S7G FWs Update SOP

REV.E_V4

1. Prerequisite FW Version

- This document is used to guide the user to process the FWs update step by step and provide the notices that need to be considered during each process.
- If the system configuration is Rev.A (BMC 3.01/ BIOS 3A03), please update BMC to Rev.B (BMC 3.09) first then proceed to Rev.E (BMC 3.60).
- Due to the BMC code base change introduced in version 3.60, please ensure the BMC firmware is updated without selecting the "Preserve all Configuration" option. Please also be informed that the BMC settings and configurations will be erased and reverted to default values after the firmware update, including the BMC IP address, user accounts, and passwords.
- There is one important information that is if the user wants to update SBIOS/VBIOS/EROT by WebUI or Redfish method after turning the DC to OFF state, please wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- Please follow below sequence for different FW version update.
 - Case 1 (if system customer get FW Rev.A- BMC 3.01/ BIOS 3A03): FW package need include 3.09 / update by WebUI.

Sequence 1: BMC update 3.01 to 3.09 \rightarrow BMC update 3.09 to 3.60 \rightarrow FPGA \rightarrow EROT update \rightarrow SBIOS \rightarrow VBIOS.

Case 2 (if system customer get FW Rev.A- BMC 3.01/ BIOS 3A03): FW package need include 3.09 / update with Command Line.

Sequence 2: BMC update 3.01 to 3.09 thru redfish \rightarrow BMC update 3.09 to 3.60 thru redfish \rightarrow FPGA thru redfish \rightarrow EROT update thru redfish \rightarrow SBIOS thru redfish \rightarrow VBIOS thru redfish.

Case 3 (if system customer get FW Rev.B/C/D- BMC 3.09/BIOS 3A06, BMC 3.19/BIOS 3A11, or BMC 3.35/BIOS 3A14): update by WebUI.

Sequence 3:

(Rev.B/C) BMC update 3.09/3.19 to 3.60 \rightarrow FPGA \rightarrow EROT update \rightarrow SBIOS \rightarrow VBIOS. (Rev.D) BMC update 3.35 to 3.60 \rightarrow SBIOS.

Case 4 (if system customer get FW Rev.B/C/D- BMC 3.09/BIOS 3A06, BMC 3.19/BIOS 3A11, or BMC 3.35/BIOS 3A14): update with Command Line.

Sequence 4:

(Rev.B/C) BMC update 3.09/3.19/3.35 to 3.60 thru redfish \rightarrow FPGA thru redfish \rightarrow EROT update thru redfish \rightarrow SBIOS thru redfish \rightarrow VBIOS thru redfish.

(Rev.D) BMC update 3.35 to 3.60 thru redfish \rightarrow SBIOS thru redfish.



	Quanta Verified Rev.(Rev.A)
вмс	3.01.00
EROT	V1.03.103
FAN CPLD	V07
FPGA	0v78
SBIOS	3A03[boot fw 00.19.00]
VBIOS	96.00.7E.00.02

	Quanta Verified Rev.(Rev.B)		
вмс	3.09.00		
EROT	V1.03.103(erot lower than 103 could skip 103 and upgrade to		
	114)		
FAN CPLD	V07		
FPGA	0v78		
SBIOS	3A06[boot fw 01.00.01]		
VBIOS	96.00.7E.00.02		

	Quanta Verified Rev.(Rev.C)		
вмс	3.19.00		
EROT	V1.03.114		
FAN CPLD	V07		
FPGA	0v8A		
SBIOS	3A11[boot fw 01.00.05]		
VBIOS	96.00.84.00.02		

	Quanta Verified Rev.(Rev.D)
вмс	3.35.00
EROT	V1.03.119
FAN CPLD	V07
FPGA	0ν96
SBIOS	3A14[boot fw 01.01.05]
VBIOS	96.00.8D.00.03

	Quanta Verified Rev.(Rev.E)
вмс	3.60.00
EROT	V1.03.119
FAN CPLD	V07
FPGA	0v96
SBIOS	3A22[boot fw 02.00.06]
VBIOS	96.00.8D.00.03

2. Update Procedure

Recommend turning the system power off (DC OFF) before operating all "Cases" of FW update, please refer to the following procedures to complete the upgrade process.

