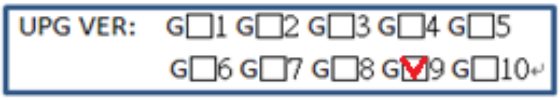
BMC Unique Pre-Programmed Password Reference Guide

1. How will I know if my product has been implemented with this new security feature?

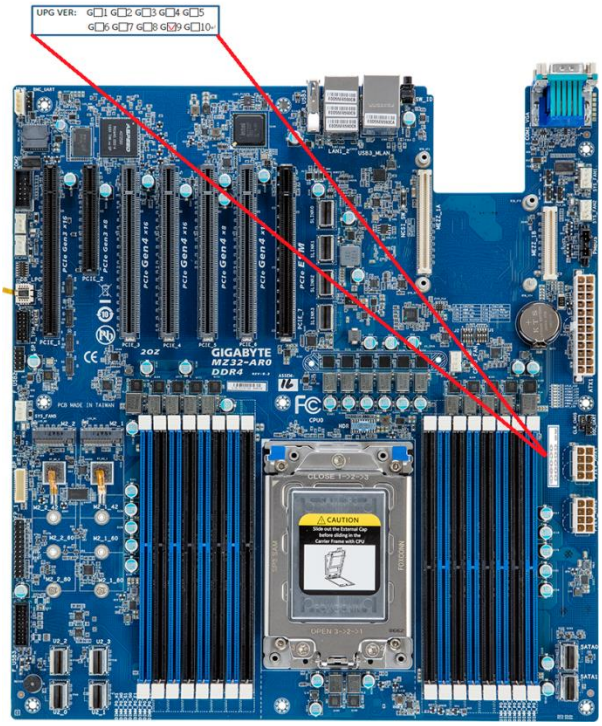
Please check the “Upgrade Version” label. If the product features a unique pre-programmed BMC password based on the product motherboard’s serial number, the upgrade version will be indicated as “**G9**”.



The “Upgrade Version” label can be found on the outside product (motherboard / server) packaging, on the motherboard anti-static packaging bag, on the motherboard itself and / or on the server chassis.

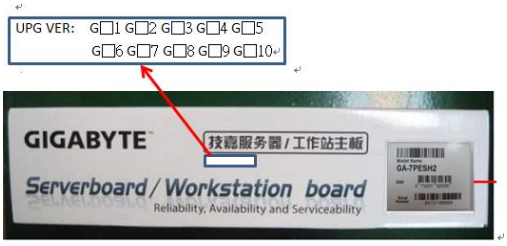
“Upgrade Version” label locations

Motherboard:

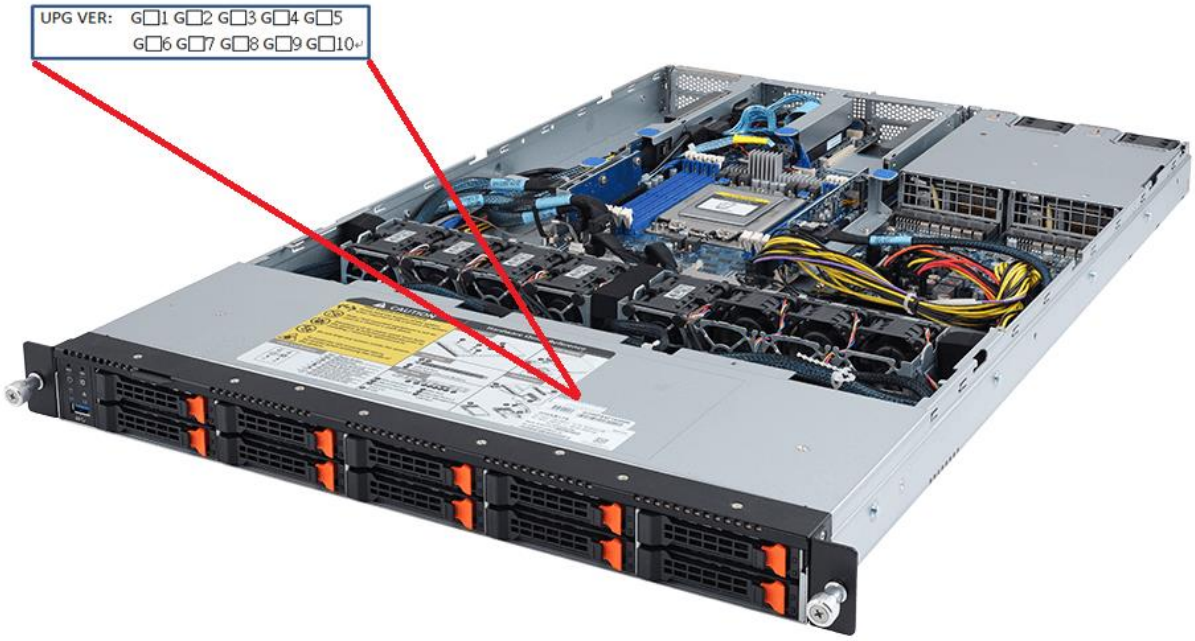


Motherboard Anti-Static Bag:

Motherboard Box:



Server Chassis:



Server Packaging:

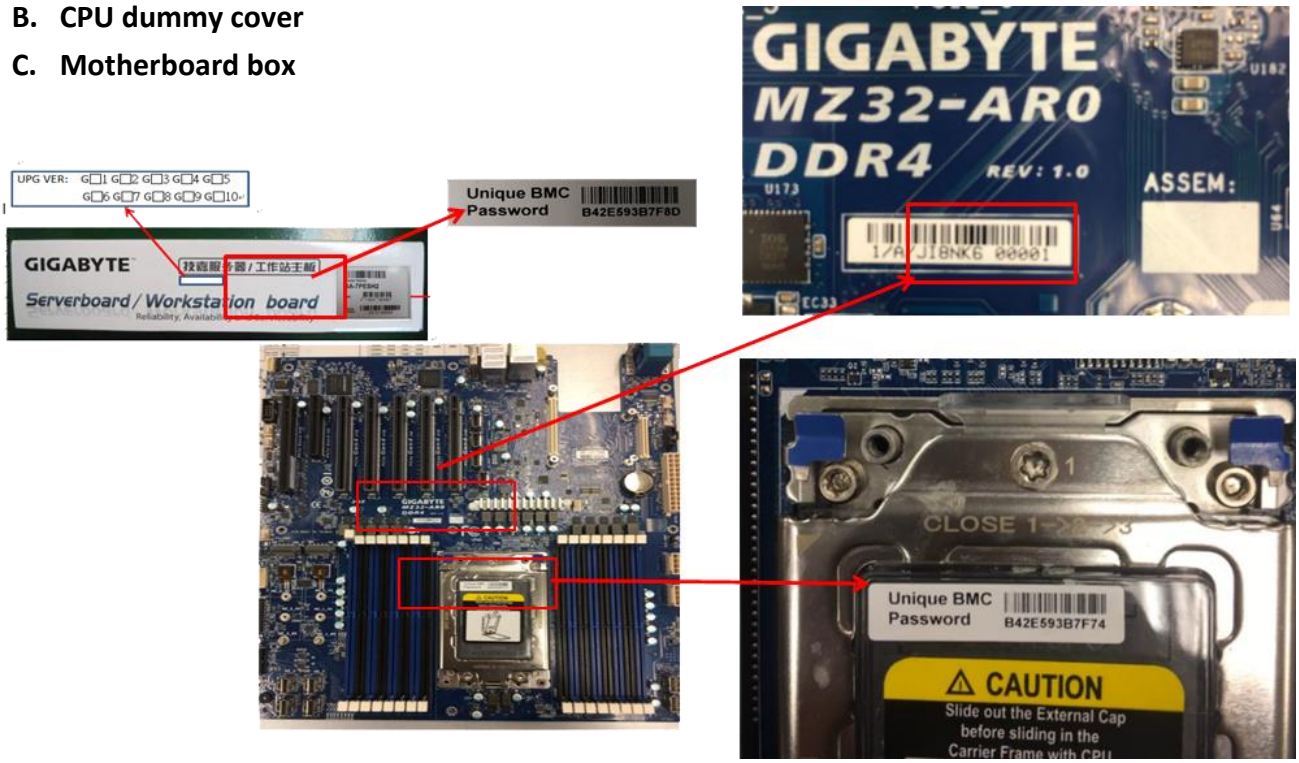
<u>Note</u>: If your product does not have G9 checked, then this security feature has not been enabled. Your default password for BMC admin login account will still be "password"

