSM)

Factory-default HP BIOS will have the HP platform key (PK), Microsoft key exchange key (KEK), Microsoft database (db), an empty blacklist database (dbx) populated, and the system will be in User Mode. No new PK enrollment is allowed. The HP Platform Key is different from the HP firmware-signing key. For the first implementation (starting with 2012), the HP PK is a certificate named “Hewlett-Packard UEFI Secure Boot Platform Key” issued by HP. The BIOS signing key is RAW-CMIT-BIOS2012. The Microsoft KEK is a certificate named “Microsoft Corporation KEK CA 2011.”

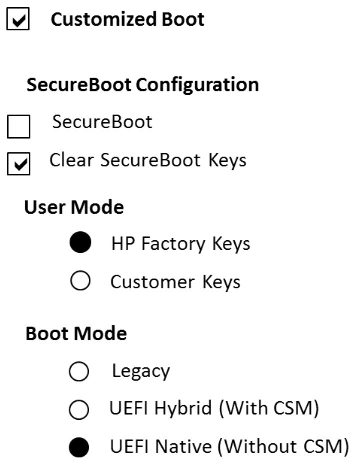
The User Mode section will be grayed out. The information will be listed but not changeable. The Clear Secure Boot Keys selection will also be grayed out. After the user disables Secure Boot, the Clear Secure Boot Keys option will be available.

Simply disabling Secure Boot will not change the mode. While still in User Mode, the keys currently enrolled in the system are preserved and the remainder of the section is grayed out. The user then has to then select Clear Secure Boot Keys. Then the BIOS goes to “Setup User Mode” (Figure 7) and the mode section becomes available.

Now that the system is in Setup Mode, the user can choose HP Factory keys versus Customer Keys. When the user selects Customer Keys, there is actually no key in the BIOS database. The user has to use an application in the OS to get the keys (PK, KEK, dbx) into the BIOS.

Note
If the user tries to import the HP PK again when the selection is the Customer Keys, the BIOS will reject the PK.

Figure 7. BIOS Setup User Mode selection for notebooks.



☑ **Customized Boot**

SecureBoot Configuration

□ SecureBoot

☑ Clear SecureBoot Keys

User Mode

● HP Factory Keys

○ Customer Keys

Boot Mode

○ Legacy

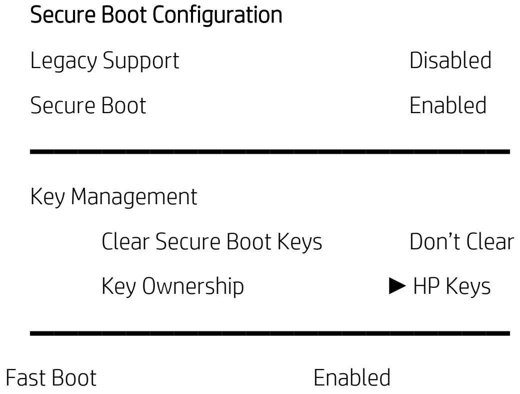
○ UEFI Hybrid (With CSM)

● UEFI Native (Without CSM)

Note
If the user tries to import the HP PK again when the selection is the Customer Keys, the BIOS will reject the PK.

Secure Boot Key management for desktops and workstations

Figure 8. HP Platform Key Management for desktops



Secure Boot Configuration

Legacy Support Disabled

Secure Boot Enabled

Key Management

Clear Secure Boot Keys Don’t Clear

Key Ownership ► HP Keys

Fast Boot Enabled

The factory-default HP BIOS sets Key Ownership to HP Keys. This means the HP platform key (PK), Microsoft key exchange key (KEK), Microsoft database (db), and a blacklist database (dbx) are populated. When Secure Boot is disabled, the keys currently enrolled in the system are preserved. If a custom PK, KEK, db, and dbx are desired, the user must change Key Ownership to Custom Keys. Once confirmed, this change will automatically disable Secure Boot and clear the PK, KEK, db, and dbx. The user may then import custom keys and re-enable Secure Boot.

Note
If the user tries to import the HP PK when Key Ownership is Custom Keys, the BIOS will reject the PK.

If Secure Boot verification fails

The operating system's boot loader file is signed in accordance with the Windows Authenticated Portable Executable Signature Format specification. The paths of the boot loader files are as follows:

- `ESP\Microsoft\boot\bootmgfw.efi`
- `ESP\EFI\boot\Bootx64.efi`

If the file is modified in any way without a corresponding signature update, the boot loader authentication will fail. Upon failure the firmware displays a dialog box with one of the following error messages:

On notebooks:	"Selected boot image did not authenticate."
On desktops/workstations:	"Secure Boot Violation. Invalid signature detected. Check Secure Boot Policy in Setup."

The dialog box requires acknowledgment, and once it is given, the system is shut down.

The BIOS Signing Key

The Windows 8 requirement "System.Fundamentals.Firmware. UEFI Secure Boot" makes it mandatory to sign all firmware components using RSA-2048 with SHA-256. This is the default policy for acceptable signature algorithms.[2]

TPM and measured boot

For systems with the Trusted Platform Module (TPM) hardware chip, Windows 8 will perform a comprehensive chain of measurements, called measured boot, during the boot process. These measurements can be used to authenticate the boot process to ensure that the operating system is not compromised by root kits and other malware. Each component is measured from firmware up through the boot start drivers. These measurements are stored in the TPM on the machine. This log is then available remotely so that the boot state of the client can be verified.

