

GIGABYTE Firmware Upgrade Guide

GIGABYTE Software

Document No.: GFUG-v0.04

Authors:

Kate Cheng

Nick Jen

Sam Su

Approved By:

TS Hwang

Storm Chen

Sam Huang

PROPRIETARY INFORMATION -- NOT FOR PUBLICATION

The information contained herein is the property of Gigabyte Technology Co., Ltd. and is supplied without liability for errors or omissions. No part may be reproduced or used except as authorized by contract or other written permission. The copyright and the foregoing restriction on reproduction and use extend to all media in which the information may be embodied.

Contents

0. General Information	3
0.1. Issue Control	3
0.2. Record of Changes	3
0.3. References	3
0.4. Acronyms	3
1. Supported Upgrade Firmware Method	4
2. Upgrade Firmware Form BMC WebUI	5
2.1. Upgrade BMC Image-1 / Image-2	5
2.2. Upgrade BIOS Image-1 / Image-2	7
2.3. Upgrade CPLD	9
2.4. Upgrade Firmware Form IPMI	12
2.5. Upgrade BMC Image-1 / Image-2	12
2.6. Upgrade BIOS Image-1 / Image-2	12
3. Upgrade Firmware Form Redfish (HTTP)	13
3.1. Upgrade BMC Image-1 / Image-2	13
3.2. Upgrade BIOS Image-1 / Image-2	14
3.3. Multipart Push BMC_FW Update	15
4. Upgrade Firmware Form Restful	17
4.1. Upgrade Active/Backup BMC	17
4.1.1 Preserve BMC Configuration	17
4.1.2 Upgrade Active/Backup BMC	18
4.1.3 Restore BMC Configuration	20
4.2. Upgrade Active/Backup BIOS	20
5. Upgrade Firmware Form Gigafly	23
5.1. Upgrade Active/Backup BMC	23

0. General Information

0.1. Issue Control

This document was edited with **Microsoft Word, Version 2010**. The graphic drawings are originally sketched in **Microsoft PowerPoint Version 2010**.

0.2. Record of Changes

Table 0-1. Record of Changes

Issue	Date	Authors	Reason for Changes
0.01	2022/2/16	Sam Huang	First create for AMI Backup configure by curl
0.02	2022/3/16	Kate Cheng	First create for Upgrade Firmware by WebUI, IPMI, Gigaflash
0.03	2022/9/14	Nick Jen	Modify update BMC Flash2 CMD
0.04	2022/9/30	Sam Su	Modify upgrade BIOS command of restful for AST2600 machine.

0.3. References

NO	Document title

0.4. Acronyms

1. Supported Upgrade Firmware Method

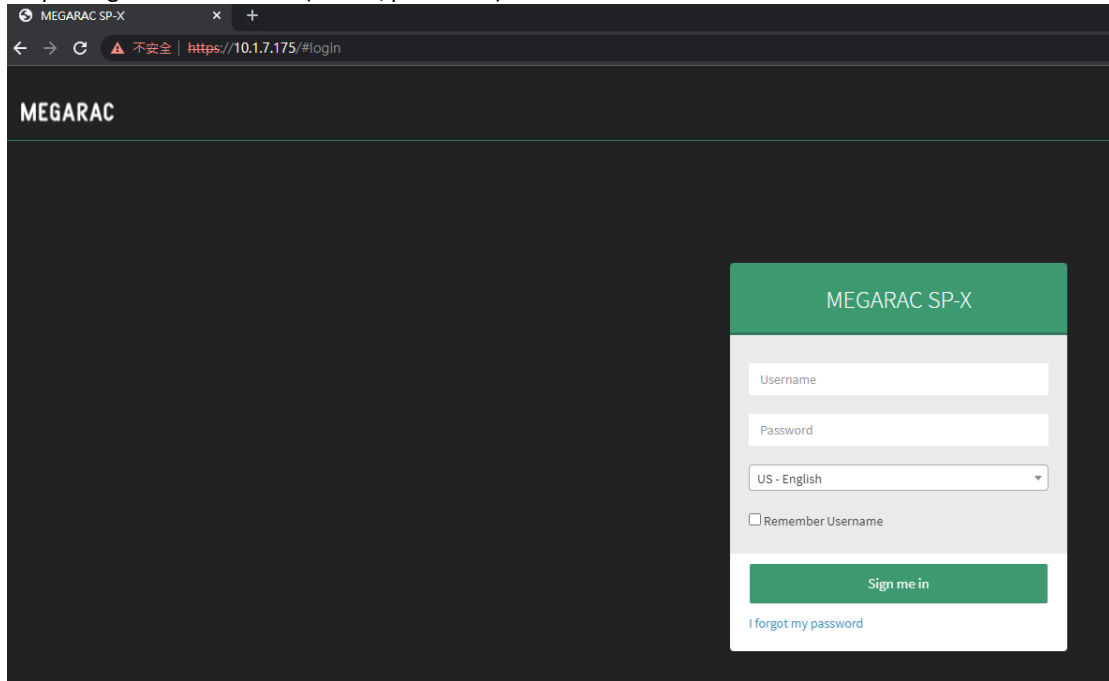
BMC WebUI (BMC/BIOS/CPLD)
IPMI HPM (BMC/BIOS)
Restful API (BMC/BIOS)
Redfish (BMC/BIOS)
Gigaflash (BMC)

2. Upgrade Firmware Form BMC WebUI

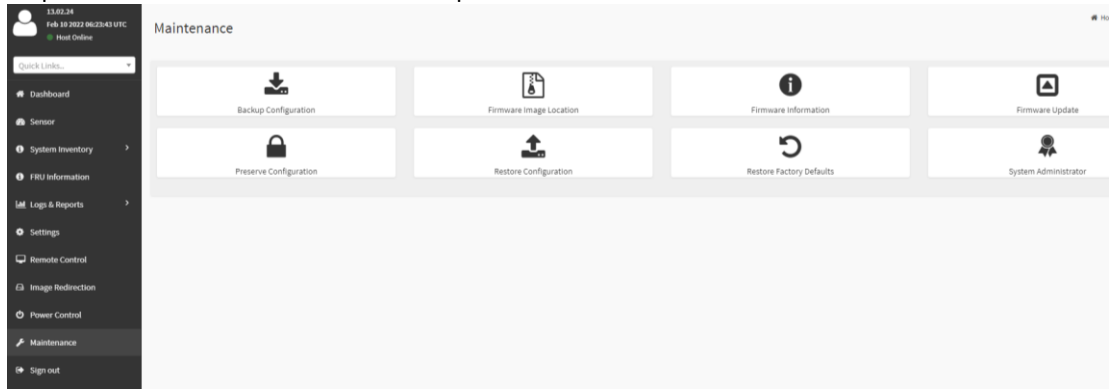
2.1. Upgrade BMC Image-1 / Image-2

Divided into six steps to explain updating FW with WEBUI:

Step1. Log in to the WebUI (admin/password):



Step2. Select Maintenance -> Firmware Update:



Step3. Select a “xxxxx.ima_enc” file:

Note:
Following are the Firmware update methods and components supported in this page.

