Falcon Composable GPU Solution

— Falcon 5012

Quick Installation Guide

Version 09
April 15th, 2026

Dear Users,

Thank you for choosing our product: Falcon 5012.

The excellent quality and performance make our products superior in the like product. For you to have a good understanding of Falcon 5012, please read the installation guide and user manual, and operate according to the suggested steps for each feature.

If you have any questions when using our machine, please contact us. We are more than happy to serve you constantly.

Technical Support: support@h3platform.com
FAQ: https://www.h3platform.com/

H3 Platform Inc. mainly researches and develops PCIe switch-based technology and solutions.

---- H3 Platform Inc

Revision History

Rev.	Date	Description
01	2024.02.26	
02	2024.04.26	Chassis overview revised
03	2024.5.24	Device Installation Guide revised
04	2024.12.27	Operation procedures updated
05	2025.02.27	Product photo and BMC use guide updated
06	2025.06.09	Rack installation guide added
07	2025.06.24	Public template applied.
08	2025.08.07	SKU label contents updated
09	2026.04.15	Host adapter firmware update settings updated

Falcon 5012 Default Settings

IP Address:	169.254.100.200
Administrator Username:	admin
Administrator Password:	admin

Table of Content

Revision History **3**
Table of Content **4**
Chapter 1. **5**
Chassis Overview **5**
Front View - System 5
Top View - System 6
- 10 GPUs (SKU A) 6
- 8 GPUs + 4 NICs (SKU B) 6

Rear View - System 7
- 10 GPUs (SKU A) 7
- 8 GPUs + 4 NICs (SKU B) 7

PCIe Port Number 8
- 10 GPUs (SKU A) 8
- 8 GPUs + 4 NICs (SKU B) 8

Chapter 2. **9**
Installation and Boot-Up Guide **9**
2.1 Confirm Label and Product Match 9
2.2 Hardware Setup and Power-On Preparation 13
2.3 Retrieve GUI IP for System Boot-Up 17
2.4 Complete Initial Setup for Falcon 5012 Management GUI 20
2.5 Device Installation in Falcon 5012 System 27
2.6 Retimer Installation and Host Configuration 34
2.7 GPU Assign and Unassign 38
2.8 Verifying GPU Resource Assignment or Unassignment on the Host 44
2.9 Updating Firmware 46
Chapter 3. **50**
Common BMC Operations Guide **50**
3.1 BMC GUI Log-in 51
3.2 Remote Powering On/Off Using BMC 52
3.3 Updating BMC Firmware 55
3.4 Updating CPLD Firmware Using BMC 57
3.5 Updating Host Adapter (Retimer) Firmware 62
Warranty **67**
Limited Warranty 67
Software Limited Warranty 68
Compatibility 69
Repair Service 69
Notice of Warranty Claims 70
DISCLAIMER OF WARRANTY 70
Limitation of Liability and Remedies. 70