Windows 8 BitLocker Platform Configuration Register (PCR) Sealing

- The Windows 8 hardware certification requirements require native UEFI boot.
- On a native UEFI boot system BitLocker will seal by default to the PCRs [0,2,4,11].
- On Connected Standby systems, BitLocker will seal to PCRs [7,11].

Note

Conflicting Connected Standby System requirements: The WHQL demands Connected Standby systems are required to implement measurements of Secure Boot policy information into PCR [7]. The TCG requires Secure Boot policy information in PCR [6]. To reference the PCR measurement numbers, refer to Table A1 in the Appendix of this paper.

Physical presence

The TCG PPI spec 1.2 includes a new NoPPIProvision flag, with a recommended BIOS default of True. The preinstall team should set this flag to True for Windows 8 and newer OSs and set it to "False" for any other OSs. When NoPPIProvision is True and there is no TPM owner, the BIOS will not prompt for physical presence when the first Enable/Activate command is received.

When the NoPPIProvision flag is False the BIOS will prompt for physical presence.

The default for NoPPIProvision Flag

The required default for the NoPPIProvision flag is True for Windows 8. This default allows Windows 8 to take ownership of the TPM without any user confirmation.

Special China requirement with Windows 8

For China, the legal requirement is that the TPM must be shipped in a disabled state and can only be enabled with the user's physical presence.

For a physical presence prompt, if the TPM presence is enabled, the BIOS will display the message below. Otherwise, the physical presence prompt will be the normal (F1, F2) message.

惠普特别提醒：在您在系统中启用TPM功能前， 请您务必确认，您将要对TPM的使用遵守相关的当地法律、

[2] A section of the Windows Hardware Certification Kit (WHCK, formerly called the Windows Logo Kit) http://msdn.microsoft.com/en-us/windows/hardware/gg487530.aspx

法规及政策，并已获得所需的一切事先批准及许可（如适用）。若因您未获得相应的操作/使用许可而发生的

合规问题，皆由您自行承担全部责任，与惠普无涉。

确认启用TPM, 按 “+”。取消， 按 “-“.

NoPPIProvision Flag in F10
The default for the NoPPIProvision flag is based on the factory setting.

TPM auto-provisioning
Windows 8 will automatically take TPM ownership to ease the deployment scenario. On an out of box setup, the OS will automatically prepare the TPM for use. It does this by making use of the new PPI flag dUEFIned in the “PPI v1.2 PC client Specific TPM interface” spec. The default scenario for first OS start is ”TPM is not ready for use” and the NoPPIProvision flag is set to True (the user will not be prompted for TPM provisioning). At this point TPM’s state is “Disabled”, “Deactivated,” and “Not Owned.” The OS will then issue the TPM command 10 and after the first boot cycle the TPM will be “Enabled and Activated.” Finally, after the second OS start, the TPM will be “Owned” and Windows will report that the TPM is ready for use. If users choose not to employ this TPM auto-provisioning option, they can use the Windows Wizard to manually provision the TPM.

POST

POST includes these tools and information:

- Drivers and firmware versions of installed software
- Information about disk drives directly attached to the chipset (not to a Smart Array Controller)

POST initializes the display in its native resolution. The logo requirements are as follows:

- Logo design:
  - Centered horizontally
  - 38.2% from top of screen
- Logo size:
  - ≤ 40% of screen height
  - ≤ 40% of screen width

POST time (for notebooks)
In order to minimize POST time, USB Initialization is bypassed on the default boot path. Fast boot initializes the internal HDD only to achieve the required boot time.

POST time (for desktops and workstations)
USB initialization is not bypassed on desktops and workstations since these systems frequently have USB keyboards and USB pointing devices.

Windows 8 Hybrid Boot and flash

By default, Hybrid Boot is enabled for Windows 8 shutdown. It is the hibernation without user data. Thus at the next boot, the OS does a resume from S4 instead of the cold boot. However, when BIOS changes certain system configurations, either via flash or some setting change during POST, a full restart is required for the OS to pick up the changes. In such cases, the BIOS must inform the OS to do a full boot using the ACPI specification.

The Firmware ACPI Control Structure (FACS) table (from the ACPI specification),contains a four-byte field at offset 8 called “Hardware Signature” with the following description:

The value of the system’s “hardware signature” at last boot is calculated by the BIOS on a best effort basis to indicate the base hardware configuration of the system such that different base hardware configurations can have different hardware signature values. OS-directed Power Management (OSPM) uses this information in waking from an S4 state, by comparing the current hardware signature to the signature values saved in the nonvolatile sleep image. If the values are not the same, OSPM assumes that the saved non-volatile image is from a different hardware configuration and cannot be restored.”

BitLocker

Systems which support TPM and wired LAN networking must support the UEFI_DHCP4_protocol, the UEFI_DHCP4_SERVICE_BINDING_PROTOCOL, the UEFI_DHCP6_protocol, and the UEFI_DHCP6_SERVICE_BINDING_PROTOCOL for wired LAN as defined in UEFI 2.3.1.

