BIOS Requirements

For

Acer Notebook/Tablet

Acer Incorporated

9F, 88, Sec. 1, Xintai 5th Rd

Xizhi, New Taipei City 221

Taiwan, R.O.C.

DOCUMENT TYPE:	**SPECIFICATION REQUIREMENTS**
Department:	Acer IT Products Business
Author:	KYD300
Document Version:	V 1.31
Release Date:	2024/6/26

Revision History

REV. #	DATE	EXPLANATION OF CHANGE
0.9	2011/12/27	1. 1st release
0.95	2012/01/09	1. Update v6.2.3 lid open behavior 2. Remove iRST BIOS setup. 3. Add behavior for during POST if the system has external display connected. 4. Add Wake on Lan in BIOS setup menu 5. Update Appendix G
0.99	2012/02/21	1. Updated USB Charge Behaviors 2. Added iRST Wake Up Trigger Events and delete appendix iRST chart 3. Moved ASF Setting description under security section to Main section and added ASF Configuration back 4. Added addition description to Appendix G behaviors 5. Added Wake on WLAN 6. Updated Wake on LAN default value
1.00	2012/03/01	1. Updated UEFI BIOS for Windows 8 system 2. Updated 2012 chipset VRAM size 3. Correct note # in Main section in setup menu 4. Removed version# in SMBIOS section tile Removed “Writing or reading data from EEPROM will through EC KB926 SMBUS protocols.” to not use particular EEPROM in EEPROM section 5. Correct wording in Main section’s Total Memory to Video Memory 6. Updated Password Flow 7. 14.1.3 For any item needs password setup before it is available, the item should not be hidden. It should display as a gray out 8. Updated enter setup menu text ‘s letter case and add”.” 9. Update iRST behaviors in S4 and iRST state in appendix

REV. #	DATE	EXPLANATION OF CHANGE
1.01	2012/04/11	1. Add Load CSM in setup menu 2. Add back no rollback 3. Load CSM will auto turn off security boot 4. Need to add starting z and y offsets 5. Change NUM Lock behavior with Full Size keyboard 6. Added Keyboard Backlit section and behaviors 7. Modify Wake on WLAN to commercial vPro only 8. Add rule : When legacy boot mode, CSM load will always be enabled

REV. #	DATE	EXPLANATION OF CHANGE
1.02	2012/5/25	1. Modified wording in Boot Mode in Boot setup screens section: When Legacy is “enabled”, load CSM is automatic Enable. Previous statement was “disabled” 2. Added SMBIOS BIOS’s “release date” format (mm/dd/yyyy) 3. Modified Acer HDD Password flow. Removed enter service key to enter service key page flow , keep current design 4. Added only HDD0 is displayed when configured as RAID in BIOS setup screens section’s boot menu and security menu 5. Removed “Zero Power” will wake up for ultrabook when lid open in Lid switch section 6. Added "Erase all Secure Boot Setting", "Restore Secure Boot to Factory Default", and "Add an UEFI file as trust for executing" in BIOS setup screens section’s security menu 7. Modify wording of “Legacy” mode to “Legacy BIOS” mode in the BIOS setup screens section’s boot menu 8. Added Windows boot manager is displayed on top of boot device when OS is installed in BIOS setup screen’s boot device menu 9. Added requirement to external display must base on EDID information to display correct ratio logo 16:9 or 4:3 in Post Logo Section 10. Added clear statement "Press to enter …" message on the bottom of the screen should only display in legacy mode in POST Summary session 11. Added SMIBIOS System SKU Number (Type 1) format definition : . 12. Changed document title to UEFI BIOS Requirements instead of just BIOS Requirements 13. Modified Security Boot Mode option definition as a display status instead of an action to trigger other action in BIOS Setup screen‘s secure menu. 14. Removed Load CSM option in BIOS setup screen’s boot menu. 15. Removed BGRT OEM Brand logo section’s example logo 16. Added all brand Windows8 post and BGRT OEM brand logo 17. Add confirmation pop up message when users switch boot mode between legacy and UEFI. 18. Added Admin password check for security boot setting modify in BIOS setup screen’s secure menu 19. Added admin password check for security boot enabled/disabled in BIOS setup screen’s boot menu 20. SMBIOS System SKU Number’s version between major and mirror # should be . . not _

REV. #	DATE	EXPLANATION OF CHANGE
		21. Added RAID Mode in SATA mode option in BIOS setup screen's Main menu 22. Removed RTC from IRST Wake up event in battery mode 23. Change wording from shut to lid closed 24. Removed DVI, HD15, Component, and S-video and added VGA into external display order when lid is closed. 25. When boot mode change, available boot device is gray out in the setup screen's Boot Menu 26. Added Internal keyboard HW ID defined in internal device information requirements section 27. Under network boot section, LAN boot is disabled in UEF boot mode.

REV. #	DATE	EXPLANATION OF CHANGE
1.03	2012/6/15	1. Added Acer security boot public key sets in Secure Features – Security Boot section 2. Touch Pad should maintain previous enable or disable status after S3/S4/S5 in Touchpad On/Off section 3. Modified BIOS setup screen's Network boot default is "Disabled" 4. Added Windows Boot Manager, Windows USB To Go, Network device IPv4 and IPv6 into Boot device 's screen example 5. Added boot description to" Select an UEFI file as trusted for executing", the added boot description will become an entry into boot priority 6. Non Physical boot device can be deleted in Boot priority Order in BIOS setup menu 7. Adding security boot requirements to ensure key import's is depending on standard interface during the code build up rather than tools 8. Removed "Authenticated variables will be kept after flashed." In Crisis Recovery 9. Removed brand name of Upack/Authentec/LTT/Validity in "Finger print: support 10 fingers" 10. Removed "TechG requirement in TPM section 11. Removed note1 in System wake up source under ACPI Mode section 12. Removed "Tech G" requirement in Boot device sequence section 13. Changed Quite boot to legacy BIOS boot only in POST logo section (Highlight color changed) 14. Removed Windows USB to Go in Boot device priority order 15. Changed Information menu's System BIOS Version example version "v"xx.xx from lower case to upper case Vxx.xx 16. Bluetooth is on by default 17. Set all occurrence of product name to standard format in Product Name, System Management BIOS, and Information Menu sections
1.04	2012/7/6	1. Added xHCI support option in BIOS setup screen's Information Menu (For systems only have USB 3.0 ports) 2. Added Appendix H for Graphic BIOS Setup Menu visual design requirements (Only apply to systems whose have been selected to adopt) 3. Updated Acer Security key package to include Acer DB key in security boot section

REV. #	DATE	EXPLANATION OF CHANGE
1.05	2012/7/20	1. Updated Boot Mode type behavior: After BIOS flash, load setup default 2. Added OA and OS matrix table in “SLP 1.0and OA2.0… “section 3. Update Logo image file: Win8_POST_BGRT_Logo_0718_2012.rar to include brand logo for UEFI BIOS’s legacy boot mode. So when post resolution is set to 1024x 768 in legacy boot, images will display correctly 4. Added flash rules for separate BIOS in “Flash Utility” section. 5. Added comment to “Wireless LAN & Bluetooth after loading default setting” section : BT in OS should turn off SW radio signal, but BT HW signal should default “On” 6. In “Secure sequence” section, updated In the case of Password of Supervisor for boot up is equal to Hard disk Password, it should Bypass Supervisor ask 7. Change Note 6 location to express this note is under S3 and Lid Open, not Lid open as general in “System Wake Up source under ACPI Mode” section. 8. Updated Lid open resume behaviors for Ultra book (SSD SKUL only) projects in “System Wake Up source under ACPI Mode” section. 9. Added Commercial projects’ legacy BIOS boot mode definition in “Boot mode” section
1.06	2012/7/27	1. Changed VRAM Size defined to follow vendor platform recommend size in “Main Menu” section 2. Added NUM Lock behaviors will follow OS designed behaviors after enter OS in “NUM Lock“ chapter 3. Added display message when upgrade/downgrade BIOS to disallow scenario in Flash Utility Section 4. Modified password check’s sequence as HDD first and Admin later In “Secure sequence” section 5. Removed Power on display in user password chapter
1.07	2012/8/24	1. Removed SMBIOS type 05, 06, 09 (Memory Controller Information, Memory Module Information, System Slots) 2. Added SMBIOS check list to appendix I

REV. #	DATE	EXPLANATION OF CHANGE
1.08	2012/10/22	1. Modify customized security boot restore spec. in “Secure Features – Secure Boot” section.(p32) 2. Add Secure Boot Check Status restore behavior in the “Secure Boot” section. (p60) 3. Highlight Graphic Mode only support on the commercial platform with XP support.(p49) 4. Modify definition of product name to standard format in Product Name, System Management BIOS and Information Menu section. (p26, p40 and p46)
1.09	2012/11/06	1. Add Windows 8 Radio Management Specification in “Button – Wireless LAN & Bluetooth Radio Management” sections”. (p18) 2. Revise customized security boot restore spec. in “Secure Features – Secure Boot” section.(p32) 3. Revise Secure Boot Check Status restore behavior in the “Secure Boot” section. (p60) 4. Add Boot Mode change and Secure Boot Status definition. In the “Boot Mode” section. (p60)

REV. #	DATE	EXPLANATION OF CHANGE
1.10	2012/12/28	1. Add spec. for Linpus with Secure Boot feature in UEFI Compatibility OS support list. (p12, p34) 2. Add spec for POST and POST Logo resolution under [Legacy] Boot Mode. (p21) 3. Update Asset Tag default value spec. (p27) 4. Add clear CMOS action spec. (p29) 5. Update hard disk password set action. (p30) 6. Update TPM spec. and add TCM spec. (p32) 7. Update Secure Boot variable protection spec. for BIOS flash (p33, p38) 8. Update S3 wake up from USB device spec. under lid close. (p36) 9. Update Crisis Recovery spec with secure flash feature in new project. (p39) 10. Add Microsoft Windows To Go spec. (p25, p42, p58, p60) 11. Add default SCU resolution spec. (p44) 12. Update xHCI support spec. (p50) 13. Update item in Security Menu presentation spec. (p52) 14. Add TCM support. in Security Menu and update TPM/TCM presentation spec. (p55) 15. Update Secure Boot feature spec. (p56) 16. Update Exit Menu spec. (p60) 17. Update ACPI S4 requirement for invoking SCU for Win8 (p64) 18. Update Supervisor Password spec for Supervisor Password reset purpose.(p29) 19. Update Add notes for Password change/remove spec.(p32)

REV. #	DATE	EXPLANATION OF CHANGE
1.11	2013/10/31	The contents of the spec have been reorganized. It only lists the change highlights, but doesn't include all changes. Please review the entire spec. 1. Add Boot failure feature for 2014 projects. For Critical low battery no boot feature, it will be replaced by the boot failure definition. 2. Remove USB charger port couldn't support wake description 3. When USB Boot is disabled, under Boot priority order, USB boot device type is displayed but no device detected. No USB bootable device shows on F12 Boot Manager. 4. Add Win8.1 OS support 5. Remove Intel AT support 6. Add Precision Touchpad support 7. Add flash tool must check battery remaining capacity more than 15% 8. Add VRAM size definition 9. SCU doesn't support Touchpad 10. BIOS disable PCI-E L0S support by default 11. Change SMBIOS product name maximum length to 25 bytes 12. Add connected standby BIOS spec 13. Update secure boot Acer key package 14. Remove eMachine and Founder brand 15. Add Critical low battery wake up event trigger on 6% remaining capacity 16. Add Alt+ F10 support 17. Change SLIC Table support matrix due to MS spec change 18. Update BIOS Setup Menu for commercial projects 19. Add new pop up wording when end user switch boot mode from UEFI to Legacy 20. Add description to the F2/F12 prompt message no longer display and POST logo using BGRT no matter UEFI or Legacy under win7/win8. 21. Add RF button definition 22. Update password control flow 23. Add Windows To Go section 24. Add description about the boot mode default setting. BIOS need to check OS type for the default setting. 25. For certain regions restricted to ship products with TPM, such as China, BIOS must disable TPM by default.

REV. #	DATE	EXPLANATION OF CHANGE
1.12		1. Change Product name length to 25 bytes (P.21, 23) 2. Remove table from 4.1.5 Graphic to avoid confusion (P.54) 3. Modify the embedded display and external display description (P.54) 4. Add critical low battery as wake up event for S0 blank (P.61) 5. Update Key Code excel file to V1.6 (P.5) 6. Add sending “Standby Immediately” command to HDD and SSD before actually shutdown system caused by 4 second Power Button override event. (P.46) 7. Update password flow chart (P.37) 8. Update SMBIOS check item list to V1.02 (P.41) 9. Add Acer System Diagnose and Acer Disk Sanitizer sections (P.49) 10. Add note to describe the occasion to update boot block. (P.17) 11. Update boot failure icon (P.46) 12. Update VRAM size table to add definition of Beema and Kaveri (P.54)

REV. #	DATE	EXPLANATION OF CHANGE
1.13	2014/10/1	1. Create Chapter 5 for commercial BIOS requirements 2. Create Chapter 6 for Tablet BIOS Requirements 3. Change SMBIOS spec to V2.8 4. Divide Commercial BIOS setup options into “Advanced” page 5. Move section 3.2.4 Absolute Computrace to chapter 5 6. Move section 3.12 Acer System Tool to chapter 5 7. Add Fingerprint PBA support into chapter 5 8. Change BIOS spec title to replace netbook with tablet 9. Add GPT partition save/restore feature description and BIOS setup options 10. Correct OS support typo for win7 SP2 11. Add vPro support description 12. Refine BIOS setup options sequence: BIOS version/VGA BIOS version/GOP version/Total Memory/D2D Recovery 13. Remove options: Video Memory/Graphic Mode/Quiet Boot/ 14. Add option: Lid Open Resume/Clear TPM(TCM) 15. Remove section Ch3.1.2 Graphic Model BIOS Setup Menu to Ch6 Tablet Requirement 16. Add Chassis Type (SMBIOS Type 3) data in SMBIOS Definition 17. Correct SMBIOS Type1 Manufacture Name offset from 1Bh to 04h 18. Redefine RF/Communication key behavior 19. Add "Device must not boot up by buttons, keyboard, touchpad when lid is closed" 20. Add "Lid open wakes system from S3 state if Lid Open Resume is Enabled" 21. Modify default value of "Battery Threshold" to 30% 22. Align pre-OS hotkey of "Enter BIOS setup"/Display Boot Menu"/"Crisis Recovery" for tablet 23. Add "D2D Recovery" entry in BIOS setup menu of tablet 24. Remove "D2D Recovery" option from BIOS setup menu of tablet 25. Add "Individual windows button could wake up system from S3." for tablet 26. Add "Not enable fast boot if tablet bundle with USB docking" for tablet 27. Set Quite boot default as “Enable” 28. Add "Valid Power button event is keep pressing 2 sec power button by HW silicon judgment" for tablet 29. Add picture of "D2D Recovery" and its prompt confirmation dialog 30. Add picture of "Clear TPM" and its prompt confirmation dialog 31. Add "Firmware Capsule Update WHCK Process" attachment 32. Update "key code" attachment to V2.00.

REV. #	DATE	EXPLANATION OF CHANGE
		33. Update "Acer Indicator spec for Win8" attachment 34. Add "Charging Indicator" section for tablet 35. Add boot mode automatic change support for commercial projects 36. Bind VRAM table directly into spec and update the new platform definition 37. Add description “To change password in SCU, entering current password and retry three times error, system halt.” 38. Add description about non-support Fn function keys under non-ACPI 39. Add PTP into wake up event 40. Add SCU option for PTP support 41. Modified boot failure description in more detail 42. Add Smart learning battery support 43. Add description about eMMC must have size information on SCU 44. Modified SLIC table requirement 45. Add Power Button on Keyboard support 46. Update TPM support policy and SCU layout 47. Sync up power-off USB charge behavior with Quick Access 48. Remove special symbol empty title 49. Add fingerprint enable/disable SCU option 50. Add section “6.7 Smooth Battery Percentage” 51. Hidden “Special Key” BIOS setup option for Acer Brand model 52. Removed “for Non-CS system” of “Selected an UEFI file as trusted for executing”.

REV. #	DATE	EXPLANATION OF CHANGE
1.14	2014/12/10	1. Remove “Hidden only when Legacy Boot Type” statement of “Change TPM status (for TPM 2.0)” option of BIOS SCU 2. Add a new section 4.1.15.3.2 Battery Percentage 3. Add Power-off USB charge port not support USB wake 4. AHCI support (for both Intel 965/945 chipset family)==>remove 965/945 wording 5. Add note to the title about "InsydeH2O Setup Utility" instead of BIOS setup utility 6. Add description about auto hidden GPT recovery option if partition is not GPT 7. Add description about the limitation of GPT partition recovery to maximum 8 partitions 8. Remove 4.3.1 due to iRST phrasing out 9. Remove iRST description from LID open resume support for ultrabook 10. Modified RAID section description 11. Add to LID Open resume default depends on projects request 12. Add description about the power button on keyboard behavior limiting to S0. 13. Add enable capsule update support for all NB 14. Modified 3.7 video switch to leverage win+P 15. change win8.1 to “win8.1 and above” 16. Update LED spec to V0.7 17. Add hiding xHCI enable/disable if platform only exist one of the controller 18. Add panel off definition for WLAN, wake on WLAN 19. Move SCU Wake on WLAN to commercial SCU 20. Correct typo of Carrizo 21. Remove pressing “ESC” switching to text mode support 22. Add SwitchLock option and behavior in BIOS setup menu of Tablet Modified SLIC table control table

REV. #	DATE	EXPLANATION OF CHANGE
1.15	2015/8/30	1. Add WiGig enable/disable option into advance page 2. Modify Hotkey support of tablet 3. Add USB Docking Hot plug support section 4. Add statement in Smooth Battery Percentage section. "If Full Charge bit is supported in gas gauge design, please implement and follow Battery Percentage algorithm in Notebook section” 5. Remove statement of D2D Recovery option of GUI SCU. "The option is only visible on tablet without windows button" of D2D Recovery option 6. Add "Current TPM" & "Change TPM state" to replace "TPM support" option of GUI SCU 7. Add “Network Boot” option of GUI SCU. Option is hidden and default is Enabled. 8. Add “Network Boot-IPV4” Boot device in Boot Priority order of GUI SCU. 9. Add “GPT Partition Recovery/Record” option in Main page of GUI SCU. 10. Remove CPU speed display from SCU and change CPU Type to CPU Info 11. Remove SATA mode selection from SCU main page 12. Add SATA Mode display on SCU information tab 13. Define RAID SKU should set SATA mode to RAID 14. Add LID close disable keyboard, touch pad and touch panel into spec 15. Add TPM China policy: If systems ship to China, TPM must be disabled 16. Move total memory from “Main” tab to “Information” tab 17. Add type C related definition 18. Add disable unexposed I/O port 19. Add WLAN country code identification 20. Add touch panel hot key behavior description 21. Update SMBIOS check list “SMBIOS type0 BIOS vender should be Insyde/Phoenix” 22. Update AMD pre-allocate VRAM size 23. Remove Chipset Feature title since there is no content 24. Change power-off charge port support USB wake as normal USB port definition 25. Add eMMc as default boot device if eMMc plus HDD exist in the same system 26. Add NVMe not support HDD security display on SCU. 27. Add statement of XHCI support of GUI SCU. “Hidden the option if

REV. #	DATE	EXPLANATION OF CHANGE
		platform only exist one of the controller (xHCI or EHCI) alone 28. Add HW button PTP definition 29. Add LTE description into commercial SCU 3G device enable/disable 30. Add “Clear” function into GPT recovery feature. 31. Add error message into GPT recovery section 32. Update Copyright to 2016 33. Add description for USB LAN dongle support PXE no matter legacy or UEFI 34. Add SMBIOS family name rule 35. Update SLIC table 36. Modify Capsule update UI 37. Add to follow “Convertible Mode Usage PES” for convertible projects 38. Adjust allowing BIOS flash battery capacity to 25% to follow Capsule update 39. Add Predator serial Logo
1.16	2016/2/04	1. Add Type C enable/disable option 2. Change GPT clear option layout 3. Remove Type-C type detection requirement 4. Update family name table for SMBIOS type 1 Offset 1Ah 5. Fix typo of WiGig enable/disable option description 6. Remove coldboot request after set HDD password 7. Remove display only HDD0 password if 2nd HDD configure as RAID 8. If keyboard printing of Acer/PB/GW is the same, hide [Function key/Special key] switch option 9. Change UUID display to every system no matter it has internal LAN or not 10. Update SMBIOS support to V3.0 11. Update chassis type definition 12. All key press and power button event can’t be triggered during Capsule update 13. Remove non necessary description on boot device failure 14. Update Intel platform pre-allocate VRAM size to 64MB due to 4K display support on win10 15. Revise AMD Stoney Ridge pre-allocate VRAM size 16. Update keyboard backlight behavior description 17. Update SLIC table 18. Update Acer logo to remove tagline

REV. #	DATE	EXPLANATION OF CHANGE
1.17	2016/7/30	1. Update SMBIOS definition in order to support 2017 MDA 2. BIOS time zone default set to UTC+8 Taipei time 3. Add and modify WLAN regulatory support description and attach document 4. Password change to Unicode (UTF-8) format and update valid characters set corresponding to this change 5. Define dimming behavior when adjust keyboard backlit 6. Add gaming product follow “Acer Indicator Spec for Win8_Win10” description 7. Add description about HDD password could be modified even in frozen state 8. Remove “Special Key” option from SCU since keyboard printing are the same between Acer/GW/PB 9. Remove the available options for SCU user view 10. Add description about “BIOS should load default setting after flashing”. 11. Boot device order behavior change to UEFI definition. Only display bootable devices. 12. LID open resume default enable for all projects 13. SMBIOS check list update V1.06 14. Add Advanced Page for Virtualization and SATA Configuration menu 15. Add Virtualization must enable if platform support it 16. If commercial dock plug in, power button should function well even LID closed. 17. Update Industry spec version 18. Update “Acer indicator Spec for Win8_Win10_V0.9draft8” 19. Update “key codeV2.02” 20. Update capsule update process description and screenshot 21. Add connected standby and modern standby wake up event state. 22. Sync TXT mode SCU items with graphic mode SCU. 23. Update Acer Disk Sanitizer PES V0.04 24. Update Acer System Diagnose PES V0.06 25. Discrete GPU doesn’t support GOP and VBIOS version display 26. Update copyright message 27. For Intel platform which support Software Guard Extension (A.K.A SGX), BIOS must set to “Software control” for SGX configuration. 28. Correct WiGig SCU description 29. Add Kabylake Pre-allocate VRAM size 30. Update Graphic SCU product name length to 25 bytes (same as

REV. #	DATE	EXPLANATION OF CHANGE
		TXT SCU) 31. When system battery capacity reaching stop charging condition, it won't support USB S3 wake-up through type C. 32. Add one more layer to the Advanced page for commercial projects. Shift all device control into a sub-menu of Advanced page.
1.18	2016/11/15	1. Add screenshots for 2017 modified graphic SCU 2. Update screenshots for text mode SCU 3. Add description about battery capacity calculation rule. It must round the value with remaining capacity divided by full charge capacity. 4. Add acoustic setting definition for Intel platform 5. Add PCI pay load setting definition for Intel platform which support the adjustment 6. Add "Wake on USB while lid closed" option to the SCU main tab 7. Add "TBT Detection Gain" option to the Advanced SCU tab 8. Change Absolute section. ODM get latest implementation guide/BIOS package/test report template from vendor directly. 9. Add iSST support for Intel platform. 10. Update UUID display format

REV. #	DATE	EXPLANATION OF CHANGE
1.19	2017/08/02	1. Force Wi-Fi device power limit to 2000 for Intel big core platform (4.1.6.3). 2. Change “Linpus” to “Linux” support 3. Remove BIOS timezone definition 4. Update description of PCI-E power saving section (4.1.18) 5. Add special design highlight to embedded display (4.1.5.1). If system design has limitation to retrieve EDID from embedded display (e.g. panel connect to system through MIPI), BIOS must provide EDID data for OS to query. 6. Add “POST Animation & Sound effect” section (3.15). Also add SCU item for user to control. 7. Remove GPT feature 8. Add Media Key/Function Key switch (4.1.1.3). Also add BIOS setup option. 9. Update CHID table 10. Add HWP enabling by default 11. Add enabling SGX by default if system adapt ePayment which leverage SGX technology (4.4) 12. Add Wake up on time option into commercial SCU advanced page 13. Add speaker & headphone, microphone, Optical drive enable/disable option into commercial SCU device control 14. Change password length from 12 to 16 characters 15. Update pre-allocate VRAM size for new platform (4.1.5.3) 16. Remove Touchpad configuring option due to not necessary for the new platform 17. Hide SATA device control option if BIOS set to RAID 18. Add TBT wake support and BIOS SCU setting 19. Modify USB wake capability to follow SCU setting 20. Update WLAN Regulatory Support document for Dynamic power switch 21. Update SMBIOS check list for Dynamic power switch 22. Add AMD-SVM control option 23. Add OPAL support description (3.2.1.1) and SCU items 24. Add Firmware capsule update power check requirement 25. Add embedded panel backlight on/off requirement for system built with USB keyboard (4.1.1.5) 26. BIOS fixes panel backlight to 150 nits during whole POST period. 27. Hide “Wake on USB while LID close” option on modern standby design 28. Add SATA mode option into Main page 29. Add Optane memory section (4.1.21)

REV. #	DATE	EXPLANATION OF CHANGE
		30. Replace connected standby with modern standby to avoid confusion 31. Remove Lightning bolt section due to no long support 32. Update Graphic SCU mapping to text SCU modification 33. Update RF button and communication key control flow (4.1.1.4) 34. Remove iRST from wake up event table 35. Add Win 10 S support 36. Modify BIOS flash forbidden rule to “If BIOS binary is not newer than system BIOS version” 37. Update Copyright year to 2018 38. Modify TBT detection gain description 39. Add OPAL password behavior in different power state and if it could keep after BIOS update 40. Update Firmware Capsule Update WHCK process document 41. Update Key Code table to V2.04 42. Add OPAL device to information page 43. Add a to z into password scope 44. Add “For PCIE storage device, L1.2 is required.”

REV. #	DATE	EXPLANATION OF CHANGE
1.20	2018/2/27	1. Modify chapter 2.3 Windows Connected Standby statement to Windows Modern Standby 2. [Setup Menu]Modify TBT wake and USB wake option description 3. Add if IHV doesn't support legacy in the platform, hide legacy option from boot mode setting in SCU 4. Modify Type-C charging behavior 5. Modify HDD serial number display rule. If no hard disk or other devices are installed, "None" should be shown on this field. 6. Remove storage device name display after windows boot manager no matter at SCU boot order screen or F12 boot menu 7. Hotkey and LED spec will release by SWPM independently and separate from BIOS SPEC. ODM could get specs from FTP (/DQC/Design Guide/NB_WTablet/BIOS) 8. Correct description of SATA mode setting on graphic SCU 9. Modified SATA mode setting description to avoid confusion. "Set to [RST Premium with Optane] if project features support RAID SKU (AMD platform set to [RAID])" 10. Define EC Reset and RTC Reset hotkey 11. Define "Wake up system on time" option default setting to "Disabled". Grey out Wake up hour/minute/second options if function is disabled. 12. Remove "EC reference design guide" wording 13. Update Chipset Abbreviation of CHID-8 14. Add "Progressing bar" as required display of capsule update because of MDA 15. Add force STBI section to prevent SSD entering recovery mode and causing problem 16. CAUTION: Due to current critical design issue relating to Re-mapping and OPAL protocol under S3, only implement the support when project must adapt OPAL. In that case, project must disable Re-mapping to avoid problem. 17. Add boot path definition for UEFL shell 18. Change SATA configuration to Storage Device configuration. SATA and PCIE storage devices both included. Display mapping to information tab. 19. Change description of critical battery LED control to follow LED SPEC. "If end user press button when battery capacity <= 3%, EC need to follow LED spec blinking and prevent system from booting." 20. Add OS combination key support to Tablet SPEC. For Intel platform, Tablet project must adapt Intel HID filter driver.