- BMC Firmware update.
- Dual Firmware update.
- BIOS update (*.rbu). --- Easy BIOS Refresh
- MB_CPLD update (*.rcu).
- BPB_CPLD update (*.rcu).
- ME
- MMC
- AEP
- CPLD
- PLDM Firmware update.
- BIOS Firmware update
- NVMe MI SSDs Firmware update
- FPGA Firmware update (*.rpd).

Select Firmware Image

rom_v130226.ima_enc

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT, and APP components of Firmware.

Step4. Choose image1 or both image because image2 will only be used when image1 broken.
*Of course you can also just update image2.

Select Firmware Image

rom_v130226.ima_enc

Protocol Type: HTTP

Update Type: BMC

The dual image formation to be used for firmware update is displayed as follows. To configure Image to be booted from upon Reset, choose 'Dual Image Configuration' under Maintenance.

Current Active Image Image-1

Image to be Updated

Inactive Image

Inactive Image

Image 1

Image 2

Both Images

☐ Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

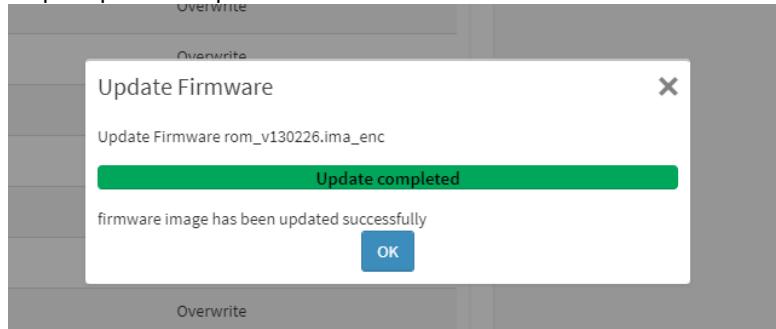
Step5. The screen to confirm and start updating is the same as below:

on setting: 10.1.7.175 顯示

We will start the firmware upgrade now. You will not be able to access BMC until it flashes and restarts. Do you want to continue?

Preserve Status

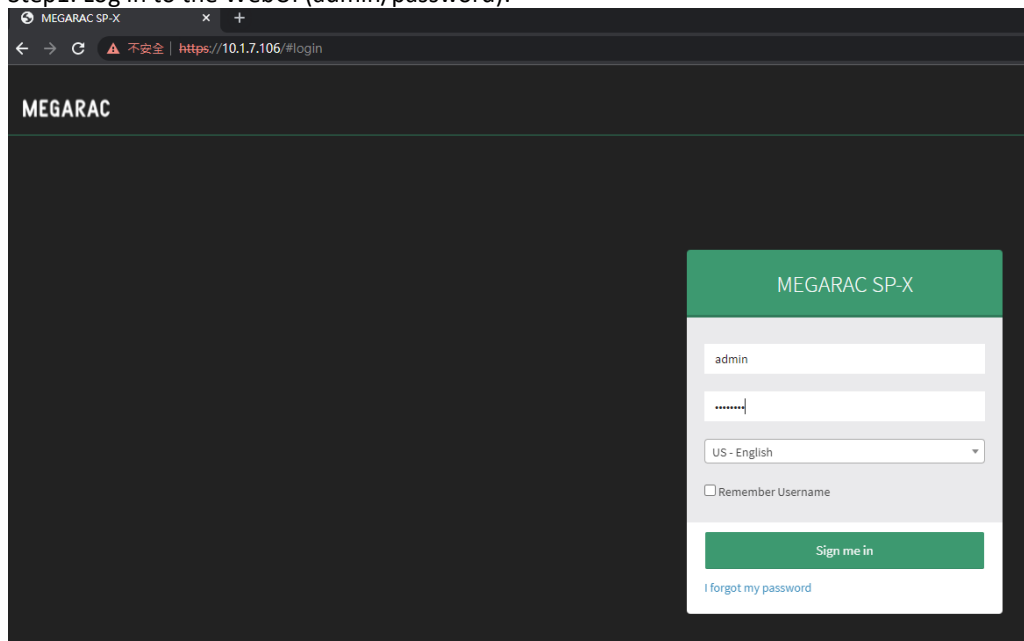
Step6. Update complete:



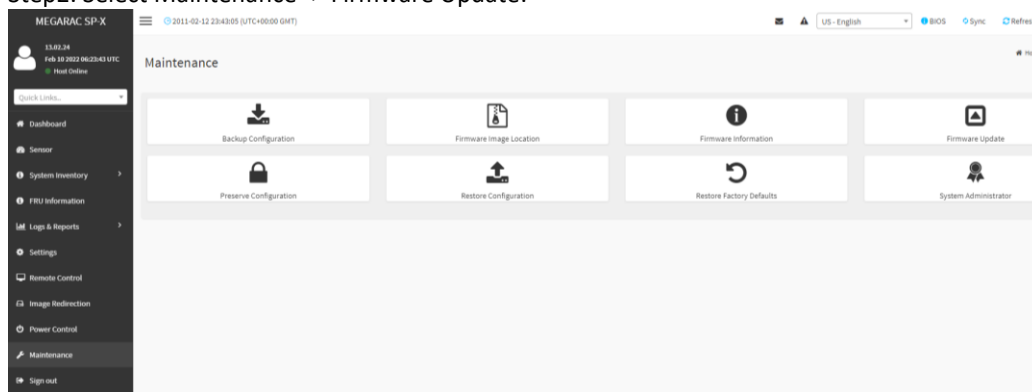
2.2. Upgrade BIOS Image-1 / Image-2

Divided into six steps to explain updating FW with WEBUI:

Step1. Log in to the WebUI (admin/password):



Step2. Select Maintenance -> Firmware Update:



Step3. Select a "image **RBU**" file:

Note:
Following are the Firmware update methods and components supported in this page.