Case1 (System FW is Rev.A)-update via WebUI:

If the system configuration is Rev.A (BMC 3.01/ BIOS 3A03), the FW package needs to include BMC v3.09 for update to v3.60, and the update method is by **WebUI and IPMI tool (for FPGA)**.

Please Power off (DC off) system before doing the upgrade, connect to BMC and login WebUI:

- > Default BMC Account/Password for v3.01: admin/admin
- > Default BMC Account/Password for v3.09 or later: admin/cmb9.admin

Baseboard Management Controller	
	admin
	US - English Remember Username Sign me in
	I forgot my password

A. BMC v3.01 to v3.09:

1. Open WebUI->Maintenance->Firmware Update.



- 2. Open file browser and select the "encrypted_rom.ima_enc" of V3.09 package file.
- 3. Click "Start firmware update" button.
- 4. Choose "Both Images" item.
- 5. Uncheck the "Preserved" box.
- 6. Click "Proceed to Flash" button.

Note:	
Following are the Firmware update metho	ods and components supported in this page.
 Dual Firmware update. 	
 HPM Firmware update supports the 	e following components.
BOOT and APP BOOT	
 EBCA Ermuse undate 	
 BDCM DAID (the undate bas 	no progress percentage, please wait a few minutes for the success alerti
 CPLD 	in the first of the second s
PLDM Firmware update.	
 BIOS Firmware update 	
encrypted rom.ima enc 2.	۵
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type:	e
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: [The dual image formation to be used for	HTTPS Trimware update is displayed as follows. To configure Image to be booted from upon Keset, choose
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: I he dual image formation to be used for Dual image Configuration' under Mainte	HTTPS Thimware update is displayed as follows. To configure Image to be booted from upon Reset, choose citative.
encrypted rom.ima enc 2. Start firmware update 3. Protocod Type: I he dual image formation to be used for Dual image Configuration' under Mainto Current Active image	HTTPS ctrimware update is displayed as follows. Io contigure Image to be booted from upon Keset, choose charace. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: I he dual image formation to be used for Dual image Configuration' under Mainte Current Active image image to be Updated	HTTPS Cfirmware update is displayed as follows. To configure Image to be booted from upon Keset, choose charace. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocod Type: I he dual image formation to be used for Dual image Configuration' under Mainte Current Active image Image to be Updated Inactive Image	HTTPS Thrmware update is displayed as follows. To configure image to be booted from upon Reset, choose charace. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: I he dual image formation to be used for Dual image Configuration' under Mainto Current Active image Image to be Updated Inactive Image Inactive Image	HTTPS Cfirmware update is displayed as follows. To configure Image to be booted from upon Keset, choose charace. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: The dual image formation to be used for Dual image Configuration' under Mainte Current Active Image Image to be Updated Inactive Image Inactive Image Inactive Image Inactive Image Inactive Image	HTTPS Trimware update is displayed as follows. To contigure Image to be booted from upon Reset, choose ensure. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocol Type: The dual image formation to be used for Dual image Configuration' under Mainte Current Active Image image to be Updated Inactive Image Inactive Image Inactive Image Image 2 4.	HTTPS Thimware update is displayed as follows. To configure Image to be booted from upon Reset, choose charket. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocod Type: I he dual image formation to be used for Dual image Configuration' under Mainte Current Active Image Image to be Updated Inactive Image Inactive Image Inactive Image Inactive Image Inactive Image Image 2 4. Both Images	HTTPS Thrmware update is displayed as follows. To configure image to be booted from upon Reset, choose criatice. Image 1
encrypted rom.ima enc 2. Start firmware update 3. Protocod Type: I he dual image formation to be used for Dual image Configuration" under Mainte Current Active image Image to be Updated Inactive Image Inactive Image Inactive Image Inactive Image Inactive Image Inactive Image Inactive Image Image 1 4. Both Images	HTTPS Thrmware update is displayed as follows. To configure image to be booted from upon Reset, choose criative. Image 1
encrypted rom.ima enc 2. Start firmwarc updatc 3. Protocol Type: The dual image formation to be used for Dual image Configuration' under Mainte Current Active Image image to be Updated Inactive Image Inactive Image Inactive Image Inactive Image Image 2 4. Both Imaget Preserve all Configuration. This will tem marked as preserve/overwrite in th	HTTPS Thirmware update is displayed as follows. To configure Image to be booted from upon Reset, choose charket. Image 1 I preserve all the configuration settings during the firmware update - Intespective of the Individual to table below.