REV. #	DATE	EXPLANATION OF CHANGE
1.21	2019/01/31	1. Add Modern Standby system power button behavior in section 2.3.7 2. Add Amber Lake and Comet Lake definition into platform abbreviation list 3. Add option to mute the sound of POST animation 4. Add option to disable Internal KB Numpad support 5. Add option to enable/disable Fast Boot. The purpose is to support the case that User required long POST time. Skip UEFI defined timeout variable if Fast Boot enabled. 6. Change how storage naming for Info/Security/Device control page. Remove single OPAL storage display. Only add (OPAL) for identification. 7. Add “Save & Shutdown” option in “Exit” tab of SCU 8. Linux SKU, configure PTP to I2C (>=Win8.1) 9. Remove ASF Configuration from SCU 10. Add CNVI WLAN/BT control option to SCU 11. Update SMBIOS checklist to V1.08 to correct SMBIOS type F9h/371d to the right value F9h/249d 12. Modified SATA option for better understanding 13. Add definition of Intel RST software feature mask setting configured by SATA BIOS option 14. Correct Capsule Update warning icon 15. Define RPMC support for Intel platform 16. Add enable/disable keyboard backlight timeout 17. Crisis should clear whole variable section. Remove secure boot key from crisis secure data. 18. Add OEM table ID definition 19. Add preserving FUB variable after flashing BIOS 20. Add USB-C Docking Station support

REV. #	DATE	EXPLANATION OF CHANGE
1.22	2019/09/05	1. Update Copyright year to 2019 (P67) 2. Add Battery over Discharging Protection of USB charging (P94) 3. Add statement for MDA requirement (P30) 4. Add new platform definition into platform abbreviation list (P30) 5. Add VRAM size definition new platform support (P84) 6. Add Display Language option into Main page (P41) 7. Add RTC reset option into Main page (P41) 8. Change wording from “Wake Up System on time“ to “Power On by RTC Alarm” (P99) 9. Change password behavior (P51) 10. Change SATA mode behavior (P42) 11. Remove Commercial BIOS “Boot Mode automatic change support “ section (P108) 12. Add BIOS Update option into Commercial BIOS Advanced page (P100) 13. Add Lock BIOS Version option into Commercial BIOS Advanced page (P100) 14. Add Rollback BIOS Version option into Commercial BIOS Advanced page (P100) 15. Add Acer Battery System Management support (P97) 16. Modify Precision touchpad description (P91)

REV. #	DATE	EXPLANATION OF CHANGE
1.23	2020/01/10	1. Adjust hotkey support table and remove RTC reset hotkey & SCU option (P46) (P78) 2. Add combination key support chapter (P83) 3. Add UUID definition in SMBIOS Type1 (P68) 4. Add “BIOS SCU settings should be kept after flashing” description. (P26) 5. Add Export BIOS Settings to USB Storage option into Commercial BIOS Advanced page (P101) 6. Add Import BIOS Settings from USB Storage option into Commercial BIOS Advanced page (P101) 7. Change Load Setup Defaults option to Load Factory Setup Default option in Commercial BIOS Exit page (P113) 8. Add Save Settings to User Setup Defaults option into Commercial BIOS Exit page (P113) 9. Add Load User Setup Defaults option into Commercial BIOS Exit page (P113) 10. Add USB Filter option into Commercial BIOS Advanced page (P111) 11. Add Absolute Persistence Module option into Commercial BIOS Security page (P112) 12. Update System Firmware Capsule Update SPEC 2.6 (P30) 13. Add VMD(Intel Volume Manage Device Bootcamp) support (P40) (P43) 14. Adjust TPM China policy (P94) 15. Adjust Backlight Keyboard description (P80)

REV. #	DATE	EXPLANATION OF CHANGE
1.24	2020/08/04	1. Update Copyright year to 2020 (P70) 2. Add Russian and France language support (P47) 3. List BIOS supported 12 languages (P47) 4. Add customized POST logo replacement support into Commercial BIOS (P119) 5. Rename “USB filter” item to “USB Device Filter” in Commercial BIOS (P114) 6. Add project name check mechanism when importing BIOS Settings from USB Storage into Commercial BIOS (106) 7. Add warning dialog if user chooses Permanently Disable for Absolute Persistent Module into Commercial BIOS (P116) 8. Add dialog box for “Save Settings to User Setup Defaults” item into Commercial BIOS (P118) 9. Add Thunderbolt Controller enable/disable option support into Commercial BIOS (P113) 10. Update Predator and ConceptD POST logo (P73) 11. Add new platform definition into platform abbreviation list (P33) 12. Gray out Boot Mode option if only support uEFI mode (P61) 13. Define OPAL password length up to 32 characters (P65) 14. Update Windows OEM Activation table (P38) 15. Crisis recovery no need to keep BIOS SCU settings (P27) 16. Default enable BT audio offload for Intel CNVi design (P102) 17. Add MS state support for Battery over Discharging Protection of USB charging (P98) 18. Add ME capsule update support (P31) 19. Add Device Firmware should meet power check criteria (P31) 20. Add combination key support (P85)
1.25	2021/02/09	1. Add FUB variable support (P29) 2. Remove Device Firmware to do Intel CSME/CSE capsule update (P30) 3. Virtual Keyboard support in Tablet BIOS requirements (P124) 4. Modify Type C support behavior (P98) 5. MAPT and WOL from Dock support for commercial BIOS (P105) (P107) 6. Add System Health Indicator support for commercial BIOS (P105) (P116) 7. Remove 6.11 chapter Graphics BIOS Setup Utility support (P124) 8. Add Modern Standby Indicator support (P37) 9. Replace Packard Bell and Predator logo (P73) 10. Change HDD password behavior(P54)

REV. #	DATE	EXPLANATION OF CHANGE
1.26	2021/09/07	1. Redefined chapter 3.5.3 to Power button Behavior (P79) 2. Change Product name maximum length to 50 bytes (P43) (P44) (P72) 3. Update Copyright year to 2021 (P74) 4. Default to hide TBT Detection Gain item (P53) 5. Modify MAPT and WOL from docking behavior (P111) 6. Support customized MAC address for MAPT (P111) 7. Modify EC reset behavior (P84) 8. Add new platform definition into platform abbreviation list (P34) 9. Modify Intel CNVi Bluetooth settings description (P106) 10. Add NVMe RAID mode option for AMD platform (P45) 11. Add Resizable Bar feature support (P45) 12. Add Privacy Screen support for commercial BIOS (P109) 13. Update WLAN Regulatory Support BIOS design guide to v1.5 (P82) 14. Crisis Recovery doesn`t need support Lock BIOS Version (P110) 15. Update Power State Password check table OPAL password behavior (P70) 16. Add the restrictions for OPAL password support (P69) 17. Add one hotkey backlit brightness behavior (P87) 18. Adjust TPM China policy (P100) (P126) 19. Add NVME SSD password support for commercial BIOS (P54) (P122) 20. Add product name check for BIOS update option for commercial BIOS (P110) 21. Add Win 11 support and remove unsupported OS (P35) 22. Add Modern Standby Indicator description (P39) 23. Add PD adapter warning message support (P101) 24. Modify TXT function criteria for commercial BIOS (P126) 25. Add Boot Guard support requirement (P106) 26. Add Nvidia Display mode support (P52) 27. Add Secured-Core PC variable support and modify preserved variable data for Secured data (P31) 28. Add Secured-Core PC support for commercial BIOS (P126) 29. Add MSFT DFCI support (P126)

REV. #	DATE	EXPLANATION OF CHANGE
1.27	2022/03/30	1. Add “Service Key” combination key (section 4.1.1.10) 2. Add Executed Revert Count option for commercial BIOS (section 5.4.3) 3. Add DFCI/ABST support option (section 3.1.1.1) 4. Add Secured-Core PC device identifier for commercial BIOS (section 5.5.5) 5. Modify TXT function description for commercial BIOS (section 5.5.3) 6. Modify Secured-core PC support description for commercial BIOS (section 5.5.4) 7. Add “Authorized Signatures” option for SCPC (section 5.4.3) 8. Supplement Intel TXT(Trusted Execution Technology) option for commercial BIOS (section 5.4.2) 9. Add NVIDIA GPU only support and warning message for Display Mode (section 3.1.1.3) 10. Add Memory size and speed in information tab of commercial features. (section 5.4.1) 11. Add LAN MAC Address in information tab of commercial features. (section 5.4.1) 12. Intel Chasm Falls Support Scope (section 5.9) 13. Update WLAN Regulatory Support BIOS design guide to v1.7 (section 3.12) 14. Pre-allocate VRAM Size for Intel platform. (section 4.1.5.3) 15. Discrete TPM Firmware Capsule update for commercial projects. (section 5.10) 16. TPM design update. (section 4.1.15.1) 17. Add Active Efficient Cores enable/disable control. (section 3.1.1.3) 18. Add AMD GPU support for Hybrid Graphic (section 3.1.1.3) 19. Screen display when crisis recovery (section 1.2.3) 20. Remove above 4G decoding (section 3.1.1.2) 21. Add new platform definition into platform list (section 1.3.2) 22. Optimize F2/F12 boot process (section 4.1.1.1) 23. Camera firmware capsule support (section 1.3)

REV. #	DATE	EXPLANATION OF CHANGE
1.28	2022/10/13	1. Update Acer copyright string. (section 3.4.1.1) 2. eMMC/UFS don’t support HDD password. (section 3.2.1) 3. Education product support World-Facing LED. (section 5.4.2) 4. Modify Chinese string. (section 3.1.1.2) 5. Support eMMC/UFS (section 3.1.1.1). (section 3.1.1.3) 6. Modify string to full range charging (section 4.1.18) 7. Add modern standby support critical low battery wake. (section 4.2) 8. Add Intel GNA device and MEBx sub-page. (section 3.1.1.3) (section 5.4.2) 9. Add Type-A for Power-off USB Charge port. (section 4.1.11) 10. Add ownership tag feature. (section 3.3.1) 11. ABST support to read/write asset tag and ownership tag. (section 3.3.1) 12. Save encrypted key in USB storage for password unlock. (section 3.2.2) 13. Add Core Frequency for CPU. (section 3.1.1.1) 14. Add new platform definition into platform list (section 1.3.2) 15. Add AMD A/B Recovery Support. (section 5.11) 16. Add TPM Device Selection for commercial projects. (section 5.4.3) 17. TPM design update for consumer projects. (section 4.1.15.1) 18. Update Supervisor/User/HDD password style. (section 3.1.1.4) 19. Tender Request Enabling. (section 5.12) (section 1.2.4) 20. Align HDD and Opal password’s behavior after reboot (section 3.2.2)

REV. #	DATE	EXPLANATION OF CHANGE
1.29	2023/4/20	1. Update On Board Memory information in Information page (section 5.4.1) (section 3.1.1.1) 2. Add Frequency and Voltage information for each memory device (section 3.1.1.1) 3. Add Unconfigure ME for COMMERCIAL BIOS REQUIREMENTS (section 5.4.2) 4. Add Asset Tag Number and OwnerShip Tag Number to Secured Data (section 1.2.4) 5. Update Display mode behavior for Nvidia (section 3.1.1.3) 6. Update one BIOS for all brands and product lines (section 3.9) 7. Add Acer Application Base Driver Requirement for BIOS ACPI device (3.15) 8. Remove “AcerDeviceEnablingServiceFlag” variable from Secured Data (section 1.2.4) 9. Modify Supervisor and User Password reset password description (section 3.2.2) 10. Add Acer Application Base Driver Requirement and Power Shell WMI feature to Tender Request Enabling (5.12) 11. Remove Touch Pad Item under Setup menu main tab (section 3.1.1.2) 12. Remove "ctrl" + "D" hot key for display "System Diagnose" and "Disk Sanitizer" item. (section 5.4.2)

REV. #	DATE	EXPLANATION OF CHANGE
1.30	2023/10/15	1. Add New platform abbreviation (Section 1.3.2) 2. Modify Family name max length from 30 to 50 characters (Section 1.3.2) 3. Add section Battery Charge Limiting and Microsoft Smart Charging UX Support (4.1.22) 4. Set AMD-IOMMU item to always hidden in SCU (Section 3.1.1.3) 5. Set AMD-SVM item to always hidden in SCU (Section 3.1.1.3) 6. MAC Address should add an “External” String on Boot Menu (Section 3.1.1.5) 7. Modify description of TPM Device Selection (Section 5.4.3) 8. Add TPM Device Selection Option to Consumer (Section 3.1.1.4) 9. Change 3G/LTE to WWAN (Section 5.4.2) (Section 3.10) (Section 4.1.6.2) 10. Modify USB Device filter (Section 5.4.2) 11. Absolute should always grayed out if user set the value to Permanently disabled. 12. Add Kazakh to display language. 13. Change Text mode to GUI mode remove Information Tab (Section 3.1.1.1 and Section5.4.1) , Main Tab (Section 3.1.1.2) , Advanced Tab (Section 3.1.1.3 and Section 5.4.2) , Security Tab (Section 3.1.1.4 and Section 5.4.3) , Boot Tab (Section 3.1.1.5) , Exit Tab (Section 3.1.1.6 and Section 5.4.4) Modify to Graphis Set HDD Password (section 3.1.1.4), Change Supervisor Password (section 3.1.1.4), Erase all Secure boot settings (section 3.1.1.4), Selector UEFI file as trusted for executing (in section 3.1.1.4), Restore secure boot to factory default (in section 3.1.1.4), Exit Saving Changes (section 3.1.1.6 and 5.4.4), Load Setup Default (section 3.1.1.6), Exit Discarding Changes (section 3.1.1.6 and 5.4.4), Load Factory Setup Defaults(section 5.4.4), Save Settings to User Setup Default(section 5.4.4), Load User Setup Defaults(section 5.4.4) 14. Modify External monitor description. (Section 4.1.5.2) 15. Secure boot factory default keys data need to reload after Crisis. (Section 1.2.4) 16. Modify TBT Wake from S4 Support description (Section 3.1.1.2)

REV. #	DATE	EXPLANATION OF CHANGE
1.31	2024/6/11	1. Remove Charge/Discharge relative define. (Section 4.1.18) 2. Provision for Copilot Key (Section 5.12.1) 3. Modify NFUB variable to FUB with different GUID (Section 1.2.4) 4. Remove Pre-allocate VRAM Size Section (Remove Section 4.1.5.3) 5. Add Dash and AIMT Support for AMD Pro (Section 5.4.2) 6. Add I2C HID / PS2 Switch in BIOS SCU (Section 3.1.1.2) 7. Add the temperature section to define for reading. (Section 3.1.1) 8. RF Button and Communication key Change for HID Keyboard (Section 4.1.1.4) 9. update display language for Ukrainian (Section 3.1.1.2) 10. Add CSR (Connected System Recovery) (Section 3.2.4) 11. Add Battery Information (Section 3.1.1.1) 12. Remove wake event while battery hit 6% under S0ix (Section 4.2) 13. Remove USB type A charge protect (Section 4.1.21) 14. Keep Password on Boot after RTC reset and crisis (Section 1.2.4)

1.Industry Specifications

INDUSTRY SPECIFICATION REQUIREMENTS	VERSION
Both of legacy BIOS and EFI architecture support	
PXE Specification version	2.1 or Later
SMBIOS Reference Specification	version 3.0 or later
USB Specification revision 1.1/2.0/3.0	V3.0 or later
ASF Specification	version 2.0 or later
PCI/PCI Express Base Specification	revision 3.0 or later
PCI BIOS Specification	revision 3.0 or later
BIOS Boot Specification	version 1.01 or later
Simple Boot Flag Specification	2.1 or Later
System Management Bus Specification	version 2.0 or later
AHCI support	

INDUSTRY SPECIFICATION REQUIREMENTS	VERSION
Microsoft XP/Vista/Windows 7/ Windows 8/win10 Windows Logo Program requirements	XP and above
Microsoft SLP 1.0 support	Latest
Microsoft OA 2.0/2.1 support	Latest
Microsoft OA 3.0 support	Latest
ACPI Specification	5.0 or Later
UEFI SPEC	2.6 or Later
Intel V-pro implementation	Latest
AMD Virtualization technology support and provide its options in BIOS Setup	Latest
Nvidia Optimus enabled	Latest
I2C	Latest
SMBUS	Latest
TCG Storage Security Subsystem Class:OPAL	SSC V2.01 rev.1.00 or Later

1.1 Brand System Identification

BRAND	SMBIOS TYPE 1 MANUFACTURER STRING CONTENT
Acer	Acer
Gateway	Gateway
Packard Bell	Packard Bell

BRAND	ALL OEM ID IN ACPI
Acer/Gateway/Packard Bell	ACRSYS

BRAND	ALL OEM TABLE ID IN ACPI
Acer/Gateway/Packard Bell	ACRPRDCT

1.2 Firmware Update

Platform must support a secure firmware update process that ensures only signed firmware components that can be verified using the signature database (and are not invalidated by the forbidden signature database) can be installed.

BIOS SCU settings should be kept after flashing, but crisis recovery no need to keep SCU settings.

1.2.1 Firmware Utility

- Utilities are provided to flash BIOS in project supporting OS environments
- Utility can self-execute and contains BIOS data for flashing.
- One single Flash utility to flash all SKUs.

1.2.2 Firmware Flash

	BEFORE FIRMWARE FLASH	DURING FIRMWARE FLASH	AFTER FIRMWARE FLASH
Behavior	The following should be prohibited to flash firmware • BIOS Binary is not intended for the system • AC or DC doesn't exist. • Battery capacity is lower than 25%. • If BIOS binary is not newer than system BIOS version,(Commercial BIOS "Rollback BIOS Version" option is Supported is an exception) • If Commercial BIOS "Lock BIOS Version" option is enabled • Other process or application are running which may conflict the firmware burning process • secure firmware update procedures are not implemented or met		• System Reboot
Message Display		• Display warning message reminds users: "Not to remove AC power source". • Display current flash progress and time elapse	

1.2.3 Crisis

This feature provides an opportunity for system that cannot boot up and this operation is not intended to be done by the customers. With a USB flash disk, the system can be performed crisis recovery by using keyboard or Boot Block DIP2 switch.

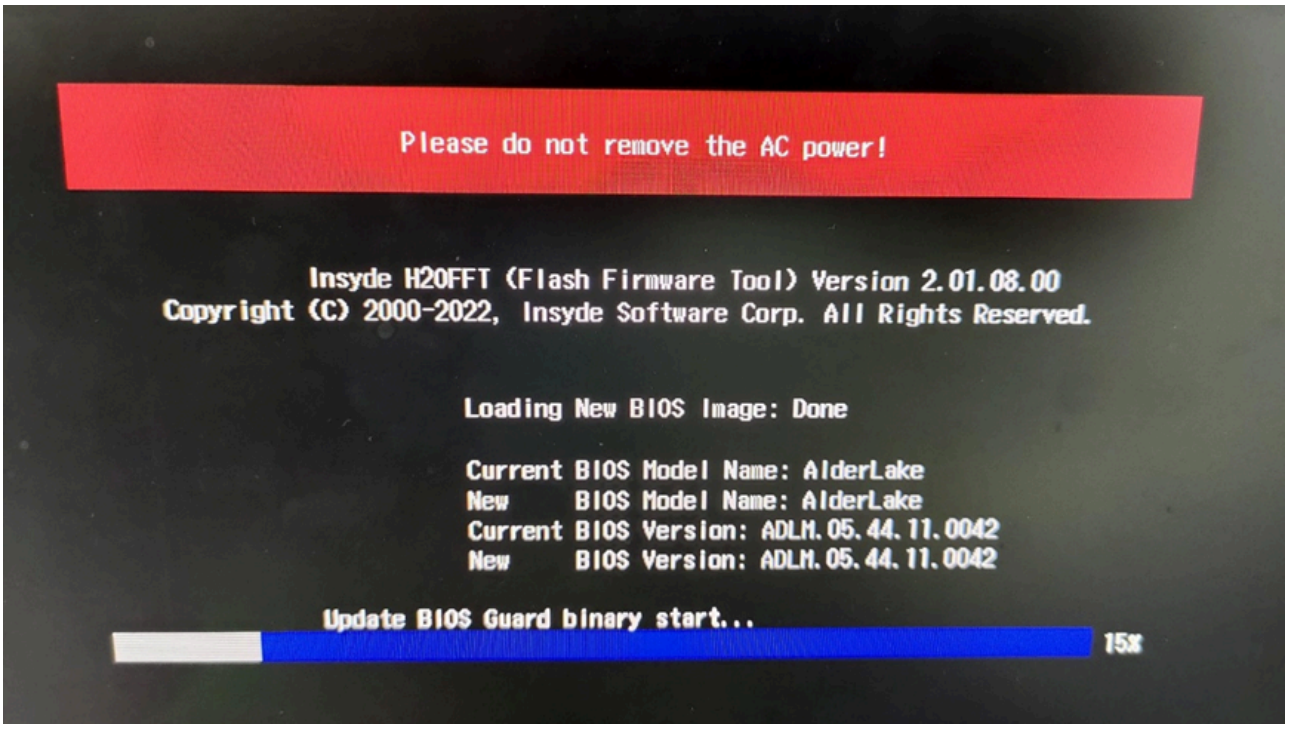
Flash ROM includes a special non-volatile region that can never be erased. This region, call the boot block (Note. 1), contains a fail-safe recovery routine. If the boot block finds corrupted BIOS,

Crisis Recovery also must meet the secure firmware update process described in Secure Boot section.

BEFORE FIRMWARE FLASH	DURING FIRMWARE FLASH	AFTER FIRMWARE FLASH
• Steps: Power off the system -> apply AC power source -> Plug-in the USB Flash Disk which contains BIOS crisis ROM file -> Power on the system from off state (i.e. cold boot) while holding down Fn + ESC key (Make sure AC adapter is powered and plugged-in) -> After POST, release Fn + ESC key. They system should boot from source and perform crisis recovery action. • secure firmware update process requirement must be met • Check if AC adapter is plug in	• Power LED flash every one second if system can't show crisis recovery progress on screen. • System will have screen to show crisis recovery progress. (Note.2)	• System Shutdown

Note.1 Boot block only refreshed when it is necessary to update by platform reference code change.

Note 2. Progress sample as below for reference.



1.3 Firmware capsule update

BIOS must enable capsule update support.

Please refer to Microsoft document 'Windows UEFI Firmware Update Platform.xps' for implementation details of system/device firmware update. Followings are additional requirement against the UEFI firmware capsule update.

System firmware (BIOS) must be deployed as driver package (INF).

If a device firmware could be upgraded by UEFI capsule, then the firmware should be deployed as device driver (installed via INF file).

Must specify a Firmware Resource in the EFI System Resource Table (ESRT)

- The Firmware Resource will allow Windows to surface a device instance with a Hardware ID, which will be used to target the system or device firmware update to appropriate systems and devices. It also describes current firmware version and provides status for previous updates.

- There exists a single entry for system firmware updates.

- All devices with updateable firmware must have a resource specified in the ESRT. Except if a device's firmware is updated as part of a system firmware update.

- Firmware capsule update must not rollback system/device firmware. In case of target version is equal to installed version, the firmware package must be re-flashed again.

- All key press and power button event can't be triggered during Capsule update

- Complete capsules include .INF, .FD and .CAT. The .CAT file is about signature and will be provided by Microsoft when Acer submits a legal and PASS WHCK report to Microsoft. Please refer to attached document of process between Acer and ODM about generate the capsule firmware WHCK report (.HCKX).

- BIOS must follow latest System Firmware Capsule Update SPEC to implement.

- BIOS must support Intel CSME/CSE capsule update and please follow System Firmware Capsule Update SPEC to implement. The change start from Tiger Lake, Jasper Lake and later platforms.

● All on board Device Firmware should meet power check criteria, the details please refer to System Firmware Capsule Update SPEC chapter 2.3.

● For devices with Enhanced Sign-in Security-capable USB cameras, BIOS should support firmware capsule and a Secure Devices (SDEV) table is required.

1.3.1 UI components of capsule update

Please refer to the chapter 4, 'UEFI firmwareupdateuserexperience' in Microsoft document 'Windows UEFI Firmware Update Platform.xps' for UI implementation details during capsule update.

l If the capsule update is handled by Windows loader, the UI component should have: Acer logo (same as POST screen) and update text by Windows loader, as the picture below shows (the display offset/percentage is only for reference). Progress Bar is required, but could be under or above the texts.

If the capsule is handled by BIOS code instead of Windows loader, the UI components should have Acer logo and update text as well. Attachment 'FlashBIOSUpdateText.zip' contains three picture of update text.

l In order to indicate users the device update is under processing, BIOS must show UpdateText-0.png picture in the 'FlashBIOSUpdateText.7z' until flash completed.

1.3.2 Capsule update require SMBIOS support

Since Windows requires certain information for windows update to identify the specific system to do the firmware update, BIOS needs to fill in the precise data into SMBIOS. All items list on Acer SMBIOS check list must be done.

To fulfill new MDA requirement, some SMBIOS definitions require changes below:

- Family (Sub brand) [Type 1] è *Ref Marketing Name of BOM , Length =50 characters, the string from BOM should not contain "Manufacture Name"*

- SKU Number [Type 1]à "0000000000000000" 16 "0"

- Baseboard Manufacture (Platform abbreviation) [Type 2]

- Baseboard Product (Remove SN) (Project Name =code name) [Type 2]

MDA 2017	**CHID-8**
Manufacturer	**Acer**
Product Name	**Aspire XXXX**
Baseboard Manufacture	**SKL**
Baseboard Product	**Project Name (Code Name)**

The content of Baseboard Manufacture will be filled in platform abbreviation listing below:

CHIPSET	**ABBREVIATION**
Panther Lake	PTL
Twin Lake	TWL
Lunar Lake	LNL
Arrow Lake	ARL
Meteor Lake	MTL
Raptor Lake/Raptor Lake-R	RPL

CHIPSET	ABBREVIATION
Alder Lake	ADL
Alder Lake-N	ADN
Rocket Lake	RKL
Tiger Lake/Tiger Lake-R	TGL
Comet Lake	CML
Amber Lake	AML
Ice Lake	IL
Whiskey Lake	WL
Canon Lake	CNL
Coffee Lake	CFL
Kaby Lake/Kaby Lake-R	KBL
Skylake	SKL
Broadwell	BDW
Haswell	HSW
Jasper Lake	JSL
Gemini Lake\Gemini Lake-R	GLK
Apollo Lake	APL
Braswell	BSW
Baytrial-M	BTM
Baytrial-T	BYT
BayTrial-T CR	BYT-CR
CherryTrail	CHT
CherryTrail-CR	CHT-CR
Carrizo	CZ
Carrizo lite	CZL
Beema	BE
Kabini	KB
Bristol Ridge	BR
Stoney Ridge/Stoney Ridge Refresh	SR
Raven Ridge	RR
Summit Ridge	SM

CHIPSET	ABBREVIATION
Pinncale Ridge	PRS
Picasso	PK
Renoir	RO
Dali	DL
Lucienne	LN
Cezanne	CZ
Pollock	PL
Barcelo	BC
Rembrandt / Rembrandt+	RB
Phoenix	PHX
Mendocino	MDC
Strix	STX
Mendocino	MDN
Hawk Point	HWK
Strix Halo	SHO
Granite Ridge	GNR
StrixPoint	SXP
Krakan	KRK

2.OS Support

SUPPORT OS
Linux
Android
Windows 8
Windows 8.1
Win 10
Win 10 S
Win 11
Win 11 Pro S

SUPPORT OS

Boot to UEFI Shell

2.1 Windows Secure Boot

- Windows secure boot requirement must be met according to the supporting OS.