At pre-boot, BitLocker must be able to discover its Network Unlock provider on a Windows Deployment Server (WDS) via DHCP, and unlock the OS volume after retrieving information from WDS.

Boot order

In UEFI design, the Boot Order variable contains an array of UINT16's that makes up an ordered list of the Boot*XXXX* variables (each defining one boot option). The first element in the array is the value for the first logical boot option, the second element is the value for the second logical boot option, etc. The Boot Order list is used by the firmware's boot manager as the default boot order. Both the OS and the BIOS can add/remove Boot numbers. This is different than the boot options provided in the legacy F10 boot order menu.

Boot Order for notebooks

On notebooks, HP suggests that the user create two separate Boot Orders in the BIOS:

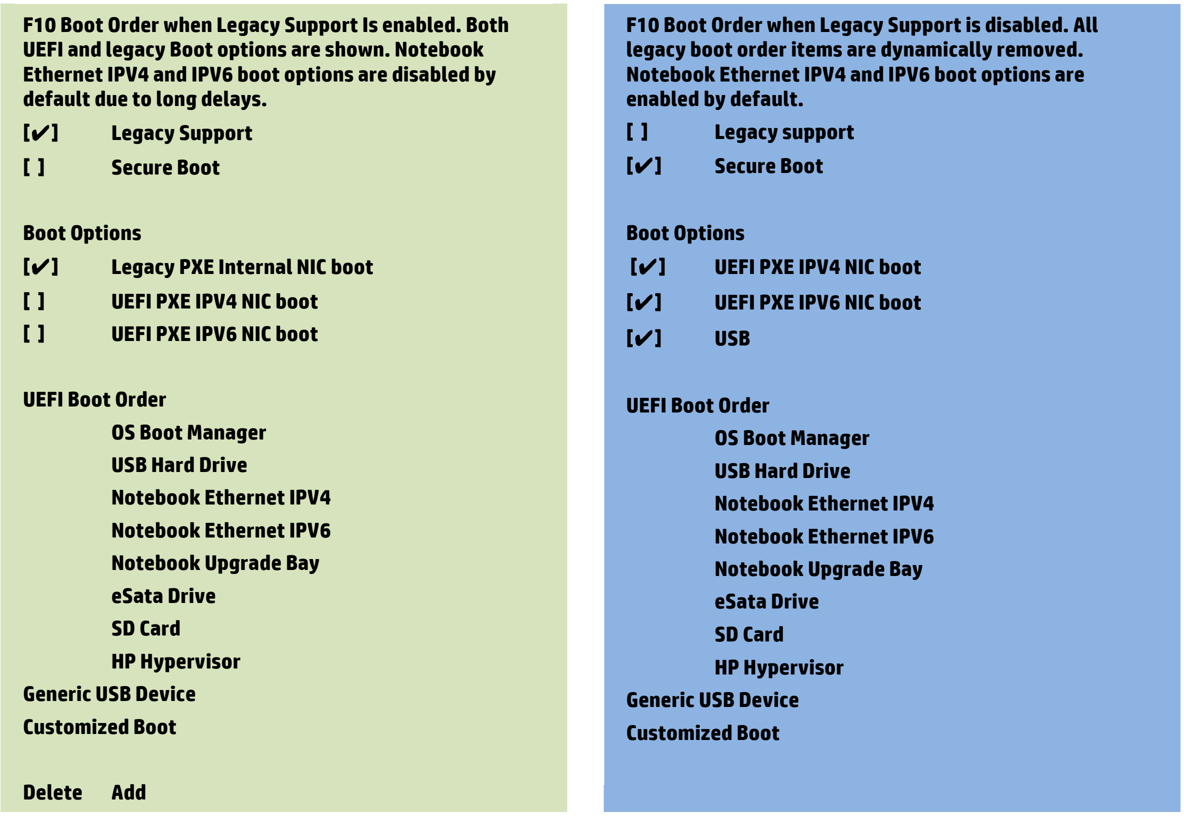
- The legacy Boot Order, as it exists when Legacy Support is enabled.
- A UEFI Boot Order list when Legacy Support is disabled.

For the UEFI F10 Static Boot Order, the BIOS assigns certain Boot numbers for the fixed devices in the system. For example, Boot 0000 can be OS Boot Manager for a hard drive, Boot0001 can be PXE IPV4, and Boot0002 can be for a built-in DVD. Certain HP-supported UEFI apps should also be listed, such as HP UEFI diagnostics. Windows 8 will add Boot numbers for "Windows Boot Manager," for the hard drive, and "Windows to go" for the USB disk.

When Legacy Support is disabled, the BIOS is in native UEFI mode and POST time is critical. If the generic USB device or USB hard drive is not listed first in the Boot Order and the next boot is not set to "USB Hard Drive" or "generic USB device" by the OS, the BIOS will not enumerate USB. Thus any removable USB devices attached to the system will not be enumerated and Boot Order will not show the detailed USB device information. The only entry will be the generic USB device, and there be no external USB optical drive or external USB disk devices in the F10 Boot Order.

When no button is pressed during POST, the BIOS will pass this static Boot Order list to the OS. In turn, the OS will display it in its Advanced Options.