- Dual Firmware update.
- BIOS update (*.rbu). --- Easy BIOS Refresh
- MB_CPLD update (*.rcu).
- BPB_CPLD update (*.rcu).
- CPLD
- BIOS Firmware update

Select Firmware Image

image.RBU

Protocol Type: HTTPS

Update Type: BIOS

WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BIOS and APP components of firmware.

Step4. Choose BIOS1 or BIOS2:

Note:
Following are the Firmware update methods and components supported in this page.

- Dual Firmware update.
- HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
 - BRCM RAID
 - CPLD
- BIOS Firmware update

Select Firmware Image

image.RBU

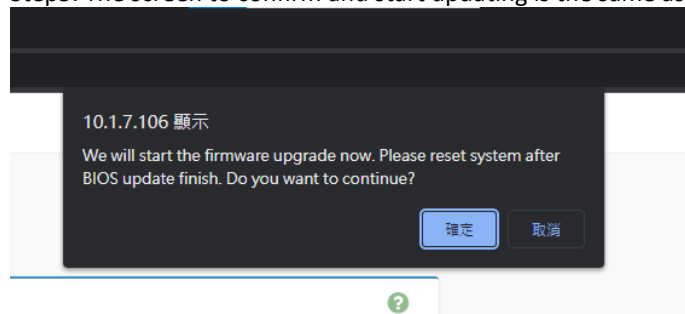
Protocol Type: HTTPS

Update Type: BIOS

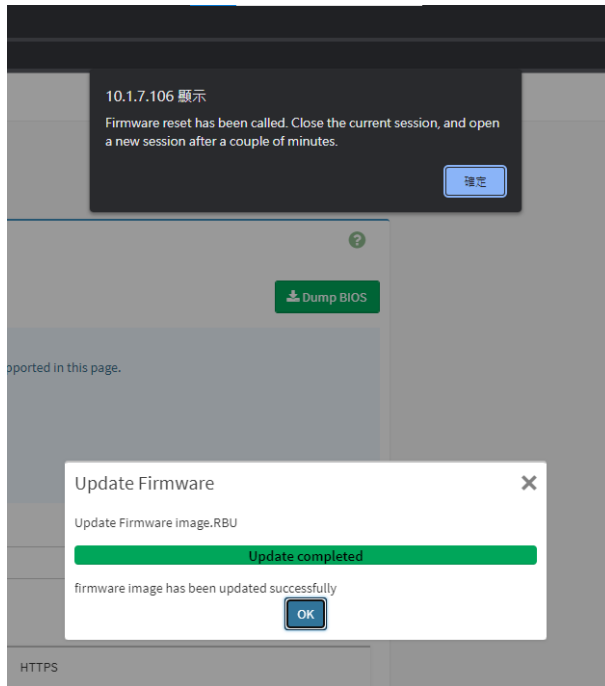
select BIOS

☒ BIOS1 ☐ BIOS2

Step5. The screen to confirm and start updating is the same as below:



Step6. Update complete:

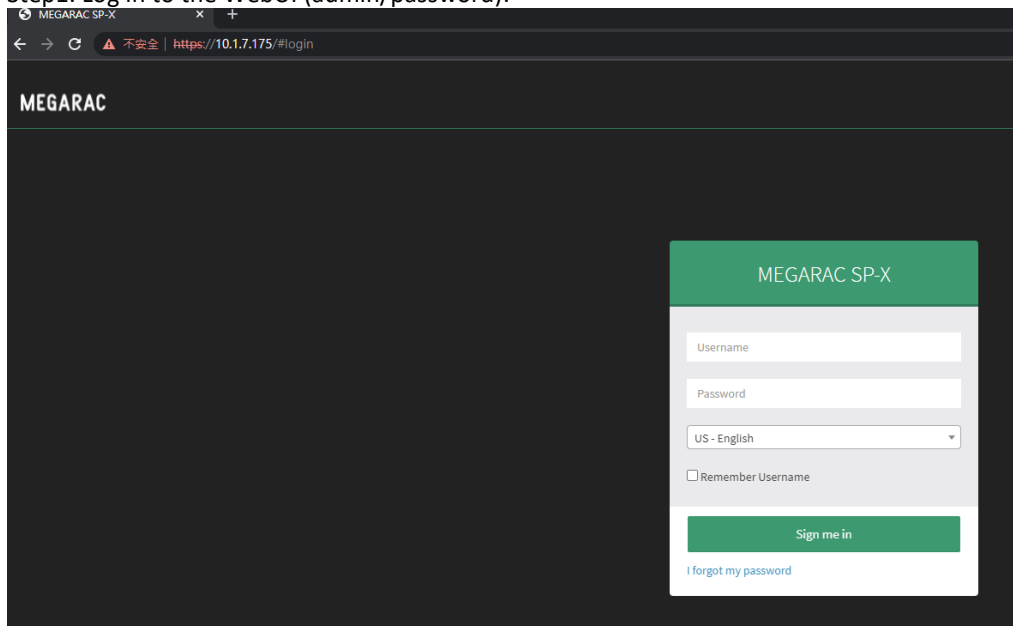


2.3. Upgrade CPLD

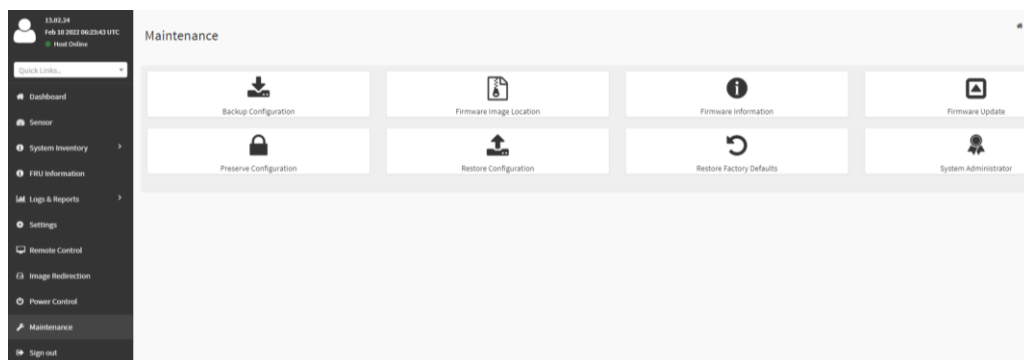
Divided into five steps to explain updating FW with WEBUI:

BMC IP: 10.1.7.175

Step1. Log in to the WebUI (admin/password):



Step2. Select Maintenance -> Firmware Update:



Step3. Select a “xxxx.rcu” file:

Note:
Following are the Firmware update methods and components supported in this page.

- Dual Firmware update.
- BIOS update (*.rbu). --- Easy BIOS Refresh
- MB_CPLD update (*.rcu).
- BPB_CPLD update (*.rcu).
- CPLD
- BIOS Firmware update

Select Firmware Image

選擇檔案 AMD_Genao_20211222_R82_test2_0x4D40_change_version.rcu

Start firmware update

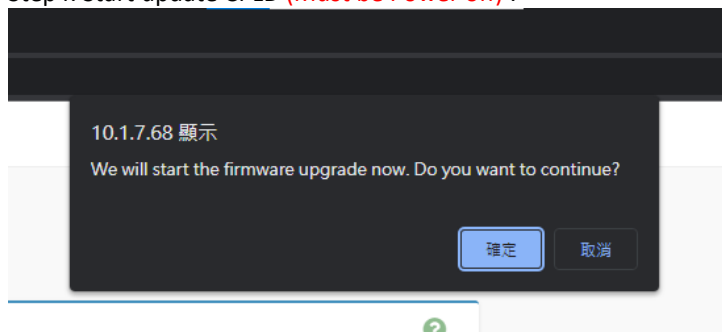
Protocol Type: HTTPS

Update Type: MB_CPLD

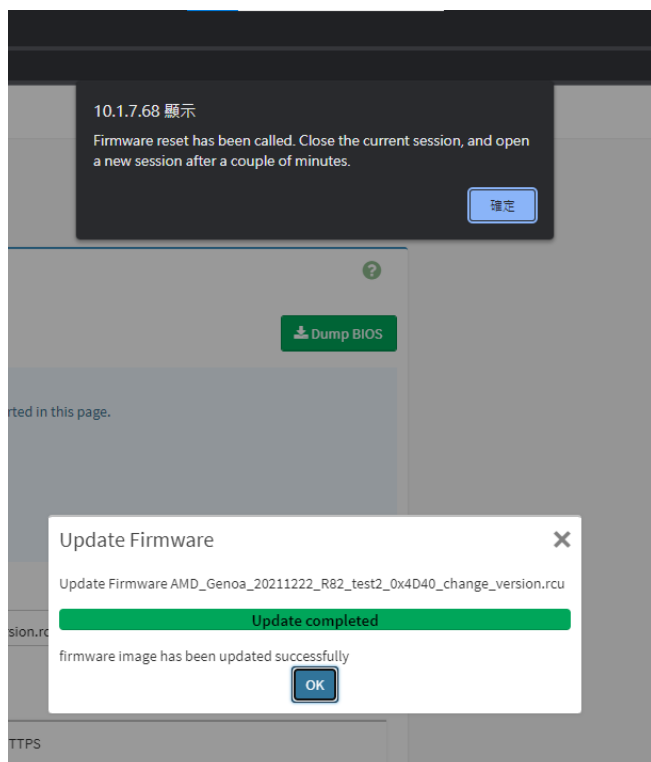
Proceed to Flash

WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

Step4. Start update CPLD (Must be Power off) :



Step5. Update complete:



2.4. Upgrade Firmware Form IPMI

Using Utility:

- IPMI

2.5. Upgrade BMC Image-1 / Image-2

2.5.1.1. Update BMC Image-1 form IPMI with HPM

- \$ ipmitool -H <BMC IP> -U <username> -P <password> -I lanplus hpm upgrade <BMC HPM image path> -z 8192 force

Example:

\$ ipmitool -H 10.1.7.137 -U admin -P password -I lanplus hpm upgrade rom_v12.52.05.hpm -z 8192 force

Result:

```
kate@NFE2-229:/project/kate/v13$ ipmitool -H 10.1.7.68 -U admin -P password -I lanplus hpm upgrade rom_v130224.hpm -z 8192 force
Setting large buffer to 8192

PICMG HPM.1 Upgrade Agent 1.0.9:

Validating firmware image integrity...OK
Performing preparation stage...
  Invalid image file for product 4165

Image Information
  Device Id : 0x20
  Prod Id : 0x0201
  Manuf Id : 0x000000
Board Information
  Device Id : 0x20
  Prod Id : 0x1045
  Manuf Id : 0x003c0a
Continue ignoring DeviceID/ProductID/ManufacturingID (Y/N): Y

Services may be affected during upgrade. Do you wish to continue? (y/n): y
OK

Performing upgrade stage:

-----
| ID | Name | Active | Versions | File | % |
|----|-----|-----|-----|-----|---|
| * 0 | BOOT | 13.01 00000000 | ----- | 13.01 00000000 | 100% |
|   |   |   | Image Size: 1114264 bytes |   |   |
| * 1 | APP | 13.02 1A000000 | ----- | 13.02 18000000 | 100% |
|   |   |   | Image Size: 64946464 bytes |   |   |
|----|-----|-----|-----|-----|---|
(*) Component requires Payload Cold Reset

Firmware upgrade procedure successful
```

2.5.1.2. Update BMC Image-2 form IPMI with HPM

- \$ ipmitool -H <BMC IP> -U <username> -P <password> -I lanplus hpm upgrade <BMC HPM image path> -z 8192 force

Node: Backup form hpm file

2.6. Upgrade BIOS Image-1 / Image-2

2.6.1.1. Update BIOS Image-1 form IPMI with HPM

- \$ ipmitool -H <BMC IP> -U <username> -P <password> -I lanplus hpm upgrade <BIOS HPM image path> -z 8192 force

2.6.1.2. Update BIOS Image-2 form IPMI with HPM

- <Switch to BIOS 2st SPI by IPMI>
\$ ipmitool -H <BMC IP> -U <username> -P <password> -I lanplus raw 0x2e 0x20 0x0a 0x3c 0 132 0x52
- \$ ipmitool -H <BMC IP> -U <username> -P <password> -I lanplus hpm upgrade <BIOS HPM image path> -z 8192 force

3. Upgrade Firmware Form Redfish (HTTP)

Please logout all BMC WebGUI connection and don't try to login BMC WebGUI when doing follow steps.