- For selected project shipped with Linpus that support UEFI Secure Boot feature, Microsoft Corporation Third Party Marketplace Key and Acer Security Key must be added into BIOS.

- GUID for the key is “92fcafcd-c861-4b8b-aff2-a3d5a3e093f8”

2.2 Windows To Go

- In Windows To Go Startup Options under Windows 8, if “YES” has been selected for automatically boot system from a Windows To Go workspace and save changes, an USB class boot entry named “USB Entry for Windows To Go” will be generated as the 1st boot device in Boot Priority Order List (Boot Menu) and Boot Option Menu (F12).

- If user manually modifies the priority of “USB Entry for Windows To GO” from 1st priority to others, the option in Windows To GO Startup Options will be changed from “Yes” to “No” automatically by Windows 8.

- If “USB Entry for Windows To Go” is presented in 1st boot priority present and user select No in Windows To Go Startup Options under Windows 8, “USB Entry for Windows To Go” entry will be removed from Boot Priority Order List and Boot Option Menu by Windows.

2.3 Windows Modern Standby (Connected Standby/Disconnected Standby)

Windows 10 Modern Standby (MS) expands the Windows 8.1 Connected Standby power model. In Modern Standby, the PC uses the S0 low power idle model. Modern Standby has the flexibility to configure the default behavior to limit network activity while in the low power state.

Windows 10 reduces power consumption by the OS and only wakes from the lowest power state when absolutely necessary. With Modern Standby, the system wakes when there is real time action required, such as OS maintenance, or a user wakes the system.

Modern Standby is available for both Windows 10 desktop and Windows 10 Mobile.

2.3.1 Platform design requirements for modern standby

In order to meet modern standby requirements, besides the selection of the SoC chip, DRAM, networking device, and other key hardware components.

Here are some additional platform requirements for enabling modern standby on Windows 8 and higher that needs System firmware developer to implement

•The system ACPI firmware must set the ACPI_S0_LOW_POWER_IDLE FADT flag to indicate the platform hardware supports the low-power idle mode for modern connected standby.

•The system ACPI firmware must not provide an S3 object in the root of the namespace. Windows supports a platform exposing either the S3 object or the ACPI_S0_LOW_POWER_IDLE FADT flag, but not both at the same time. Note The FADT bit takes precedence over an S3 object.

•For non-Intel based platforms, the core silicon or SoC manufacturer must provide a power engine plug-in (PEP) that coordinates device state and processor idle state dependencies. A minimal PEP is required to communicate to Windows when the device power state dependencies have been achieved for the lowest SoC idle power mode.

•x86/x64-based modern connected standby PCs must also support Hibernate. Hibernate is used to save the state of desktop/Win32 applications when critical-low battery capacity is reached.

2.3.2 Battery control

Battery charging needs to behave like in normal operating. As well as all the battery information reported to the OS.

2.3.3 Fan & thermal

Fan needs to be turned off while in MS. And all MS systems with fans must expose its activity to the OS.

Though system wouldn't heat up while it is in MS, EC still needs to monitor CPU temperature. And EC can judge to turn on fan and force shutdown system while something goes wrong and the temperature of system keep over threshold for safety concern.

2.3.4 LED

For LED definition and behavior, please refer to the latest document Acer Indicator Spec. It will be released by Acer SWPM team.

2.3.5 Keyboard Backlight

The backlight of keyboard for platforms support connected-standby and bundle a keyboard with backlight (no matter the driven method of its light source). While resuming, unlike other LEDs which only restore their previous status, the keyboard backlight need to follow "ACER ALS design PES" and recalculate what's the level it should be.

2.3.6 Power-off USB Charge

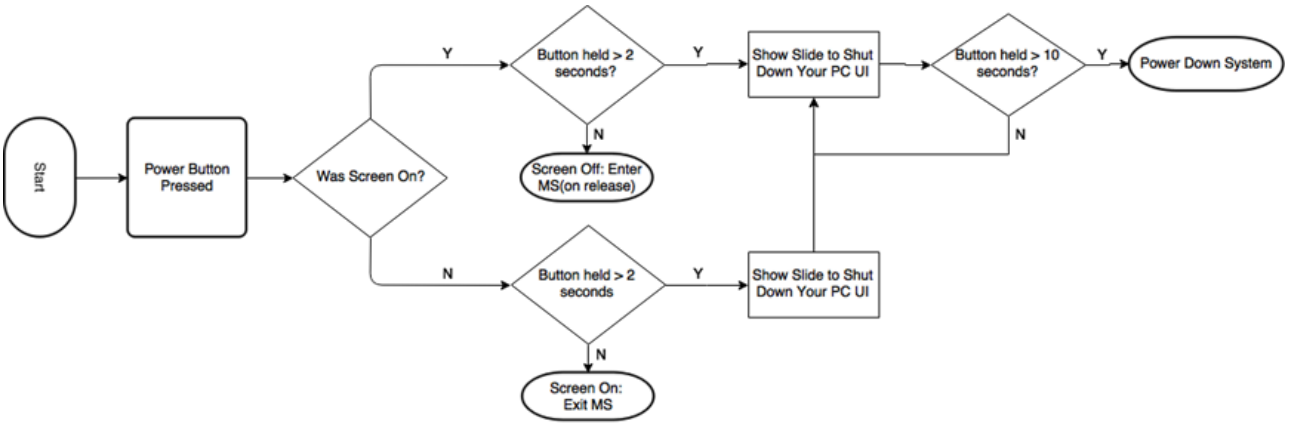
For some specific platforms will support power-off USB charge feature. These platforms can supply USB bus power (DC 5V) to the specific USB port even when the computer is in MS/S4/S5 states. When this feature is enabled, the power-off USB charge port can for USB wakeup. When using battery power and less than battery threshold (%), the USB charge port should not support USB charge and wake.

MS platform USB charge port behavior will follow non-MS platform USB charge behavior under S3. Please refer to NB_UEFI_BIOS spec for detail.

2.3.7 Power Button Behavior

To prevent hard power off which causes complete data loss, MSFT recommended support shutdown slider feature. When press power button and hold over 2 seconds, the screen will pop up "Slide to shut down your PC" message. The operating system must be able to reliability detect and distinguish power button down press and power button up release events. With these two events, OS can determine the elapsed time between press and release to show the shutdown slider UI and take appropriate action before system power down.

The flowchart to describe the user experience. And Intel HID event filter driver allows the SBIOS to send Intel HID messages and button events to the operating system for various key presses. Follow latest "Intel HID Event Filter Release Notes and Bring Up Guide" to implement the feature.



2.3.8 Modern Standby Indicator

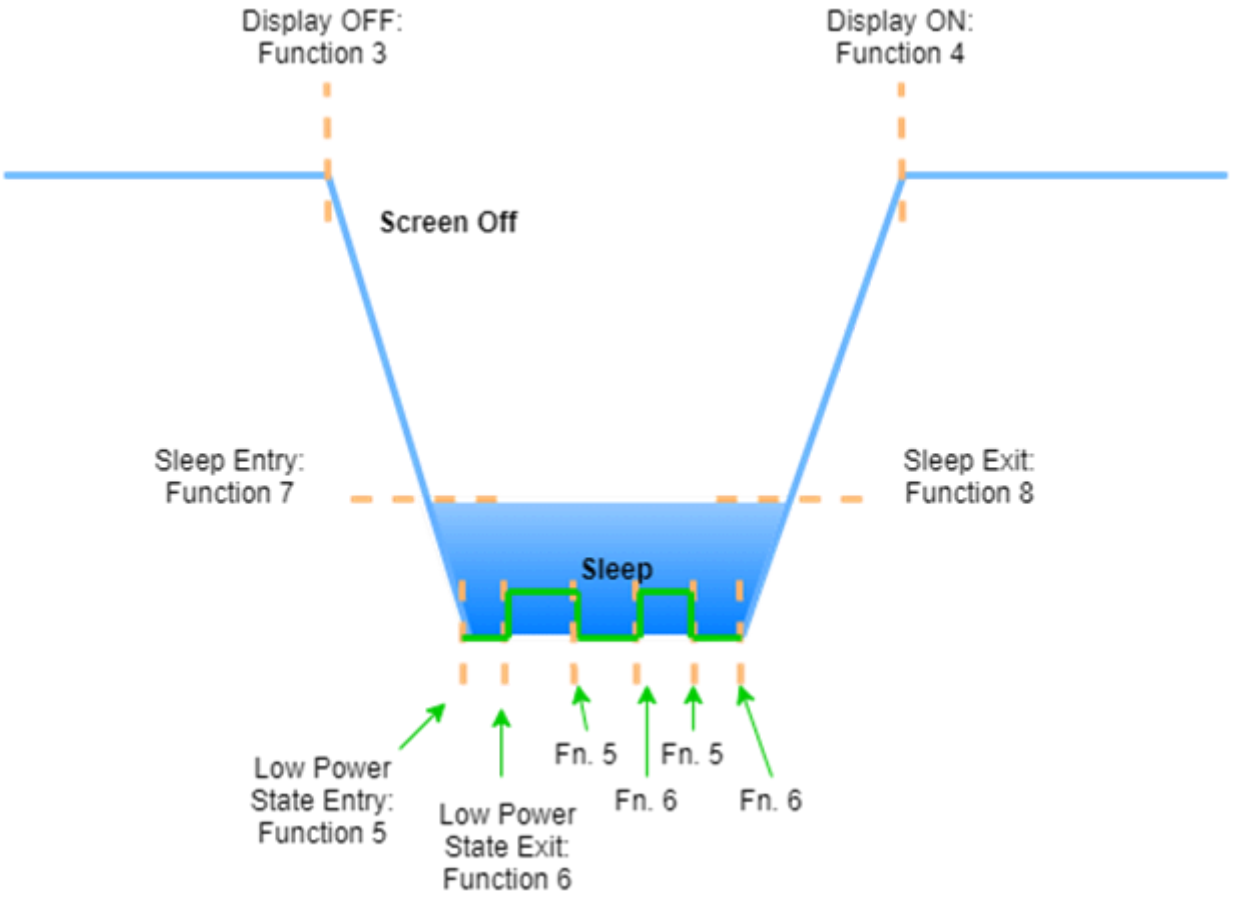
In order to make the system indicator consistent when modern standby enter/exit, MSFT provides _DSM (Device Specific Method) functions that can be used by the OS to interact with BIOS for power and functionality optimizations.

The ACPI device must be exposed through the Namespace. The device must include a _CID object containing EISAID (“PNP0D80”) and contain the following _DSM definition.

BIOS has to use function 7 & 8 to mirror behavior from S3, like as LED behavior, fan behavior and etc. For more detail implementation guidance, please refer to MSFT “Modern Standby System States and Transition Notifications” document and should use the **20H1 8C** release and newer OS revision to implement the function.

When the system enters modern standby and the value-adding software activities still run intermittently. And the system state is under Low Power Phase, all indicators turned off is normal.

UUID	REVISION	FUNCTION	DESCRIPTION
11E00D56-CE64-47ce-837B-1F898F9AA461	0	0	Enumerates Functions
0	3	Display Off Notification	
0	4	Display On Notification	
0	5	Lowest Power State Entry Notification	
0	6	Lowest Power State Exit Notification	
0	7	Sleep Entry Notification	
0	8	Sleep Exit Notification	



2.4 Windows OEM Activation

PRIORITY	OS SKU	SLP 1.0	OA2.1 +SLIC TABLE	OA3.0
2	Win10 Standard		X (note1)	V
2	Win10 Pro (Downgrade Right)		X (note1)	V
2	Win10 Pro (National Academic)		X (note1)	V
1	Win10 with family: CHT,CHT-CR,BYT,BYT-CR (note2)		X	V
3	Non Windows OS	X	X(note1)	X

Note1: Both SLIC table and OA2.x key should still implement but hidden, can be active for special cases, never remove them for both commercial & consumer projects.

Note2: Specific platform don't support legacy mode. Reference to section 1.3.2 Baseboard Manufacture definition in SMBIOS type2

SLP 1.0	OA2.1	OA3.0
• System supports SLP1.0 should satisfy SLP1.0 requirements • The SLP string is a constant and should be stored in BIOS segment F. • The SLP String: "AcerSystem" should be put in address range from F000:0000 to F000:FFFF. The way to verify the string existence, uses Microsoft debug tool—Debug.exe to search the SLP string with the specified memory range.	System supports OA2.1 should satisfy “OA2.1 OEM Activation 2.1 for Windows® Operating Systems”, and “OEM SLIC Table Implementation for non-Windows® PC Systems”, and requirements. • The values of OEMID and OEMTableID in the Windows Marker and the ACPI_SLIC header must match the OEMID and OEMTableID in either the ACPI RSDT or XSDT header.	• DPK can be inject into ACPI MSDM table • System supports OA3.0 should satisfy OA3.0 requirements from OA3.0 white paper, and OA3.0_Flash Utility Guide

3. Acer BIOS Feature

3.1 Setup Menu

3.1.1 BIOS Setup Menu

Acer Setup Menu’s resolution is set to panel default.

The System Temperature should read the Board Sensor on system, and the temperature required to show on Right field of Setup menu. The actually board sensor need to consult thermal RD to realize the temperature to display. For the abridged general view attached in BIOS_GUI_20230519.7z, the purpose is to identify the look and feel for sub menu or pop up screen. The exactly options displayed depends on system design and latest BIOS SPEC definition for the setup menu. The graphic layout should reference the defined from UI/UX

3.1.1.1 Information Tab

PRODUCT INFORMATION	EXAMPLE	REMARK
CPU Info	Intel® Core™ i5-2450M CPU	· Should be same with processor brand string.
Core Frequency	2.50 GHz	· Display Processor Base Core Frequency.
System BIOS Version	V1.00	· Should be same with SMBIOS Type 0 Offset 05h.
VGA BIOS Version	Intel V2137	· VGA BIOS Version will only be shown when Boot Mode is [Legacy]. · dGPU doesn't support VBIOS version display
GOP Version	Intel ® GOP Driver [2.0.34.1016]	· GOP Version will only be shown when Boot Mode is [UEFI]. · dGPU doesn't support GOP version display
HDD/eMMC/UFS Model Name	WDC WD3200BEK	· This item show the model name of HDD/eMMC/UFS installed. · The hard disk model name is automatically detected by the system. If there is no hard disk present or unknown type, "None" should be shown on this field. · For multiple storage, add number after HDD starting from 0 · If storage leverage OPAL protocol, add (OPAL) for identification
HDD/eMMC/UFS Serial Number	WD-WXL 1A9103553	· This item will show the serial number of HDD/eMMC/UFS installed. · If no hard disk or other devices are installed, "None" should be shown on this field. · If system has more than 1 device, the item should be listed as below: Ex: HDD0 Model Name HDD0 Serial Number HDD1 Model Name HDD1 Serial Number · If storage leverage OPAL protocol, add (OPAL) for identification
ATAPI Model Name	PIONEER BD-ROM BCD3	

PRODUCT INFORMATION	EXAMPLE	REMARK
SATA Mode	AHCI	· Display SATA Mode setting. Mapping to BIOS setup option. · If platform support VMD, the SATA mode item should be hidden.
Total Memory	2048 MB	· The field reports the system total installed memory
On Board Memory Vendor	Micron	· Should show the vendor of memory manufacturer · Also show the information of Memory type · If there is no On Board Memory design, hide this item.
On Board Memory Size	16384 MB	· Should same as the summary of all Type 17 which the form factor (offset 0x0E) is 0x0B in SMBIOS · If there is no On Board Memory design, hide this item.
On Board Memory Speed	3200 MHz	· Identifies the configured speed of the memory device. · If there is no On Board Memory design, hide this item.
On Board Memory Voltage	500 mV	· Identifies the configured voltage of the memory device. · # means memory's number. If there is only one memory on board, hide this item.
Memory # Vendor	Micron	· Should show the vendor of memory manufacturer · Also show the information of Memory type · # means memory's number. If there is only have on board memory, hide this item.
Memory # Size	4096 MB	· Shows each size of onboard/installed memory. · # means memory's number. If there is only have on board memory, hide this item.
Memory # Speed	3200MHz	· Identifies the configured speed of the memory device. · # means memory's number. If there is only have on board memory, hide this item.

PRODUCT INFORMATION	EXAMPLE	REMARK
Memory # Voltage	500 mV	· Identifies the configured voltage of the memory device. · # means memory's number. If there is only have on board memory, hide this item.
Serial Number	22 characters	· Should be same with SMBIOS Type 1 Offset 07h.
Asset Tag Number	22 characters minimum	· Should be same with SMBIOS Type 3 Offset 08h.
Product Name	Acer Brand Example - (Aspire) Aspire XXXX - (TravelMate) TravelMate XXXX -(Aspire One) Aspire One XXX -(Iconia) ICONIA XXXX -(N/A) XXXX	· Should be same with SMBIOS Type 1 Offset 05h. · Product Name is defined by project POR. · The string is case sensitive and the maximum length is 50 bytes.
	Gateway Brand Example - (N/A) XXXX	
	Packard Bell Brand Example - (EasyNote) EasyNote XXXX - (N/A) XXXX	
Manufacture Name	Acer/Gateway/Packard Bell /Founder	· Should be same with SMBOS Type 1 Offset 04h. · The string is case sensitive.
UUID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	· It is required for all systems. · Display format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (follow UUID Standard)
DFCI/ABST support	DFCI/ABST	· This item default should be hidden · Only visible after user press "Service key" in this page (Information Tab) · This item just reminds the user whether the system supports DFCI or ABST · The default value is ABST
Manufacture Date	2023/05/09	· This item should be the battery Manufacturing Date
First Use Date	2023/12/15	· This Item should be the date of user first time to utilize battery resource

PRODUCT INFORMATION	EXAMPLE	REMARK
Health	100%	· The battery health indicator · This item required with a help string under line “Battery health may rise or fall depending on the state of the last charge/discharge cycle.”
Battery Temperature	29 ℃	· Show the temperature of battery
Cycle Count	6	· Show the battery charge cycle count. · This item required with a help string under line “Due to quality inspection before shipping, the figure may not be zero on first use.”

3.1.1.2 Main Tab

ITEM NAME	EXAMPLE	REMARK
System Time	HH:MM:SS	· The format is the number of string. · The hours are displayed with 24 hour format. · The values set in the two fields take effect immediately.
System Date	MM/DD/YY	
Network Boot	[Enabled] / [Disabled]	• Default Network Boot value in different Boot Mode: - [UEFI] Boot Mode : [Disabled] - [Legacy] Boot Mode : [Enabled]
F12 Boot Menu	[Enabled] / [Disabled]	• This function enables or disables the ability that user can press F12 while POST to quickly select boot device. • The boot device change is only for one time change. In other words, the next time system reboots, the boot device sequence will be the same as the one defined in the BIOS Setup Utility -> Boot Menu. • The default value is [Disabled]

ITEM NAME	EXAMPLE	REMARK
SATA Mode	Intel:[AHCI] / [Optane without RAID]/[Optane with RAID] AMD: [AHCI]/[RAID]	· This item default should be hidden. · Only visible if the platform support the function after user press “Ctrl” + “S” in this page (Main Tab). · Default set to [Optane without RAID] if system is Optane ready but required RAID function · Default set to [Optane with RAID] if project features support RAID SKU (AMD platform set to [RAID]) · Remove “Optane with RAID” option if project doesn’t require RAID · Default set to [AHCI] if project doesn’t require Optane or RAID support. · If platform support VMD, this item should be replaced by [VMD Controller].
VMD Controller	[Enabled] / [Disabled]	· This item default should be hidden. · Only visible if the platform support the function after user press “Ctrl” + “S” in this page (Main Tab). · VMD stands for Intel Volume Manage Device Bootcamp. · The detail VMD configuration should depends on actual HW layout. · The default value is [Enabled].
NVMe RAID mode	[Enter]	· This item default should be hidden. · Only visible if the platform support the function after user press “Ctrl” + “S” in this page (Main Tab). · Enter NVMe RAID mode page
Re-Size BAR Support	[Enabled] / [Disabled]	· This item default should be hidden · Only visible if the platform support the function after user press “Ctrl” + “S” in this page (Main Tab) · Default set as [Enabled] if project requires to support NVIDIA resizable BAR or AMD smart access memory. Otherwise, default set as [Disabled]
Wake On LAN	[Enabled] / [Disabled]	· Wake on LAN feature allows someone to turn on a network computer remotely by sending Magic Packet even if system is in off state. · The default value is [Disabled]. · Panel off when wake on LAN
TBT Wake	[Enabled]/[Disabled]	· Enable/Disable S3 wake capability of TBT · The default value is [Enabled]
TBT Wake from S4 Support	[Enabled]/[Disabled]	· Support TBT wake from S4 · This option allow to combine with “USB Wake from S4 Support” if platform cannot separate individual XHCI controller. · The default value is [Disabled]

ITEM NAME	EXAMPLE	REMARK
USB Wake from S4 Support	[Enabled]/[Disabled]	· Support USB wake S4 · The default value is [Disabled]
Function key behavior	[Function Key] / [Media Key]	· [Media Key]: Perform the media function by default. Hold the key to activate F1 to F12 · [Function Key]: Activate F1 to F12 by default, Hold the key to perform media function. · Media functions are only active under Windows. F1 to F12 act as normal function keys during device boot or while in BIOS. · Default setting depends on product line definition. · Built-in USB keyboard/ 5 ROW keyboard layout follow keyboard's design and no need to add BIOS switch
Lid Open Resume	[Enabled]/[Disabled]	· System will resume from S3 state by Lid open. · The option is only visible and working on non-modern standby supported system · The default value is [Enabled]
Wake on USB while lid closed	[Enabled]/[Disabled]	· If enabled, USB devices can wake the system, even if the lid is closed · *The option grey out on modern standby supported system when "USB wake from S4 Support" disabled* · The default value is [Disabled]
D2D Recovery	[Enabled] / [Disabled]	· This function enables/disables Acer disc-to-disc Recovery. · To do Acer disc-to-disc system recovery via Alt+F10 key during POST.
xHCI Support	[Enabled] / [Disabled]	· For product routes all 14 ports to xHCI Controller or USB 3.0 port only system (Not a requirement if the platform supports xHCI debug) · xHCI Support should follow behavior: [Enabled]: Enable xHCI [Disabled]: Disable xHCI and enable eHCI. · The default value is [Enabled]. · Hidden the option if platform only exist one of the controller (xHCI or EHCI) alone.

ITEM NAME	EXAMPLE	REMARK
POST Animation & Sound	[Enabled] / [Disabled]	· The option is only for the project supporting POST Animation & Sound. The purpose is to enable/disable POST Animation & Sound effect · The default value is [Enabled]. · [Enabled]: Enable POST Animation & Sound · [Disabled]: Disable POST Animation & Sound
Sound	[Mute] / [Unmute]	· The option is only for the project supporting POST Animation & Sound. The purpose is to mute/unmute the sound of POST Animation · The default value is [Unmute]. · [Mute]: Mute POST Animation Sound · [Unmute]: Unmute POST Animation Sound · Grey out the option if disable POST Animation & Sound. Leave the setting no change when greying out
Keyboard backlight timeout	[Enabled] / [Disabled]	· The option only exists for the product support keyboard backlight and controlled by EC (USB keyboard not support) · When the option set to “Disabled”, keyboard backlight stay on no matter AC/DC. · The default value is [Enabled].
Internal KB Numpad	[Enabled] / [Disabled]	· The option only exists for the product using the keyboard with combination Numpad sharing the location with letter. · When the option set to “Disabled”, internal keyboard Numpad worked as normal letter key even turning on “Numlock”. · The default value is [Enabled].
Fast Boot	[Enabled] / [Disabled]	· Enable/Disable Fast Boot. · skip timeout variable when Fast Boot enabled · The default value is [Enabled].
Display Language	[English]	· BIOS display language · BIOS supports 14 languages, which are English / Spanish / Chinese / German / Dutch / Brazilian Portuguese / Danish / Italian / Norwegian / Swedish / Russian / France / Kazakh / Ukrainian · The default display language is [English]
Keyboard	[HID I2C] / [PS2]	· The option is only support while the project supporting HID I2C Keyboard. The purpose is to switch HID I2C and PS2 interface. · The default value is [HID I2C] mode. · This option is always hidden, and only visible after press service key.

Sub-menu of NVMe RAID mode:

ITEM NAME	EXAMPLE	REMARK
NVMe RAID mode	[Enabled] / [Disabled]	• NVMe RAID follow AMD design • When set to disabled, below items will be hidden; When set to enabled, reboot the system once, and below items will appear • When set to enabled, allow user to adjust RAIDXpert2 Configuration as the following items • The default value is [Disabled]
Controller Management	Follow CRB Setup options	• Managers controller properties
Array Management	Follow CRB Setup options	• Display Array properties and performs operations such as create, delete
Physical Disk Management	Follow CRB Setup options	• Displays physical disk properties and performs operations such as assign/unassign hot spare

3.1.1.3 Advanced Tab

ITEM NAME	EXAMPLE	REMARK
VTX	[Enabled] / [Disabled]	· This is Intel VTX function switch · Display when platform support the function · The default value is [Enabled].
VTD	[Enabled] / [Disabled]	· This is Intel VTD function switch · Display when platform support the function · The default value is [Enabled].
Active Efficient Cores	[Enabled] / [Disabled]	· With Intel Hybrid CPU architecture, appears "Active Efficient Cores" for E-Core(Small Core). It can control all Efficient Cores to active or inactive. · The default value is [Enabled].
GNA Device	[Enabled] / [Disabled]	· This option only appears when system is Intel CPU which support GNA device. · The default value is Enabled
AMD-SVM	[Enabled] / [Disabled]	· This is AMD Secure Virtual Machine function switch · The default value is [Enabled]. · Always hidden this option.

ITEM NAME	EXAMPLE	REMARK
AMD-IOMMU	[Enabled] / [Disabled]	· This is AMD input/output memory management unit function switch · The default value is [Enabled]. · Always hidden this option.
TBT Detection Gain	[Enabled] / [Disabled]	· This item default should be hidden. · Only visible after user press “Ctrl” + “S” in this page (Advanced Tab). · For all the tuning settings to support multiple layer TBT devices detection, combined all settings into this option. When it set to “Enabled”, all settings take effect. · Display when platform support Thunderbolt · The default value is [Disabled].
Storage Device Configuration		· Enter to configure storage device port enable/disable (such as SATA/PCIE storage device port) · Only visible if system set to AHCI
Display mode	[Auto Select] / [Optimus] / [Nvidia GPU only]	· This is for Nvidia discrete GPU. · The default value is [Auto Select] if project SKU supports Nvidia DDS function. Otherwise the default value is [Optimus] and [Auto Select] option should be hidden. · If user select [Nvidia GPU only], pop up warning message to inform user, and message should be “Type-C DisplayPort could not be available in this mode.” (This message is not required if all Type-C DisplayPort works under Nvidia GPU only mode.)
Display mode	[Int Graphics (IGD)] / [Ext Graphics (PEG)]	· This is for AMD discrete GPU which support Hybrid Graphic function for BIOS static Mux configuration. · This item default should be hidden and visible after user press “Ctrl” + “S” in the page. · The default value is [Int Graphics (IGD)]. · If project SKU does not support eDP display from discrete GPU, hide this item.