7. When the update process is completed, the BMC will restart and the user needs to change the password by using the default password "cmb9.admin" to a new one for the next steps of the BMC update.

Oakhboard Sensor System Inventory FRU information Let. Logs & Reports	Note: Pollowing are the Firmware update methods and components supported Data Firmware update. Hist Row Components. BOOT update supports the following components. BOOT update supports the following components. PEOA Firmware update. PCND Remark and the.	Firmware reset has been called. Close the current session, and open a new session after a couple of minutes.
Settings Remote Control	BIOS Firmware update Select Firmware image	
Image Redirection	encrypted_rom.ima_enc	i st⊜ar i
E PLDM	Start fermioare apdate	
O Power Control	Protocol Type: HTTP5	
 Maintenance € Sign out 	The dual image formation to be used for firmware update is displayed as spon Reset, choose "budge Configuration" under Maintenance. Current Active image Image Image 1 Image to be Updated Both Images	tollows. To configure image to P-shooted from Processing
	Reboot the device after update	
	Preserve all Configuration. This will preserve all the configuration irrespective of the individual items marked as preserve/overwrite in the	artings during the firmware update - table below.
	Resetting	
	firmware Update (Comp	leted.)

B. Update BMC v3.09 to v3.60:

Upgrade process is the same as steps1~7 of "A", the difference is only to select the "encrypted_rom.ima_enc" of the v3.60 package.

[Note]

- 1. Due to changes in the codebase, BMC v3.09 to v3.60 will update both the active and inactive images simultaneously.
- 2. Please note that the BMC configuration will be erased and reverted to the default values after the firmware is updated, including the BMC IP, User account and Password, as the "Preserve Configuration"

	0	
lote: ollowing are the Firmware update meth • Dual Firmware update. • PLDM Firmware update supports I • BIOS • GPU • EROT	ods and components supported in this page. the following components.	
lect Firmware Image		
Protocol Type: The dual image formation to be used for	HTTPS or firmware update is displayed as follows. To configure Image to be booted from unation' under Maintenance.	
Current Active Image	Image-1	
Image to be Updated		
Image to be Updated Both Images	~	
Image to be Updated Both Images Inactive Image Image 1 Image 2 Both Images	~	
Image to be Updated Both Images Inactive Image Image 1 Image 2 Both Images 5. Preserve all Configuration. This wi rrespective of the individual items mark	Il preserve all the configuration settings during the firmware update - ked as preserve/overwrite in the table below.	

C. Update FPGA (Out-Band command support only):

- 1. Prepare a Linux system with ipmitool installed (WSL is not supported) and open a terminal window.
- 2. Unzip FPGA FW package and change folder to FPGA package location.
- 3. Execute below command by root account:

#./ipmitool_cpld_oob.sh <Username> <Password> <IP> 2 FPGA_lego-cg1_0v96.rpd.hpm
Ex:

./ipmitool_cpld_oob.sh admin adminadmin 192.168.0.120 2 FPGA_lego-cg1_0v96.rpd.hpm