Need Setup a HTTP Server and upload new BMC firmware to HTTP Server.

3.1. Upgrade BMC Image-1 / Image-2

3.1.1.1. Export Environment Parameter

Export BMC IP, HTTP Server IP and firmware path:

```
export bmc_ip=10.1.7.193
export http_server_ip=10.1.7.86:8080
export firmware_path=rom_v13.01.16.ima_enc
```

3.1.1.2. Call Redfish do the upgrade BMC job

Run below command to call Redfish do upgrade BMC job:

```
curl -k -X POST https://$bmc_ip/redfish/v1/UpdateService/Actions/SimpleUpdate -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d '{"UpdateComponent": "BMC", "TransferProtocol": "HTTP", "ImageURI": "http://$http_sever_ip/$firmware_path"}' -u admin:password
```

Can get below Redfish response:

```
{"@odata.type": "#UpdateService.v1_6_0.UpdateService",
"Messages": [{"@odata.type": "#Message.v1_0_8.Message",
"Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
"MessageArgs": ["/redfish/v1/TaskService/Tasks/1"],
"MessageId": "Task.1.0.New", "Resolution": "None", "Severity": "OK"},
{"@odata.type": "#Message.v1_0_8.Message",
"Message": "Device is prepareing flash firmware for action SimpleUpdate.",
"MessageArgs": ["SimpleUpdate"],
"MessageId": "UpdateService.1.0.PrepareUpdate",
"Resolution": "None", "Severity": "OK"}]}
```

3.1.1.3. Check BMC update status by Redfish

wait about 180 secs for Redfish prepare flash area, upgrade file and verify firmware.

Run below command to check BMC update process:

```
curl -k -X GET https://$bmc_ip/redfish/v1/UpdateService -u admin:password
```

Can get below Redfish response:

```
{"@odata.context": "/redfish/v1/$metadata#UpdateService.UpdateService",
"@odata.etag": "W/\"1609498363\"", "@odata.id": "/redfish/v1/UpdateService",
"@odata.type": "#UpdateService.v1_6_0.UpdateService", "Description": "Redfish Update Service",
"FirmwareInventory": {"@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"}, "Id": "UpdateService",
"MaxImageSizeBytes": 190910464, "MultipartHttpPushUri": "/redfish/v1/UpdateService/upload",
```

```
"Name": "Update Service",
"Oem": {"AMIUpdateService": {"@odata.type": "#AMIUpdateService.v1_0_0.AMIUpdateService",
"FlashPercentage": "3% done.", "UpdateStatus": "Flashing", "UpdateTarget": "BMC"},
"BMC": {"@odata.type": "#AMIUpdateService.v1_0_0.BMC"}}, "ServiceEnabled": true,
"Status": {"Health": "OK", "State": "Enabled"}}
```

3.2. Upgrade BIOS Image-1 / Image-2

3.2.1.1. Export Environment Parameter

Export BIOS IP, HTTP Server IP and firmware path:

```
export bmc_ip=192.168.100.51
export http_server_ip=192.168.100.47
export firmware_name=image_MR92_F09
export redfish_username=admin
export redfish_password=password
```

3.2.1.2. Call Redfish do the upgrade BIOS job

Run below command to call Redfish do upgrade BIOS job:

```
curl -k -X POST https://$bmc_ip/redfish/v1/UpdateService/Actions/SimpleUpdate -H 'Content-Type:
application/json' -H 'cache-control: no-cache' -d '{"UpdateComponent": "BIOS", "TransferProtocol": "HTTP",
"ImageURI": "http://$http_server_ip/$firmware_name.RBU"}' -u $redfish_username:$redfish_password
```

Can get below Redfish response:

```
{"@odata.type": "#UpdateService.v1_6_0.UpdateService", "Messages": [{"@odata.type": "#Message.v1_0_8.Message", "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.", "MessageArgs": ["/redfish/v1/TaskService/Tasks/1"], "MessageId": "Task.1.0.New", "Resolution": "None", "Severity": "OK"}, {"@odata.type": "#Message.v1_0_8.Message", "Message": "Device is preparing flash firmware for action SimpleUpdate.", "MessageArgs": ["SimpleUpdate"], "MessageId": "UpdateService.1.0.PrepareUpdate", "Resolution": "None", "Severity": "OK"}]}
```

Example:

```
sysadmin [~]# curl -k -X POST https://192.168.100.51/redfish/v1/UpdateService/Actions/SimpleUpdate -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d '{"UpdateComponent": "BIOS", "TransferProtocol": "HTTP", "ImageURI": "http://192.168.100.47/image_MR92_F09.RBU"}' -u admin:password
{"@odata.type": "#UpdateService.v1_6_0.UpdateService", "Messages": [{"@odata.type": "#Message.v1_0_8.Message", "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.", "MessageArgs": ["/redfish/v1/TaskService/Tasks/1"], "MessageId": "Task.1.0.New", "Resolution": "None", "Severity": "OK"}, {"@odata.type": "#Message.v1_0_8.Message", "Message": "Device is preparing flash firmware for action SimpleUpdate.", "MessageArgs": ["SimpleUpdate"], "MessageId": "UpdateService.1.0.PrepareUpdate", "Resolution": "None", "Severity": "OK"}]}sysadmin [~]#
```

3.2.1.3. Check BIOS update status by Redfish

wait about 180 secs for Redfish prepare flash area, upgrade file and verify firmware.