Sub-menu of Storage Device Configuration:

ITEM NAME	EXAMPLE	REMARK
HDDx/eMMC/UFS Port	[Enabled] / [Disabled]	· Enabled/Disabled the device connected port · HDDx/eMMC/UFS mapping to HDD0/HDD1/eMMC/UFS……displayed on information tab · The default value is [Enabled]. · If storage leverage OPAL protocol, add (OPAL) for identification

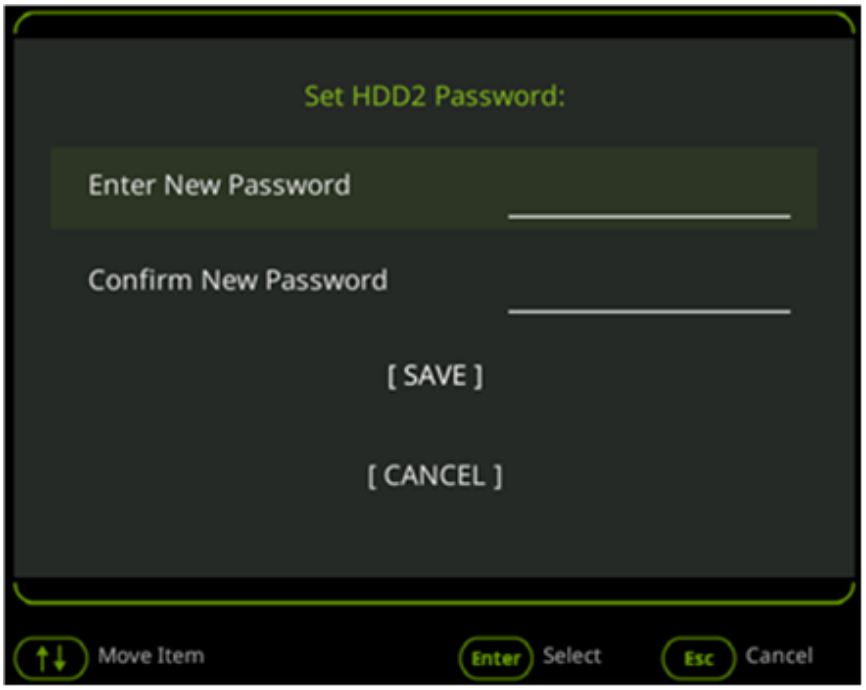
Note: The scope of the storage devices showing here is defined as the ports actually could connect devices. Once port disabled, BIOS would display the device as HDDx//eMMC/UFS in advanced page and information page.

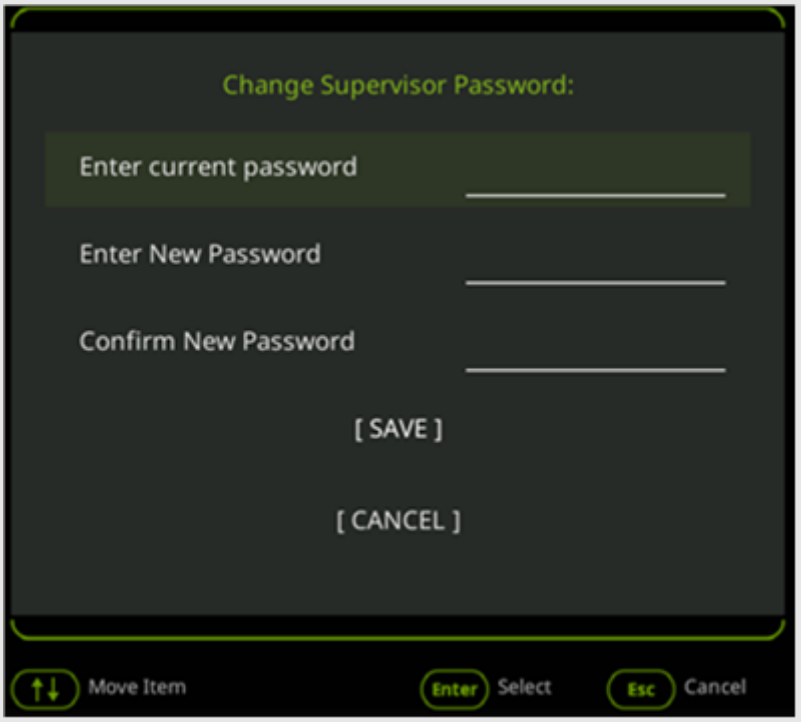
3.1.1.4 Security Tab

For action required a password setup, item display should not be hidden; the item is displayed as gray out item. Systems without TPM/ TCM, "Current TPM (TCM) State", "Change TPM (TCM) State" and “Clear TPM (TCM)” setup option should not exist in the setup page.

For item related to Secure Boot feature, please refer Secure Boot feature requirement below.

The following is Security Menu if both of the passwords are disabled, or enter Supervisor password when password is enabled.

ITEM NAME	EXAMPLE	REMARK
Set Supervisor Password Set User Password Set HDD Password	[Enabled] / [Disabled]	[Disabled] means password is not set. After set password, item value will be change to [Enabled]. If Supervisor Password it not set, Set User Password should be a grayed out item. After press [Disabled], pop up a window to ask user to enter new password. Refer to following picture.  If there is an old password, pop up a window to ask user to enter old password first. If the password entered does not match old password, pop-up warning message “Invalid password”. If the password entered match old password, the password will be clear and change the item to disabled. For the format of the password, please refer “Valid Password Characters” in Security Feature – Password section.

ITEM NAME	EXAMPLE	REMARK
Change Supervisor Password Change User Password Change HDD Password	[N/A]/ [Change]	[N/A] means password is not set. After set password, item value will be change to [Change]. After press [Change], pop up a window to ask user to enter current password. Refer to following picture.  User should enter current password first and then type new password in field “Enter New Password”, and re-enter password in field “Confirm New Password” for verification. If the verification is OK, password setting is complete after user pressed enter. If the current password entered does not match the actual current password, pop-up warning message “Invalid password”. If the new password and confirm new password do not match, pop-up warning message “Password do not match” For the format of the password, please refer “Valid Password Characters” in Security Feature – Password section.If system has more than 1 HDD, HDD password items that listed on the Security Menu should be as below: Set HDD0 Password Change HDD0 Password Set HDD1 Password Change HDD1 Password
Password on Boot	[Enabled] / [Disabled]	Defines whether a password is required or not while the events defined in this group happened. Password on Boot option requires the Supervisor Password. During login, this should be grayed out if the User Password was used to enter BIOS Setup Utility. Allows user to specify whether or not a password is required to boot. The default value is [Disabled]

ITEM NAME	EXAMPLE	REMARK
Current TPM (TCM) State (For TPM 1.2)		This field indicates current TPM (TCM) State. Current TPM or TCM State description is according current TPM or TCM is connected. Current TPM (TCM) State is displayed on BIOS Setup Utility no matter Supervisor /User Password is set or not and is grayed out item that can't be modified manually.
Change TPM (TCM) State (For TPM 1.2)	[No Change] / [Enable & Active] / [Deactive & Disable]	Change TPM or TCM State description is according current TPM or TCM is connected. Change TPM (TCM) State is displayed on BIOS Setup Utility no matter Supervisor / User Password is set or not. If Supervisor Password is not set, it should be a grayed out item. Default TPM (TCM) state is set to [Enabled] and requires Supervisor Password to change the state. Change TPM (TCM) state will support the items list in left.
Current TPM (TCM) State(For TPM 2.0)		This field indicates current TPM State. Current TPM or TCM State description is according current TPM or TCM is connected. Current TPM State is displayed on BIOS Setup Utility no matter Supervisor /User Password is set or not and is grayed out item that can't be modified manually.
Change TPM (TCM) State(For TPM 2.0)	[Enabled] / [Disabled]	Change TPM State is displayed on BIOS Setup Utility no matter Supervisor / User Password is set or not. If Supervisor Password is not set, it should be a grayed out item. Default TPM state for UEFI Mode is set to [Enabled] and requires Supervisor Password to change the state. [Disabled]: BIOS don't initial TPM 2.0 device and hide the TPM 2.0 device in ACPI table, it makes no TPM device in Windows device manager. Change TPM state will support the items list in left.
Clear TPM (TCM)	[Clear]	Change TPM State is displayed on BIOS Setup Utility no matter Supervisor / User Password is set or not. If Supervisor Password is not set, it should be a grayed out item.

ITEM NAME	EXAMPLE	REMARK
TPM Device Selection	[iPTT] / [dTPM] /[PSP fTPM] / [Pluton fTPM]	[iPTT]: Intel PTT. [dTPM]: Discrete TPM only. [PSP fTPM]: AMD PSP firmware TPM. [Pluton fTPM]: If the project region is for WW, the default value is [dTPM] or [Pluton fTPM]. Only visible on AMD platform which support Pluton. If project only support one type of TPM, the item should be removed. If the project region is for China, the default value is [iPTT], [PSP fTPM] or [Pluton fTPM]. Only visible on which support Pluton platform. If project only support one type of TPM, the item should be removed. This item should permanently grayout and cannot be load default.
Authorized Signatures	[Enabled] / [Disabled]	This item default should be hidden. Only visible after the Secured-core PC identifier variable “BuiltAsSecuredCorePC” be set to non-zero value. [Enabled]: Load MSFT 3rd Party UEFI CA. [Disabled]: Do not load MSFT 3rd Party UEFI CA and gray out “Select and UEFI file as trusted” option.
Reinstall Windows from cloud	[Recover this device]	This item should display if project support Microsoft cBMR function.

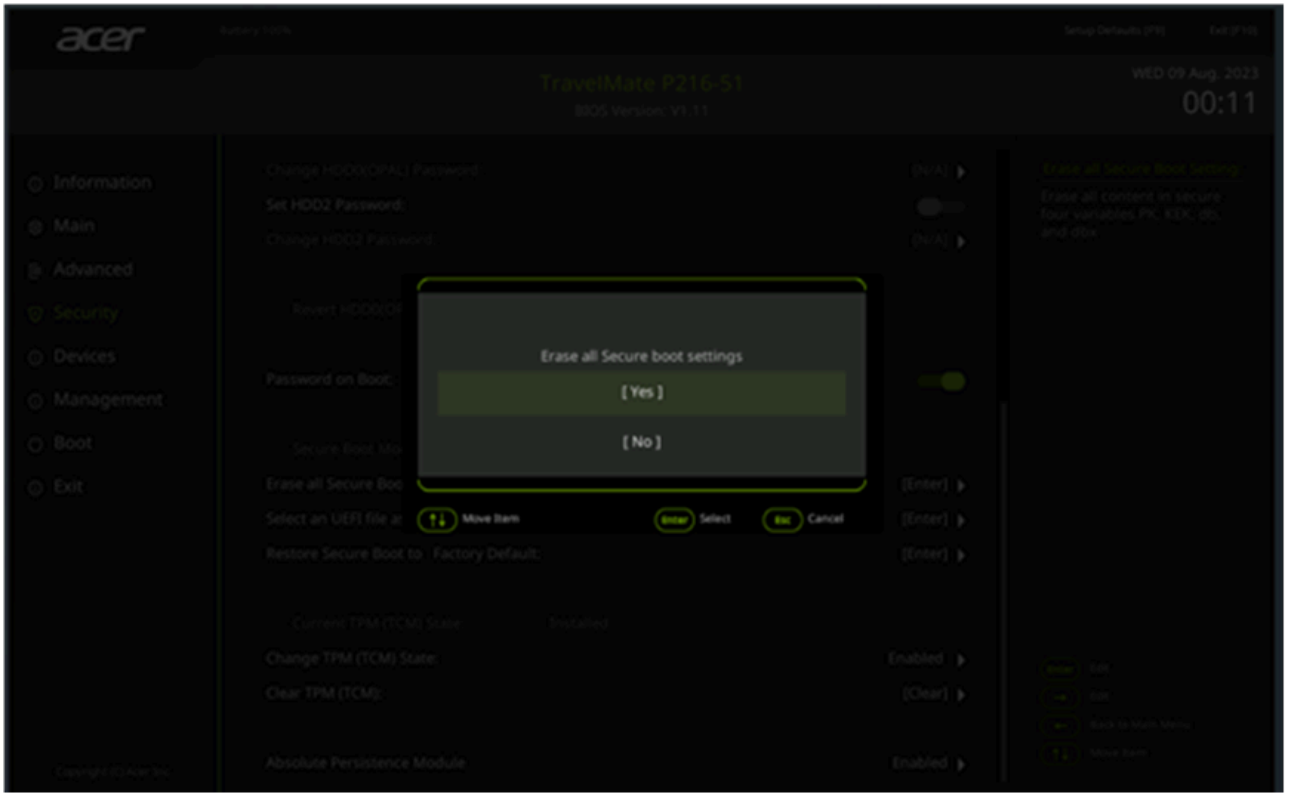
As long as supervisor password set, TPM state could be changed. User password is not required to modify TPM setting.

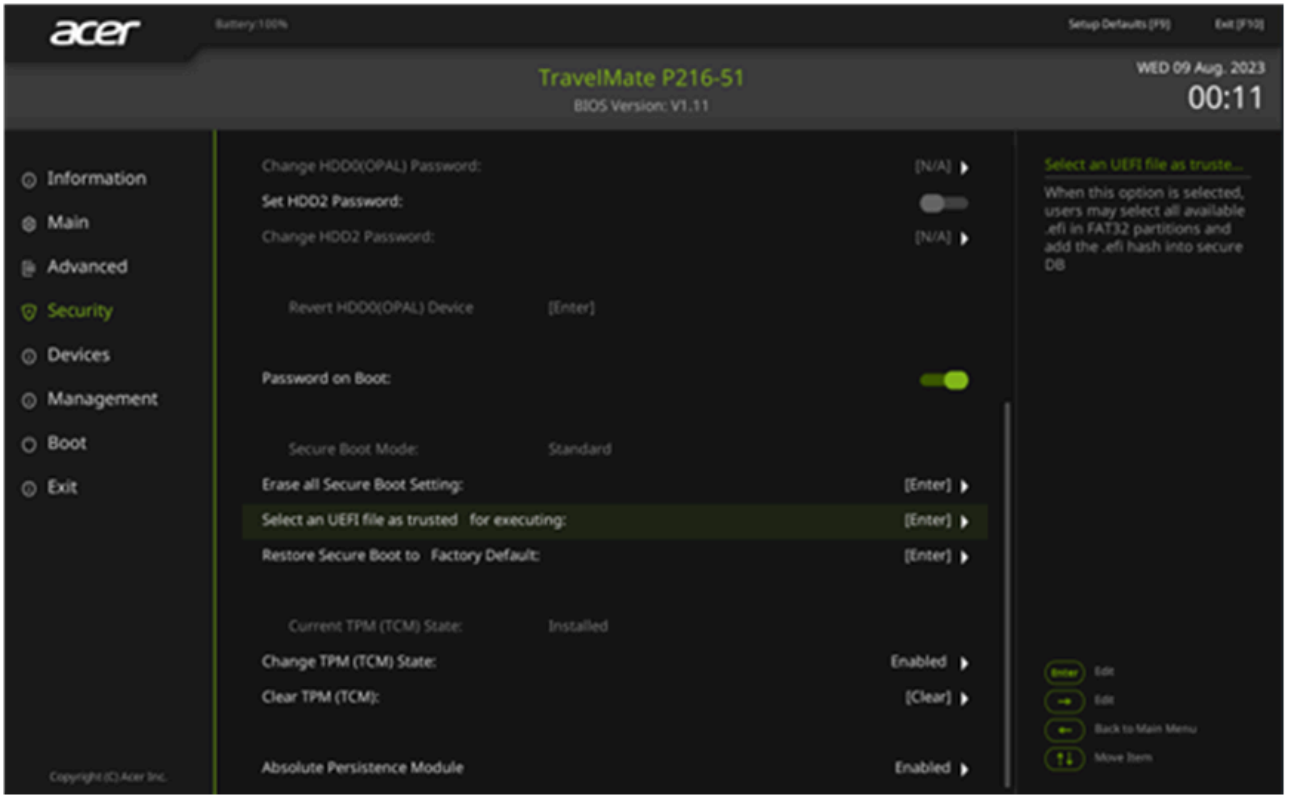
BIOS doesn’t need to forbid the HDD password modification even when HDD is in frozen state.

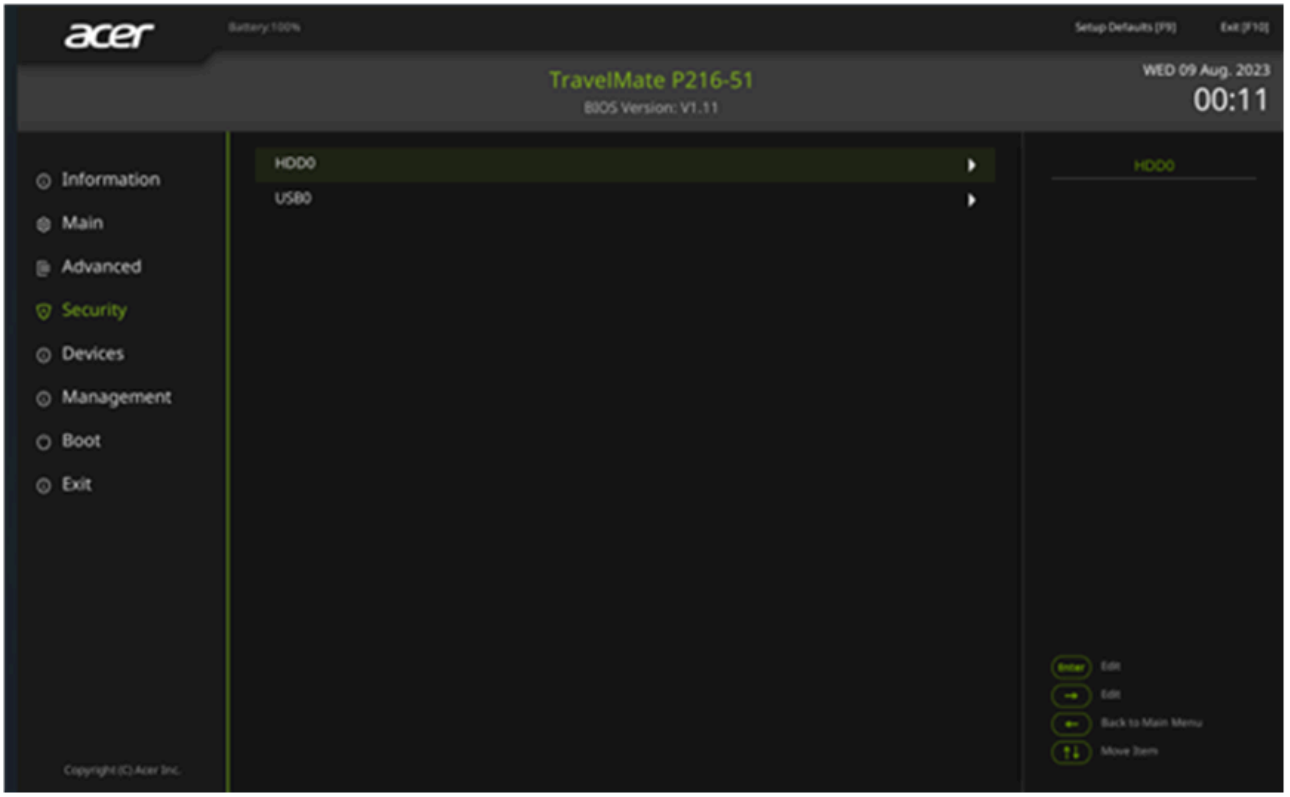
Following UEFI Secure Boot Feature is only available in BIOS Setup Utility if Boot Mode is [UEFI] and will be hid if Boot Mode is [Legacy]. The entire item must also follow below requirements.

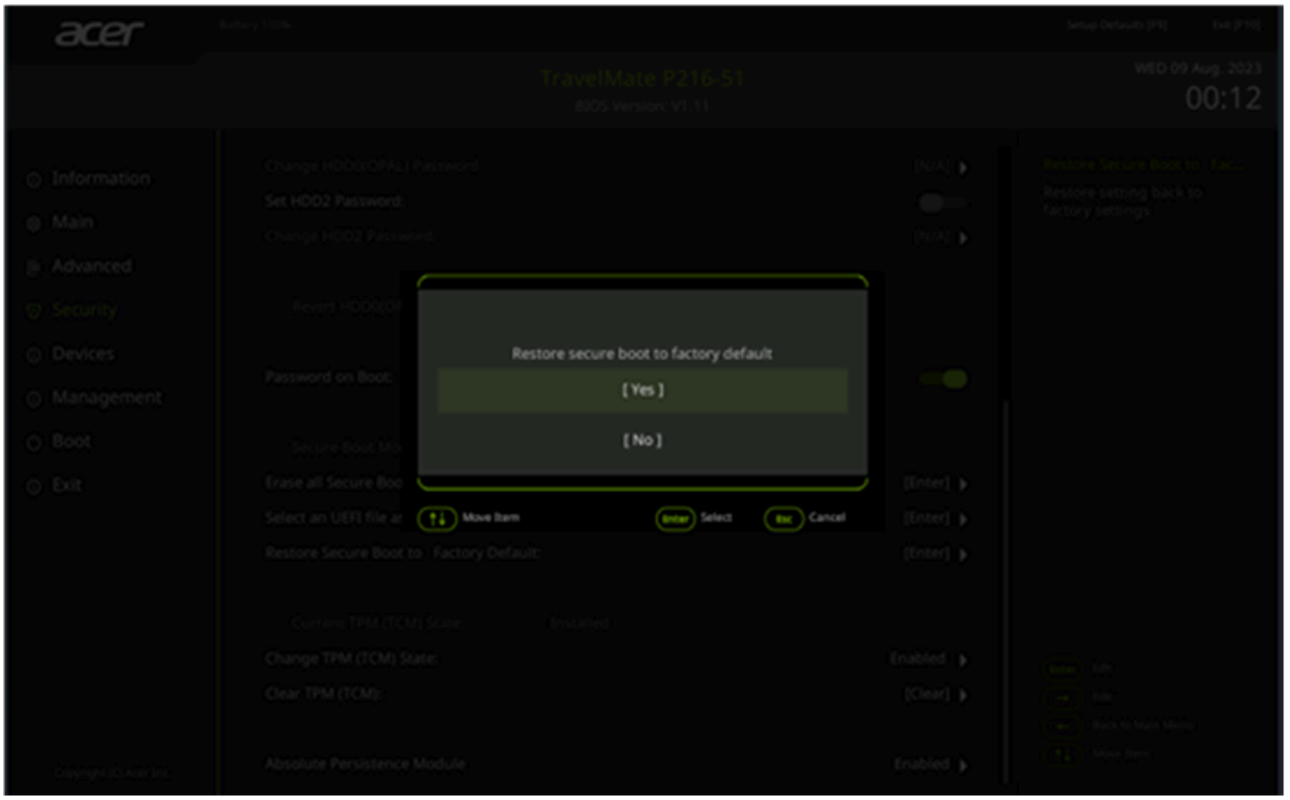
If Supervisor Password is not set or User Password was used to enter BIOS Setup Utility, all the items should be grayed out.

If Boot Mode is [UEFI] and Secure Boot in Boot Menu is [Disabled], all the items should be grayed out.






acer
Battery:100%
Setup Defaults [F9]
Exit [F10]
TravelMate P216-51
BIOS Version: V1.11
WED 09 Aug. 2023
00:11
Information
Main
Advanced
Security
Devices
Management
Boot
Exit
HDD0
USB0
HDD0
Enter Edit
Edit
Back to Main Menu
Move Item
Copyright (C) Acer Inc.


acer
TravelMate P216-51
BIOS Version: V1.11
WED 09 Aug. 2023
00:12
Information
Main
Advanced
Security
Devices
Management
Boot
Exit
Restore secure boot to factory default
[Yes]
[No]
Move Item
Enter Select
Esc Cancel

ITEM NAME	EXAMPLE	REMARK
Secure Boot Mode	[Standard] / [Custom]	Display current Secure Boot Mode Status. [Standard]: No manual change has been done to Secure Boot setting or user has previous restore Secure Boot to Factory Default. [Custom]: Contents of Secure Boot signature database had been modified with “Erase all Secure Boot Setting” or “Select an UEFI file as trusted for executing before. The default value is [Standard].
Erase All Secure Boot Setting	[Enter]	Erase all contents in secure four variables PK, KEK, DB and DBX. A confirmation dialog will pop up to confirm user’s action.
Select an UEFI file as trusted for executing	[Enter]	This action allows user to select all available .efi files in FAT32 partition and add the .efi hash into secure DB. This action will follow below method: Display available device for users to select .efi file location. Display all files in the device and allow user to select intended file (Only efi file can be added to the signature database) and interface will allow users to go up or enter directory. If Yes, is selected, file hash will be added to signature database and return to Security Menu. If No is selected, return back to previous file selection menu. Added efi file’s Boot description will be added into boot device order list’s last place, max 5 entries are allowed.
Restore Secure Boot to Factory Default	[Enter]	Restore setting back to factory settings. When save and exit the BIOS Setup Utility, default Secure Boot factory settings will be restored. By executing this action, Secure Boot Mode will be reset to [Standard] upon next entry to the BIOS Setup Utility.

3.1.1.5 Boot Tab

This menu allows the user to decide the order of boot devices to load the operating system. Bootable devices include the diskette drive in module bay, the onboard hard disk drive and the CD-ROM in module bay.

Boot Priority order will only display bootable device based on the Boot Mode selection. When Boot Mode is changed, a pop up like message should indicate to user the available boot devices will not change until a reboot. If users insist to change boot mode, boot priority order will become gray out unless user switch boot mode back to original boot mode settings.

Following requirements must be met under [UEFI] Boot Mode:

· Wire connection will display Network boot device IPV4 and Network boot device IPV6 as two separate network boot devices

· After Windows 8 OS is installed, a boot entry named “Windows Boot Manager” will be generated and displayed on top of the boot device priority.

Following requirements must be met under [UEFI] and [Legacy] (Note1) Boot Mode:

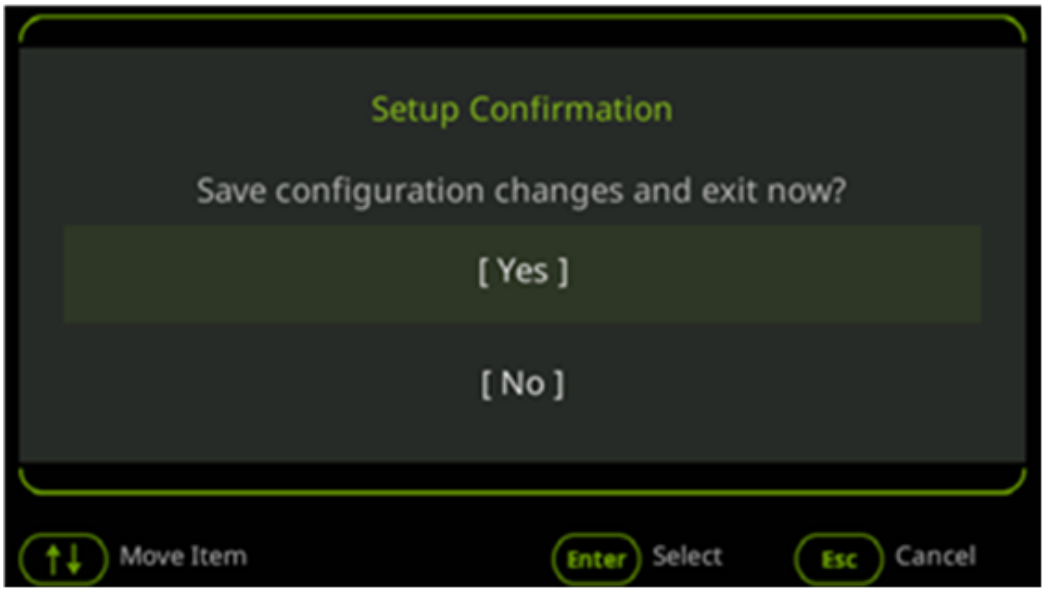
· Nonphysical boot device can be deleted in the Boot Priority Order List, includes: A trusted boot entry, Windows To Go, Windows Boot Manager, IPV4, and IPV6 should not be able to be removed by users. However the firmware should automatically removes non-current Windows Boot Manager entry and adds current Window Manager entry based on current storage’s unique partition (ESP) GUID.