Figure 9. F10 Boot Order when Legacy Support is enabled and disabled (notebooks)



F10 Boot Order when Legacy Support Is enabled. Both UEFI and legacy Boot options are shown. Notebook Ethernet IPV4 and IPV6 boot options are disabled by default due to long delays.

[✔] Legacy Support

[ ] Secure Boot

Boot Options

[✔] Legacy PXE Internal NIC boot

[ ] UEFI PXE IPV4 NIC boot

[ ] UEFI PXE IPV6 NIC boot

UEFI Boot Order

OS Boot Manager
USB Hard Drive
Notebook Ethernet IPV4
Notebook Ethernet IPV6
Notebook Upgrade Bay
eSata Drive
SD Card
HP Hypervisor

Generic USB Device

Customized Boot

Delete Add

F10 Boot Order when Legacy Support is disabled. All legacy boot order items are dynamically removed. Notebook Ethernet IPV4 and IPV6 boot options are enabled by default.

[ ] Legacy support

[✔] Secure Boot

Boot Options

[✔] UEFI PXE IPV4 NIC boot

[✔] UEFI PXE IPV6 NIC boot

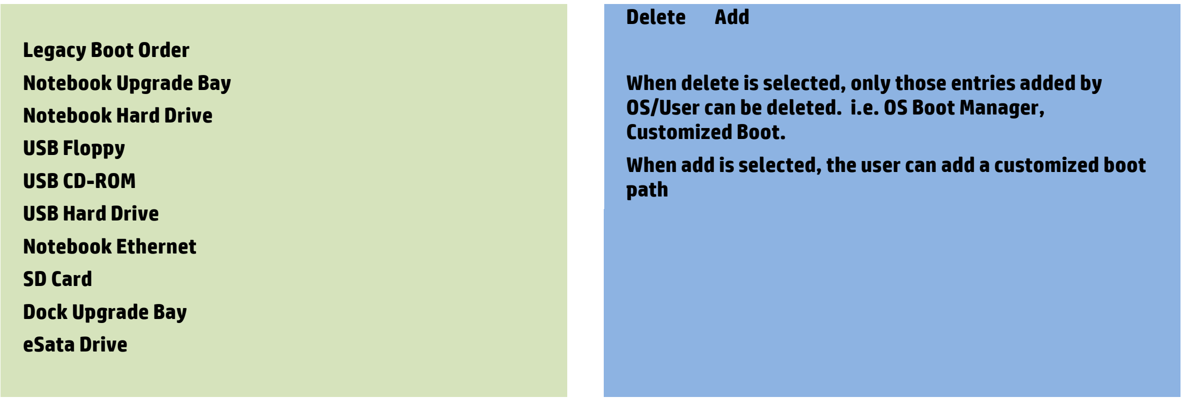
[✔] USB

UEFI Boot Order

OS Boot Manager
USB Hard Drive
Notebook Ethernet IPV4
Notebook Ethernet IPV6
Notebook Upgrade Bay
eSata Drive
SD Card
HP Hypervisor

Generic USB Device

Customized Boot



Legacy Boot Order
Notebook Upgrade Bay
Notebook Hard Drive
USB Floppy
USB CD-ROM
USB Hard Drive
Notebook Ethernet
SD Card
Dock Upgrade Bay
eSata Drive

Delete Add

When delete is selected, only those entries added by OS/User can be deleted. i.e. OS Boot Manager, Customized Boot.

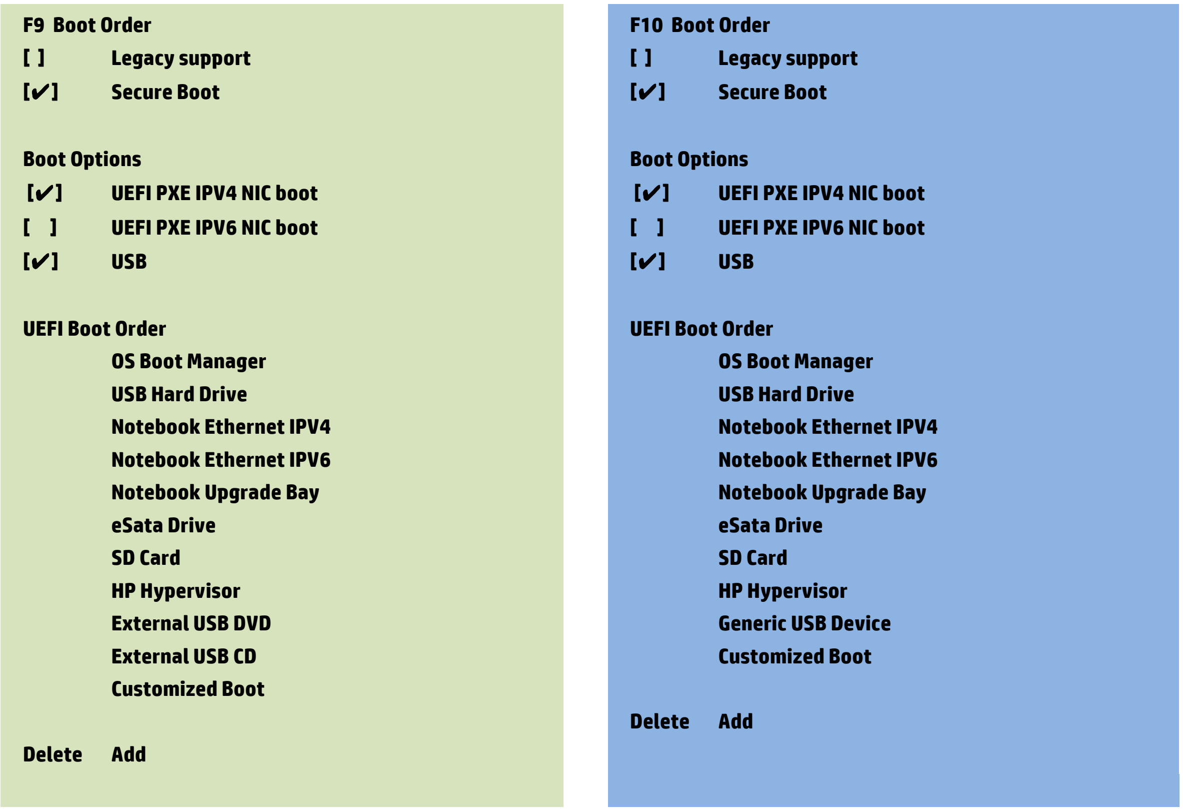
When add is selected, the user can add a customized boot path

