HP Commercial Systems Automatic BIOS Update Through Windows Update Whitepaper

Version 0.4.92 - 10/21/2021

Update *(Previous Version 0.4.8 – May 3, 2021) - The process for releasing firmware or BIOS updates through Microsoft WU has re-started. In early July, HP has released BIOS updates through WU through the Windows Insider Program to select 400 and 600 series notebooks and desktops to validate the process and ensure successful updates. Additional platforms will be added for validation and test through September through the end of the year - with a target of January 2022, for all platforms to be eligible for Automatic BIOS update through Windows Update (WU)*

***

Introduction

The purpose of this paper is to detail changes to HP's process for releasing system firmware to Microsoft Windows Update ('WU'). This paper will provide details on the upcoming change, the benefits of this new policy, as well as methods an IT Administrator can take to block these updates if desired.

HP Platforms Covered in This Document

The platform list within this document (below) indicates HP's initial list of PCs eligible to update firmware through Microsoft Windows Update. New platforms released after the creation-date of this paper will be made eligible for firmware updates via Microsoft Windows Update.

	BU	Series	BIOS Family	Marketing Name	BIOS version
2021	NB	400	T78	HP ProBook 455 G8 Notebook PC HP ProBook 445 G8 Notebook PC	01.06.00
2020	DT	405	S25	HP ProDesk 405 G6 DM	02.03.00
2020	DT	400	S08	HP ProDesk 400 G7 Small Form Factor PC	02.06.02
2021	NB	400	T70	HP ProBook 430 G8 Notebook PC HP ProBook 440 G8 Notebook PC HP ProBook 450 G8 Notebook PC	01.06.03

2020	DT	600	S12	HP ProOne 600 G6 AiO HP ProOne 400 G6 AiO HP ProOne 440 G6 AiO	02.08.01
2020	DT	400	S05/S15	HP ProDesk 405 G6 SFF	02.05.01
2020	NB	800	S74	HP EliteBook x360 830 G7 Notebook PC	01.06.00
2020	NB	800	S77	HP EliteBook 855 G7 Notebook PC HP EliteBook 845 G7 Notebook PC HP EliteBook 835 G7 Notebook PC	01.06.01
2020	NB	400	S79	HP ProBook 445 G7 Notebook PC HP ProBook 455 G7 Notebook PC	01.06.00
2020	NB	EDU	S95	HP ProBook x360 11 G6 Education Edition	01.07.02
2020	NB	400	S71	HP ProBook 430 G7 Notebook PC HP ProBook 440 G7 Notebook PC HP ProBook 450 G7 Notebook PC	01.10.00
2020	NB	600	S83	HP ProBook 640 G7 Notebook PC HP ProBook 650 G7 Notebook PC	01.06.00
2020	DT	800	S21	HP EliteDesk 800 G6 DM	02.08.01

Why is HP Releasing BIOS Updates as Automatic via Windows Update?

Modern devices depend on up-to-date firmware for performance and security. Updating a system BIOS can be challenging, particularly as remote work is proliferating and leveraging Windows Update for BIOS updates simplifies the process. The additional advantage of servicing BIOS via Windows Update is security vulnerabilities which require a BIOS update can be remediated in a quick, efficient, and automatic manner. HP believes this change is in the best interest of our customers and will increase adoption of updated system firmware without undue end-user friction.

How is BIOS Updated Through Windows Update?

To update system firmware Windows Update leverages a mechanism built into the Unified Extensible Firmware Interface (UEFI) standard called UEFI Capsule.

What is a UEFI Capsule?

The UEFI capsule is the mechanism by which the firmware being updated is transferred from the operating system to the UEFI BIOS. Along with the firmware image and code to perform the update securely, the

capsule contains a header used to identify device and content. It is delivered by device vendors to Windows systems via Microsoft Windows Update service or Linux® systems via Linux Vendor Firmware Service (LVFS). With UEFI capsule, firmware updates behave the same way as software/driver updates at the OS level, but the updates occur in the UEFI environment on the next reboot.

Does HP Already Submit BIOS to Windows Update?

Yes. HP posts every BIOS update release so that it is available as a manual/optional update via WU.

Manual Updates via Windows Update

- Microsoft will not push the manual/optional BIOS capsule package. To install, a customer needs to search for the System Firmware update from ***Device manager -> Firmware > System Firmware*** on the client system.