4. It will show the upgrade process as following

[root@localhost FPGA_V96_Update_PKG_SecureBoot]# ./ipmitool_cpld_oob.sh admin adminadmin 192.168.0.120 2 FPGA_lego-cg1_0v96.rpd.hpm Username = admin, Password = adminadmin, IP = 192.168.0.120, 2:(MB_CPLD)3:(FAN_CPLD) = 2, File_path = FPGA_lego-cg1_0v96.rpd.hpm
Setting large buffer to 16383
PICMG HPM.1 Upgrade Agent 1.0.9:
Validating firmware image integrityOK Performing preparation stage Invalid image file for product 14151
Image Information Device Id : 0x20 Prod Id : 0x36ab Manuf Id : 0x001c4c Board Information Device Id : 0x20 Prod Id : 0x3747 Manuf Id : 0x001c4c Continue ignoring DeviceID/ProductID/ManufacturingID (Y/N): Services may be affected during upgrade. Do you wish to continue? (y/n): 0K
Performing upgrade stage:
ID Name Versions % Active Backup File
(*) Component requires Payload Cold Reset
Firmware upgrade procedure successful

[Note]

It might have compatibility issue if using non-Linux system as terminal or using WSL to update FPGA. To run the update process by Redfish, please refer to Case 2.

- D. Update EROT:
- If the system is DC ON, please turn DC off and wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- 1. Open WebUI->Maintenance->Firmware Update.



- 2. Open file browser and select the "cec1736-ecfw-01.03.0119.0000-n01-rel-prod.fwpkg" of FW package file.
- 3. Click "Start firmware update" button.
- 4. Make sure the EID number 11/12 are presented.
- Make sure the version number of the "Uploaded Version" field in the EIDs is "cec1736PkgEcfw-01.03.0119.0000" and it is not the same as the "Existing Version"
- 6. Click Proceed button.
- 7. Click "OK" to agree the update.

rmware	Update	3 1. 1!	92.168.0.120 說 re you sure you want to fla	ish?		
					7. 確定	取消
Note: Following • Dua • PLD	are the Firmw Il Firmware up M Firmware u o BIOS o GPU o EROT	are update methods and componen odate. update supports the following compo	its supported in this page. onents.			
Select Firm	vare Image					
		3. Preparing to	flash			
Please not to comple	e that PLDM te Firmware U	Firmware Update process time will Jpdate.	depend on vendor specific.So it	t may take some time		
# EID	Medium	Uploaded Version	5. Existing Version	Upgrade		
1 11	PCIe	ec1736PkgEcfw-01.03.0119.0000	01.03.0114.0000_n01	×		
2 12	PCle	:ec1736PkgEcfw-01.03.0119.0000	01.03.0114.0000_n01	~		
Proceed						
Proceed	Cancer	Unloadin	ng 100%			
Pr ceed	Cancer	Uploadin	ng 100%			

- 8. Wait the progress bar change from 0% to 100% directly, and a complete message box will pop up on the top.
- 9. Click "OK" to finish the EROT update.



10. After FPGA/EROT update, use IPMI command to reload FPGA/EROT.

Execute Out-band command to cause the BMC to operate some actions and reboot for FGPA and EROT to reload new FW:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x36 0x88

[Note]

This command only works on DC off, please ensure the power status is "OFF" before executing this command to avoid the unexcepted system shutdown.

11. While the BMC rebooted, follow below IPMI commands to check each FW version is new one.

Set EROTs Version get command:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0xC0 0 0xC0
0x01

Get GPU EROT:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0x70 7 0x07 Return value: **01 03 77 00 00 00 14**

Get CPU EROT:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0x60 7 0x07 Return value: **01 03 77 00 00 00 14**

Get FPGA version:

#ipmitool -H <BMC_IP> -U <BMC username> -P <BMC PW> -I lanplus raw 0x06 0x52 0x03 0x16 3 0x04
Return value: 00 09 06