Note1: Selected commercial systems with Win8 to Win7 downgrade support.

ITEM NAME	EXAMPLE	REMARK
Boot Mode	[UEFI] / [Legacy]	· Default Boot Mode: BIOS need to check OS type for this default setting. Win7 default: [Legacy]/Other OS(including Win8) default: [UEFI]. · When [Legacy] Boot Mode has been set, Secure Boot will be disabled, Items related to Secure Boot feature in Boot Menu and Security Menu will be hidden. Firmware will be able to load CSM module during boot. · When Boot Mode changed, a confirmation message that confirm with user’s decision and info user the boot device list won’t be refresh to different boot mode until next BIOS Setup Utility entry and the change of Boot Mode will not take effect until next boot. · After user flash BIOS or load Setup Defaults, Boot Mode should return to factory default value. · If IHV doesn’t support legacy in the platform, hide the legacy option and gray out the Boot Mode option

ITEM NAME	EXAMPLE	REMARK
Secure Boot	[Enabled] / [Disabled]	· When default Boot Mode is [UEFI], default Secure Boot status is [Enabled] and CSM module can't be loaded during boot. · If user sets Secure Boot to [Disabled], firmware will bypass secure boot verification. · The Secure Boot status is only available on [UEFI] Boot Mode but hid under [Legacy] Boot Mode. · In [UEFI] Boot Mode, Secure Boot following actions will gray out while below condition Supervisor password had been set and Setup Config. Utility was log in by User Password. · When BIOS "Load Setup Defaults" is executed, if default Boot Mode is [UEFI], Secure Boot will reset to [Enabled], on the contrary, if default Boot Mode is [Legacy], Secure Boot will be disable and hid in Boot Menu. · When user change Boot mode from [Legacy] to [UEFI], Secure Boot will be set to [Enabled] and shown on Boot Menu.
Boot Priority Order		· When Boot Mode changed, the Boot Priority Order won't be refreshed until next BIOS Setup Utility entry. · When Boot Mode is [UEFI] or [Legacy] (UEFI+CSM) and users enable Windows To GO Startup Options under OS, an USB class boot entry name "USB Entry for Windows To GO" will be inserted into the top of the Boot Priority Order and Boot Option Menu. · If "USB Entry for Windows To Go" present, and BIOS "Load Setup Defaults" is executed, "USB Entry for Windows To Go" will be set to 1st Boot Device in Boot Priority Order. · For legacy boot mode, when eMMc plus HDD exist in the same time, eMMc is the default boot device · Only display bootable devices · If the Network Boot device is USB External LAN, it should add an "External" string in option . Should take effect on Boot Priority Order and Boot Option Menu.

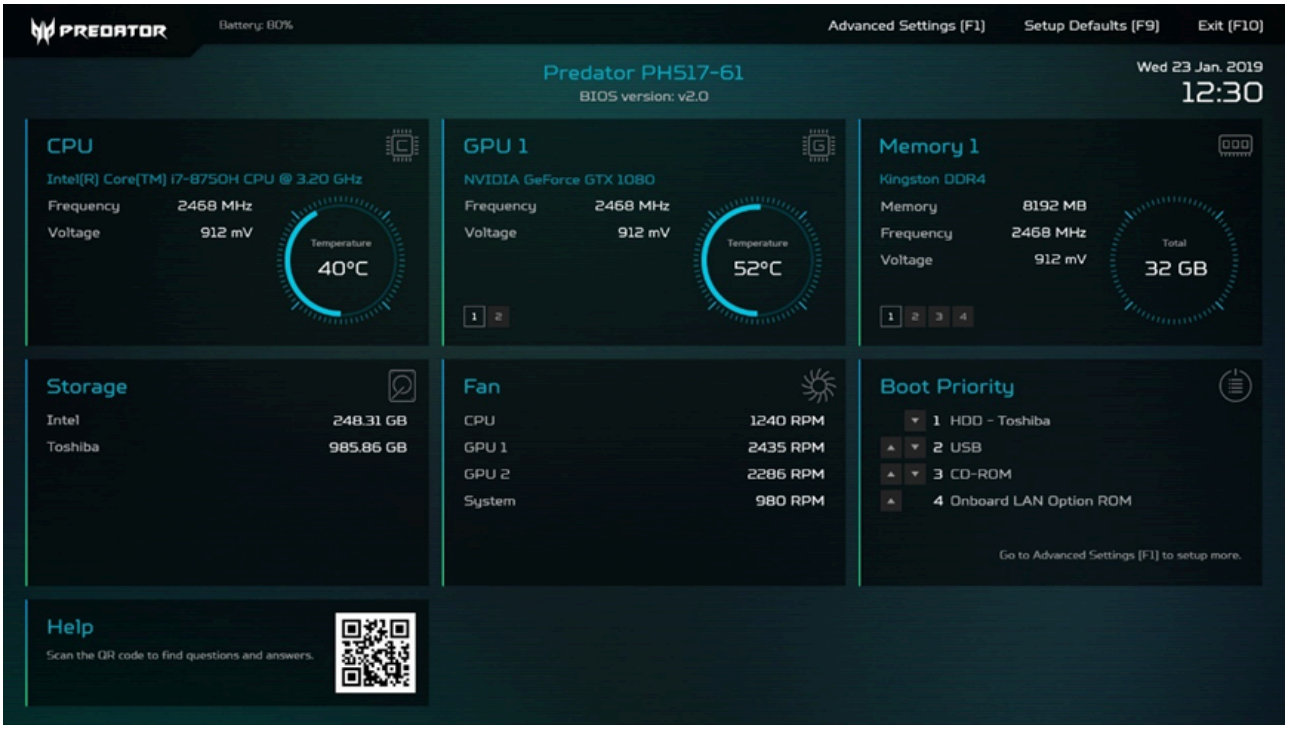
3.1.1.6 Exit Tab

ITEM	REMARK
Exit Saving Changes	· Allow users to save changes and reboot the system. · A confirmation message will pop up as below when user executes this item. System will save changes and then continue to reboot if “Yes” is selected or will stay in Setup Utility if No is selected. 
Exit Discarding Changes	· Allow users to discard changes before exiting Setup Utility. · A confirmation message will pop up as below when user executes this item. System will discard changes then continue to reboot if “Yes” is selected or will stay in Setup Utility if No is selected. 
Save & Shutdown	· Allow users to save changes and shutdown the system. · A confirmation message will pop up as below when user executes this item. System will save changes and then continue to shutdown if “Yes” is selected or will stay in Setup Utility if “No” is selected.

ITEM	REMARK
Load Setup Defaults	· Allow user to load factory default configurations in Setup Utility. · A confirmation message will pop up as below when user executes this item. System will stay in Setup Utility after either selection. 

3.1.2 EZ Mode

Acer EZ mode Setup Menu's resolution is set to panel default. For the General view should look like as below picture. The exactly options displayed depends on system design and latest BIOS SPEC definition. In this page, support user press F1 to "Advanced Settings" , F9 to "Setup Defaults" and F10 to "Exit". The help field should have a QR code to let user visit Acer website.



3.1.2.1 Simple System information

ITEM NAME	EXAMPLE	REMARK
Battery Percentage	Battery: 80%	· Should show the battery capacity for percentage.
System time	FRI 13 Oct. 2023 15:36	· Display the system time format as [Week] [Day] [Month] [Year] [Hour] [Minute]
System BIOS Version	BIOS Version: V1.08	· Should be same with SMBIOS Type 0 Offset 05h.

3.1.2.2 CPU

ITEM NAME	EXAMPLE	REMARK
CPU Info	Intel® Core™ i5-2450M CPU	· Should be same with processor brand string.
Frequency	2.50 GHz	· Display Processor Base Core Frequency.
Voltage	BIOS Version: V1.08	· Display the voltage for CPU
Temperature	58	· Display the Temperature for CPU

3.1.2.3 GPU

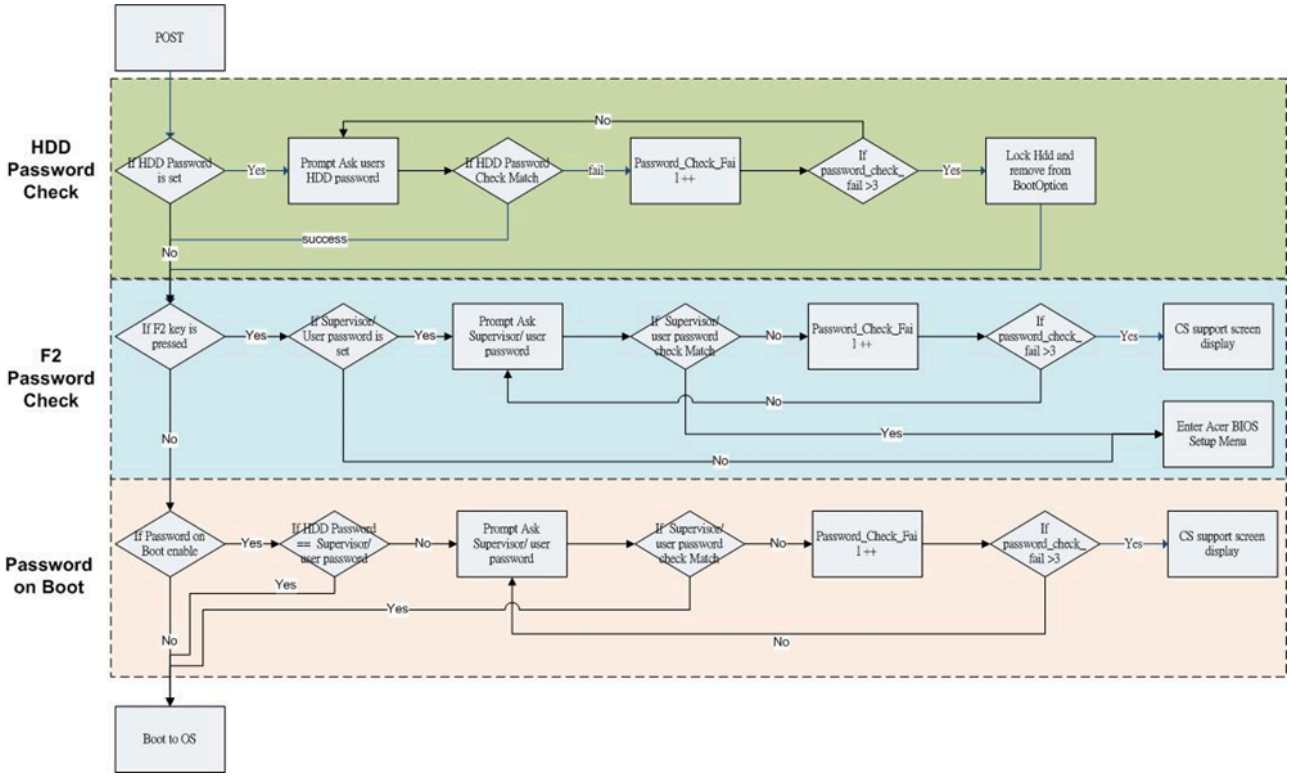
ITEM NAME	EXAMPLE	REMARK
GPU Info	NVIDIA GeForce RTX 3070 Ti Laptop GPU	· Display the model name of GPU.
Frequency	1380 MHz	· Display GPU Frequency.
Voltage	1200 mv	· Display the voltage for GPU
Temperature	52	· Display the Temperature for GPU

3.1.2.4 Memory

On Board Memory should summary to one page. And the title should be “On Board Memory”. If the system is designed as SO DIMM and On Board DIMM, All On Board DIMM should be in one page, other SO DIMM should be in other pages, EX Memory 1, Memory 2…etc.

ITEM NAME	EXAMPLE	REMARK
Memory manufacturer	Micron Technology	· Display the manufacturer of Memory or module. · Reference SMBIOS Type 17.
Memory	32768 MB	· Display the memory size for On board memory or one DIMM
Voltage	500 mv	· Display the voltage for memory

3.2 Security



OPAL Storage password leverage HDD password flow, but no fail three times unlock storage option.

3.2.1 HDD Password

The hard disk drive provides two kinds of password: User and Master Password. The Hard Disk Password set by user from the BIOS Setup Utility should be stored as the “User Password” of the hard disk. The “Master Password” of the hard disk will be reserved as the service password. BIOS should set the hard disk security level to “High”, so both the user and master password can be used to unlock the hard disk.

After unlocking the hard disk and before booting to OS, BIOS should set “Security Freeze Lock”

Allowed HDD password length is 16 characters. eMMC/UFS don’t support HDD password.

3.2.1.1 OPAL Protocol Support

BIOS support OPAL protocol starting from Intel CFL/CNL/GLK platform. Secure Encrypted Disk (SED) and NVME storage with OPAL/Pyrite support should leverage the protocol. BIOS SCU need to identify the storage going for SATA or OPAL.

BIOS provide a revert method if user forget password. This revert method can’t recover data. It only return the storage to factory default state. There is a label printing PSID of the storage. User keys in the PSID to trig “revert”. Storage follow OPAL SPEC to revert, and all data lost.

Allowed OPAL password length is 32 characters.

It require system supervisor password to revert the storage.

OPAL password is only available for OPAL family devices which supports PSID revert feature.

CAUTION: Due to current critical design issue relating to Re-mapping and OPAL protocol under S3, only implement the support when project must adapt OPAL. In that case, project must disable Re-mapping to avoid problem.

3.2.2 Supervisor and User Password

Only when Supervisor Password is set, then, User Password is able to set.. Password on boot is able to set when Supervisor Password is set.

Once Supervisor Password remove, and User password should also been clean.

Both passwords contains up to 16 characters.

To change password in SCU, entering current password and retry three times error, system halt.

If the Supervisor / User Password is set and Password to boot is enabled, the system will pop up the password dialog to ask for the password when system is power on or resuming from S4 state.

The Supervisor Password set by user from BIOS Setup Utility should be stored as the User Supervisor Password. When user re-tries 3 times User Supervisor Password fail and select “Enter Unlock Code”, an encrypted key(code.txt) will be stored in USB storage. User should insert FAT/FAT32 USB storage, save code.txt in it and provide the content of code.txt for Acer Services. After that, Acer services can provide unlock code for user and user can use it to reset User Supervisor Password. Please note that system can’t be shutdown or reboot before unlock process completes.

Power State Password check table:

STATE	HDD PASSWORD	OPAL PASSWORD	SUPERVISOR/ USER PASSWORD WHEN F2 IS PRESSED	POWER ON PASSWORD
S3	X	X	X	X
S4	V	V	V	V
S5	V	V	V	V
Reboot	X	X	V	V

3.2.3 Validate Password Characters

Valid Password characters are the same character set used for BIOS password in Security Menu in BIOS Setting. The password is stored as Unicode (UTF8).

While setting a new password, three failures to enter the old password will result in the system hold.

All the passwords can be set or cleared in Security Page of BIOS Setup Utility.

User can change/remove password during resuming from S4 with Windows8 Hybrid boot.

The password entry consists up to 16 alphanumeric characters. At least 1 character must be assigned in the field.

The valid characters are listed in below table.

SYMBOL CHARACTER	SYMBOL NAME
A-Z	Alphabets A through Z
a-z	Alphabets a through z
0-9	Numerical Characters.
-	HYPHEN-MINUS
=	Equal Sign
[	Left Bracket
]	Right Bracket
.	Period
,	Comma
;	Semi-colon
/	Slash
\	Back-slash
`	Grave Accent
~	TILDE
!	EXCLAMATION MARK
@	COMMERCIAL AT
#	NUMBER SIGN
$	Dollar Sign
%	Percent Sign
^	CIRCUMFLEX ACCENT
&	AMPERSAND
*	ASTERISK

SYMBOL CHARACTER	SYMBOL NAME
(	LEFT PARENTHESIS
)	RIGHT PARENTHESIS
_	LOW LINE
+	PLUS SIGN
{	LEFT CURLY BRACKET
}	Right CURLY BRACKET
|	VERTICAL LINE
:	COLON
“	QUOTATION MARK
<	LESS-THAN SIGN
>	GREATER-THAN SIGN
?	QUESTION MARK
‘	APOSTROPHE

3.3 SMBIOS

3.3.1 Acer SMBIOS Definition

The system firmware must implement support for SMBIOS that compliant with System Management BIOS reference Specification Version 2.8 or later. About the SMBIOS spec, please refer to: http://www.dmtf.org/standards/smbios

The SMBIOS implementation must follow all conventions and include all required structures and fields as indicated in the latest SMBIOS Specification, and follow all conformance requirements as indicated in Section 4. However, BIOS needs to provide component information for each platform.

To let the management software or the customer service site can get the useful system information, the following system information cannot be erased or destroyed when update the system BIOS.

BIOS Vendor (SMBIOS Type 0). SMBIOS type0 BIOS vender should be IBV brand name, ex. Insyde/Phoenix

BIOS Release Date (SMBIOS type 0), Follow SMBIOS SPEC mm/dd/yyyy.

BIOS Version (SMBIOS Type 0)

BIOS Major Release Version (SMBIOS Type 0)

BIOS Minor Release Version1 (SMBIOS Type 0)

Embedded Controller Major Release Version (SMBIOS Type 0)

Embedded Controller Minor Release Version (SMBIOS Type 0)

System Manufacture Name (SMBIOS Type 1)

System Product Name (SMBIOS Type 1)

System Version (SMBIOS Type 1)

System Family (SMBIOS Type 1)

System Serial Number (SMBIOS Type 1)

System SKU Number (SMBIOS Type 1) , “0000000000000000” 16 “0”

System UUID (SMBIOS Type 1)

Base Board Manufacture Name (SMBIOS Type 2)

Base Board Product Name (SMBIOS Type 2)

Base Board Version (SMBIOS Type 2)

Base Board Serial Number (SMBIOS Type 2)

Asset Tag Number (SMBIOS Type 3)

Chassis Type (SMBIOS Type 3), to fill 0Ah(Notebook), 1Eh(Tablet), 1Fh(Convertible) and 20h (Detachable) follow product type’s definition

Dynamic SAR Flag(SMBIOS Type F9h)

Below table are summaries some information that needs BIOS to provide correct information. For the detail, please check SMBIOS Check List to implement Acer SMBIOS information.

PRODUCT INFORMATION	EXAMPLE	REMARK
System BIOS Version	Vx.xx	SMBIOS Type 0 Offset 05h
Serial Number	1234567890123456789012	SMBIOS Type 1 Offset 07h and the maximum length is 22 bytes
Product Name	Acer: (Aspire) Aspire XXXX (TravelMate) TravelMate XXXX (Aspire One) Aspire One XXX (Iconia) ICONIA XXX (N/A) XXXX	SMBIOS Type 1 Offset 05h. Product Name is defined by project POR. The string is case sensitive and the maximum length is 50 bytes
	Gateway: (N/A) XXXXX	
	Packard Bell: (EasyNote) EasyNote XXXX (N/A) XXXX	
Manufacture Name	Acer/Gateway/Packard Bell	SMBIOS Type 1 Offset 04h
Asset Tag Number	22 characters maximum	SMBIOS Type 3 Offset 08h. ODM should provide an utility which can modify the Asset Tag and Acer BIOS Setting Tool (ABST) also can read/write it. Default is 22 empty characters For tender case, the default value follows tender case's feature and project requirement
UUID	16 characters maximum	Required for all systems. If the UUID raw data is string type {00112233-4455-6677-8899-AABBCCDDEEFF}, it would be represented as data type: 33 22 11 00 55 44 77 66 88 99 AA BB CC DD EE FF. If the UUID raw data is data type, keep original UUID raw data. Fill in the raw data into SMBIOS Type1 field. Acer Shop Floor Information Center requires UUID as data type.

PRODUCT INFORMATION	EXAMPLE	REMARK
Ownership Tag	50 characters maximum	SMBIOS Type 11 string 02h. ODM should provide an utility which can modify the Ownership Tag and Acer BIOS Setting Tool (ABST) also can read/write it.

3.3.2 Acer Specific SMBIOS Support

Acer BIOS needs to implement Acer specific SMBIOS type for special function support. Please refer Acer SMBIOS Type of WMI spec.

3.3.3 Acer SMBIOS Check List

Attached list should be reviewed for each project to ensure acer SMBIOS standard is consistent cross different systems.

3.4 Boot

3.4.1 Quiet Mode

When Quiet Mode is enabled under [Legacy] boot mode, no text should be displayed and follow BGRT display.

Set “Quite boot” default as “Enable” and remove “Quite boot” option from BIOS setup menu.

3.4.1.1 Copyright Message

The ODM suppliers should put Acer copyright file, the attached file below, into system BIOS and the system BIOS should base on manufacture name in SMBIOS type 1 to display proper Acer copyright string during POST, when BIOS Quiet Boot is disabled and Boot Mode is [Legacy], below the BIOS vendor information.

The Acer copyright string is only required for the projects with Acer brand.

Example:

Acer Brand -

Gateway Brand (For both commercial and consumer projects)

This BIOS is exclusively for Gateway only.

Packard Bell Brand (For both commercial and consumer projects)

This BIOS is exclusively for Packard Bell only.

3.4.1 UEFI Boot

System firmware must not fail back to [Legacy] Boot Mode without explicit user action for OS which didn't support UEFI.

System firmware must expose timing and class information (SEC, PEI, DXE and BDS).

System with TPM that support wired LAN in pre-OS support UEFI 2.3.1

On a system with multiple graphic adapters, firmware allows user to configure the usage of adapter.

System must support IPV4 and IPV6, when wired connection is available.

UEFI system must allow OS to create both generic and device specific boot entries with Messaging Device path, specifically USB Class Device Path. The firmware must respect these settings and not modify them once the OS has changed them and report the boot entries to the OS accurately.

Firmware must ensure that the boot order is reported consistently across the various on/off transitions.

System firmware must not present any error message or require user intervention when the device corresponding to a boot entry isn't found. Firmware should proceed to the next boot entry silently.

3.4.3 Post Logo

Under Both [UEFI] and [Legacy] boot mode:

1. The integrated display must always be set to its native resolution and native timing. To maintain the consistent user boot experience between win7/win8 and above, BIOS POST logo will transit to BGRT no matter UEFI or Legacy under win7/win8 and above.
2. F2 and F12 prompt message will no longer display even under win7.
3. We would like to advise end user when they manually switch boot mode from UEFI to legacy under SCU.

“Microsoft recommends executing Windows 8 and the version above under UEFI boot mode to enjoy the full features.”

4. The OEM model should use the follow POST bitmap. After the scaling on widescreen, the OEM logo should be normal without any distortion. Below is the example of OEM BIOS POST Logo.

Logo starting (x, y) offset should follow below formulas:

x = 0.5 * (Screen’s native width in pixels) – 0.5 * (Logo’s width in pixels)

y = 0.382 * (Screen’s native height in pixels) – 0.5 * (Logo’s height in pixels)

Each brand logo should have 2 ratio aspects: 16:9 and 4:3. When the lid is shut and external display is connected, firmware should base on the external display EDID information to show right ratio logo. If external display has no EDID display, use 4:3 as default.

Acer brand

Packard Bell brand

Gateway brand

Predator Serial

ConceptD Serial

3.4.4 Boot Failure

There are 3 defined boot failures in the system.

TYPE OF FAILURE	FAIL DESCRIPTION
Low Battery	System is low battery, below 5% percentage and the boot process may be interrupted by unexpected power interrupt.
Secure Boot	Secure boot fail.
No Bootable device is found	Bootable device list is empty

Describe behavior below.

1. All icon support 1024x768 only for ROM size concern. It will display within the same aspect rate and the same percentage of the whole screen area.
2. No impact to the WinRE current behavior
3. For hotkey support, “Low Battery” failure won’t support any hotkey due to the critical level is high. Failure icon will display for 5 sec then the system will automatically shut down. For secure boot and no bootable device failure, hotkey works fine.
4. If end user press button when battery capacity <= 3%, EC need to follow LED spec blinking and prevent system from booting.

5. If end user press button when battery capacity > 3% and RSOC <=5%, EC can normal boot units and BIOS show low battery icon
6. For secure boot and no bootable device failure, the failure icon will hold right that and wait for end user's next action.
7. "No Bootable Device" means that the bootable device list is empty. For the case that bootable device exist, but fail to boot, it doesn't define as "No Bootable Device". Example: Enable PXE, but doesn't plug in LAN cable. Since there will be an PXE bootable device on the list, it won't show boot failure for "No Bootable Device" even it failed to boot from PXE.

Please use the attachment as boot failure icon.

3.4.4.1 Active Key definition for boot failure

BOOT FAILURE TYPE	ACTIVE KEY
Low battery	No active key
No Bootable device is found	Ctrl + Alt + Del
Secure boot fail	Only allow "Enter" key to try on next bootable device Ctrl + Alt + Del

3.4.5 Boot path definition

Boot path defined for UEFI shell is //EFI/UEFISHELL/bootx64.efi. BIOS shows "UEFI_SHELL" for the boot entry.
For other boot paths, follow ISV's SPEC.

3.5 Power

3.5.1 Beep for AC Charging

A beep is required whenever there is an AC plug-in or plug-out.

3.5.2 Power Button

The Power Button should act as the ACPI defined Power Button and user can determine its policy through the OS settings, like Windows Power Options.

The Power Button whether implemented as an ACPI Control Method Power Button or as part of the Windows compatible Button Array, must be able to power-up the system. It also must be able to generate the Power Button Override Event when held down for 4 seconds to force shutdown system anytime.

Before BIOS actually shutdown the system caused by Power Button 4 second override event, BIOS must issue “Standby Immediate” command to HDD and SSD to avoid the risk of data lost or device crash.

3.5.3 Power Button Behavior

	MODERN STANDBY	NON MODERN STANDBY
Behavior	l Short press (Press < 2 seconds) (Note1) n Power button actions l Long press (2seconds <= press < 10 seconds) n Slide to shut down l Power button override (press >= 10 seconds)	l Short press (Press < 1.5 seconds) n Do nothing l Long press (1.5 seconds <= press < 4 second) n Invoke Acer Power Button Utility l Power button override (press >= 4 seconds)

Behavior above is only applied to S0. For S3 (MS)/S4/S5, work as normal power button.

Note1: If system is power button on keyboard, the short press period should be (0.5 second < press < 2 seconds). That means press < 500ms is do nothing.

3.5.4 Power Button utility support

	WITH POWER BUTTON UTILITY	WITHOUT POWER BUTTON UTILITY
Behavior	l Set a bit to BIOS/EC to notify the Acer Power Button Utility installed l Send Acer define WMI/scancode/HID to invoke Acer Power Button Utility UI	Send power button event, follow OS defined behavior

3.6 SVID and SSID Requirements

The system BIOS should write Acer SVID into PCI configuration space register 2Ch and write Acer SSID into PCI configuration space register 2Eh for each onboard PCI/PCIe device.

