Revision History
Q03 ROM Family

Models Supported: HP ProDesk 400/480 G5 Micro Tower Business PC

Version 2.16.00

ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine v12.0.81.1753 (Production)
SIO19 F/W 7.9.51
Intel VBIOS 9.2.1014 (2018/06/21)
Intel GOP 9.0.1075 (2018/04/13)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom Rtk:V2.66
Intel/Realtek UEFI PXE rom Rtk:V2.035
- Adds a feature "IPv6 during UEFI Boot" in F10 setup interface where user has ability to disable IPv6 during preboot phase.
- Enhancement to address security vulnerabilities CVE-2020-8703, CVE-2020-8704, CVE-2020-24506 and CVE-2020-24507.
- Enhancement to address security vulnerabilities CVE-2020-24512, CVE-2020-24511.

FIXES:
- Fixes an issue where Security Device Error message pop out after enable Power-on Password.
- Fixes an issue where the system cannot resume from S3 with both PCIE x16 graphic card and PS/2 devices installed.

PCR0(with TPM2.0 SHA256) =
BF4AA35E9AFAF796CD74C1043A6603CDB4772B7152AD262329D6AB6832522C4A

Version 2.15.00

ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.70.1652 (Production)
SIO19 F/W 7.9.51
Intel VBIOS 9.2.1014 (2018/06/21)
Intel GOP 9.0.1075 (2018/04/13)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom Rtk:V2.66
Intel/Realtek UEFI PXE rom Rtk:V2.035
- Update Intel Reference code to 7.0.74.20

FIXES:
- Fixes an issue where "After Power Loss" in BIOS setup lost function after s3 resume.

PCR0(with TPM2.0 SHA256) =
8F1A4BDB87538DC608467A675951EB655BCF3D37D5119264B6A424C62B7E4C86

Version 2.14.01

ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.70.1652 (Production)
SIO19 F/W 7.9.51
Intel VBIOS 9.2.1014 (2018/06/21)

Intel GOP 9.0.1075 (2018/04/13)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom Rtk:V2.66
Intel/Realtek UEFI PXE rom Rtk:V2.035
- Enhancement to address security vulnerabilities CVE-2020-8696, CVE-2020-8695, CVE-2020-8694, CVE-2020-8744, CVE-2020-8745, CVE-2020-8746, CVE-2020-8747, CVE-2020-8749, CVE-2020-8752, CVE-2020-8753, CVE-2020-8754, CVE-2020-8756, CVE-2020-8757, CVE-2020-8760, CVE-2020-8705, CVE-2020-12297, CVE-2020-12303, CVE-2020-12355, CVE-2020-12356.
- Critical Security Update.

FIXES:
- Fixes an issue where Secure Erase cannot be executed when Display Language is changed to non-English.
- Fixes an issue where system takes a long time to resume from sleep when Video Memory is changed to 512 MB.

PCR0(with TPM2.0 SHA256) =
9A6894BDE3A59B5A7C746077C6A821D4CD99E557F36495E35B00AEDE3C28DF35

Version 2.12.00
ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.68.1606 (Production)
SIO19 F/W 7.9.50
Intel VBIOS 9.2.1014 (2018/06/21)
Intel GOP 9.0.1075 (2018/04/13)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom Rtk:V2.66
Intel/Realtek UEFI PXE rom Rtk:V2.035
- Enhancement to address security vulnerabilities CVE-2020-0543, CVE-2020-0548, CVE-2020-0549, CVE-2020-8758, CVE-2020-8672.
- Adds a feature ""Wake on LAN Power-on Password Policy"" in F10 setup interface.
- Adds a feature ""Allow User to Modify Power-on Password"" in F10 setup interface.

FIXES:
- Fixes an issue where message of Physical Presence Interface display incomplete when change to Non-English language.
- Fixes an issue where system unexpected hang up when a EFI folder is created in Recovery partition.
- Fixes an issue where Physical Presence Interface cannot set to disable when change to non-English language in F10 setup interface.
- Fixes an issue where original boot entry is deleted while third party encryption software creates their own boot entry.
- Fixes an issue where Automatic DriveLock option is enabled and greyed out after the BIOS Administrator Password is removed.
- Fixes an issue where system does not boot to OS directly when choose ""Postpone this BIOS until the next Reboot"" option at scheduled BIOS update via F10 setup interface.