D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x36 0x88 D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x06 0x52 0x03 0xC0 0 0xC0 0xC D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x06 0x52 0x03 0x70 7 0x07 OI 03 77 00 00 00 14 D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x06 0x52 0x03 0x70 7 0x07 OI 03 77 00 00 00 14 D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x06 0x52 0x03 0x60 7 0x07 OI 03 77 00 00 00 14 D:\FAE\Tool\IFMI Tool\ipmitool-1.8.18-cygwin-binary>ipmitool.exe -H 10.10.10.9 -I lanplus -U admin -P adminadmin raw 0x06 0x52 0x03 0x60 7 0x07 OI 03 77 00 00 00 14

E. Update SBIOS

- 1. If the system is DC ON, please turn DC off and wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- 1. Open WebUI->Maintenance->Firmware Update.



- 2. Open file browser and select the "S7G_3A22.fwpkg" of FW package file.
- 3. Click "Start firmware update" button.
- 4. Make sure the EID number 11 is presented.
- 5. Make sure the version number of the "Uploaded Version" field in the EIDs is "cec1736ApFw-3A22".

(The same version update is not allowed before 3A14).

- 6. Click Proceed button.
- 7. Clock "OK" to agree the update.

Firmware Update 1.	10.10.11.110 顯示 Are you sure you wa	ant to flash? 7. 取消	確定		ff Home
Note: Following are the Firmware update. • PLOM Firmware update su • BIOS • GPU • CPU • EROT	te methods and component	s supported in this page. nents.			
Select Firmware Image					
S7G_3A22.fwpkg 2.					b
Start firmware update 3.					
		Preparing to flash			
Please note that PLDM Firmware	Update process time will d	epend on vendor specific.So it may	/ take some ti	me to complete Firmwar	re Update.
# EID Medium	Uploaded Version	Existing Version	Upgrad	e Progress	
1 11 PCIe	cec1736ApFw-3A22	3A22	~	2	
Preserve BIOS NVRAM Regio	n				
6. Proceed Cancel					
		Uploading 100%			
WARNING:Please note that after e automatically closed. If the upgrad Firmware.	ntering the update mode, th dation is cancelled in the mid	e widgets, other web pages and sen ddle of the wizard, the device will be	vices will not v reset only for	vork. All the open widgets BMC BOOT,and APP com	s will be ponents of

Wait the progress bar change from 0% to 100%, and a complete message box will pop up on the top.

- 8. Click "OK" to finish the SBIOS update.
- 9. DC ON to POST_END.
- 10. Send below commands to check the SBIOS version:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus mc getsysinfo system_fw_version
Return value: 3A22

F. Update VBIOS

- 1. Please wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- 1. Open WebUI->Maintenance->Firmware Update.



- 2. Open file browser and select the "g530_0206_888__96008D0003-prod.fwpkg" of FW package file.
- 3. Click "Start firmware update" button.
- 4. Make sure the EID number 12 is presented.
- Make sure the version number of the "Uploaded Version" field in the EIDs is "cec1736ApFwPkg-08d00003".
 (The same version update is not allowed).
- 6. Click Proceed button.
- 7. Clock "OK" to agree the update.

	Are you sure you want to	flash?	
Firmware Update <mark>1</mark> .		7. Bit size	取消
	-	Ø	
Note: Following are the Firmware update method • Dual Firmware update. • PLDM Firmware update supports the • BIOS • GPU • EROT	s and components supported in this page. following components.		
select Firmware Image g530 0206 888 96008D0003-prod.fwpkg	2	>	
Start firmware update 3.	Preparing to flack	_	
Please note that PLDM Firmware Update p	rocess time will depend on vendor specific.S	So it may take some time	
to complete Firmware Update.	on Existing Version	Upgrade	
1 12 PCIe cec1736ApFwPl 6 Proceed Cancel	kg-08d00003 01.03.0119.0000_n01	~	
	Uploading 100%		

- 8. Wait the progress bar change from 0% to 100%, and a complete message box will pop up on the top.
- 9. Click "OK" to finish the VBIOS update.
- 10. Perform "Power Cycle" and DC ON to POST_END.
- 11. Send below commands to check the VBIOS version:
 - #ipmitool -H <BMC IP> -U <BMC username> -P <BMC PW> -I lanplus raw 0x36 0x65 0x4c 0x1c 0x00 0x3 0x45