3.7 Video output Switch

Leverage Win+P. Refer to 4.1.1 key code spec for more detail.

3.8 Lid Switch

	CLOSE THE LID STATUS	OPEN THE LID STATUS
Pre-OS	Backlight Off	Backlight On
OS	1. The operating system will determine what action to take when the lid is opened and closed 2. The function of lid switch will follow the OS setting in power management (Nothing, Standby, Hibernate or Power Off). If nothing, the backlight must still turn off when the lid is closed. 3. Turn off keyboard, touchpad, touch panel when LID close	

SINGLE MONITOR WITH D-SUB/DVI/HDMI/DP CONNECTION		
Original Status	Close Lid	Re-open Lid
Internal display mode	External Mode	Internal Mode
Clone Mode	External Mode	Clone Mode
Projector only	Do Nothing	Back to state before switching to external mode.
Extended Mode	External Mode	Extended Mode

3.9 One BIOS for all Brand and product lines

To achieve one BIOS for all brands and product lines, the ODM suppliers should implement the following requirements into system BIOS.

- Put the required brand logos (Acer, Packard Bell, Gateway) and product line logos into system BIOS.
- Unify BIOS hotkeys for all brands.
- Identify the system by manufacturer name and family, and then display proper brand or product line logo during POST.
- Identify the system by manufacturer name and then display proper copyright string during POST.
- Identify the system by product name and then write proper SSID during POST.

Besides the BIOS solution, the ODM suppliers should also add the following procedures in the manufacturing site.

- User tool to write proper brand name (manufacturer name) into SMBIOS type 1.
- User tool to write proper product name into SMBIOS type 1.

3.10 Radio Management

The section describes the Radio Device Management and Radio Device Keystroke behavior. Following table is system factory status of the Radio Device.

	WIRELESS LAN	WWAN	BLUETOOTH
POST	ON	ON	ON

BIOS must use _OSI method in ASL (ACPI Source Language) to identify the host operating system when system resume from S3, S4, Warm-Boot or Cold-Boot. If the host operating system is Windows 8 and above BIOS/EC will set Wireless LAN, WWAN, Bluetooth hardware ON and bypass H/W (GPIO) Radio Device ON/OFF

If operating system is not Windows 8 and above, system resume from S3, S4, warm-boot or cold boot will keep the previous state of Radio Device.

3.11 Acer Fast Boot

Please refer to the latest Acer fast boot PES for implementation detail.

3.12 WLAN Regulatory Support

BIOS need to implement corresponding design following by vendor's spec in order to support WLAN regulatory.

To meet different country's radio regulation, driver might request specific SMBIOS information to identify the shipping country code. BIOS need to add the necessary SMBIOS data table following by vendor's spec.

Some selected projects might need to adapt power profile for WLAN driver usage or support dynamic power switch. For detail process and the implementation information, please refer to latest "Acer BIOS Design Guide for WLAN Regulatory".

3.13 Convertible Mode detection

For the convertible projects, BIOS must have ability to detect different mode for different usage. Implementation details refer to latest "Convertible Mode Usage PRODUCT EXTERNAL SPECIFICATION".

3.14 POST Animation & Sound effect

For Acer gaming projects, BIOS need to support POST Animation & Sound effect. User could enable/disable this effect from BIOS setup option.

There is a sub-option of “POST Animation & Sound” called “Sound”. User could select mute/unmute when enabling “POST Animation & Sound”. If disable “POST Animation & Sound”, grey out “Sound” option and keep the original setting.

3.15 Acer Application Base Driver Requirement

To support Acer Application Base Driver, BIOS needs to declare following ACPI device for different product line. The Four Part ID and Subsystem ID please reference “Base_Extension_Driver_BIOS Declaration Guideline v0.6.pptx” or later.

- Might a Tender Request or special case to disable Acer Application Base Driver. If no Acer Sense Application for tender request or special case, Acer Application Base Driver can be disabled by disable TenderRequestEnabling variable in section 5.12

4. HW Support

4.1 By Bus and Device

4.1.1 Keyboard

Keyboard matrix and key scan is the basic requirement. And the specific key functions scan code, please get specs from FTP (/DQC/Design Guide/NB_WTablet/BIOS). Normal keys are listed in USB HID to PS/2 Scan Code Translation Table. Further details on media key please refer to Microsoft Keyboard Scan Code Specification.

4.1.1.1 Hot Key

HOT KEY BRAND	ENTER BIOS SETUP	DISPLAY BOOT MENU	RECOVER OS	EC RESET
Acer/ Gateway/ Packard Bell	F2 (Note2)	F12 (Note2)	Alt + F10	Keep Pressing Power Button 15s (Note1)

Note 1: No need to recalculate 15s when power button is pressed in each state.

Note 2: Due to FastBoot, the system needs to be restarted once to re-initialize all devices when F2/F12 is pressed. Before starting the FastBoot process, the EC can report the status of F2/F12. Allow BIOS to cancel FastBoot to ignore a system restart.

	POST	S3	S4	S5 (HYBRID SHUTDOWN)	BIOS SETUP MENU	OS
F2: Enter BIOS Setup	V					OS Defined
F12: Display Boot Menu	V					OS Defined
Alt+ F10: Acer Recovery	V					OS Defined
FN+ Function Key						OS Defined
EC Reset	V	V	V	V	V	V

4.1.1.2 FN Function Key

FN Function key should work following Quick Access (Launch Manager for win7) Specification, Acer GW EM Hotkey List, and Scan Code SPEC/Table. In Modern Standby, BIOS needs to follow the project design to support hot key function under MS mode. For example: User can adjust audio volume up/down when system in MS mode.

Don’t need to support Fn function keys listing below during Non-ACPI (such as POST, BIOS setup menu, DOS, EFI Shell, etc.)

NON-SUPPORT FN FUNCTION KEYS UNDER NON-ACPI	**SLEEP, VIDEO OUTPUT SWITCH, TOUCHPAD ON/OFF, KB BACKLIGHT ON/OFF, MUTE, VOLUME UP/DOWN, BRIGHTNESS UP/DOWN, COMMUNICATION KEY/AIRPLANE MODE, BACKLIGHT ON/OFF, KB LOCK, LCD ROTATION.**

4.1.1.2 FN Function Key

• User could switch between Media key mode and function key mode from BIOS SCU. Default setting depends on product line definition.

n Media Key: Perform the media function by default. Hold the key to activate F1 to F12

n Function Key: Activate F1 to F12 by default, Hold the key to perform Media function.

• Media functions are only active under Windows. F1 to F12 act as normal function keys during device boot or while in BIOS.

• Built-in USB keyboard/ 5 ROW keyboard layout follow keyboard's design and no need to add BIOS switch

4.1.1.3 Media Key/Function Key switch

• User could switch between Media key mode and function key mode from BIOS SCU. Default setting depends on product line definition.

n Media Key: Perform the media function by default. Hold the key to activate F1 to F12

n Function Key: Activate F1 to F12 by default, Hold the key to perform Media function.

• Media functions are only active under Windows. F1 to F12 act as normal function keys during device boot or while in BIOS.

• Built-in USB keyboard/ 5 ROW keyboard layout follow keyboard's design and no need to add BIOS switch

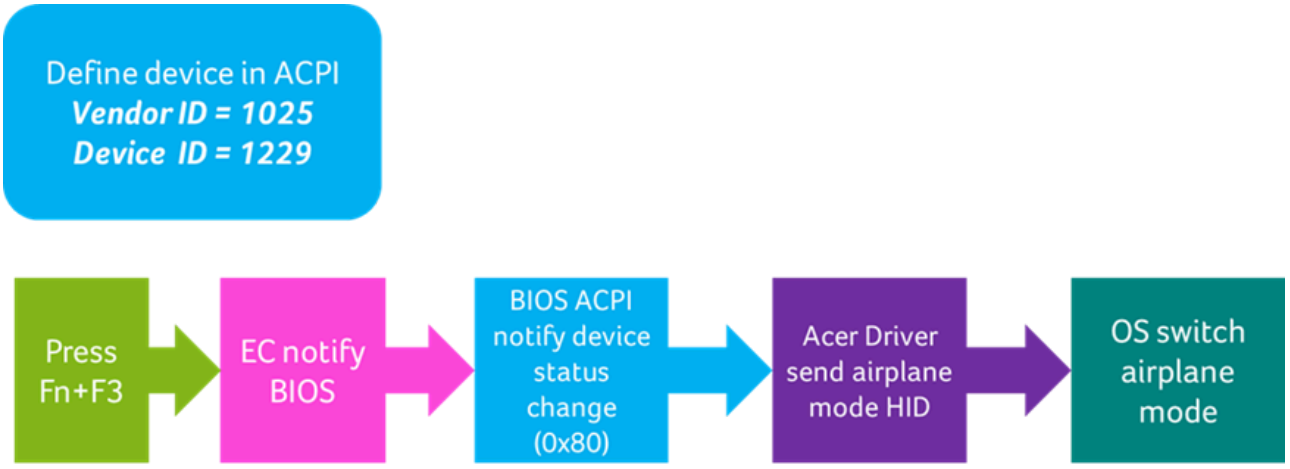
4.1.1.4 RF Button and Communication key

For Win7 (not include pre-boot phase), if Launch Manager is not installed, when end user press RF button, it works like airplane mode to toggle all devices on/off.

For Win8 and above, RF button works as airplane mode trigger.

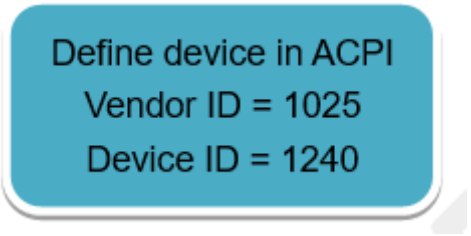
WIN7	RF KEY BEHAVIOR	COMMUNICATION KEY BEHAVIOR
w/ LM	l LM control all SW RF to toggle between all on and all off l Send WMI to control RF button LED	l LM shows Wireless Control Window and control the SW RF status. l If any change, need to apply RF button LED
w/o LM	l BIOS/EC control all wireless DEVICES to toggle between all on and all off l control RF button LED	l BIOS/EC control all wireless DEVICES to toggle between all on and all off l control RF button LED

For Win8 and above OS and PS2 keyboard, BIOS must define an ACPI device for dedicated driver to install. In other case if keyboard is the I2C/USB HID interface BIOS no need to define this device.
Control flow list as below:



4.1.1.5 Embedded Panel Backlight on/off

For the system built with USB keyboard (including 2-in-1 Dock with USB keyboard), BIOS must define an ACPI device for dedicated driver to install.



4.1.1.6 Backlit Keyboard

Backlit keyboard can be turn on and off with FN hotkey and behavior with the following table.

	BACKLIT UNDER AC	BACKLIT UNDER DC
BIOS POST	On	On
Under OS	Passive(Note1)	Passive(Note1)
Resume from S3/S4/S5	Follow above under OS behavior in AC or DC mode	

Note1: When users turn on backlit, it will also enable a timer. This timer will turn off backlit if no users input from keyboard for 30 seconds and when users resume typing the backlit will back on again.

For products support two hotkeys to adjust backlit brightness levels but no ALS design, the keyboard backlit brightness is divided into 3-levels (0%, 50% and 100%) and default setting is maximum level. When system restarts or resumes from S3, keep last time brightness level. When system resumes from S4/S5, go back to default setting.

For products that support one hotkey to adjust backlit brightness levels but no ALS design, the keyboard backlit brightness is divided into 5-levels (0%, 25%, 50%, 75% and 100%) for gaming series, 3-levels(0%, 50% and 100%) for other series and keeps the sequence from 0% to 100% continuous loop. The default setting is maximum level. When system restarts or resumes from S3, keep last time brightness level. When system resumes from S4/S5, go back to default setting.

For keyboard backlit dimming, transition between light intensity must be smooth. The brightness ramping time per lever takes 500ms.

Gaming products follow “Acer Indicator Spec for Win8_Win10” spec definition to implement.

4.1.1.7 NUM Lock

Default Numlock will always be set to off, regardless keyboard size and external Numlock status should always sync with Internal Numlock status, if an external keyboard is connected. After enter OS, Numlock behaviors should follow OS designed behaviors.

4.1.1.8 Alt+F10

In order to provide easy way for system recovery, BIOS should follow “BIOS Requirement for UEFI GPT boot” v1.2.2 and above to support Alt+F10 function key for both win7/win8(and above) and cover single/dual load.

Except the original way to press Alt+F10 during BIOS POST, user could press Alt+F10 before pressing power button to ensure the alt+F10 actually being trigged.

Support Matrix:

	SINGLE LOAD	DUAL LOAD
Win7	MBR	(UEFI+CSM) GPT
Win8 and above	GPT	(UEFI/UEFI+CSM) GPT

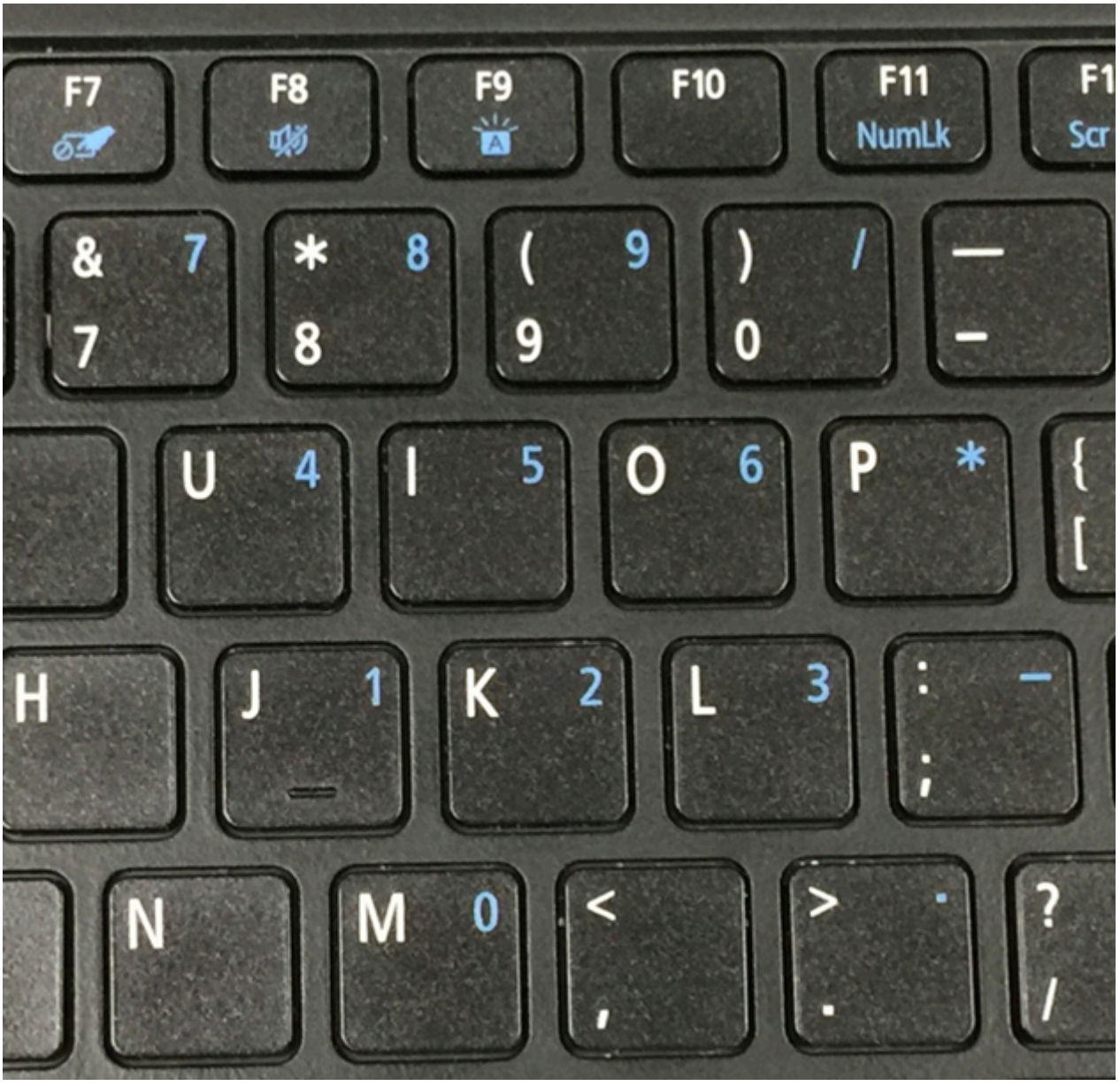
4.1.1.9 Internal KB Numpad

User could disable internal keyboard Numpad by set “Disabled” to the “Internal KB Numpad” option in BIOS setup.

When set to “Disabled”, internal keyboard Numpad still work as normal letter key even turning on Numlock.

Default value for the “Internal KB Numpad” is “Enabled”. This option located in “Main” tab.

The option only exists for the product using the keyboard with combination Numpad sharing the location with letter. Refer to the photo below.



4.1.1.10 Combination key

RTC RESET	DISPLAY HIDDEN SCU ITEMS	PAUSE	BREAK	SYSTEM REQUEST	SCROLL LOCK
“Fn” + “Esc” + “R” and hold 3 seconds(Note 1)	Ctrl + “S”	Fn + "B"	Ctrl + "Fn" + "B"	Fn + "Q"	Fn + "S"
System Usage	Service key				
Fn + “F”	Ctrl + “D” (Note3)				

	UEFI MODE (NOTE2)	S3	S4	S5 (HYBRID SHUTDOWN)	BIOS SETUP MENU	OS
RTC Reset			V	V		
Display hidden SCU items					V	
Pause	V				V	V
Break	V				V	V
System request	V				V	V
Scroll lock	V				V	V
Fn + “F”						V
Service key					V	

Note1: Any other key pressing during the 3 seconds will reset the counter, users have to release the combination key then press again. RTC reset take effect right after it triggered by combination key, user will experience multiple reboots. And the RTC reset combination key only apply to internal keyboard, not applicable on USB keyboard.

Note2: uEFI mode means system in pre-OS environment, like as Shell mode.

Note3: When trigger the service key, the corresponding hidden SCU items for service will be displayed.

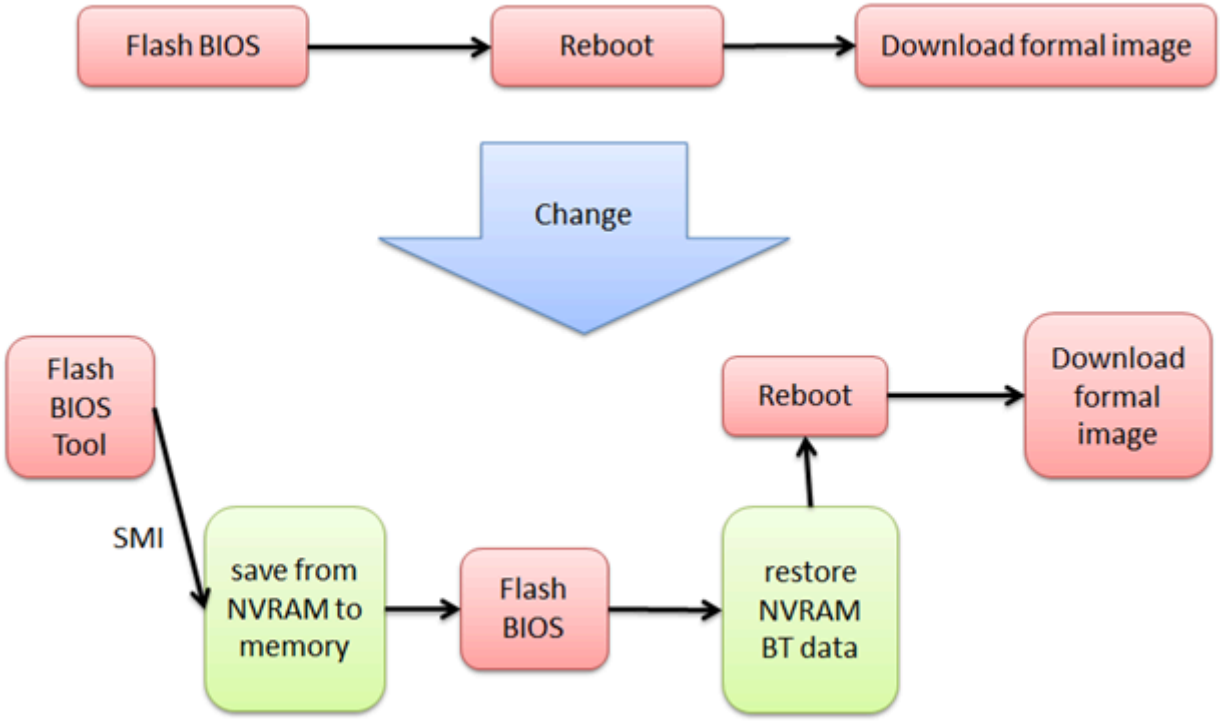
4.1.2 Touch Pad

Device needs to own their HID for driver install, System BIOS needs to program Acer project ID for driver identify.

In Windows modern standby, device must support Runtime D3 to reduce power consumption.

4.1.3 Bluetooth

In UEFI environment, BIOS need to keep BT pairing information in NVRAM after flashing BIOS. Please refer below flow chart for update BIOS process.



4.1.4 Boot Device Support

System BIOS will provide the user with the ability to select the devices for attempting to boot an OS. End user will be able to specify which system device will be attempted 1st, 2nd, and so on. This list of possible boot device will include:

- eMMc
- HDD
- CD-ROM/DVD Drive

- Removable devices
- Network Boot
- USB Entry for Windows To GO

If a specified device (drive or media) is not currently available in the system or is not in a bootable state, the system will proceed to the next user selection device. If none of the selected devices are present or in a bootable condition then they system will display “No bootable device is found” icon as boot failure definition.

4.1.5 Graphic

4.1.5.1 Embedded Display

The panel resolution needs to set its native resolution via EDID.

But setup menu is set to 1024x768.

BIOS fixes panel backlight to 150 nits during whole POST period.

If system design has limitation to retrieve EDID from embedded display (e.g. panel connect to system through MIPI), BIOS must provide EDID data for OS to query.

4.1.5.2 External Display

Display the Pre-OS screen only on the integrated display. If the system is connected with external display devices and lid is closed, the POST screen must be displayed on connected monitor.

4.1.6 Network

4.1.6.1 PXE Boot

System BIOS need to implement PXE boot, and it also to meet UEFI spec. For the detail information of PXE boot, please refer to below link:

http://www.intel.com/design/archives/wfm/downloads/pxespec.htm.

PXE BOOT	LEGACY BIOS	UEFI BIOS
IPv4	V	V
IPv6	X	V

For the projects without on board LAN, it needs to support USB LAN dongle PXE for both legacy and UEFI. Support USB LAN dongle list by project defined.

4.1.6.2 Bluetooth/Wi-Fi/WWAN

System BIOS and device need to support wireless radio control method. For software radio control, please refer to Chapter Radio Management.

In Modern Standby, BT and Wi-Fi need to support low power feature.

4.1.6.3 Wi-Fi power limit default for Intel big core platform

In order to keep the highest through put for W-Fi device, default value for Wi-Fi device power limit need to set to 2000. (Currently the setting is only supported by Intel big core platform)

4.1.7 Express Card

Hot plug needs to be supported

4.1.8 USB Legacy Support

BIOS has responsibility to enumerate external USB device during POST. If bootable USB device is attached, system should be able to boot into it.

For BIOS setup menu, BIOS will support external USB keyboard for input. If setup menu is graphic setup menu, both keyboard and mouse need to be supported via USB.

USB keyboard needs to be used during POST, and under DOS/UEFI shell without additional driver installation.

Based on Acer crisis recovery request, USB legacy should be enabled.

Mentioned above, Acer platform will support both USB2.0 and 3.0.

4.1.9 Touch Screen

There are two interfaces for Touch Screen, one is USB interface and the other is I2C interface. System BIOS needs to support USB selective suspend or Runtime D3 function.

POWER SAVING FUNCTION	USB INTERFACE	I2C INTERFACE
USB Selective Suspend	V	X
Device Runtime D3	V	V

If project supports hot key of Touch Screen enable/disable, when system enters S0, touch screen function should be always enabled by default.

When system enters S3/S4/S5, touch screen power should be turned off to avoid accident screen touch waking up system.

SYSTEM STATE	TOUCH SCREEN FUNCTION	HOT KEY OF TOUCH SCREEN FUNCTION ON/OFF	WAKE UP SYSTEM
S0	Enable by default	Enable (Note 1)	N/A
S3/S4/S5	Disable function and turn off power	N/A	Not support

Note1: Based on "Acer Convertible Mode Usage PES" document, user can use the touch screen hot key to enable/disable touch function during Laptop mode and Viewing mode.

4.1.10 Sensor Hub

The firmware update method should support DFU (direct firmware update), so the related functions need to be defined in ASL file.

In Windows modern standby, it needs to support Runtime D3 feature to reduce the power consumption.

4.1.11 Power-off USB Charge

For platforms support power-off USB charge feature, they can supply USB bus power (DC 5V) to the specific USB Type-A port even when the computer is in S3/S4/S5 states. User could choose to stop power-off USB charge when battery capacity is lower than certain percentage under DC mode. Default low limit is 30%. Power-off USB charge always enable under AC mode. User could decide to disable the feature under DC mode.

User could configure related setting through AP. For commercial projects, the settings also exist in SCU.

The USB charge port support USB wake up as normal USB port definition.

Behavior matrix:

POWER-OFF USB CHARGE	DC(>=LOW LIMIT)	DC(<LOW LIMIT)
Enable	○	╳
Disable	╳	╳

Note: When power-off USB charge is disabled, the charge power is the same as normal USB port.

4.1.12 Audio

System BIOS need to program verb table to audio codec during initialization during POST. Due to all codecs pin configuration are 32 bits register, so verb table size is 4*N. If verb table size is NOT 4 * N, system will hang up during program verb table.

In some case, system cannot save audio verb table when system into S3 state. So audio verb table data will lose after resuming from S3 state, and then OS will lode audio codec default verb table, but that isn’t match project HW design and it will cause some audio issue as no sound. In order to fix issue, System BIOS needs to program verb table when system resuming from S3.

For Intel Smart Sound Technology, System BIOS needs to support Runtime D3 for Codec power consumption.

4.1.13 SATA

The main stream storage inherits from IDE(Integrated Drive Electronics). The Specification is maintained and updated by SATA-IO(http://www.sata-io.org/). The latest version is Ver3.1. The compelling advantage is from better performance, Low pin count and optimized voltage support.

1. Better performance: 133MB/sec ☒ 6.0GB/sec(SATA3.0 SPEC)
2. Lower pin count: 40pins to 8 signal pins+ 16 power pins (optional).
3. Optimized voltage support: 5V to dynamical change (< 0.7V)

4.1.13.1 Zero Power ODD

The higher power consumption is the concern, so the enhanced feature Zero power ODD generated from SATA 3.1.

4.1.13.2 RAID

RAID is optional by project request. Once RAID feature needed, it sets SATA mode to RAID. No ctrl+I support on pre-boot phrase.

4.1.13.3 e-SATA device

To ensure the hot-plug is enabled and the attribute is external port on what SATA port platform wants to use for e-SATA.

4.1.13.4 Slumber and Device sleep

SATA can support slumber and/or device sleep features to enhance power consumptions. For more information, please refer to SATA AHCI spec and BIOS writer guide.

4.1.13.5 Force STBI

To prevent storage, especially SSD, having problem during suddenly losing power, BIOS should issue STBI to storage under below occasions.