2. Where can I find the unique pre-programmed password to access the admin account of the BMC firmware?

In addition to the original motherboard serial number sticker which can be found on the motherboard, there will be additional stickers to display the unique BMC password located on the motherboard dummy CPU cover and the motherboard box (for motherboards sold separately). In the case of server systems, this sticker will be located on the server chassis and on the server packaging box.

<u>"Unique BMC Password" sticker motherboard locations:</u>

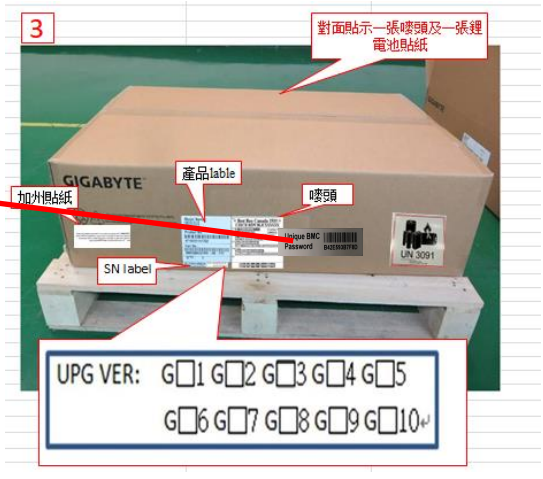
A. (reference original S/N sticker on motherboard)
B. CPU dummy cover
C. Motherboard box



“Unique BMC Password” sticker server system locations

1U Rack Server	**A. (reference original S/N sticker on motherboard)** **B. Server chassis front: sliding plastic tongue**  **C. Outside box**
2U Rack Server	**A. (reference original S/N sticker on motherboard)** **B. Server chassis side:**  **C. Outside box**
2U 4 Node Server (H252/H261/H262 Series)	**A. (reference original S/N sticker on motherboard)** **B. Server chassis front: sliding plastic tongue**  **C. Outside box**

2U 4 Node Server (H242 Series)	**A. (reference original S/N sticker on motherboard)** **B. Server chassis front: node handle**  **C. Outside box**
4U Rack Server	**A. (reference original S/N sticker on motherboard)** **B. Server chassis side** **C. Outside box** 
5U Rack Server	**A. (reference original S/N sticker on motherboard)** **B. Server chassis side** **C. Outside box** 

OCP Server (RACKLUTION)	**A. (reference original S/N sticker on motherboard)** **B. Server chassis front: sliding plastic tongue** **C. Outside box** 
Tower Server	**A. (reference original S/N sticker on motherboard)** **B. Tower chassis top** **C. Outside box** 
Server Packaging	 

3. How Do I Reset the BMC Password of my Servers Back to Default En Masse?

This change may be inconvenient for customers who are deploying a large number of servers and wish to perform a BIOS/ FW update, FRU overwrite or BIOS setting overwrite en masse. Therefore, GIGABYTE can also provide the list of pre-programmed unique passwords (a "**MAC to password" file**) of your purchased server systems upon request. This list can be used to restore the passwords of our servers back to the default setting (username: "admin" & password: "password").