Return value: 96 00 8d 00 03

Case2 (System FW is Rev.A)-update via Redfish:

If the system configuration is Rev.A (BMC 3.01/ BIOS 3A03), the FW package needs include BMC v3.09 for update to v3.60, and the update method is by **Redfish.**

For execute Redfish command update, the user needs make sure the Redfish password already changed from "superuser" to new one, if it has not been changed, please runs below command first: sudo curl -v -s -k -u Administrator:superuser -H "Content-Type:application/json" -H "If-None-Match:"1"" -X PATCH -d '{"Password": "xxx.xxx"}' https://{BMC IP}/redfish/v1/AccountService/Accounts/1

A. BMC v3.01 to v3.09:

- 1. Change folder to BMC v3.09 location.
- 2. Execute below command to update Image 1:

sudo curl -v -k -u Administrator:\${**New PASSWORD**} -H "expect:" -H "content-type:multipart/form-data" -X POST -F

'UpdateParameters={"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BMCImage1"]};type=appli cation/json' -F 'OemParameters={"ImageType":"BMC"};type=application/json' -F UpdateFile=@encrypted_rom.ima_enc https://\${BMC IP}/redfish/v1/UpdateService/upload

- 3. Wait update completed, the BMC will restart.
- 4. Change redfish password again for Image2 update.
- 5. Execute below command to update Image 2:

sudo curl -v -k -u Administrator:\${New PASSWORD} -H "expect:" -H "content-type:multipart/form-data" -X POST -F

'UpdateParameters={"Targets":["/redfish/v1/UpdateService/FirmwareInventory/BMCImage2"]};type=appli cation/json' -F 'OemParameters={"ImageType":"BMC"};type=application/json' -F UpdateFile=@encrypted_rom.ima_enc https://\${BMC IP}/redfish/v1/UpdateService/upload

6. Wait update completed, the BMC will restart.

B. BMC v3.09 to v3.60:

- 1. Change folder to BMC v3.60 location.
- 2. Change redfish password again.
- 3. Execute the "Disable Preserved configuration" command:

Sudo curl -v -s -k -u Administrator:\${New PASSWORD} -H "Content-Type:application/json" -H "If-None-Match:"1"" -X PATCH -d '{"Oem": {"AMIUpdateService": {"PreserveConfiguration": false}}}' https://\${BMC IP}/redfish/v1/UpdateService 4. Follow steps 2 and 3 of "A." to update BMC version to 3.60.

[Note]

- 1. Due to changes in the codebase, BMC v3.09 to v3.60 will update both the active and inactive images simultaneously.
- Please note that the BMC configuration will be erased and reverted to the default values after the firmware is updated, including the BMC IP, User account and Password, as the "Disable Preserved configuration" command is used in Step 3.

C. Update FPGA:

- 1. Change folder to FPGA FW package v96.
- 2. Execute below command to update FPGA:

sudo curl -s -v -k -u Administrator:\${New PASSWORD} -H "expect:" -H "content-type:multipart/form-data" -X POST -F

'UpdateParameters={"Targets":["/redfish/v1/UpdateService/FirmwareInventory/FPGA_0"]};type=applicatio n/json' -F 'OemParameters={"ImageType":"HPM"};type=application/json' -F UpdateFile=@FPGA_legocg1_0v96.rpd.hpm https://\${BMC IP}/redfish/v1/UpdateService/upload



 To monitor the update status, send below command to get the task status: sudo curl -s -k -u Administrator:\${New PASSWORD} -H "Cache-Control: no-cache" -H "contenttype:application/json" -X GET -H "If-None-Match:W/"1"" <u>https://\${BMC_</u> <u>IP}/redfish/v1/TaskService/Tasks/</u>\${TASK} | python3 -m json.tool



- D. Update EROT:
- Please wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.