- Shutdown caused by BIOS flash (Windows/Shell Flash and BIOS Capsule via WU, but crisis update not included)
- 4 seconds force shutdown (Only cover ACPI-OS environment)
- Shutdown commands handled by BIOS or EC for shipment mode

4.1.14 I2C/SMBus

4.1.14.1 ALS Sensor

When EC or System BIOS get the ambient light illuminance, System BIOS needs to inform ALS sensor and let VGA to control the panel brightness. For Acer design, System BIOS/EC needs to support ALS with Keyboard backlight behavior.

4.1.14.2 Thermal Sensor(X) thermal table

The EC use two cooling modes (active cooling/passive cooling) to do thermal management. Active cooling requires increased power to reduce the system thermal (like turning on a fan) and passive cooling requires decreased power to reduce the system thermal (like CPU throttling).

4.1.1.3 Battery

The system battery must follow the standard Smart Battery Data Specification of Smart Battery System (SBS). And the Embedded Controller (EC) can utilize the SMBus protocol to communicate with battery gauge IC for monitoring status and controlling behavior for battery management. Batteries for ACER platform must meet ACER project requirement for authentication purpose.

4.1.1.3.1 Support Smart Learning battery

To support the battery with smart learning feature, BIOS need to have the ability to update FCC (Full Charge Capacity) to OS if FCC changed during system on.

4.1.1.3.2 Battery percentage

When battery was charged to 99%, EC should change the charger LED and report the battery capacity as 100% full charged to OS in a short time (0 to 10 mins). However, the charger should keep on charging the battery until it really been full charged.

To prevent battery be charged too frequently, a fully charged battery can only be charged when Full Charge bit is cleared. Once Full Charge bit asserts with AC attached, just report 100% percentage to OS.

Example: (mostly, Full charge bit would be clear around 95%.)

BATTERY CAPACITY	**0% ~ 95%**	**96% ~ 100 %**		
Fully Charge Bit	0	0	1	
Battery is chargeable?	Yes	Yes	No	
Capacity EC report to OS	AC power	0% ~ 95%	96% ~ 100 %	100%
DC power	0% ~ 95%	96% ~ 100 %	96% ~ 100 %	

If Full Charge bit is not support in gas gauge design, please implement and follow Smooth battery percentage algorithm in Tablet section.

4.1.15 SPI/eSPI

4.1.15.1 TPM/TCM

Platform which supports TPM/TCM should set TPM/TCM default status as “enabled”. Related BIOS Setup options follow Setup Menu section.

For a system that implements TPM 2.0, the platform meets the requirements defined in Microsoft Windows Logo Requirement System.Fundamentals.TPM20.TPM20 section.

For the platforms support firmware TPM, it is required to enable the firmware TPM by default for all OS (Win7 and above). Firmware TPM must meet TPM 2.0 WHCK requirement.

TPM SUPPORT		
boot mode	UEFI	Legacy
TPM 1.2	Enabled (Note1)	Enabled (Note1)
TPM 2.0	Enabled	Enabled
Note1: Hide option “Disable & Deactivate” of Change TPM State for windows 8 and above if the project has discrete TPM v1.2 to avoid the status sync problem under win8 and above.		

The systems only support firmware TPM (Intel iPTT or AMD PSP fTPM) for consumer WW and China projects. For commercial projects, please refer to section 5.4.3.

For Microsoft Pluton firmware TPM, please refer to section 4.14.

4.1.15.2 Embedded Controller

In ACER platform it is responsible to control peripheral low-speed devices like battery, charger, fan, LED, keyboard, and etc. And it also needs to maintain safety and responsiveness of platform.

4.1.16 LED

For LED definition and behavior, please get the latest Acer Indicator Spec from FTP (/DQC/Design Guide/NB_WTablet/BIOS).

4.1.17 PCI-E Power Saving

BIOS disable L0S but enable L1 for all PCI-E devices (PEG included). It could be adjust if project design has special concern.

For PCIE storage device, L1.2 is required.

4.1.18 Type C

USB devices connected through type C must support behavior below.

If disable USB wake from S4 support option:

S0 CHARGE	**ALWAYS CHARGE**
S3 charge	DC mode, set charge current to 1.5A when capacity reaching 30% Charge if Battery Capacity Greater than 2%
S4/S5 charge	No charge
S3 Wake-up	Support

If enable USB wake from S4 support option:

S0 CHARGE	**ALWAYS CHARGE**
S3/S4 charge	DC mode, set charge current to 1.5A when capacity reaching 30% Charge if Battery Capacity Greater than 2%
S5 charge	No charge
S3/S4 Wake-up	Support

BIOS has to remind the user if the insufficient watts PD adapter is inserted when the system supports UCSI (USB Type-CTM Connector System Software Interface)

Report by GET_CONNECTOR_STATUS offset[64] Battery Charging Capability Status with below tables

VALUE	MEANING	PD ADAPTER RANGE
0	Not Charging	The system has no PDO available
1	Normal Charging Rate	Above system design power
2	Slow Charging Rate	System design power > PD adapter > design power x 60%
3	Very Slow Charging Rate	PD adapter < design power x 60%

4.1.19 Unexposed I/O port

BIOS should disable unexposed I/O port (Com port/LPT port….etc.)

4.1.20 Optane Memory

For the system support Optane memory solution, BIOS default set to Optane mode(with or without RAID depending on project support). BIOS also need to configure remapping in order to detect Optane device when switching to Optane mode.

Describe the definition of Intel RST software feature mask setting configured by BIOS option:

BIOS OPTION	RST SOFTWARE FEATURE MASK
AHCI	N/A
Optane without RAID	R0/R1/R5/R10/RRT set to disable
Optane with RAID	R0/R1/R5/R10 set to enable RRT set to disable

4.1.21 Battery Charge Limiting and Microsoft Smart Charging UX Support

To support Battery Healthy Mode and Microsoft Smart Charging, BIOS/EC should report true charge level to the OSPM. At all times for all installed batteries. Limit the batter from reaching its Full Charge Capacity when Battery Charge Limiting is active. Set _BST Battery Stat Bit[3] when Battery Charge Limiting is active. Ensure the _BST Battery State (Bit0 and Bit 1) reflect true charging/discharging state of battery OSPM must recognize the following settings:

_BST BIT[3]	_BST BIT[0]	_BST BIT[1]	INTERPRETATION
0	NA	NA	Battery Charge Limiting is disengaged
1	0	0	Battery Charge Limiting is engaged, and the battery has reached the steady state, it will not be charged or discharged.
1	0	1	Battery Charge Limiting is engaged, and the battery has not reached the steady state.
1	1	0	Battery Charge Limiting is engaged, and the battery has not reached the steady state.

For detail specification please reference

4.1.23 HID over I2C EC device

System BIOS should declare ACPI device for a HID device. This device is use to OS could communication with EC thru HID interface. Below is the force requirement.

OBJECT	VALUE
_HID	1025174B
_CID	PNP0C50

Please reference the sample ASL code.

4.2 Wake Up Event

The table above defines the system wakeup source under ACPI Mode in AC adapter and Battery only mode.

· When system is in S5/S4/S3/Modern Standby state and lid is closed. Device must not boot up or resume by pressing power button, individual windows button, keyboard and touchpad. (If commercial dock plug in, power button should function well even LID closed.)

· For wake source support on Modern Standby platforms, follow by Microsoft defined.

l With AC adapter

EVENTS	S0 (BLANK SCREEN)	S3	S4	S5
Any Key	V	V		
Power button		V	V	V
Touch Pad	V			
Precision Touch Pad(Note6)	V	V		
Modem Ring (Mini-PCI Modem and Onboard Modem)		V		
LAN (Onboard)		V	V	V
RTC		V	V	V
Critical low battery				
USB device(Note1)	V	V	V	
Lid Open		V (Note4)	V (Note5)	
TBT (Note 7)		V	V	

l With Battery only

EVENTS	S0 (BLANK SCREEN)	S3	S4	S5
Any Key	V	V		
Power button		V	V	V

EVENTS	S0 (BLANK SCREEN)	S3	S4	S5
Touch Pad	V			
Precision Touch Pad(Note6)	V	V		
Modem Ring (Mini-PCI Modem and Onboard Modem)		V		
LAN (Onboard) (Note3)		V		
RTC		V		
Critical low battery(Note2)	V	V		
USB device(Note1,)	V	V	V	
Lid Open		V (Note4)	V (Note5)	
TBT (Note 7)		V	V	

- *Note1: When lid close, System S3 wake up from USB devices should be disabled. Supported wake capability depends on BIOS option setting. It includes TYPE-C USB device.*

- *Note2: When battery capacity hits 6% under S3 or modern standby, BIOS should wake the system to Full ON. It is to give the system a chance to enter deeper sleep state, such as S4. (Round the battery capacity with remaining capacity divided by fully charge capacity)*

- *Note3: The feature is not required, if system supports Deep S3 feature*

- *Note4: if Lid Open Resume option is Enabled*

- *Note5: Apply to Ultra Book with SSD SKU project only. S4 resume also includes Windows 8's Hybrid shutdown.*

- *Note6:If end user uses hotkey to disable precision touch pad, it won't support wake up from PTP. It also not support S3 wake up under win7 OS.*

- *Note7: Supported wake capability depends on BIOS option setting.*

4.3 Virtualization

System must enable virtualization for CPU and I/O if platform supports the technology. BIOS needs to provide setup option for the virtualization following platform design. (The terms of virtualization for Intel are known as Intel VT-X and VT-D).

4.4 Intel Software Guard Extension

For Intel platform which support Software Guard Extension (A.K.A SGX), BIOS must set to “Software control” for SGX configuration.

For system support ePayment which leverage SGX technology, BIOS must default enable SGX.

4.5 Acoustic Setting for Intel platform

For Intel platform, BIOS must configure acoustic related setting as below:

OPTION NAME	SETTING
Acoustic Noise Mitigation	Enable
Disable Fast PKG C state Ramp for IA Domain	False
Slow Slew Rate for IA Domain	By project design

Caution: Slow Slew Rate for IA Domain can`t be smaller than 1/8.

4.6 PCI payload size for Intel platform

For Intel platform which support the adjustment of PCI payload size, it must set to the maximum support value.

4.7 Support iSST for Intel platform

For Intel platform which support Intel Smart Sound Technology (iSST), BIOS must enable this feature.

In order to handle the OS compatibility issue for win7, BIOS must select UAA Compliance.

4.8 Support HWP for Intel platform

BIOS enable HWP (A.K.A. Intel Speed Shift Technology) by default for the platform supported this feature. It could be adjust if project design has special concern.

4.9 RPMC

For Intel platform which supports Intel® RPMC (Replay Protection Monotonic Counter), RPMC feature needs to be enabled.

BIOS must configure RPMC related settings in CSME as below:

OPTION NAME	SETTING
Intel(R) PTT RPMC Supported	Yes
Intel(R) PTT RPMC Rebinding Enabled	Yes

4.10 USB-C Docking Station

For the project support Acer USB-C Docking Station, BIOS/EC must implement functions below.

l MAC address pass through

l LED status sync

l Power button Mirror

l PXE

l WOL over Docking Station

l System Charging

Please refer to latest “Acer USB-C Docking Station Firmware Implementation Guide”.

4.11 Acer Battery System Management

For battery life enhancement, the projects has to support acer battery system management.

Please refer to latest “acer Battery Management Spec” for more detail implementation.

4.12 Intel CNVi Bluetooth settings

For battery life enhancement, if Intel platform which supports BT audio offload, please default enable BT audio offload for CNVi design.

Intel Advanced Menu -> CNVi Configuration -> Bluetooth® Audio Offload

4.13 Intel Boot Guard

For the project which requires to support Intel Boot Guard, the Boot Guard Policy Profiles should be set to Profile 5 (FVME)

Index	Name	FACB	Verify	Measure	ENF
0	No_FVME	0	0	0	00
1	VE	0	1	0	01
2	VME	0	1	1	01
3	VM	0	1	1	00
4	FVE	1	1	0	11
5	FVME	1	1	1	11

4.14 Microsoft Pluton

Microsoft Pluton is designed from Microsoft, and it is security IP. It includes Microsoft security feature (Ex. FW Attestation/Zero Trust) and Pluton fTPM, and realized through by IHV.

For the project which requires to support Pluton, the CPU model need include Pluton SoC. And make sure if platform support Pluton. (Ex. AMD Rembrandt).

Pluton platform firmware should only be included in the BIOS of platforms enabling Pluton fTPM and/or Pluton Security Processor (non-fTPM). Project design that do not intend to have any Pluton functionality, must not have Pluton Platform Firmware as a part of their BIOS image.

To enumerate Pluton devices (both Pluton TPM and Pluton Security Processor) and enable full Pluton functionality, the following OS are required Windows 11 11C/12B Cumulative Update – build 22000.346 or higher. Pluton is not supported on Windows 10 and Linux.

4.14.1 Pluton Firmware TPM

- Support MSFT security Level1, Level2 and Level3.
- Support Windows Update to patch or update TPM firmware.
- Support Secure-Core PC(DRTM).
- The Pluton fTPM is not compulsory to enable, it is one of function in Pluton.

4.14.2 Support HSP for AMD platform

- HSP is the module that AMD uses to support Pluton.
- Follow AMD BIOS Design Guide for Microsoft Pluton Security Processor Enablement specification.
- ACPI table “MHSP” need define OEM ID, please refer section 1.1.

5. Commercial BIOS Requirements

5.1 Absolute Computrace

For selected project which absolute Computrace is implemented, get the latest implementation guide/BIOS package/test report template from vendor directly.

BIOS must complete the validation following vendor’s requirement.

5.2 Fingerprint PBA(Pre-Boot Authentication)

For selected project which Fingerprint PBA is implemented, you can set up PBA for the protection of your computer at the BIOS level.

5.3 Acer System Tool

5.3.1 Acer Disk Sanitizer

Acer Disk Sanitizer is sunset. Disk Sanitizer function will use 3rd party solution if have tender request. If project need to enable 3rd party solution, please refer to section 5.12.

5.3.2 Acer System Diagnose

Acer System Diagnose is sunset. System Diagnose function will use 3rd party solution if have tender request. If project need to enable 3rd party solution, please refer to section 5.12.

5.4 Setup Menu

5.4.1 Information Tab

PRODUCT INFORMATION	EXAMPLE	REMARK
Memory # Size	4096 MB	· Shows each size of onboard/installed memory. · # means memory's number. If there is only one memory on board, hide this item.
Memory # Speed	3200MHz	· Identifies the configured speed of the memory device. · # means memory's number. If there is only one memory on board, hide this item.
Ownership Tag		· Should be same with SMBIOS Type 11 string 02h. · Maximum length is 50 characters
LAN MAC Address	xx – xx – xx – xx – xx – xx	· Shows LAN MAC address · If system have no onboard LAN, BIOS has to save one MAC address that applied at IEEE OUI and shows the virtual LAN MAC address

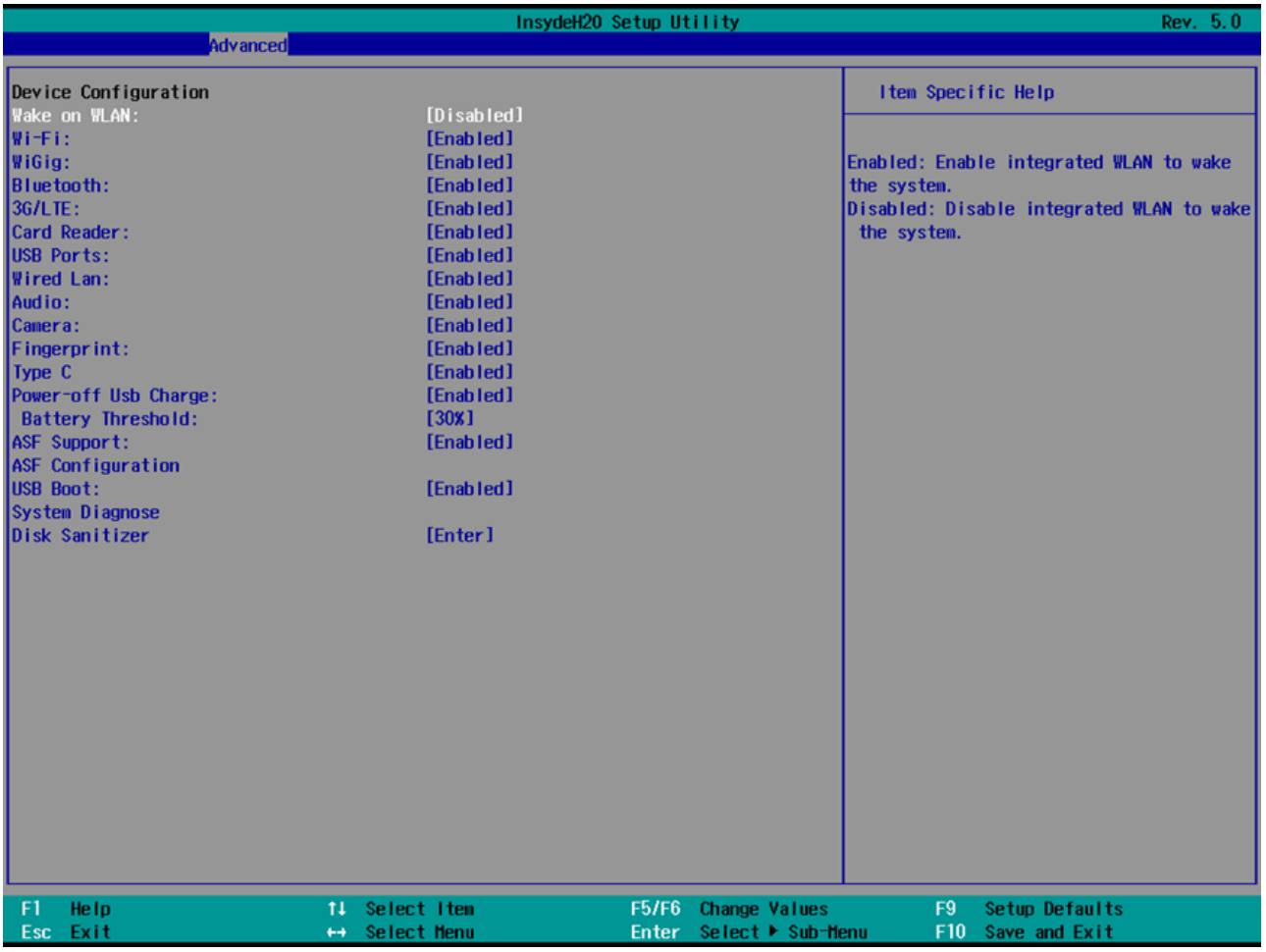
5.4.2 Advanced Tab

ITEM NAME	EXAMPLE	REMARK
Trusted Execution Technology	[Enabled] / [Disabled]	· This option only appears when system is vPro SKU · The default value is disabled · If the system configure as MSFT Security Level 3, set this option default enabled
MEBx		· Only vPro SKU appears this sub-page · Add MEBx sub-page and all the options in the MEBx page follow Intel CRB settings.
Unconfigure ME	[Reset]	· Only visible after Supervisor set with vPro SKU · Unconfigure ME with resetting MEBx password to default on next boot.
DASH	[Enabled] / [Disabled]	· This option only appears when system is AMD Pro CPU SKU · The default value is disabled
AIMT-Support	[Enabled] / [Disabled]	· This option only appears when system is AMD Pro CPU SKU · Add AIMT-Support sub-page and all the options in the AIMT-Support page follow AMD CRB settings. · The default value is disabled
Power on system by RTC Alarm	[Enabled] / [Disabled]	· Enable/Disable RTC wake from S3/S4/S5 function · Default value set to Disabled
Hour	[0~23]	· Setup wake up hour (ISO 8601), allow 0~23 · Grey out if “Power on system by RTC Alarm” set to disabled
Minute	[0~59]	· Setup wake up minute , allow 0~59 · Grey out if “Power on system by RTC Alarm” set to disabled
Second	[0~59]	· Setup wake up second , allow 0~59 · Grey out if “Power on system by RTC Alarm” set to disabled
Device Configuration		· Enter to configure device enabled/disabled

ITEM NAME	EXAMPLE	REMARK
BIOS Update	[Enter]	· This action allows user to update BIOS via USB storage · This action will follow below method 1. List available USB storages for user to select BIOS location 2. List supported files in the device root directory and allow user to select intended file. And interface will allow users to go back or enter directory. 3. If select yes and the intended file product name is matched, it will exit the dialog and prepare to update BIOS. If the selected file product name is not matched, it will do not allow user to continue. 4. If Lock BIOS Version is [Enabled], BIOS Update option status is gray out.
Lock BIOS Version	[Enabled] / [Disabled]	· BIOS flash function switch option. When set to [Enabled], it do not allow user to do BIOS flash and the BIOS version is fixed, but Crisis Recovery is not within this limit. · Lock BIOS Version is default gray out and could only be modified by following actions: Supervisor password had been set. · The default value is [Disabled].
Rollback BIOS Version	[Supported] / [Unsupported]	· BIOS flash function switch option. When it set to [Supported], it allows user rollback BIOS to previous version. · If Lock BIOS Version is [Enabled], Rollback BIOS Version option status is gray out, and shows [Unsupported]. · Rollback BIOS Version is default gray out and could only be modified by following actions: Supervisor password had been set. · The default value is [Unsupported].
Export BIOS Settings to USB Storage	[Enter]	· This action allows user to save current BIOS settings to USB storage. · This action will follow below method: 1. Display available USB storage for users to save settings file. 2. The interface will allow users to go up or enter directory. · If Yes, is selected, it will save current BIOS settings as a file, and exit the dialog.

ITEM NAME	EXAMPLE	REMARK
Import BIOS Settings from USB Storage	[Enter]	· This action allows user to restore BIOS settings from USB storage. · Only profile with same project name can be imported. If project name is not same, pop up warning message to inform user. · This action will follow below method: 1. Display available USB storage for users to select settings file location. 2. Display all files in the device and allow user to select intended file (only supported file can be loaded), and interface will allow users to go up or enters directory. · If Yes be selected, the file will load into BIOS, then exit the dialog.
MAC Address Pass Through	[Disabled] / [System MAC address] / [Customized MAC address]	· [System MAC address]: Clone onboard LAN MAC address to acer Type-C docking. · If system have no onboard LAN, BIOS has to save one MAC address that applied at IEEE OUI. · The details implementation please refer to Acer USB-C Docking Station Firmware Implementation Guide. · [Customized MAC address]: Allows user to input MAC address by itself. · The input rule as below: Valid characters: Alphabets A through F and numerical characters 0-9 The second Byte must be even digit, either 0, 2, 4, 6, 8, A, C or E. · The default setting is [System MAC address]
Wake On LAN from Dock	[Enabled] / [Disabled]	· If support acer VDM (Vendor Define Message) Type C docking, BIOS has to support this option. · This option allow to be adjusted when docking is inserted. Otherwise gray out this option. · Enable/Disable WOL from Dock function · If set to “Enabled”, allow WOL event trigged from Dock to wake the system · The default value is [Enabled].
Privacy Screen	[Enabled] / [Disabled]	· This option appears when video panel support privacy screen feature. Otherwise hide this option. · When disabled, the privacy screen is not applied to the display panel · When enabled, the privacy screen is applied to the display panel and can be toggled between public mode and privacy mode when press privacy screen Fn key · The default value is [Enabled]

ITEM NAME	EXAMPLE	REMARK
World-Facing LED	[Disabled] / [S3/S4/S5 Only] / [Enabled]	· This option appears in education product which support World-Facing LED. Otherwise remove this option. · The default value is [Enabled]
System Health Indicator	[Enter]	· Enter System Health Indicator Page.



The following advanced settings are for commercial product only and only displayed when device is existed. It should be protected by supervisor password.

ITEM NAME	EXAMPLE	REMARK
Wake On WLAN	[Enabled] / [Disabled]	· This is Commercial vPro Feature Only. · Wake on WLAN feature allows system to woken by Wireless LAN. · The default value is [Disabled]. · Panel off when wake on WLAN
Wi-Fi	[Enabled] / [Disabled]	· This option allows user to enable or disable Wi-Fi device in BIOS Setup Utility. · If Wi-Fi device is disabled, the device can’t be utilized until enable it in BIOS. · The default value is [Enabled]

ITEM NAME	EXAMPLE	REMARK
WiGig	[Enabled] / [Disabled]	· This option allows user to enable or disable WiGig device in BIOS Setup Utility. · If WiGig device is disabled, the device can’t be utilized until enable it in BIOS. · The default value is [Enabled]
Bluetooth	[Enabled] / [Disabled]	· This option allows user to enable or disable Bluetooth device in BIOS Setup Utility. · If Bluetooth device is disabled, the device can’t be utilized until enable it in BIOS. · The default value is [Enabled].
CNVI WLAN/BT	[Enabled] / [Disabled]	· This option allows user to enable or disable WLAN/BT devices connected through CNVI in BIOS Setup Utility. It could only enable/disable the two devices in the same time. · If WLAN/BT devices are disabled, the devices can’t be utilized until enable it in BIOS. · The default value is [Enabled].
WWAN	[Enabled] / [Disabled]	· This option allows user to enable or disable WWAN device in BIOS Setup Utility. · If WWAN device is disabled, the device can’t be utilized until enable it in BIOS. · The default value is [Enabled]
Card Reader	[Enabled] / [Disabled]	· This option allows user to enable or disable multi-function card reader device in BIOS Setup Utility. · If card reader device is disabled, the device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
USB Ports	[Enabled] / [Disabled]	• This option allows user to enable or disable external USB ports for both USB 2.0 and USB 3.0. It is included USB Port in Port Replicator and Dock. • If USB Ports is disabled, all external USB Ports can’t be utilized until enable it in BIOS Setup Utility. • The default value is [Enabled].
Wired LAN	[Enabled] / [Disabled]	· This option allows user to enable or disable external LAN ports, included LAN Port in Port Replicator and Dock. · If Wired LAN is disabled, the device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Optical Drive	[Enabled] / [Disabled]	· This option allows user to enable or disable Optical Drive · If Optical Drive is disabled, the device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].

ITEM NAME	EXAMPLE	REMARK
Audio	[Enabled] / [Disabled]	· This option allows user to enable or disable Audio device, include Audio Port in Port Replicator and Dock. · If Audio device is disabled, the audio device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Speaker & Headphone	[Enabled] / [Disabled]	· This option allows user to enable or disable Speaker & Headphone · When Audio device is disabled, grey out the option but leave the setting no change · If Speaker & Headphone are disabled, those devices can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Microphone	[Enabled] / [Disabled]	· This option allows user to enable or disable Microphone · When Audio device is disabled, grey out the option but leave the setting no change · If Microphone is disabled, the device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Camera	[Enabled] / [Disabled]	· This option allows user to enable or disable camera device. · If camera device is disabled, the camera device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Fingerprint	[Enabled] / [Disabled]	· This option allows user to enable or disable fingerprint device. · If finger print device is disabled, the fingerprint device can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled].
Type C	[Enabled] / [Disabled]	· This option allows user to enable or disable the devices connected through Type C (DP not included). · If Type C is disabled, any devices connected through Type C can’t be utilized until enable it in BIOS Setup Utility. (DP not included) · The default value is [Enabled]. · Item Specific Help wording: Enable/Disable device connected through Type C (Display Port not included)
Thunderbolt Controller	[Enabled] / [Disabled]	· This option allows user to enable or disable the devices connected through TBT. · If TBT is disabled, any devices connected through TBT can’t be utilized until enable it in BIOS Setup Utility. · The default value is [Enabled]. · Item Specific Help wording: Enable/Disable device connected through Thunderbolt Controller

ITEM NAME	EXAMPLE	REMARK
Power-off USB Charge	[Enabled] / [Disabled]	· This option allow user to enable or disable USB charge function when system is off or in Sleep mode. · Add below description for item specific help: Enables you to charge mobile devices when your computer is off or in Sleep mode. · The default value is [Enabled].
Battery Threshold	[10%] / [20%] / [30%]	· If Power-off USB Charge is enabled, when battery power lower than battery threshold, Power-off USB Charge won't charge the external USB device. · If Power-off USB Charge is disabled, battery threshold is grayed out. · The string of "Battery Threshold" should indent one character. · Add below description for item specific help: Set a computer battery charge limit, below which charging stops. · The default value is [30%].
ASF Support	[Enabled] / [Disabled]	· This option allow user to enable or disable ASF feature (Alert Standard Format). · The default value is [Disabled].
USB Boot	[Enabled] / [Disabled]	· Default is enabled · When USB Boot is disabled, under Boot priority order, USB boot device type is displayed but no device detected. No USB bootable device shows on F12 Boot Manager.
System Diagnose		· Enter to select 3rd HDD Test and Memory test sub menu
Disk Sanitizer		· Enter to select 3rd Disk Sanitizer function
USB Device Filter	[All Allowed]	· Enter to select USB filtered devices on USB Ports 3 types: All Allowed Keyboard/Mouse Only Read-Only · Don't take effective on interior devices. · The default value is [All Allowed].