Chapter 1.
Chassis Overview

Front View - System

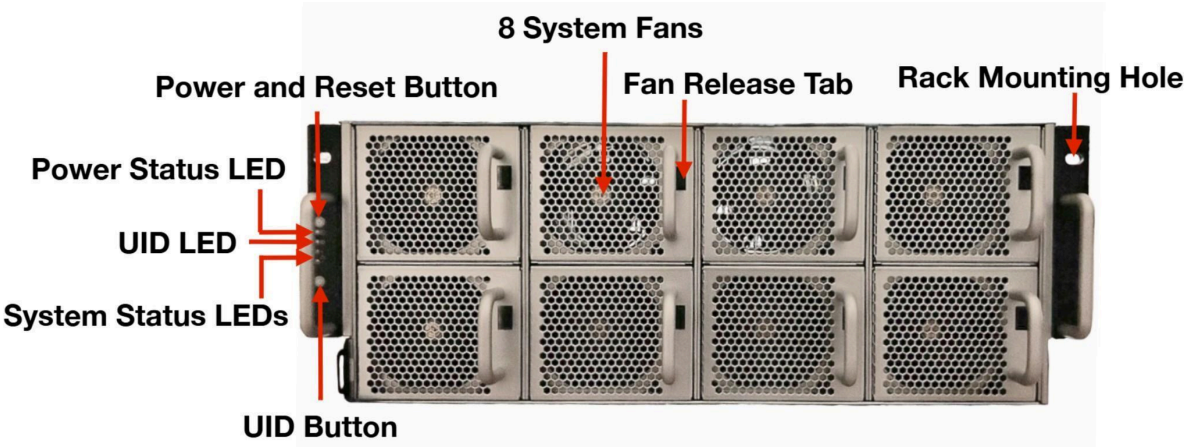
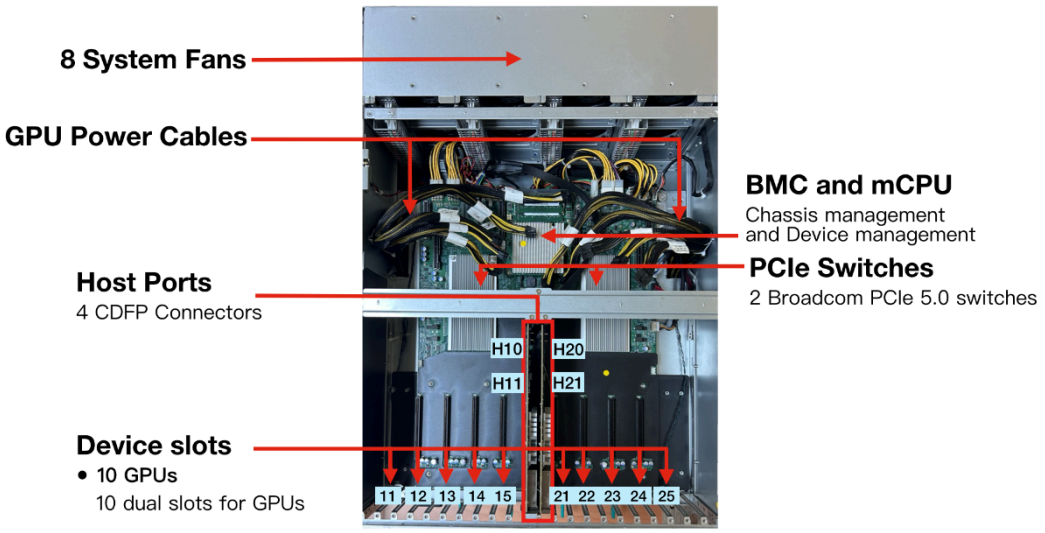


Figure 1. Image of PCIe Gen5 GPU box front view

Top View - System

- 10 GPUs (SKU A)



- 8 GPUs + 4 NICs (SKU B)