- 1. Change folder to EROT FW location.
- 2. Change redfish password again.
- 3. Execute below command to update EROT:

sudo curl -v -k -u Administrator:\${**New PASSWORD**} -H "expect:" -H "content-type:multipart/form-data" -X POST -F 'UpdateParameters={"Targets":[]};type=application/json' -F 'OemParameters={"ImageType":"PLDM"};type=application/json' -F UpdateFile=@cec1736-ecfw-

01.03.0119.0000-n01-rel-prod.fwpkg https://\${BMCIP}/redfish/v1/UpdateService/upload





- To monitor the update status, send below command to get the task status: sudo curl -s -k -u Administrator:\${New PASSWORD} -H "Cache-Control: no-cache" -H "contenttype:application/json" -X GET -H "If-None-Match:W/"1"" https://\${BMC IP}/redfish/v1/TaskService/Tasks/\${TASK} | python3 -m json.tool
- 5. After FPGA/EROT update, use IPMI command to reload FPGA/EROT.

Execute Out-band command to cause the BMC to operate some actions and reboot for FGPA and EROT to reload new FW:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x36 0x88
[Note]

This command only works on DC off, please ensure the power status is "OFF" before executing this command to avoid the unexcepted system shutdown.

6. While the BMC rebooted, follow below IPMI commands to check each FW version is new one.

Before using IPMI command, please sure IPMI password had been changed to new one since BMC will be revert to the default value after the firmware is updated.

Set EROT Version get command:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0xC0 0 0xC0
0x01

Get GPU EROT:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0x70 7 0x07 Return value: **01 03 77 00 00 00 14**

Get CPU EROT:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x06 0x52 0x03 0x60 7 0x07 Return value: **01 03 77 00 00 00 14**

Get FPGA version:

#ipmitool -H <BMC_IP> -U <BMC username> -P <BMC PW> -I lanplus raw 0x06 0x52 0x03 0x16 3 0x04
Return value: 00 09 06

E. Update SBIOS

- If the system is DC ON, please turn DC off and wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- 1. Change folder to SBIOS FW location.
- 2. Execute below command to update SBIOS:

sudo curl -v -k -u Administrator:\${<mark>New PASSWORD</mark>} -H "expect:" -H "content-type:multipart/form-data" -X POST -F 'UpdateParameters={"Targets":[]};type=application/json' -F

'OemParameters={"ImageType":"PLDM"};type=application/json' -F UpdateFile=@S7G_3A22.fwpkg https://\${BMC IP}/redfish/v1/UpdateService/upload



- To monitor the update status, send below command to get the task status: sudo curl -s -k -u Administrator:\${New PASSWORD} -H "Cache-Control: no-cache" -H "contenttype:application/json" -X GET -H "If-None-Match:W/"1"" https://\${BMC IP}/redfish/v1/TaskService/Tasks/\${TASK ID}| python3 -m json.tool
- 4. When update status is "Completed", DC cycle to the POST_END.
- Send below commands to check the SBIOS version:
 #ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus mc getsysinfo system_fw_version Return value: 3A22
- F. Update VBIOS:
- Please wait for about 90 seconds to let the EIDs become available for the BMC update code can access the update device.
- 1. Change folder to VBIOS FW location.
- 2. Execute below command to update VBIOS:

sudo curl -v -k -u Administrator:\${**New PASSWORD**} -H "expect:" -H "content-type:multipart/form-data" -X POST -F 'UpdateParameters={"Targets":[]};type=application/json' -F 'OemParameters={"ImageType":"PLDM"};type=application/json' -F UpdateFile=@g530_0206_888__96008D0003-prod.fwpkg https://\${BMC IP}/redfish/v1/UpdateService/upload