Run below command to check BIOS update process:

```
curl -k -X GET https://$bmc_ip/redfish/v1/UpdateService -u $redfish_username:$redfish_password
```

Can get below Redfish response:

```
{"@odata.context": "/redfish/v1/$metadata#UpdateService.UpdateService", "@odata.etag": "W/\"1647409528\"", "@odata.id": "/redfish/v1/UpdateService", "@odata.type": "#UpdateService.v1_6_0.UpdateService", "Actions": {"#UpdateService.SimpleUpdate": {"@Redfish.ActionInfo": "/redfish/v1/UpdateService/SimpleUpdateActionInfo", "target": "/redfish/v1/UpdateService/Actions/SimpleUpdate"}, "Oem": {"#UpdateService.UploadCABundl
```

```
e":{"@Redfish.ActionInfo":"/redfish/v1/UpdateService/UploadCABundleActionInfo","target":"/redfish/v1/UpdateService/Actions/Oem/UpdateService.UploadCABundle"},"Description":"Redfish Update Service","FirmwareInventory":{"@odata.id":"/redfish/v1/UpdateService/FirmwareInventory"},"Id":"UpdateService","MaxImageSizeBytes":188981248,"MultipartHttpPushUri":"/redfish/v1/UpdateService/upload","Name":"Update Service","Oem":{"AMIUpdateService":{"@odata.type":"#AMIUpdateService.v1_0_0.AMIUpdateService","FlashPercentage":null,"PreserveConfiguration":{"Authentication":true,"FRU":true,"IPMI":true,"KVM":true,"NTP":true,"Network":true,"REDFISH":true,"SDR":true,"SEL":true,"SNMP":true,"SSH":true,"Syslog":true,"WEB":true,"UpdateStatus":"Completed","UpdateTarget":"BIOS"},"BMC":{"@odata.type":"#AMIUpdateService.v1_0_0.BMC","DualImageConfigurations":{"ActiveImage":"1","BootImage":"1","FirmwareImage1Name":"Image1","FirmwareImage1Version":"13.03.01","FirmwareImage2Name":"Image2","FirmwareImage2Version":"13.03.1216"},"ServiceEnabled":true,"Status":{"Health":"OK","State":"Enabled"}}

```

3.3. Multipart Push BMC_FW Update

3.3.1.1. Request

Example Request

POST /redfish/v1/UpdateService/upload

Please prepare below file.

1. FW image. The image filename extension should be *.hpm or *.rcu or *.ima_enc
2. Create a JSON file parameters.json with content like below.

```
{
  "Targets":[
    "/redfish/v1/UpdateService/FirmwareInventory/BMC"
  ]
}
```

3. Create a JSON file oem_parameters.json with content like below.

```
{
  "ImageType":"BMC"
}
```

3.3.1.2. Parameters of Multipart Push

The details of UpdateParameters and OemParameter are given in the Tables below.

File	Parameter name	Type	Allowed value
UpdateParameters	Targets	Array of uri	/redfish/v1/UpdateService/FirmwareInventory/BIOS /redfish/v1/UpdateService/FirmwareInventory/BIOS2 /redfish/v1/UpdateService/FirmwareInventory/BMC /redfish/v1/UpdateService/FirmwareInventory/BMCImage1 /redfish/v1/UpdateService/FirmwareInventory/MB_CPLD1 /redfish/v1/UpdateService/FirmwareInventory/BPB_CPLD1 /redfish/v1/UpdateService/FirmwareInventory/SCP
OemParameters	ImageType	String	BMC BIOS HPM_BMC HPM_BIOS HPM_SCP MB_CPLD BPB_CPLD

	Targets	ImageType
Mapping	/redfish/v1/UpdateService/FirmwareInventory/BIOS	BIOS
	/redfish/v1/UpdateService/FirmwareInventory/BIOS2	HPM_BIOS
	/redfish/v1/UpdateService/FirmwareInventory/ BMCImage1	BMC
	/redfish/v1/UpdateService/FirmwareInventory/ BMC	HPM_BMC
	/redfish/v1/UpdateService/FirmwareInventory/ MB_CPLD1	MB_CPLD
	/redfish/v1/UpdateService/FirmwareInventory/ BPB_CPLD1	BPB_CPLD
	/redfish/v1/UpdateService/FirmwareInventory/SCP	HPM_SCP

It is able to look up the list of available Targets URI with GET FirmwareInventory Collection.

Request:

`GET /redfish/v1/UpdateService/FirmwareInventory`

Response:

```
{
  "@odata.context": "/redfish/v1/$metadata#SoftwareInventoryCollection.SoftwareInventoryCollection",
  "@odata.etag": "W/\"1262888059\"",
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory",
  "@odata.type": "#SoftwareInventoryCollection.SoftwareInventoryCollection",
  "Description": "Collection of Firmware Inventory resources available to the UpdateService",
  "Members": [
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BMCImage1"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BPB_CPLD1"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BIOS"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BIOS2"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/BMCImage2"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/SCP"
    },
    {
      "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/MB_CPLD1"
    }
  ],
  "Members@odata.count": 7,
  "Name": "Firmware Inventory Collection"
}
```

3.3.1.3. Command

Example command

```
curl -k -L -X POST https://{BMC_IP}/redfish/v1/UpdateService/upload -u ${account}:${password} -F
"UpdateParameters=@parameters.json;type=application/json" -F "OemParameters=@
oem_parameters.json;type=application/json" -F UpdateFile=@{ local_image_path } -H 'Expect:'
```

4. Upgrade Firmware Form Restful

Using Utility:

- Curl
- IPMI

4.1. Upgrade Active/Backup BMC

Please logout all BMC WebGUI connection and don't try to login BMC WebGUI when doing follow steps.

4.1.1 Preserve BMC Configuration

4.1.1.1. Get Session CSRF Token

Example:

BMC IP: 10.1.27.31

Run below command to get CSRF Token:

```
curl -s -c cookie -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d "username=admin&password=password" https://10.1.27.31/api/session
```

Can get below response:

```
{ "ok": 0, "privilege": 4, "extendedpriv": 259, "racsession_id": 16, "remote_addr": "10.1.112.223", "server_name": "10.1.27.31", "server_addr": "10.1.27.31", "HTTPSEnabled": 1, "CSRFToken": "83FYT2La", "channel": 1, "passwordStatus": 0 }
```

Recode CSRFToken value.