What is changing?

With the new capabilities of Windows Update - with respect to firmware update - and the increasing importance of firmware updates to the security posture of the system, HP will begin submitting updates to Windows Update that are marked to be Automatic Updates when the following criteria are met.

  - Fix high priority security issues
  - Fix critical customer and functional issues

Automatic Updates via Windows Update Criteria

- Microsoft will push the BIOS capsule package to client systems and perform the update without any user interaction. The customer doesn't need to do anything additional to apply the update.

Which OS Versions are targeted?

- HP targets Windows Update with Windows 10, Version v1809(RS5) and later OS versions.

Quality Assurance via Windows Update

When updates are submitted to Windows Update, they are deployed using a flighting process to ensure the install process is a high-quality experience. This flighting Process works as follows:

- HP submits the Windows Update (WU) package with Windows update designated as updates for high priority security issues or, updates for critical customer and functional issues.
- Microsoft will run the insider flighting for two weeks after Microsoft approval.
- During flighting period both Microsoft and HP will monitor the Firmware Telemetry reporting through insider adoption process. The insider flighting will stop if problems are detected.
- When flighting process is successfully completed, Microsoft will start the gradual rollout
- Starting to push BIOS capsule package to general population. Microsoft will continue monitoring the data telemetry this time and the roll out will stop if problems are detected.

When this new update process will start

HP plans to start Windows Update Automatic submission for BIOS in **January 2021**.

Potential Issues an IT Administrator Needs to Consider

BitLocker Recovery Key

If using any Bitlocker policies other than the Windows 10 defaults and BIOS updates via Windows Update are desired, it is recommended that customers consult with Microsoft on the likelihood of these updates triggering a Bitlocker Recovery key request. HP Strongly recommends that all customers or IT Administrators know how to find a Bit locker recovery key. It is also recommended that some systems be placed on the insider ring so that they will receive early access to these updates for test.

EFI Partition Size Requirements

When a capsule update is done, the OS copies the capsule to the EFI partition on the disk. If this partition does not exist or has become full, the update may not occur.

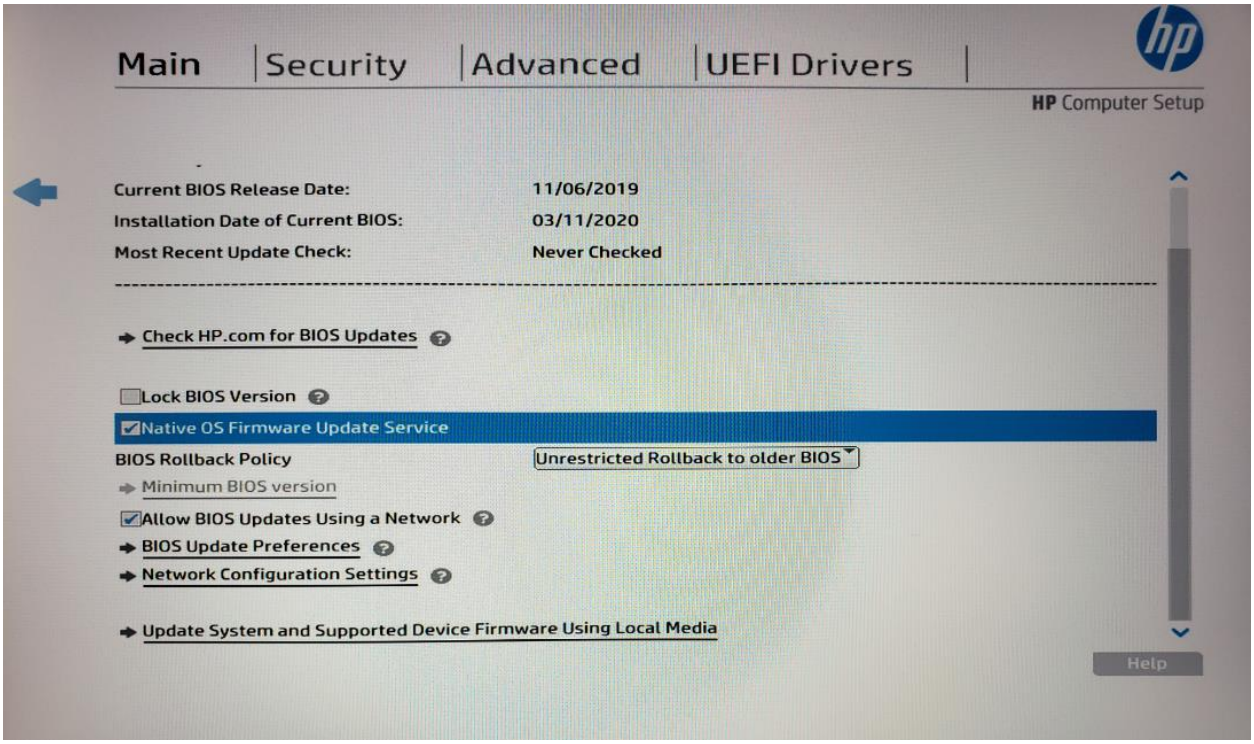
Details on the EFI partition can be found here: https://support.hp.com/us-en/document/c06466416