Windows Vista, Windows 7, and some Linux systems don't support UEFI Secure Boot. For these systems, enable Legacy Support and disable Secure Boot. With Secure Boot disabled and Legacy Support enabled, note that both UEFI and legacy boot sources are available for boot. This configuration allows for the most flexibility in booting from various devices, but at the cost of not having Secure Boot.

The BIOS will base the boot sequence from the boot order list. If the first device on the boot order list is not bootable, then BIOS will try the next device. The user can permanently change the boot order by changing the F10 Boot Order. For a one-time boot order change, the user can use the Windows 8 interface to set Next Boot to a certain device. This will only be effective at the next boot.

If the user presses F9 during POST, the BIOS will now enumerate all USB devices attached to the system and display a dynamic F9 Boot Order list. For example, if there is one USB DVD and one USB hard disk attached to the platform and the user disables the UEFI PXE IPV6 NIC boot, the static F10 Boot Order and the dynamic F9 Boot Order will be different. Also the BIOS will pass the F9 Boot Order to the OS in such a case.

Figure 10. The dynamic F9 Boot Order and the static F10 Boot Order.



F9 Boot Order
[ ] Legacy support
[✔] Secure Boot

Boot Options
[✔] UEFI PXE IPV4 NIC boot
[ ] UEFI PXE IPV6 NIC boot
[✔] USB

UEFI Boot Order
OS Boot Manager
USB Hard Drive
Notebook Ethernet IPV4
Notebook Ethernet IPV6
Notebook Upgrade Bay
eSata Drive
SD Card
HP Hypervisor
External USB DVD
External USB CD
Customized Boot

Delete Add

F10 Boot Order
[ ] Legacy support
[✔] Secure Boot

Boot Options
[✔] UEFI PXE IPV4 NIC boot
[ ] UEFI PXE IPV6 NIC boot
[✔] USB

UEFI Boot Order
OS Boot Manager
USB Hard Drive
Notebook Ethernet IPV4
Notebook Ethernet IPV6
Notebook Upgrade Bay
eSata Drive
SD Card
HP Hypervisor
Generic USB Device
Customized Boot

Delete Add

Boot order for desktops and workstations

On desktops and workstations, the Boot Order menu displays all of the available boot sources in a categorized hierarchy. Each available boot source is presented (as shown below in Figure 11) for one of two primary categories: UEFI Boot Sources or Legacy Boot Sources. Additionally, the Legacy Boot Sources category has a "Hard Drive" sub-category that lists the connection point for each physically-attached, hard-drive-like device. The user may move an entry up or down within any category or sub-category by positioning the cursor next to the desired entry, pressing the ENTER key to select it, using the up and down arrows to reposition the selected entry, and pressing the ENTER key again to accept the new order. The user may also disable any device or category heading in the boot order by using the up and down cursor keys to select the desired entry and pressing the F5 key to change the entry's state. When disabled, boot order entries are shown in grey, and the text " : Disabled" is appended to the entry's descriptive string.