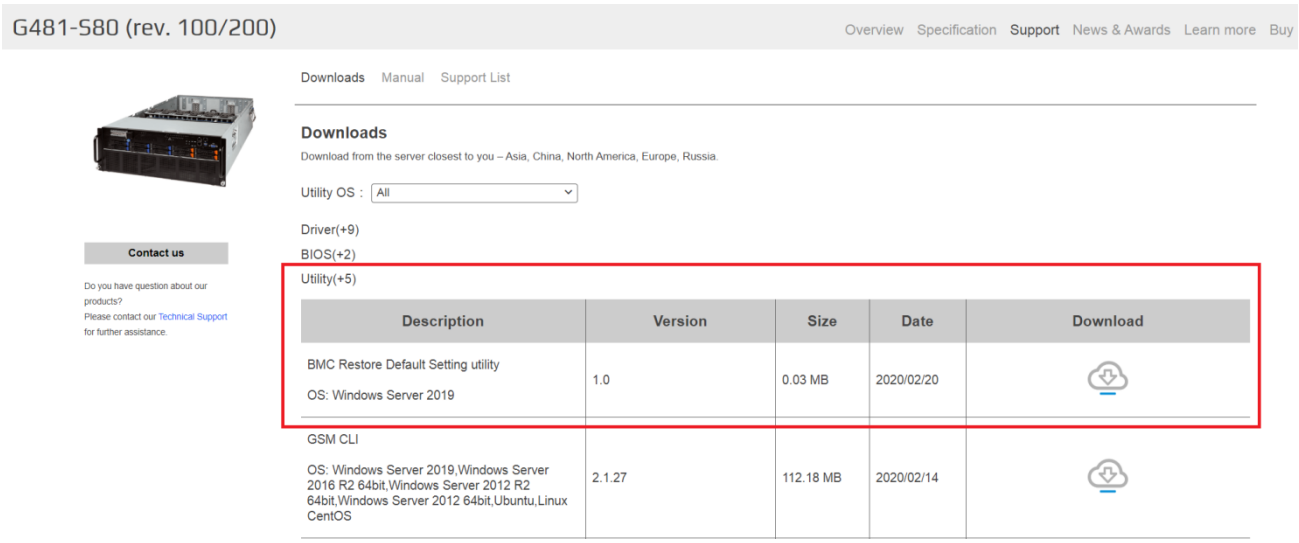
The "MAC to password" file will list out both the IPMI MAC address of the BMC and the unique password of BMC (separated by commas) of each of the servers you have purchased from GIGABYTE.

Example:

mac2password.txt

```
1C:1B:0D:0A:BB:48,S16C79000042
e0:d5:5e:65:a9:e4,S1822400026
e0d55e659256,S1915000026
…
```

After requesting the "MAC to password" file from your GIGABYTE representative, please download the "**bmc_restore_default_password.py**" Python script from the support section of the GIGABYTE product page (located in the "**server_utility_BMC_Restore_Default_Setting.zip**" download package):



Reset Password Process Prerequisites

[Debian or Ubuntu]

- Install Python 3.6.9 or above
  # sudo apt-get install python3

- Install Python module
  # sudo apt-get install python3-pip
  # sudo python3 -m pip install subprocess.run
  # sudo python3 -m pip install argparse

- Install ipmitool
  # sudo apt-get install ipmitool

- All servers should be on the same subnet network

Password Reset Process

Execute the **bmc_restore_default_password.py** Python script with the input file name (e.g. *mac2password.txt*) and the BMC IP range:

$ python3 bmc_restore_default_password.py <File> <Start IP> <End IP>

After completion, the message “Restore OK” will be displayed together with the list of BMC IP addresses that have had their password restored back to the default:

Restore OK
10.1.27.36
10.1.27.37
…
Restore Done