Blocking Windows Update BIOS Updates with BIOS Settings

Native OS Firmware Update Service

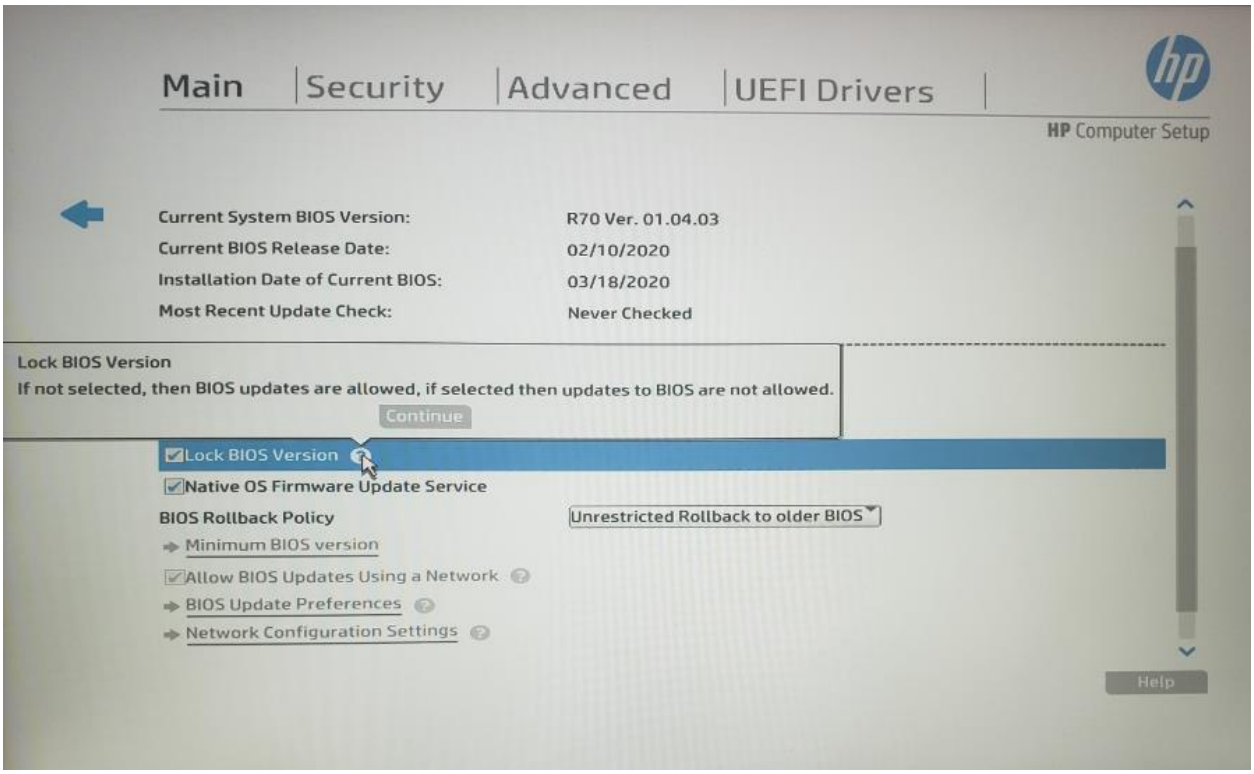
The setting titled "Native OS Firmware Update Service" is the primary mechanism to enable or disable the UEFI Capsule BIOS update on an HP client. The default value for this setting is "Enable." When enabled the HP BIOS will accept updates from UEFI Capsule via Windows Update. To block the update from Windows Update set this setting to "Disable."