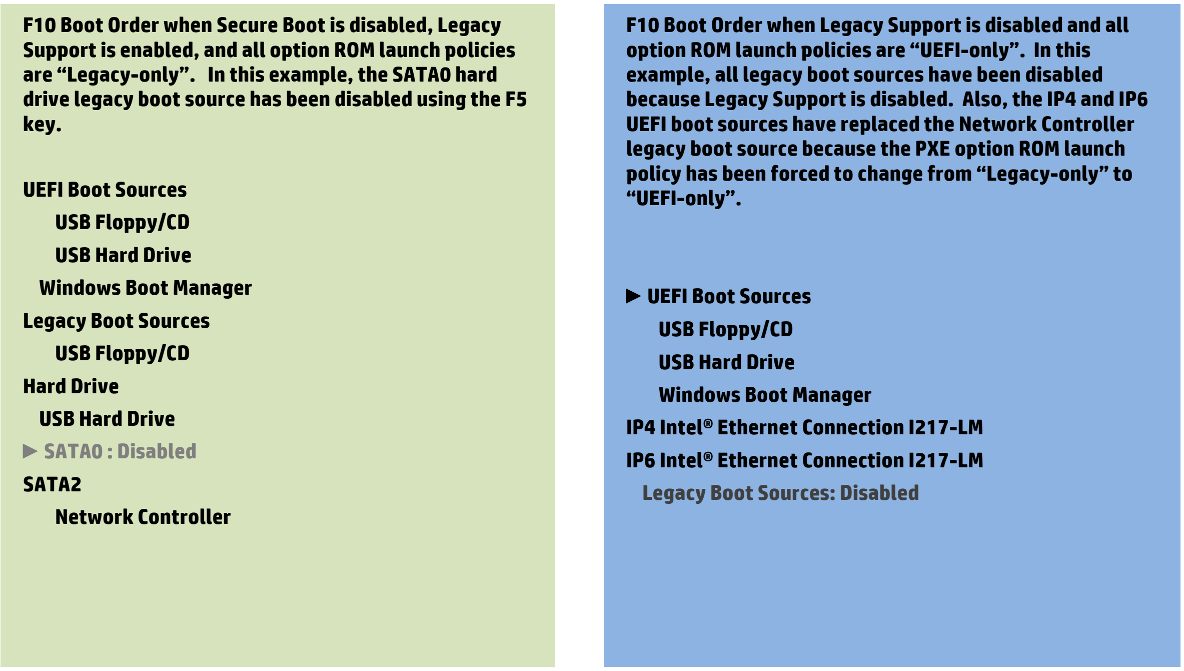
The content of the Boot Order menu can be affected by several other F10 settings.

Legacy Support is automatically disabled when Secure Boot is enabled.

When Legacy Support is disabled in the Secure Boot Configuration Menu, the Legacy Boot Sources category in the Boot Order menu is automatically disabled. Similarly, the Legacy Boot Sources category is automatically enabled when Legacy Support is changed from disabled to enabled.

The Option ROM Launch Policy menu allows the user to control whether only legacy option ROMs, only UEFI option ROMs, or no option ROMs are to control video, mass storage, or network controllers that are detected in the system. The option ROM launch policy for a given controller dictates whether its associated boot sources are shown in the Boot Order menu under UEFI Boot Sources, Legacy Boot Sources, or neither category. Note that all "Legacy-only" option ROM launch policies are automatically switched to "UEFI-only" when Legacy Support is disabled. Likewise, all "UEFI-only" option ROM launch policies are automatically switched to "Legacy-only" when Legacy Support is enabled.

Figure 11. F10 Boot Order when Legacy Support is enabled and disabled (desktops and workstations)



F10 Boot Order when Secure Boot is disabled, Legacy Support is enabled, and all option ROM launch policies are "Legacy-only". In this example, the SATA0 hard drive legacy boot source has been disabled using the F5 key.

UEFI Boot Sources
USB Floppy/CD
USB Hard Drive
Windows Boot Manager
Legacy Boot Sources
USB Floppy/CD
Hard Drive
USB Hard Drive
▶ SATA0 : Disabled
SATA2
Network Controller

F10 Boot Order when Legacy Support is disabled and all option ROM launch policies are "UEFI-only". In this example, all legacy boot sources have been disabled because Legacy Support is disabled. Also, the IP4 and IP6 UEFI boot sources have replaced the Network Controller legacy boot source because the PXE option ROM launch policy has been forced to change from "Legacy-only" to "UEFI-only".

▶ UEFI Boot Sources
USB Floppy/CD
USB Hard Drive
Windows Boot Manager
IP4 Intel® Ethernet Connection I217-LM
IP6 Intel® Ethernet Connection I217-LM
Legacy Boot Sources: Disabled

Windows Vista, Windows 7, and some Linux systems don't support UEFI Secure Boot. For these systems, enable Legacy Support and disable Secure Boot. With Secure Boot disabled and Legacy Support enabled, note that both UEFI and legacy boot sources are available for boot. This configuration allows for the most flexibility in booting from various devices, but at the cost of not having Secure Boot.

The BIOS will base the boot sequence from the boot order list. If the first device on the boot order list is not bootable, then BIOS will try the next device. The user can permanently change the boot order by changing the F10 Boot Order. For a one-time boot order change, the user can use the Windows 8 interface to set Next Boot to a certain device. This will only be effective at the next boot.

OA3

Windows 8 features a new version of the OEM activation mechanism, the OEM Activation 3.0 (OA 3.0). This is supported by all HP business PCs certified for Windows 8. If a customer orders an HP business PC with Windows 8, the unit is shipped with Windows 8 pre-activated—the customer does not need to activate the operating system.

Microsoft Digital Marker Key injection

A standard HP method to inject the Microsoft Digital Marker (MSDM) key into ACPI will be supported by the BIOS for use by the factory and service using the HP BIOS Configuration interface available in both Windows (Public WMI) and UEFI. The following processes are supported by the implementation.