- To monitor the update status, send below command to get the task status: sudo curl -s -k -u Administrator:\${New PASSWORD} -H "Cache-Control: no-cache" -H "contenttype:application/json" -X GET -H "If-None-Match:W/"1"" https://\${BMC IP}/redfish/v1/TaskService/Tasks/\${TASK ID} | python3 -m json.tool
- 4. When update status is "Completed", DC cycle to the POST_END.
- 5. Send below commands to check the VBIOS version:

#ipmitool -H <BMC IP> -U <BMC username> -P <BMC Password> -I lanplus raw 0x36 0x65 0x4c 0x1c 0x00
0x3 0x45

Return value: 96 00 8d 00 03

Case3 (System FW is Rev.B/C/D)-update via WebUI:

A. System FW is Rev.B/C

If the system configuration is Rev. B (BMC 3.09/ BIOS 3A06) or Rev. C (BMC 3.19/BIOS 3A11), the update method is by **WebUI and IPMI tool**.

FW Update Sequence:

BMC update 3.09 (or 3.19) to 3.60 \rightarrow FPGA \rightarrow EROT update \rightarrow SBIOS \rightarrow VBIOS

The update procedure please refer the steps "B" to "F" of <u>Case1</u> to update each FW.

*Please choose "Both Images" item and uncheck the "Preserved" box during BMC FW upgrade.

B. System FW is Rev.D

If the system configuration is Rev. D (BMC 3.35/ BIOS 3A14), the update method is by **WebUI and IPMI tool**. <u>FW Update Sequence:</u>

BMC update 3.35 to 3.60 \rightarrow SBIOS

The update procedure please refer the steps "B" and "E" of *Case1* to update BMC and SBIOS FW.

*Please uncheck the "Preserved" box during BMC FW upgrade.

[Note]

- 1. If system FW upgrade from Rev. D to Rev. E, please ignore FPGA/EROT/VBIOS update because it is the same version as Rev. D.
- 2. Due to changes in the codebase, BMC v3.35 to v3.60 will update both the active and inactive images simultaneously; choosing the "NOT preserved" option is required.
- 3. Please note the BMC configuration will be erased and reverted to the default values after the firmware is updated, including BMC IP, User account and Password.

<u>Case4 (System FW is Rev.B/C/D)-update via Redfish:</u>

A. System FW is Rev.B/C

If the system configuration is Rev. B (BMC 3.09/ BIOS 3A06) or Rev. C (BMC 3.19/BIOS 3A11), the update method is by **Redfish**.

For execute Redfish command update, the user needs make sure the Redfish password already changed from "superuser" to new one, if it has not been changed, please runs below command first: sudo curl -v -s -k -u Administrator:superuser -H "Content-Type:application/json" -H "If-None-Match:"1"" -X PATCH -d '{"Password": "xxx.xxx"}'https://{BMC IP}/redfish/v1/AccountService/Accounts/1

FW Update Sequence:

BMC update 3.09 (or 3.19) to 3.60 \rightarrow FPGA \rightarrow EROT update \rightarrow SBIOS \rightarrow VBIOS The update procedure please refer the steps "B" to "F" of <u>Case2</u> to update each FW.

B. System FW is Rev.D

If the system configuration is Rev. D (BMC 3.35/ BIOS 3A14), the update method is by **Redfish**.

For execute Redfish command update, the user needs make sure the Redfish password already changed from "superuser" to new one, if it has not been changed, please runs below command first: sudo curl -v -s -k -u Administrator:superuser -H "Content-Type:application/json" -H "If-None-Match:"1"" -X PATCH -d '{"Password": "xxx.xxx"}'https://{BMC IP}/redfish/v1/AccountService/Accounts/1

FW Update Sequence:

BMC update 3.35 to 3.60 \rightarrow SBIOS

The update procedure please refer the steps "B" and "E" of *Case2* to update BMC and SBIOS FW. [Note]

- 1. If system FW upgrade from Rev. D to Rev. E, please ignore FPGA/EROT/VBIOS update because it is the same version as Rev. D.
- 2. Please note the BMC configuration will be erased and reverted to the default values after the firmware is updated, including BMC IP, User account and Password.