If your environment requires you to qualify each BIOS release before broad roll out, this is option will block any update that might be done by WU but it will allow you to manually perform the update after a BIOS release has been qualified.



Bios Version Lock

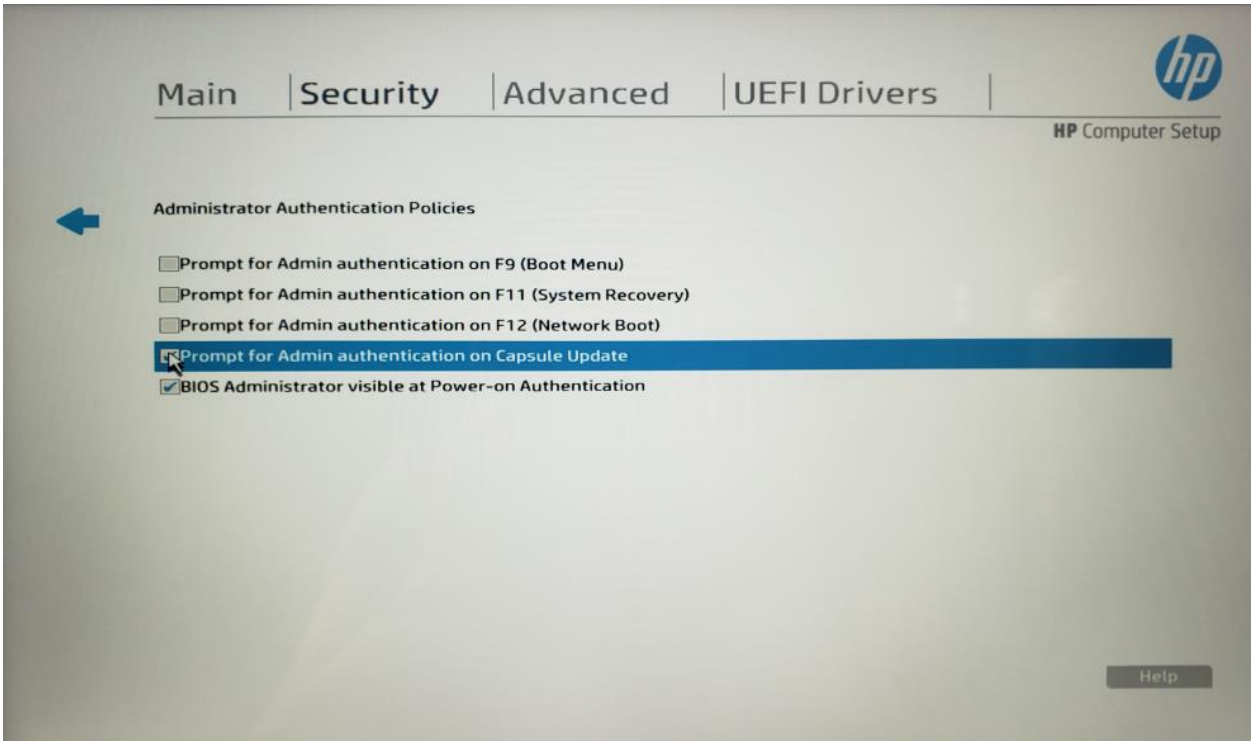
When enabled the "Lock BIOS Version" setting below will block **all** BIOS updates no matter the mechanism used (e.g., via WU or SoftPaq). Enabling this option will automatically disable the "Native OS Firmware Update Service" so WU doesn't download and attempt BIOS updates only to have them denied.



Prompt for Admin Authentication on Capsule Update

The settings titled “Prompt for Admin authentication on Capsule Update” controls the password requirement for use with BIOS updates via UEFI Capsule. The default value is “Disable,” which does not require a password for this flash mechanism.

When WU pushes an automatic update to the system and it reboots to perform the update, a prompt asking for admin authentication will be displayed. Until the credentials are entered, the system will not perform the update and unless the user reboots the machine it will wait indefinitely.