BIOS functionality

The following functionality is provided by the BIOS to manage the OA3 key:

- Reading the key:
  - The key can always be read from WMI or UEFI under "MS Digital Marker."
  - Reading the key always returns the last key value accepted by the BIOS.
  - After a full BIOS reflash, the MS Digital Marker property will not be present in the BIOS, and the ACPI MSDM table will be cleared.
- Writing a key:
  - Writing the key from WMI using "MS Digital Marker" requires a blank key slot, or that the key is first unlocked by using Physical Presence Check or by a complete BIOS flash.
  - After a key is written, a reboot is always required to set the key in the MSDM ACPI table.
  - Writing the key with all FFhs clears the MSDM Table in ACPI (See "Clearing the Key" below).
- Clearing the key:
  - A complete BIOS re-flash clears the key and the MSDM table in ACPI:
    - This method is used only in the factory environment.
    - Reading the key after the re-flash.
  - Writing the key with all FFhs clears the MSDM table in ACPI:
    - See "Writing the key" for Physical Presence Check requirements.
    - Reading the key after the write returns all FFhs.
    - A reboot is required in order to clear the MSDM ACPI table.
- SMC_RESET_PLATFORM_TO_FACTORY_DEFAULT - No other method is provided to clear the key. This includes:
  - Reset to Factory default through F10, WMI
  - SMC_RESET_BIOS_TO_FACTORY_DEFAULT_SAVE_IDENTITY
  - Standard BIOS updates

HP BIOS configuration (REPSET) functionality

The HP BIOS Configuration utility supports the following functions for Windows key insertion:

- English
- MS Digital Marker
- "Value"

The values are:

- Unlock – used to unlock the key for writing;
  - Requires reboot with Physical Presence Check
  - Not required in MPM mode or first write after re-flash
- Key – Text string representation of Windows key:
  - Write all FFhs to clear the key in the ACPI MSDM table.

Physical Presence Check

To prevent malicious software attacks, a Physical Presence Check must be performed to inject a "new" key or "clear" a key. During the next reboot after a new key is written to Public WMI, the following message will be displayed to the user:

> Microsoft Windows Product Activation Key Change
>
> A change to the Microsoft Windows Product Activation Key is pending. Please contact Hewlett-Packard support (www.hp.com/support) for instructions on how to complete the request. Otherwise press the "ESC" key to continue without any changes.
>
> Windows Product Activation Key (020)
>
> ESC – continue without changing
>
> For more information, please visit: www.hp.com/go/techcenter/startup

A Physical Presence Check is not required if the system is in Manufacturing Mode or if the key has not been set since it was last cleared by a complete BIOS re-flash.

Computrace

The Absolute Computrace Pre-boot module writes to the hard disk if it detects the needed hard drive components are no longer present. This provides persistent support and prevents the malicious deletion of files from the system. However, this method can impact OS stability. Pre-boot module support will fail when the OS partition or the hard drive is encrypted.

In Windows 8, a new method has been proposed. The Windows Platform Binary Table (WPBT) is a fixed Advanced Configuration and Power Interface (ACPI) table that enables boot firmware to provide Windows with a platform binary that the operating system can execute. The binary handoff medium is physical memory, allowing the boot firmware to provide the platform binary without modifying the Windows image on disk. In the initial version, the WPBT simply contains a physical address pointer to a flat, Portable Executable (PE) image that has been copied to physical memory.

If you are running Windows 7 or an older OS and the HDD is not encrypted, use the older method (changing the OS file).

If you are running Windows 8 and the HDD is encrypted, publish WPBT. For older OSs, the WPBT will be ignored.

For more details, refer to the WPBT published by Microsoft.

F10 Restore Default Behavior

are listed in Table 4.

Table 4.. F10 Restore default behavior

Tab	Option	Default restored?
File:		
	Update System BIOS	Yes
	Create a backup image of the System BIOS	Yes
Security:		
	Administrator Tools	
	System Management Command	Yes
	HP SpareKey	Yes
	Fingerprint Reset on Reboot	Yes
	User Tool	
	Intel®Anti Theft	No
	DriveLock password on restart	Yes
	TPM Device	No

	Embedded Security Device State	No
	TPM Reset to Factory Defaults	No
	Power-On Authentication Support	No
	Reset Authentication Credential	No
	OS Management of TPM	No
	Reset TPM from OS	No
	Utilities	
	Asset Tracking Number	No
	Ownership Tag	No
	Ownership Tag 2	No
System Configuration:		
	Language	No
	Boot Options	
	Startup Menu Delay	Yes
	Mutiboot Express Popup Delay	Yes
	Audio alerts during boot	Yes
	Custom Logo	NA
	Display Diagnostic URL	Yes
	Custom Help and URL message	Yes
	Require acknowledgment of battery errors	Yes
	Fast Boot	Yes
	CD-ROM boot	Yes
	SD card boot	Yes
	Floppy boot	Yes
	PXE Internal NIC boot	Yes
	USB device boot	Yes
	Upgrade Bay Hard Drive boot	Yes
	eSATA boot	Yes
	Boot Mode	No
	UEFI Boot Order	Yes
	Legacy Boot Order	Yes
	Device Configurations	
	USB Legacy support	Yes
	Parallel port mode	Yes