PCR0(with TPM2.0 SHA256) =
6C948838E60D5DC65B0D4E6AA5C31E3C41EA66183725AC913E61A1CDCACC932F

Version 2.11.01
ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.64.1551 (Production)
SIO19 F/W 7.9.50
Intel VBIOS 9.2.1014 (2018/06/21)
Intel GOP 9.0.1075 (2018/04/13)

USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom   Rtk:V2.66
Intel/Realtek UEFI PXE rom   Rtk:V2.035
- Enhancement to address security vulnerabilities CVE-2020-0528, CVE-2020-0529.
- Upgrade Intel Reference Code to 7.0.6E.40 for compatibility enhancement.
- Enhancement to address security vulnerabilities CVE-2020-0531, CVE-2020-0532, CVE-2020-0534, CVE-2020-0535, CVE-2020-0536, CVE-2020-0537, CVE-2020-0538, CVE-2020-0539, CVE-2020-0540, CVE-2020-0541, CVE-2020-0542.
- Adds Drivelock password feature support on OPAL SED NVMe SSD.

FIXES:
- Fixes an issue where system with some PCIe cards installed cannot boot to OS after upgrating BIOS.
- Fixes an issue where system displays "Enter current DriveLock Password" message when enabling Automatic Drivelock then restarting system several times.
- Fixes an issue where Automatic DriveLock option is enabled and greyed out after BIOS Administrator Password is removed.
- Fixes an issue where original boot entry is deleted while third party encryption software creates their own boot entry.
- Fixes an issue where system firmware is updated from recovery partition instead of EFI partition.
- Fixes an issue where hard drive still prompts DriveLock password after forcing the Master password to match BIOS Administrator Password.
- Fixes an issue where system cannot enable "Automatic Drivelock" after placing a hard drive into another system and disabling Automatic Drivelock by another system.
- Fixes an issue where system cannot enable "Automatic DriveLock" option for NVMe SSD after "create BIOS Administrator password" in F10.
- Fixes an issue where system does not prompt for Power on Authentication with BIOS Administrator and POST Power-On Password options when schedule update check is failed.

PCR0(with TPM2.0 SHA256) =
768A7D72EB3FAF926BF4EB7F2C35D553D24C946C120906A71A7DBDD7666795F6

Version 2.10.00
ENHANCEMENTS:
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.49.1534
SIO19 F/W   7.9.50
Intel VBIOS   9.2.1014 (2018/06/21)
Intel GOP   9.0.1075 (2018/04/13)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom   Rtk:V2.66
Intel/Realtek UEFI PXE rom   Rtk:V2.035

- Updates the CPU microcode for Intel processors to 0xCA.
- Updates Intel ME Firmware to 12.0.49.1534.
- Updates SuperIO firmware to v7.9.50 for stability enhancement.

FIXES:
- Fixes issue where special symbols display incorrectly if F10 setup interface is changed to Russian language.
- Fixes an issue which causes the system to boot slower than expected when a network cable is used to connect the system to a Dell or Targus USB Display Link Dock.
- Fixes issue where system BIOS fails to be updated and reported "Failed to determine if new BIOS is available" without setting Proxy Server in F10 setup interface.
- Fixes issue where system prompts Power on Authentication with BIOS Administrator and POST Power-On Password options before scheduled BIOS update.
- Fixes an issue where extra characters "Enabled by default. [Help Icon]=" shows up in the help message of "Intel

Management Engine (ME)" option.
- Adds a feature to support Automatic DriveLock feature in F10 setup interface for Pyrite NVMe SSD.
- Fixed an issue where "Retail Basic or ElitePOS Advanced I/O Connectivity Base" PUSB and Cash drawer ports don't have power when "HP MP9 G4 Retail System" wakes from sleep

PCR0(with TPM2.0 SHA256)
=E9F158B06870D62308FB31B876EB1B01F5E1D023AA11A3AE9B59F2DE1B5CE160

Version 2.09.01
This BIOS upgrade package also includes the following firmware versions: (only list appropriate ones)
Intel Management Engine 12.0.45.1509
SIO19 F/W 7.9.44
Intel VBIOS 9.2.1014 (2018/07/04)
Intel GOP 9.0.1075 (2018/03/05)
USB Type-C PD firmware FW 6.8.0
Intel/Realtek PXE rom Rtk:V2.66
Intel/Realtek UEFI PXE rom Rtk:V2.035