How to Manage BIOS Settings Related to UEFI Capsule Update

In all of the options below for modifying BIOS settings, if a BIOS password or Sure Admin is deployed to the client, authentication will be required to make these changes.

F10 BIOS Interface

The F10 Bios interface is accessed by pressing the F10 key at system start up.

HP Client Management Script Library

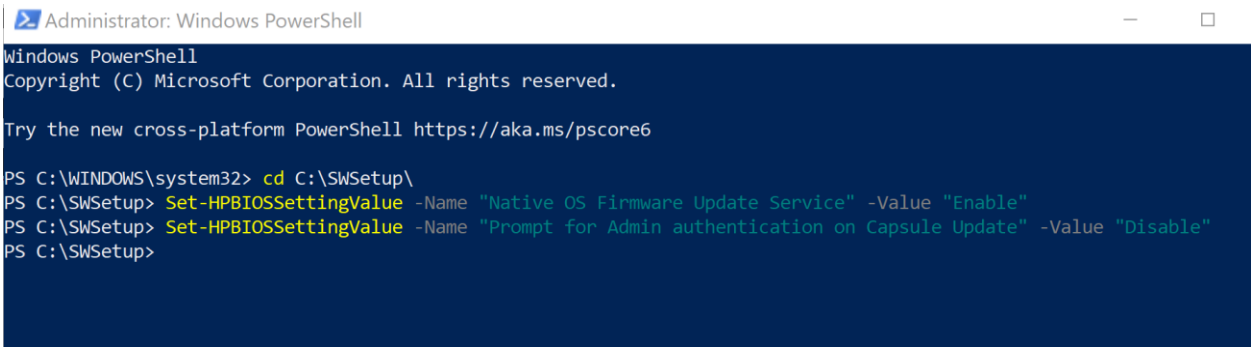
The HP Client Management Script Library is a set of PowerShell modules designed to make managing HP clients significantly easier for IT administrators. These modules can be installed from the PowerShell Gallery via install-module HPCMSL or via this download location. One of the modules deals with getting and settings BIOS settings. Documentation on this module can be found here.

Once installed, the Set-HPBIOSsettingvalue function can be used to set BIOS settings related to UEFI Capsule. The syntax for this function is Set-HPBIOSSettingValue -Name “Setting Name” -Value “Desired Value”

Examples:

Set-HPBIOSSettingValue -Name "Native OS Firmware Update Service" -Value "Enable"

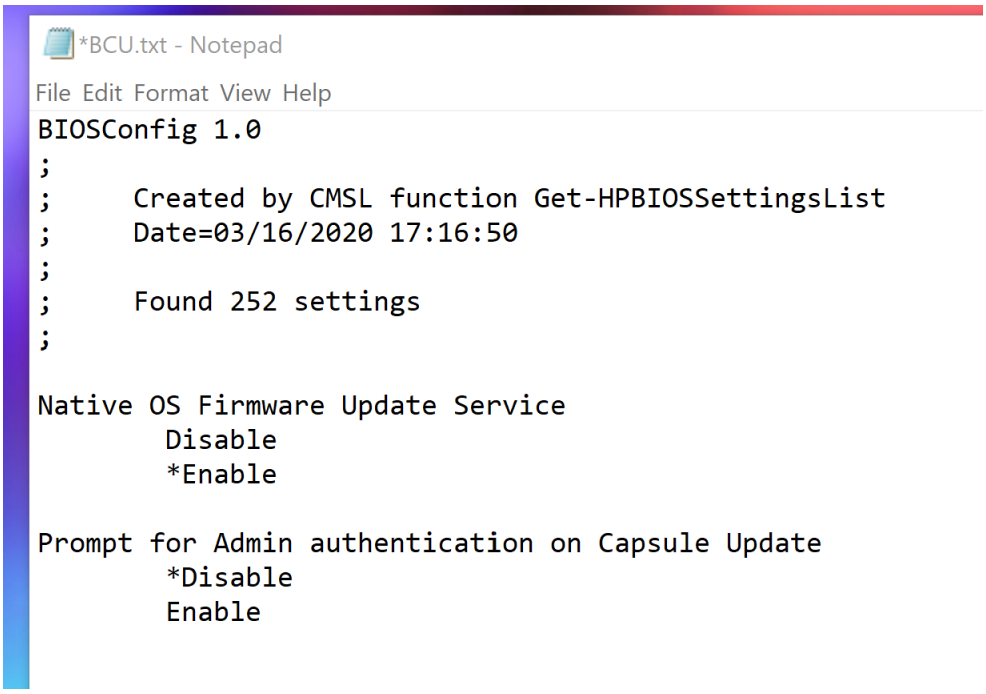
Set-HPBIOSSettingValue -Name "Prompt for Admin authentication on Capsule Update" -Value "Disable"