	Fan Always on while AC Power	Yes
	Data Execution Prevention	Yes
	Max SATA Speed	Yes
	SATA Device Mode	No
	Wake on USB	Yes
	Secondary Battery Fast Charge	Yes
	Virtualization Technology (VTx)	Yes
	Virtualization Technology for Directed I/O (VTd)	Yes
	Trusted Execution Technology (TXT)	Yes
	HP Hypervisor	Yes
	Multi Core CPU	N/A
	Intel HT Technology	N/A
	NumLock on at boot	Yes
	Express Card Link Speed	Yes
	Power on unit when AC is detected	Yes
	Deep Sleep	Yes
	Built-In Device Options	
	Wireless Button State	Yes
	Embedded WLAN Device	Yes
	Embedded Bluetooth Device	Yes
	Embedded LAN Controller	Yes
	LAN/WLAN Switching	Yes
	Wake On LAN	Yes
	Wake on LAN on DC mode	Yes
	Notebook Upgrade Bay	Yes
	Power Monitor Circuit	Yes
	Audio Device	Yes
	Microphone	Yes
	Speakers and Headphones	Yes
	Wake unit from sleep when lid is opened	Yes
	Power on unit when lid opened	Yes
	Boost Converter	Yes
	Port Options	
	Serial Port	Yes

	Parallel Port	Yes
	Flash media reader	Yes
	USB Port	Yes
	1394 Port	Yes
	Express Card Slot	Yes
	eSATA Port	Yes
	AMT Options	
	USB Key Provisioning Support	Yes
	Unconfigure AMT on next boot	Yes
	SOL Terminal Emulation Mode	Yes
	Firmware Progress Event Support	Yes
	Initiate Intel CIRA	Yes
	BIOS Power-On	
	Sunday	Yes
	Monday	Yes
	Tuesday	Yes
	Wednesday	Yes
	Thursday	Yes
	Friday	Yes
	Saturday	Yes
	BIOS Power-On Time (hh:mm)	Yes

Appendix

General UEFI requirements

The BIOS incorporated in the HP business notebooks, desktops, and workstations supporting Windows 8 conforms to the following sections of the UEFI 2.3.1 Class 2 specification:

2.3, 3.1, 4.3, 6.1 ~ 6.5, 7.1~7.5, 8.1, 8.2, 9.1, 9.5, 11.2 ~ 11.4, 11.8, 11.9, 12.4, 12.7, 12.8, 12.9, 18.5, 21.1, 21.3, 21.5, 27.1~27.8.

PCR boot measurements for notebook products

Table A1 lists the PCR boot measurements for notebook products. Section references indicated in Table A1 refer to the UEFI 2.3.1 Class 2 specification document.

Table A1..PCR boot measurements for hp business notebook products

PCR	Expected measurement	Actual measurement
PCR 0	S-CRTM's version identifier using the event type EV_S_CRTM_VERSION All Host Platform firmware using the event type EV_POST_CODE ACPI data using event type EV_UEFI_HANDOFF_TABLES	S-CRTM's version identifier using the event type EV_S_CRTM_VERSION All Host Platform firmware using the event type EV_POST_CODE
PCR 1	Not used	
PCR 2 Non-manufacturer controlled options/UEFI drivers	Not used	Currently measuring FV(??)
PCR 3	Not used	
PCR 4	If the BIOS is configured or designed to not record each device the BIOS attempts to boot, an EV_OMIT_BOOT_DEVICE_EVENTS event MUST be measured once. See Section 11.3.1 (Event Types). The BIOS MUST record the EV_ACTION event "Calling INT 19h" or the EV_UEFI_ACTION event "Calling UEFI Application from Boot Option." See Section 11.3.3 (EV_ACTION Event Types).	The BIOS MUST record the EV_ACTION event "Calling INT 19h" or the EV_UEFI_ACTION event "Calling UEFI Application from Boot Option." See Section 11.3.3 (EV_ACTION Event Types).
PCR 5	Not used	Calling UEFI application event, GPT
PCR 6	Not used (UEFI Secure Boot data in spec but MS indicates that they want that in PCR 7)	Secure Boot variables
PCR 7	Not used	

For more information

Visit the websites listed below if you need additional information.

Resource description	Web address
UEFI Specification Version 2.3.1	http://www.UEFI.org/specs/download
Windows Compatibility Support Module Opt-Out Mechanism for Legacy Free OSs v1.1 by Microsoft Windows Authenticated Portable Executable Signature Format specification	http://msdn.microsoft.com/en-us/windows/hardware/gg463180
PC Client Work Group Platform Reset Attack Mitigation Specification, Version 1.0	http://www.trustedcomputinggroup.org/resources/pc_client_work_group_platform_reset_attack_mitigation_specification_version_10
TCG UEFI Protocol Version 1.20, Revision 1.0	http://www.trustedcomputinggroup.org/resources/tcg_UEFI_protocol_version_120_revision_10
PC Client Work Group Specific Implementation Specification for Conventional Bios Specification, Version 1.2	http://www.trustedcomputinggroup.org/resources/pc_client_work_group_specific_implementation_specification_for_conventional_bios_specification_version_12
Microsoft Security Development Lifecycle	http://www.microsoft.com/security/sdl/default.aspx

Sign up for updates
hp.com/go/getupdated

Share with colleagues

★ Rate this document

708355-002, created January 2013, revised July 2013