ITEM NAME	EXAMPLE	REMARK
System Health Indicator	[Enabled] / [Disabled]	· When set to enabled, display LED indicator status and keeping update CPU temperature and Fan speed status · When set to disable, gray out below items and hide LED indicator. · The default value is [Disabled].
CPU Temperature	XX°C	· Regular to get current CPU temperature from EC

ITEM NAME	EXAMPLE	REMARK
Discrete Graphic Temperature	XX°C	· Regular to get current Discrete Graphic temperature from EC
CPU Fan Speed	XXXXRPM	· Regular to get current CPU fan speed from EC
SYS Fan 1 Speed	XXXXRPM	· BIOS to query EC if SYS Fan 1 exist than present it · Regular to get current SYS fan1 speed from EC
SYS Fan 2 Speed	XXXXRPM	· BIOS to query EC if SYS Fan 1 exist than present it · Regular to get current SYS fan1 speed from EC
Memory Status		· Base Memory test result · The default value is Normal
HDD Status		· Base on POST SMART test result · BIOS to detect how many SSD/HDD present and display corresponding status
Processor Status		· Please refer to System Indicator PES error type definition.
Motherboard Status		· Please refer to System Indicator PES error type definition.
Graphics Controller Status		· Please refer to System Indicator PES error type definition.
BIOS CHKSUM Status		· BIOS checksum error.

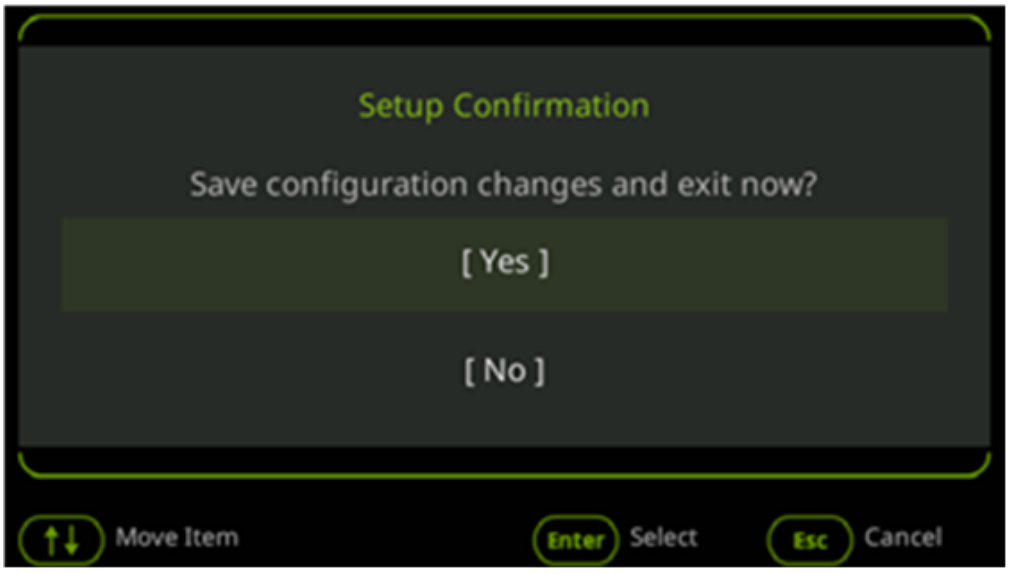
5.4.3 Security Tab

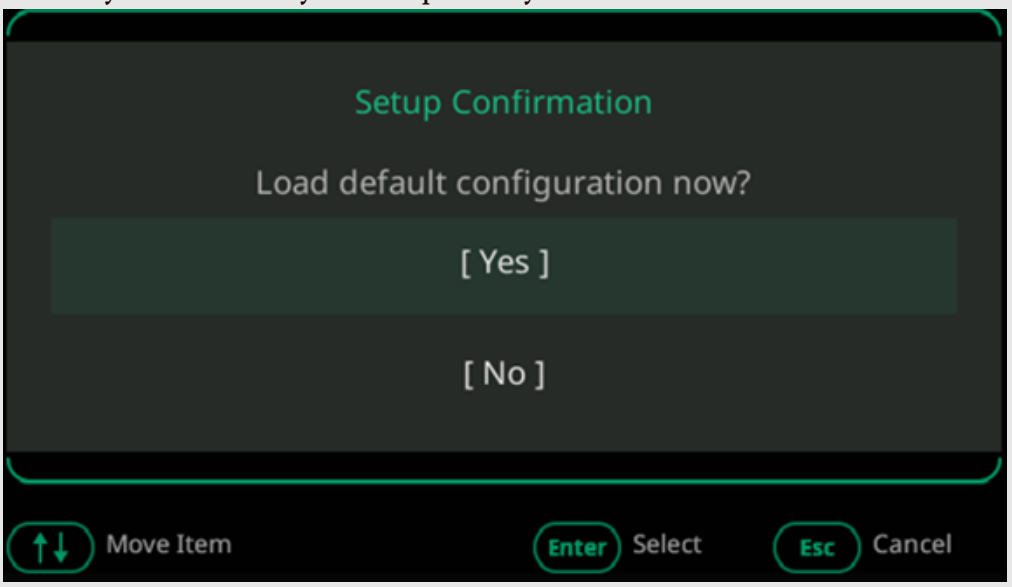
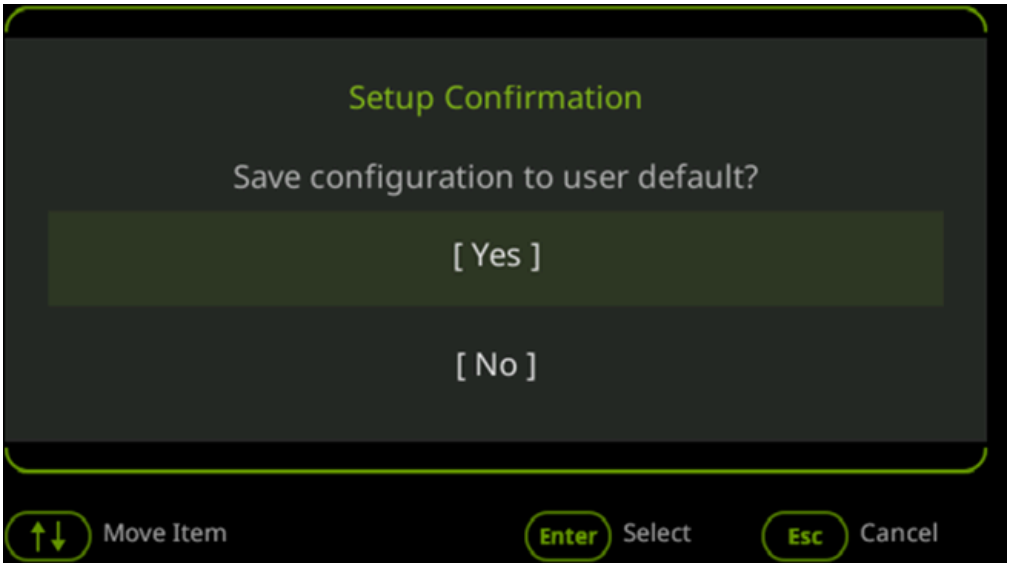
ITEM NAME	EXAMPLE	REMARK
HDD Password	[Set] / [Clear]	This field indicates if HDD Password is set or not.[Frozen]: If HDD status is frozen. [Set]: HDD Password is set. [Clear]: HDD Password it not set. The default value is [Clear]. If the storage leverage OPAL protocol, add (OPAL) as identification. NVMe SSD doesn’t support ATA and Pyrite 1.0 protocol password.

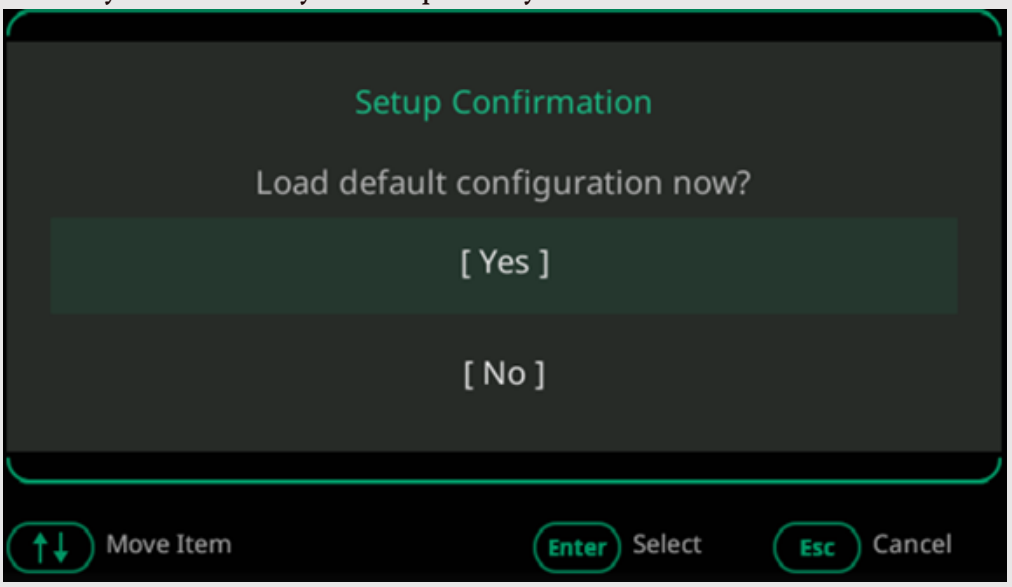
ITEM NAME	EXAMPLE	REMARK
Set HDD Password	[Enter]	This field always show default value [Enter]. HDD Password Security: This feature is available to user when HDD password is set. Password can be written on HDD only when HDD password is set. If system has more than 1 HDD, the items that listed on the Security Menu should be as below: Set HDD0 Password Set HDD1 Password If the storage leverage OPAL protocol, add (OPAL) as identification.
Revert HDD (OPAL) Device	[Enter]	This field always show default value [Enter]. Only available for the storage leverage OPAL protocol If Supervisor Password it not set, the option should be a grayed out item. User requires entering PSID printed on storage label. It revert the OPAL Device to factory default and erase all data. A caution message must pop up to let end user reconfirm the unrecoverable action. “Caution: Revert device will erase all data and can’t be recovered. Do you really want to proceed? [Y/N]” Naming rule following storage display
Executed Revert Count	Executed Date + HDD(OPAL) Device name	· This item default should be hidden. · Only visible after user press “Service key” in this page (Security Tab). · The Date format should be MM/DD/YY and get from CMOS date · This option will keep the latest five data
Authorized Signatures	[Enabled] / [Disabled]	· This item default should be hidden. · Only visible after the Secured-core PC identifier variable “BuiltAsSecuredCorePC” be set to non-zero value. · [Enabled]: Load MSFT 3rd Party UEFI CA. · [Disabled]: Do not load MSFT 3rd Party UEFI CA and gray out “Select and UEFI file as trusted” option.

ITEM NAME	EXAMPLE	REMARK
TPM Device Selection	[iPTT] / [dTPM] / [PSP fTPM] / [Pluton fTPM]	[iPTT]: Intel PTT. [dTPM]: Discrete TPM only. [PSP fTPM]: AMD PSP firmware TPM. [Pluton fTPM]: Microsoft Pluton firmware TPM, support when Microsoft processor is enabled If the project region is for WW, the default value is [dTPM] or [Pluton fTPM]. Only visible on AMD platform which support Pluton. If project only support one type of TPM, the item should be removed. If the project region is for China, the default value is [iPTT], [PSP fTPM] or [Pluton fTPM]. Only visible on which support Pluton platform. If project only support one type of TPM, the item should be removed. This item should permanently grayout and cannot be load default.
Absolute Persistence Module	[Enabled] / [Disabled] / [Permanently Disabled]	This field indicates the state of Absolute Persistence Module. · [Enabled]: The Persistence interface is enabled. Persistence may now be activated or deactivated. · [Disabled]: The Persistence interface is disabled. The Persistence Module does not run and Persistence is deactivated. · [Permanently Disabled]: Persistence is disabled and can only be enabled via a full reset at the factory. If user chooses Permanently Disabled, popup one “red” warning dialog box and describe “Absolute Persistence Module will be disabled permanently and cannot be enabled again, are you sure?” The default value is [Enabled]. If Supervisor Password is not set, it should be a grayed out item. If value is [Permanently Disabled], it should be always grayed out. (Also cannot changed by Load Default)

5.4.4 Exit Tab

ITEM	REMARK
Exit Saving Changes	· Allow users to save changes and reboot the system. · A confirmation message will pop up as below when user executes this item. System will save changes and then continue to reboot if “Yes” is selected or will stay in Setup Utility if No is selected. 
Exit Discarding Changes	· Allow users to discard changes before exiting Setup Utility. · A confirmation message will pop up as below when user executes this item. System will discard changes then continue to reboot if “Yes” is selected or will stay in Setup Utility if No is selected. 
Save & Shutdown	· Allow users to save changes and shutdown the system. · A confirmation message will pop up as below when user executes this item. System will save changes and then continue to shutdown if “Yes” is selected or will stay in Setup Utility if “No” is selected.

ITEM	REMARK
Load Factory Setup Defaults	· Allow user to load factory default configurations in Setup Utility. · A confirmation message will pop up as below when user executes this item. System will stay in Setup Utility after either selection. 
Save Settings to User Setup Defaults	· Allow users to save settings to user setup default. 

ITEM	REMARK
Load User Setup Defaults	· Allow user to load user default configurations in Setup Utility. · A confirmation message will pop up as below when user executes this item. System will stay in Setup Utility after either selection. 

5.5 vPro

For the vPro SKU, if any design violates BIOS spec definition, please follow vPro's request.

5.5.1 WOL/Wake on WLAN

Support Wake on LAN / Wake on wireless LAN from S3/S4/S5 under AC/DC to fulfill vPro validation.

5.5.2 Remove ASF SCU option

Intel vPro doesn't claim ASF. Remove ASF BIOS setup option for vPro SKU.

5.5.3 Add TXT SCU option

Add TXT BIOS setup option under advance page (default set to disabled).

If the system configure as MSFT Security Level 3, set the TXT option default enabled. And please be noticed! It should follow Intel TXT enabling guide in advance before enabling TXT.

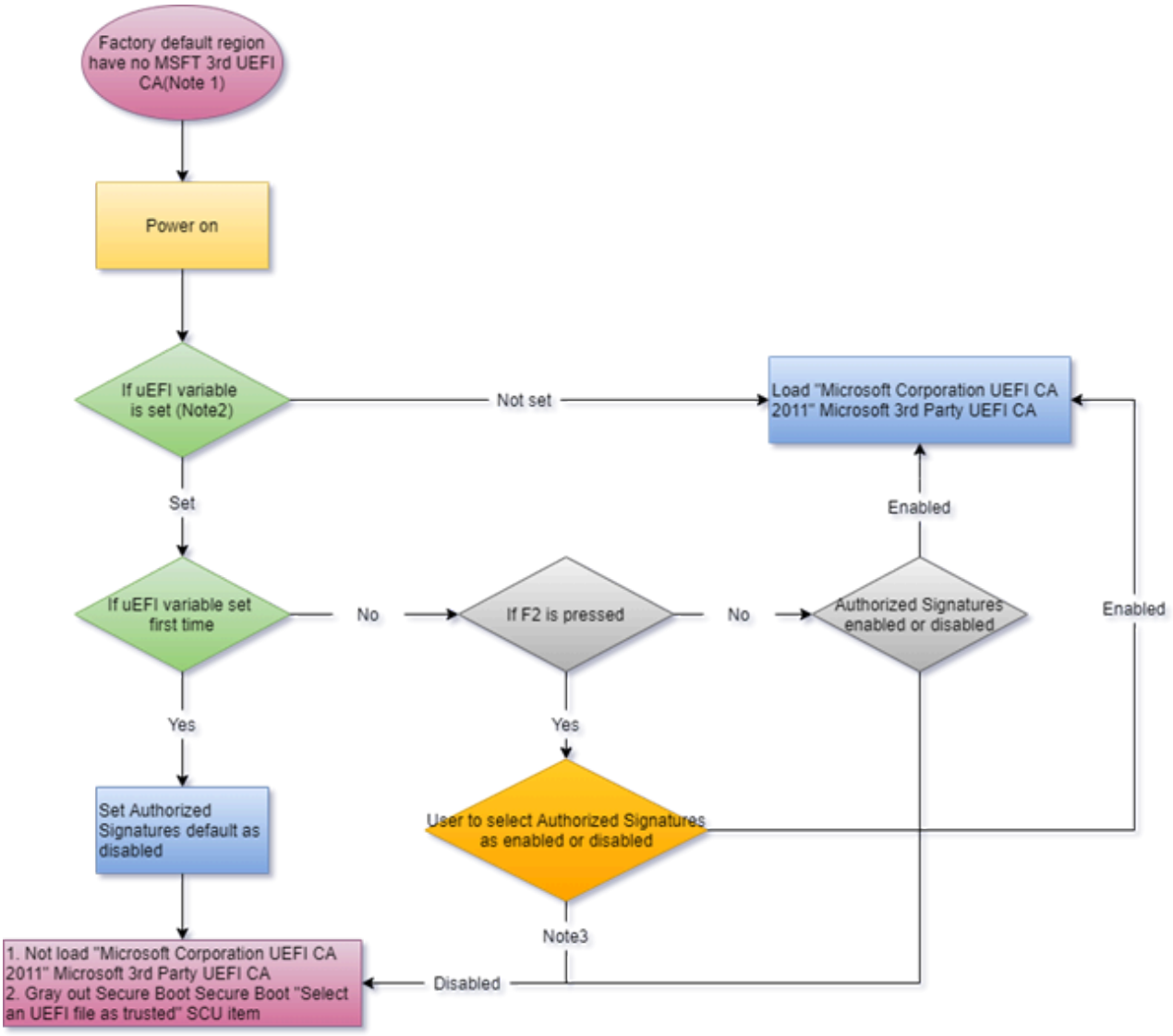
BIOS has to make sure the TXT option default setting should be preserved as below table after doing firmware update at end user side:

Security Level 3 System	Intel TXT option default setting
Yes	Enabled
No	Disabled

5.5.4 Secured-Core PC support

If the system requires to support Secured-Core PC, the Secure Boot must be enabled and not configured to trust the Microsoft 3rd Party UEFI CA by default. The BIOS SCU will have an “Authorized Signatures” option that enables changing the Secure Boot configuration to trust the 3rd Party CA.

Below flow chart describes the behavior when the Secured-core PC identifier be set to non-zero:



5.5.5 Secured-Core PC device identifier

A UEFI variable must be injected to non-zero value for Intel vPro/AMD Pro SKU at ODM factory side, and the UEFI variable format is as the following:

UEFI variable name: BuiltAsSecuredCorePC

UUID: 77fa9abd-0359-4d32-bd60-28f4e78f784b

Attributes: EFI_VARIABLE_NON_VOLATILE | EFI_VARIABLE_BOOTSERVICE_ACCESS | EFI_VARIABLE_RUNTIME_ACCESS

To set UEFI variable “BuiltAsSecuredCorePC” with 1 byte. It can use any byte 0,1,2,3…

Non-zero value: Treat the device as Secured-core

0 or value not set: Treat the device as non-Secured-core

5.6 System Health Indicator

The status LED indicators that display error status during system startup, BIOS setup utility and Acer control center. Common causes for system instability may include the system fan, CPU fan, system temperature, CPU temperature, memory and HDD.

For more detail implementation please refer to “S016 NB System Health Indicator”

5.7 Custom Logo Replacement

All commercial projects have to support custom logo replacement feature. For more details please refer to “S004 Acer NB BIOS Custom Logo Replacement PES”.

5.8 Device Firmware Configuration Interface (DFCI) Management

With Windows Autopilot Deployment and Intune, we can manage BIOS SCU settings after they're enrolled by using the DFCI. DFCI enables Windows to pass management commands from Intune to UEFI for Autopilot deployed devices. This capability allows us to limit end user's control over BIOS settings.

All commercial projects have to support DFCI. For more detailed Microsoft DFCI scenario requirements and validations, please refer to MSFT latest DFCI related document.

The DFCI and Acer ABST tool cannot coexist, it will depend on commercial project or tender request to support.

5.9 Intel Chasm Falls Support Scope

5.9.1 Feature

- Firmware Capsule update: BIOS + CSME / Microcode / ACM module
- Firmware Recovery: BIOS + CSME / Microcode / ACM module

5.9.2 Criteria

- Feature scope support NIST SP800-193, Platform Firmware Resiliency Guidelines.
- Follow Intel Chasm falls validation Architecture Specification
- ESP(EFI system partition) reserved: 120MB

5.10 Discrete TPM Firmware Capsule update

5.10.1 Update methods

- Discrete TPM have a Device Firmware in Device Management. Support firmware update via update driver manually.
- Support dTPM firmware update via Windows update.

5.10.2 Package

- ODM prepare driver package with dTPM vendor for dTPM firmware.
- Package include dTPM firmware (*.bin or *.cap), *.inf and *.cat.
- GUID of dTPM in *inf should be same as FMP driver of dTPM in BIOS.

5.10.3 Behavior and criteria

- System BIOS include dTPM FMP driver and public key .
- After capsule update, Device Firmware in Device Management will change to dTPM’s name and version.
- DTPM capsule update can’t rollback to older firmware version.

5.11 AMD A/B Recovery Support

5.11.1 Feature

- AMD A/B recovery scheme formally separates SPI flash space into different partitions; a primary, ”A” and a secondary, “B”, which hold the same set of system firmware. Normally the system boots from partition A, but if the A partition is found to be corrupted, the system will switch to partition B and boot.

- A/B recovery design which has two identical PSP FWs (PSP FW- L2A/L2B) and two identical PEI (Boot Block 1/2).

- Windows Secured-core PC requires Firmware Anti Rollback(FAR) and FAR requires A/B recovery support.

5.11.2 Criteria

- Follow AMD Platform Security Processor A/B Recovery Design Guide.

5.12 Tender Request Enabling

5.12.1 Feature

- Acer BIOS requires a Double Word UEFI variable to store tender request settings. This dword can be modified by UEFI tool. Related parameters should not release to end user.

- UEFI variable name: TenderRequestEnabling

- UUID: 543f602a-4adf-11ed-b878-0242ac120002

- Attributes: EFI_VARIABLE_NON_VOLATILE | EFI_VARIABLE_BOOTSERVICE_ACCESS | EFI_VARIABLE_RUNTIME_ACCESS

- UEFI variable length is 4 bytes(dword). Default value is zero.

BIT	NAME	BIT	NAME
0	Insyde DST 0: Disable 1: Enable	1	Insyde DWT 0: Disable 1: Enable

BIT	NAME	BIT	NAME
2	Acer Application Base Driver 0: Enable 1: Disable	3	Power Shell WMI Feature 0: Disable 1: Enable
4	Copilot Key Support 0: Default 1: Customized		

6. Tablet BIOS Requirements

The chapter lists tablet platform BIOS requirements that difference from notebook behavior in previous chapters. Scope is Acer Windows on Intel SoC tablet projects.

6.1 Hotkey

In order to support basic function during pre-OS state, define combination hotkey for detachable/tablet device that keyboard will not be present always.

HOT KEY	ENTER BIOS SETUP	DISPLAY BOOT MENU	RECOVER OS	CRISIS RECOVERY
Product with laptop mode	F2	F12	Alt + F10	NA
Product with discrete-tablet mode(i.e., Tablet/Detachable/2-in-1 device)	Power Button + Volume Up	Power Button + Volume Down	NA (D2D recovery by option in BIOS setup menu)	Power Button + Volume Up + Windows Button (or Power Button + Volume Up + Volume Down, if no Windows Button)

If product supports both laptop mode and discrete-tablet mode, it should support all above.

6.2 Wake Up Event

Individual windows button could wake up system from S3.

6.3 Acer Fast Boot

Do not enable Fast boot if tablet bundle with USB docking.

6.4 Power Button

To prevent system from booting up by hitting power button incidentally, a valid power on event is keep pressing 2 seconds power button by hardware silicon judgment.

6.5 Charging Indicator

Please refer indicator spec in LED section for charging indicator implementation if system is without LED.

6.6 USB Docking Hotplug support

In pre-OS stage, BIOS is able to support USB docking hotplug for BIOS setup utility and password input.

6.7 Smooth Battery Percentage

Below requirements are defined for better user experience of battery percentage change. If Full Charge bit is supported in gas gauge design, please implement and follow “Battery Percentage” algorithm in Notebook section.

1. Reported 100% to OS if battery has been charging at 99%.
2. Once battery percentage reaches 100%, let it be 100% always with AC adapter attached.
3. Decrease the battery percentage by 1% per change from 100% to 90%

6.8 Crisis Recovery

· Make sure AC adapter is powered and plugged-in. This requirement is not applies on the project which has form factor with one USB port shard by USB data and USB charging.

· Power on the system from off state (i.e. cold boot) while holding down “Volume Up” button + “Volume Down” button + “Power” button.

· After Post, release “Volume Up” button + “Volume Down” button + “Power” button. The system should boot from USB drive and perform crisis recovery action.

· After recovery completed, system should directly reboot normally.

6.9 Software shipping mode

In the production line, device must enter shipping mode before packaging to avoid boot up by power button is pressed incidentally. If the shipping mode cannot be implemented by EC or battery IC, BIOS must take the responsibility for SW shipping mode with following requirements.

l The only one criterion to exist shipping mode is to power on device with AC adapter connected.

l If device is powered on without AC connected. BIOS must stop boot process and shut the device off. All the routines of SW shipping mode must be completed during POST, prior to the Windows loader be loaded.

l SW shipping mode must not cause data lost on any of storages, including of BIOS storage, main storage and any rom which stores UEFI variables, device specific data and etc.

6.10 Virtual Keyboard support

In pre-OS stage, BIOS is able to support virtual keyboard for BIOS setup utility and password input.

6.11 IHV Specific design requirements

6.11.1 Intel platform

6.11.1.1 OS Combination key support

In order to support some combination key with tablet only, such as press “power button + volume down to simulate “ctrl + alt + del” combine key, the system has to adapt Intel HID event filter driver design.

Intel HID event filter driver allows the SBIOS to send Intel HID messages and button events to the operating system for various key presses. Follow latest “Intel HID Event Filter Release Notes and Bring Up Guide” to implement the feature.