BIOS Configuration Utility

HP’s BIOS Configuration Utility (BCU) is a tool designed to deploy the BIOS settings found in a file to an HP System. BCU can be found here.

Screenshot of Sample BCU file shown below



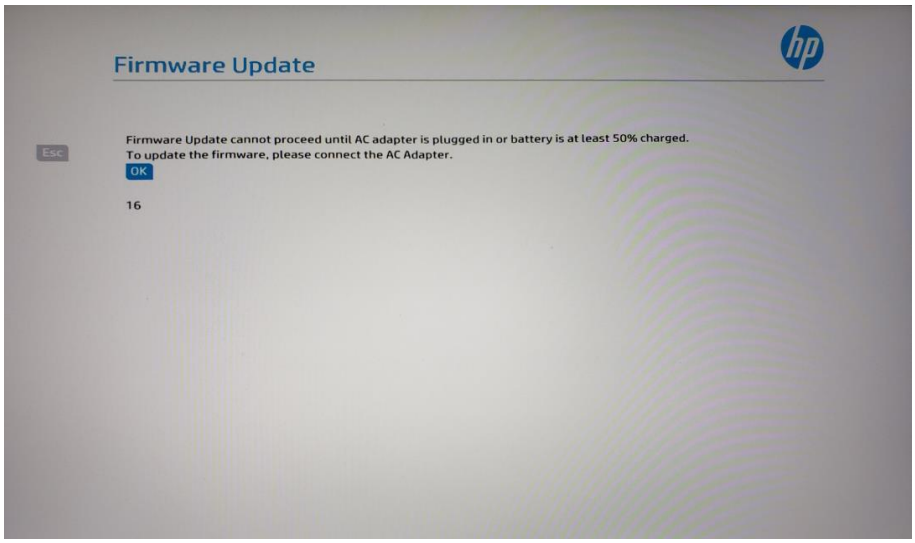
To deploy this file, after downloading and extracting BCU, open a command prompt and run

BIOSconfigutility64.exe /set:BCU.txt

FAQ

- What happens if my system is not plugged into AC when WU starts updating the BIOS?
  - Before the update starts, if AC-power is not plugged in and the remaining battery is below 50%, a message (prompting to charge the battery or connect to AC-power) will be displayed for up to 30 seconds. If an AC source is still not plugged in, the update will fail.
  - On the following boot, the system firmware device in device manager will indicate a problem by adding a yellow triangle with an exclamation point to the icon for the device (a 'yellow bang'). In the case of a manually triggered update, connect the AC adapter, and retry. In the case of an automatically triggered update, connect the AC adapter and retry.

    Example – system battery not sufficiently charged to complete a system update



    Example of a 'Yellow Bang' event in Device Manager

- What if the user locks the system to a specific BIOS version (blocks BIOS update from any method) vs. Native OS firmware update service (block firmware update from WU)?
  - If your environment requires you to qualify each BIOS release before broad roll out, it is recommended to set "Native OS firmware update service" to "Disable" so that automatic update

via WU will not occur. If you need to lock the HP BIOS to a specific version, the BIOS setting “Lock BIOS Version” should be set to “Enable” (see How to Manage BIOS Settings Related to UEFI Capsule Update for methods to do this). With some early version of BIOS, when “Lock BIOS Version” is enabled, Update via WU will still be attempted and fail. In that case, a yellow bang on system firmware device in device manager is expected.

- What are the contents of the Firmware?
  - BIOS is always released as part of system firmware. System firmware also includes EC/SIO, manageability engine and USB-C controller firmware. Device firmware may be released as part of System firmware. System firmware may include TBT (Thunderbolt) Firmware, Camera Firmware, Click pad Firmware.