4.1.1.2. Set Backup flag

Choice backup item if you want:

- "snmp":1,
- "kvm":1,
- "network":1,
- "ipmi":1,
- "ntp":1,
- "authentication":1,
- "syslog":1,
- "id":1 (reserve)

Run below command to set backup config:

```
curl -c cookie -b cookie -k -H "Content-Type: application/json" -H "X-CSRFToken: 83FYT2La" -X PUT -d '{"snmp":1,"kvm":1,"network":1,"ipmi":1,"ntp":1,"authentication":1,"syslog":1,"id":1}' https://10.1.27.31/api/maintenance/backup_config
```

Note: X-CSRFToken value from session 1.2 CSRFToken

4.1.1.3. Download Backup file

Run below command to download Backup file:

```
curl -c cookie -b cookie -k -H "X-CSRFToken: 83FYT2La" -X GET https://10.1.27.31/api/maintenance/download_config --output conf.bak
```

Note: X-CSRFTOKEN value from session 1.2 CSRFToken

4.1.2 Upgrade Active/Backup BMC

4.1.2.1. Export Environment Parameter

Export BMC IP and new firmware binary path:

```
export bmc_ip=10.1.7.193
export bmc_file=./v13.01.16/fw/rom.ima_enc
```

4.1.2.2. Reboot BMC by IPMITool

Reboot BMC by ipmi command:

```
ipmitool -I lanplus -H $bmc_ip -U admin -P password mc reset cold
```

4.1.2.3. Get Session CSRF Token

Run below command to get CSRF Token:

```
curl -s -c cookie -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d
"username=admin&password=password" https://$bmc_ip/api/session
```

Need using administrator user name and password

Can get below response:

```
{ "ok": 0, "privilege": 4, "extendedpriv": 259, "racsession_id": 1, "remote_addr": "10.1.112.229",
"server_name": "10.1.7.193", "server_addr": "10.1.7.193", "HTTPSEnabled": 1, "CSRFToken": "SgRUJUg0" }
```

4.1.2.4. Export CSRF Token

Export CSRF Token:

```
export csrf_token=SgRUJUg0
```

4.1.2.5. Set BMC Prepare to Flash BMC

Run below command to setup BMC:

```
curl -s -c cookie -b cookie -k -H "X-CSRFTOKEN:$csrf_token" -H "Content-Type: application/json" -X PUT -d
'{"flash_type":"BMC"}' https://$bmc_ip/api/maintenance/flash
```

BMC need about 30 sec. to prepare

Can get below response:

```
{ "flash_type": "BMC" }
```

4.1.2.6. Upload new BMC firmware

Run below command to upload new BMC firmware:

```
curl -s -c cookie -b cookie -k -H "X-CSRFTOKEN:$csrf_token" -H "Expect:" -X POST -F "fwimage=@$bmc_file"
"https://$bmc_ip/api/maintenance/firmware"
```

Can get below response:

```
{ "cc": 0 }
```

4.1.2.7. Verify new BMC firmware

Run below command to verify new BMC firmware:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -X GET
"https://$bmc_ip/api/maintenance/firmware/verification"
```

Can get below response and check **current_image_version1** 、 **new_image_version**

```
[ { "id": 1, "current_image_name": "boot", "current_image_version1": "2.4.000000",
"current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 0,
"verification_status": 69 }, { "id": 2, "current_image_name": "conf", "current_image_version1": "2.4.000000",
"current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 0,
"verification_status": 69 }, { "id": 3, "current_image_name": "conf", "current_image_version1": "2.4.000000",
"current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 0,
"verification_status": 69 }, { "id": 4, "current_image_name": "root", "current_image_version1": "2.4.000000",
"current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 1,
"verification_status": 69 }, { "id": 5, "current_image_name": "osimage", "current_image_version1":
"2.4.000000", "current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 1,
"verification_status": 69 }, { "id": 6, "current_image_name": "dre", "current_image_version1": "11.7.000000",
"current_image_version2": "0.0.", "new_image_version": "11.7.000000", "section_status": 1,
"verification_status": 69 }, { "id": 7, "current_image_name": "www", "current_image_version1":
"2.4.000000", "current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 1,
"verification_status": 69 }, { "id": 8, "current_image_name": "testapps", "current_image_version1":
"2.4.000000", "current_image_version2": "0.0.", "new_image_version": "2.4.000000", "section_status": 1,
"verification_status": 69 }, { "id": 9, "current_image_name": "ast2500e", "current_image_version1": "8.10.1",
"current_image_version2": "0.0.", "new_image_version": "8.29.1", "section_status": 0, "verification_status":
69 } ]
```

4.1.2.8. Start Update BMC

Run below command to start BMC update process:

With preserving BMC setting:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Content-Type: application/json" -X PUT -d
'{"preserve_config":1,"flash_status":1,"flash_type":"BMC"}'
"https://$bmc_ip/api/maintenance/firmware/upgrade"
```

Without preserving BMC setting:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Content-Type: application/json" -X PUT -d
'{"preserve_config":0,"flash_status":1,"flash_type":"BMC"}'
"https://$bmc_ip/api/maintenance/firmware/upgrade"
```

Can get below response:

With preserving BMC setting:

```
{ "preserve_config": 1, "flash_status": 1, "flash_type": "BMC" }
```

Without preserving BMC setting:

```
{ "preserve_config": 0, "flash_status": 1, "flash_type": "BMC" }
```

4.1.2.9. Check BMC update status

Run below command to check BMC update process:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -X GET  
"https://$bmc_ip/api/maintenance/firmware/flash-progress"
```

Can get below response:

In Flashing:

```
{ "id": 1, "action": "Flashing...", "progress": "13% done", "state": 0 }
```

Flash completed:

```
{ "id": 1, "action": "Firmware Update", "progress": "Completed.", "state": 2 }
```

BMC will auto reboot after flash completed.