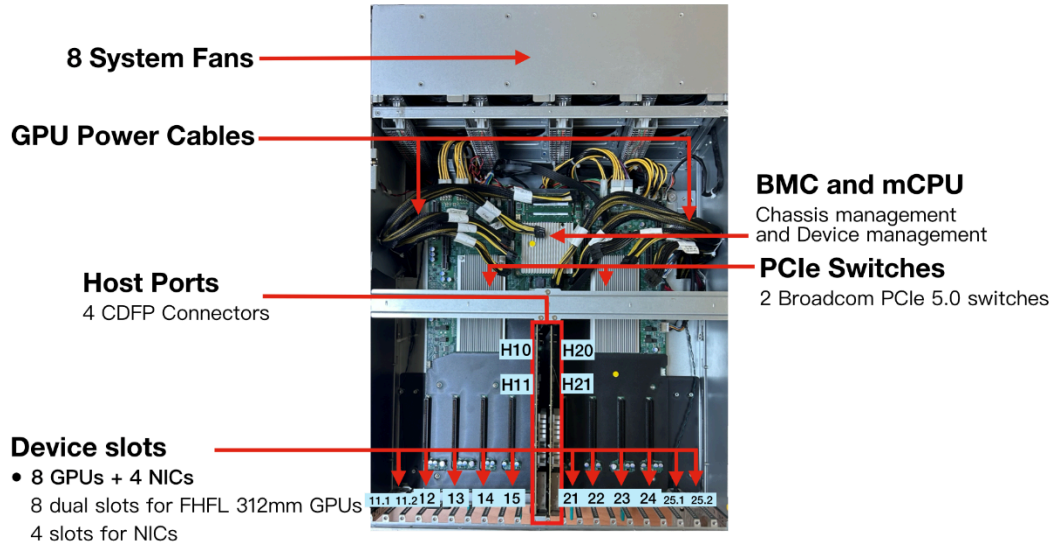
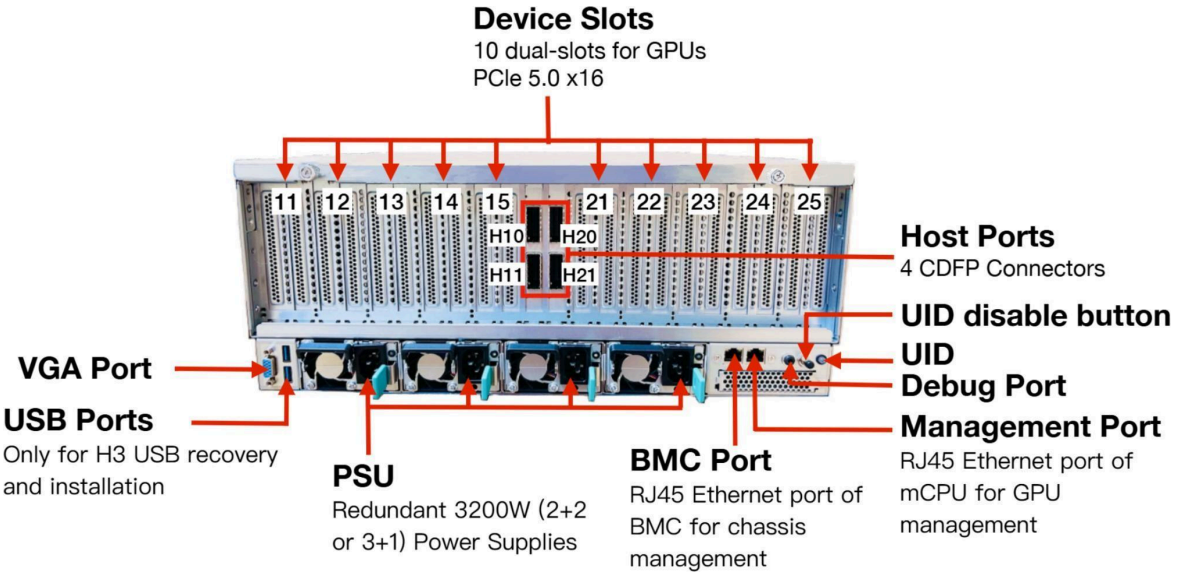


Figure 2. Images of PCIe Gen5 GPU box top view

Rear View - System

- 10 GPUs (SKU A)



- 8 GPUs + 4 NICs (SKU B)