-Enhancement to address security vulnerabilities CVE-2019-0123, CVE-2019-0117, CVE-2019-11135, CVE-2019-11139, CVE-2019-0185.
-Enhancement to address security vulnerabilities CVE-2019-0131, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-11086, CVE-2019-11087, CVE-2019-11088, CVE-2019-11090, CVE-2019-11097, CVE-2019-11100, CVE-2019-11101, CVE-2019-11102, CVE-2019-11103, CVE-2019-11104, CVE-2019-11105, CVE-2019-11106, CVE-2019-11107, CVE-2019-11108, CVE-2019-11109, CVE-2019-11110, CVE-2019-11131, CVE-2019-11132, CVE-2019-11147.
-Enhancement to address security vulnerabilities CVE-2019-0123, CVE-2019-0117.
-Enhancement to address security vulnerabilities CVE-2019-0185, CVE-2019-0152, CVE-2019-11136, CVE-2019-11137.
-Updates SuperIO firmware to v7.9.44 for stability enhancement.
-Updates Cypress PD firmware to v6.8 for compatibility enhancement.
-Adds a feature to seprate Administrator/User DriveLock password in F10 setup interface.
-Adds a feature to query DriveLock setting by HP BIOS Configuration Utility (BCU).
-Adds a feature to support Enhanced Secure Erase command for ATA drive in F10 setup interface.
-Fixes issue where PCR1 value is changed after cold boots, restarts or F10 exit.
-Fixes issue where system reports error "Failure during data transfer (maximum downloaded content size exceeded)" when unit tries to update firmware via FTP server with proxy from F10 setup interface.
-Fixes issue where system intermittently enters hibernation after idle around 2 hours in battery mode when HP Sure Run and Bitlocker is enabled.
-Fixes issue where specific SanDisk USB drive does not be listed in F9 Boot Menu.
-Fixes issue where system still can be waken up from S3/S4/S5 through onboard LAN when "Embedded LAN Controller" is disabled in BIOS F10 menu

PCR0(with TPM2.0 SHA256)
=10CF262575B1BE8EF74AD1249C8F6A6FB7E57F8814E779F5E8054A6AACD4C359

Version 2.08.00
- Updates the Intel silicon reference code to 7.0.5C.50.
- Update Intel ME firmware to 12.0.39.1431.
- Add a feature "Native OS Firmware Update Service" in F10 setup interface to enable/disable firmware update via Window Update service.
- Fixes issue where "WHEA-Logger(Event ID 17)" occurred in Windows Event Viewer.
- Fixes issue where Serial COM11 device is disabled after RTC reset.
- Fixes issue where "Authentication Failed" screen displayed when enable BIOS password under F10 and Power-on

Authentication in HPCSM, then uncheck "BIOS Administrator visible at Power-on Authentication" under F10 setup interface.
- Fixes issue where display of TPM Firmware Update interface is cut off during update process.
- Fixes issue where BIOS update via F10 setup interface failed and report: "Internal error" when set schedule to daily/weekly/monthly.
- Fixes issue where SystemDiags.log file does not be created in FTP server after execute Remote HP PC Hardware Diagnostics.

PCR0(with TPM2.0 SHA256)
=4185F26DDF9392BC335721F23AF67B0C2E33579172C413D4B917AC477E955528

Version 2.07.00
- Enhancement to address security vulnerabilities CVE-2018-12126, CVE-2018-12127, CVE-2018-12130.
- Enhancement to address security vulnerabilities CVE-2019-0086, CVE-2019-0090, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098.
- Update CCG PD firmware to 6.6.
- Update Intel reference code to 7.0.47.50.
- Locks power button function during TPM firmware update process to avoid firmware corruption.
- Adds a feature "HP Application Driver" in F10 setup interface to support HP fusion application.
- Fixed issue where USB Type-C device intermittently shows yellow bang in device manager when resuming from sleep.
- Fixed a timing issue bundle with Intel i210 add-on card which would cause "Wake on LAN/Wake on Link" to fail.
- Fixed issue where system will hang with black screen when resuming from sleep/hibernation after loading default BIOS in F10 setup interface.
- Fixed issue where user cannot exit MEBx (F6) by pressing Y or N key when setting language to Russian/Deutsch in F10.
- Fixed issue where keyboard drop-down menu still shows as English at Power-On Authentication page after changing the keyboard layout to non-English and selecting the standard user with the new password at the Power-On Authentication page.
- Fixed issue where IPv4 option is missing under Boot Order after updating BIOS by Network BIOS Update.
- Fixed issue where legacy bootable disk will be lost when hot plugging USB LAN dongle then press "Ctrl +alt +Del" key combination to boot to F9.
- Fixed issue where system with Pyrite SSC V2.0 NVMe drive could not boot into OS after enabling DriveLock then disabling it.
- Fixed issue where "Continue Boot" is not translated in startup Menu after language is set to Russian in F10.
- Fixed issue where rear USB-C still has power in hibernation or shutdown state when disabling Type-C Downstream charging.