4.1.3 Restore BMC Configuration

4.2. Upgrade Active/Backup BIOS

4.2.1.1. Export Environment Parameter

Export BMC IP and new firmware binary path:

```
export bmc_ip=10.1.7.193  
export bios_file=./bios/fw/image.RBU
```

4.2.1.2. Get Session CSRF Token

Run below command to get CSRF Token:

```
curl -s -c cookie -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d  
"username=admin&password=password" https://$bmc_ip/api/session
```

Need using administrator user name and password

Can get below response:

```
{ "ok": 0, "privilege": 4, "extendedpriv": 259, "racsession_id": 1, "remote_addr": "10.1.112.229",  
"server_name": "10.1.7.193", "server_addr": "10.1.7.193", "HTTPSEnabled": 1, "CSRFToken": "SgRUJUg0" }
```

4.2.1.3. Export CSRF Token

Export CSRF Token:

```
export csrf_token=SgRUJUg0
```

4.2.1.4. Set BMC Prepare to Flash BIOS

1. AST2500 machine (BMC Firmware is 12.X.X)

If your machine is AST2500, you can run below command to setup BMC:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Content-Type: application/json" -X PUT -d '{"flash_type":"BIOS"}' "https://$bmc_ip/api/maintenance/flash"
```

Can get below response:

```
{ "flash_type": "BIOS" }
```

2. AST2600 machine (BMC Firmware is 13.X.X)

If your machine is AST2600, you can run below command to setup BMC:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Content-Type: application/json" -X PUT -d '{"flash_type":"BIOS","preserve_config":"0"}' "https://$bmc_ip/api/maintenance/flash"
```

Can get below response:

```
{ "flash_type": "BIOS", "preserve_config": "0" }
```

4.2.1.5. Upload new BIOS firmware

Run below command to upload new BIOS firmware:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Expect:" -X POST -F "fwimage=@$bios_file" "https://$bmc_ip/api/maintenance/firmware"
```

upload file need take a few seconds.

Can get below response:

```
{ "cc": 0 }
```

4.2.1.6. Verify new BIOS firmware

Run below command to verify new BIOS firmware:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -X GET "https://$bmc_ip/api/maintenance/firmware/verification"
```

Can get below response:

```
[ ]
```

4.2.1.7. Start Update BIOS

Run below command to start BIOS update process:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -H "Content-Type: application/json" -X PUT -d '{"preserve_config":0,"flash_status":0,"flash_type":"BIOS"}' "https://$bmc_ip/api/maintenance/firmware/upgrade"
```

Can get below response:

```
{ "preserve_config": 0, "flash_status": 0, "flash_type": "BIOS" }
```

4.2.1.8. Check BIOS update status

Run below command to check BIOS update process:

```
curl -s -c cookie -b cookie -k -H "X-CSRFToken:$csrf_token" -X GET  
"https://$bmc_ip/api/maintenance/firmware/flash-progress"
```

Can get below response:

In Flashing:

```
{ "id": 1, "action": "Flashing...", "progress": "13% done", "state": 0 }
```

Flash completed:

```
{ "id": 1, "action": "Firmware Update ", "progress": "Completed.", "state": 2 }
```

5. Upgrade Firmware Form Gigaflash

5.1. Upgrade Active/Backup BMC

5.1.1.1. Upgrade BMC Fireware in Linux

1. Get Linux root permission.
2. Change path to the root directory of Upgrade Package.
3. Run "bmc_fw_update_linux.sh cs 0 flashall".

```
kate@NFE2-229:/project/kate/130223$ ./bmc_fw_update_linux.sh cs 0 flashall
gigaflash v1.8.1
Loading Firmware...
```

User command:

NAME

bmc_fw_update_linux.sh - Update script

SYNOPSIS

bmc_fw_update_linux.sh [OPTION]

DESCRIPTION

Update BMC flash script. Below is option item:

cs

Select to update Active/Backup BMC firmware. (CS=1 only support on GBT Dual Platform).

0: Active

1: Backup

Default value is 0.

flashall

Flash entire BMC without warning message.

Default: Ask user preserve configuration or not

x32

Set update tool to 32-bit mode

Default x86 64-bit mode

arm

Set update tool to arm mode (arm Linux only support 64-bit)

Default x86 64-bit mode

Example for flash entire BMC and select BMC address in address 0:

bmc_fw_update_linux.sh cs 0 flashall

5.1.1.2. Upgrade BMC Fireware in Windows

1. Open Command line with Windows Administrator permission.
2. Change path to the root directory of Upgrade Package.
3. Run "bmc_fw_update_win.bat cs 0 flashall".

```
C:\Users\kate.cheng\Desktop\130223>bmc_fw_update_win.bat cs 0 flashall
0
"Tools\gigaflash_x64.exe fw\130223.bin -a -cs 0 -2600"
gigaflash v1.8.1
Loading Firmware...
```

User command:

NAME

bmc_fw_update_win.bat - Update script

SYNOPSIS

bmc_fw_update_win.bat [OPTION]

DESCRIPTION

Update BMC flash script. Below is option item:

cs

Select to update Active/Backup BMC firmware. (CS=1 only support on GBT Dual Platform).

0: Active

1: Backup

Default value is 0.

[flashall](#)

Flash entire BMC without warning message.

Default: Ask user preserve configuration or not

[x32](#)

Set update tool to 32-bit mode

Default x86 64-bit mode

Example for flash entire BMC and select BMC address in address 0:

[bmc_fw_update_win.bat cs 0 flashall](#)

5.1.1.3. Upgrade BMC Fireware in UEFI

1. Change path to the root directory of Upgrade Package.

2. Run "bmc_fw_update_uefi.nsh cs 0 flashall"

```
FS0:\130226\> bmc_fw_update_uefi.nsh cs 0 flashall
FS0:\130226\> echo -off
gigaflash v1.8.1
```

User command:

[NAME](#)

bmc_fw_update_uefi.nsh - Update script

[SYNOPSIS](#)

bmc_fw_update_uefi.nsh [OPTION]

[DESCRIPTION](#)

Update BMC flash script. Below is option item:

[cs](#)

Select to update Active/Backup BMC firmware. (CS=1 only support on GBT Dual Platform).

0: Active

1: Backup

Default value is 0.

[flashall](#)

Flash entire BMC without warning message.

Default: Ask user preserve configuration or not

Example for flash entire BMC and select BMC address in address 0:

[bmc_fw_update_uefi.nsh cs 0 flashall](#)