PCR0(with TPM2.0 SHA256)
=B7DB4EB0AA73F7DD7377C97E29007CE6976CAFF2F84064AA6F8EC3860C4DA2BC

Version 2.06.00
- Fixed issue where remote diagnostic would fail with error message: "Could not detect network link or network cable is unplugged".
- Fixed issue where Bitlocker cannot be unlocked over network.
- Fixed issue where system updates firmware from EFI patition of system drive, instead of USB drive when selecting "Update System and Supported Device Firmware Using Local Media" from BIOS setup (F10).
- Fixed issue where virtual touch keyboard still displays in HP logo screen after entering correct PIN code.
- Fixed issue where changes made in BIOS Setup (F10) after a failed PXE boot does not be saved.
- Fixed issue where system hangs in POST when plugging in the Apple USB-C HDMI/VGA Multiport Adapter.
- Fixed issue where BIOS update triggered by Windows Update does not occur after inputting the incorrect Admin password then inputting correct password.
- Fixed issue where system still updates ME and Cypress PD Firmware when user enters incorrect BIOS administrator password.

- Fixed issue where Absolute Persistence function not work while HP Sure Run is activated.
- Fixed issue resulting in audio output distortion while plugging in a 3rd-party AC adapter.
- Fixed issue where ME firmware update process stops around 60 seconds to 120 seconds when connecting HP Thunderbolt Dock during update process.
- Fixed issue where system still pops out Physical Presence Interface when disabling Intel SGX in BIOS setup (F10) with Physical Presence Interface setting disabled.
- Fixed issue where "RFID" option disappears in BIOS setup (F10) after disabling it.
- Adds Russian Language Support in F10 setup interface.
- Adds a feature to hide BIOS administrator account in Power-On Authentication screen.
- Increases PXE IP time-to-live (TTL) value to improved compatibility with diverse end-user network environments.
- Adds Drivelock password feature support on Pyrite NVMe SSD.
- Improved Japanese touch keyboard layout.
- Updates the Intel silicon reference code for compatibility enhancement.
- Updates the CPU microcode for Intel processors to 0x9A.
- Enhancement to address security vulnerabilities CVE-2018-12201, CVE-2018- 12202, CVE-2018-12203, CVE-2018-12204, CVE-2018-12205.
- Enhancement to address security vulnerabilities CVE-2018-12188, CVE-2018-12189, CVE-2018-12190, CVE-2018-12191, CVE-2018-12192, CVE-2018-12199, CVE-2018-12198, CVE-2018-12200, CVE-2018-12187, CVE-2018-12196, CVE-2018-12185, CVE-2018-12208

PCR0(with TPM2.0 SHA256)
=D0FAE66E6D9EF63B1692D53AD4FE85D7227DFA86EFA614E176BD4DC65C667198

Version 2.04.00
- Fix onbaord D-sub Port may be without output when setting onbaord D-sub Port as secondary monitor.

PCR0(with TPM2.0 SHA256)
=55AD438DADEAA620FE443868B3357B0A2211FF877D961C8B83CD02DFB2223B83

Version 2.02.04
- Update ME to 12.0.7.1122 for Intel Quarterly Security Release.

PCR0(with TPM2.0 SHA256) =
5C9CB6811B05EFD73623ACB791E09D00F0DDBA8E552942E506E76D728782857A

Version 2.01.08
- Intel MCU Security Update.

PCR0(with TPM2.0 SHA1, 7.63.3353.0) = 05D04152F7E6E90F053CBE52935BE56B241C95D7
PCR0(with TPM2.0 SHA256, 7.63.3353.0) =
4DEF23DE82DED0D8FB8D7813000CDCEDF56F3F3B0BCA15066CF646F8FA55BBC3

Version 2.01.06
- Initial BIOS release.

PCR0(with TPM2.0 SHA1) = 344FF06F87375F5FE6393A2F16332F4C4375C636
PCR0(with TPM2.0 SHA256) =
99C8BDD7AE0BA2461466F7B52E6460DD419095960F8B4538F77DB17AAF478323