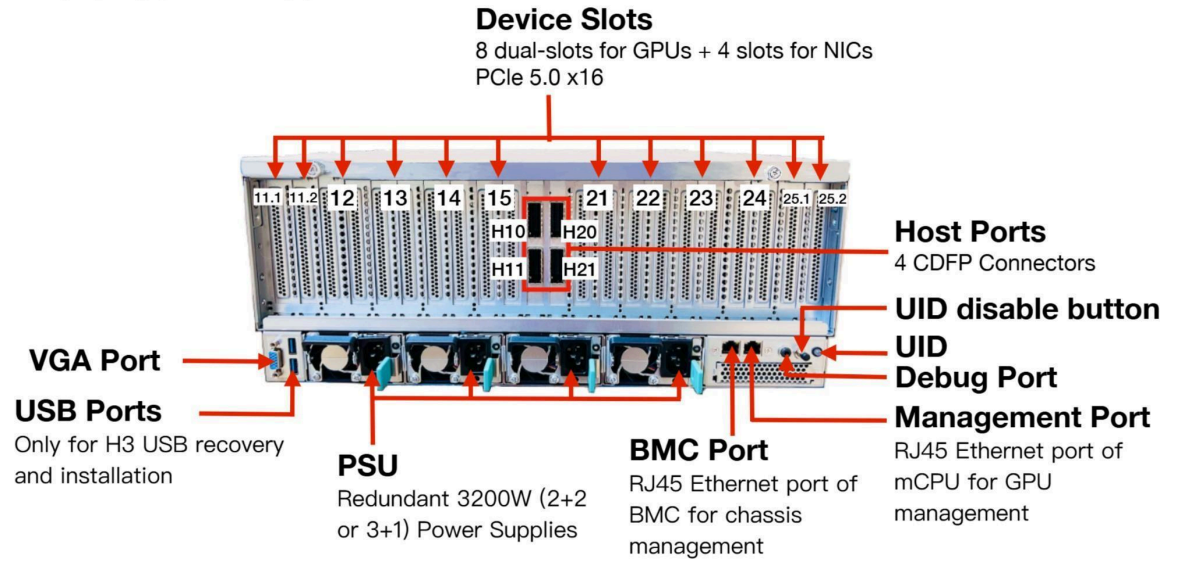
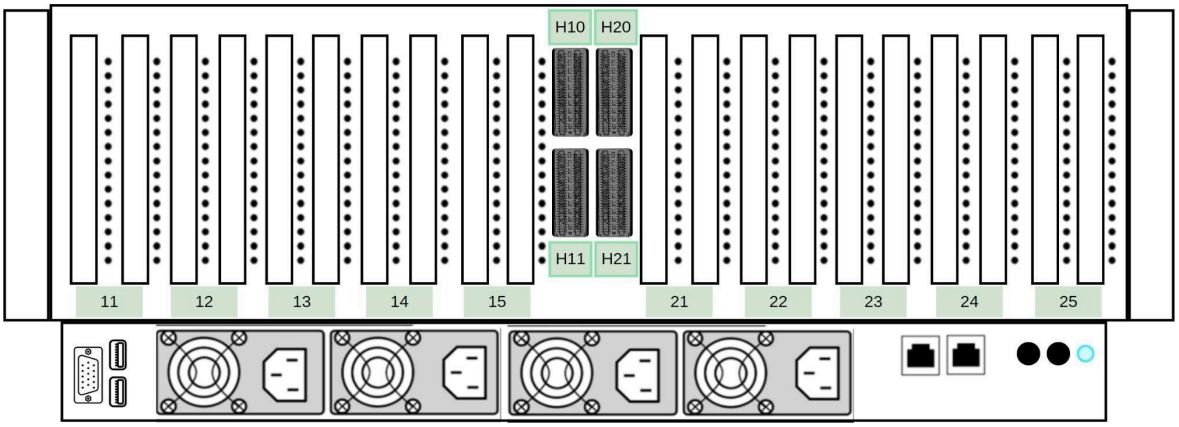


Figure 3. Images of PCIe Gen5 GPU box rear views by different application scenarios

Note: The USB port located at the rear is designated exclusively for H3 USB recovery and installation purposes. Guests are advised against its use.

PCIe Port Number

- 10 GPUs (SKU A)



- 8 GPUs + 4 NICs (SKU B)

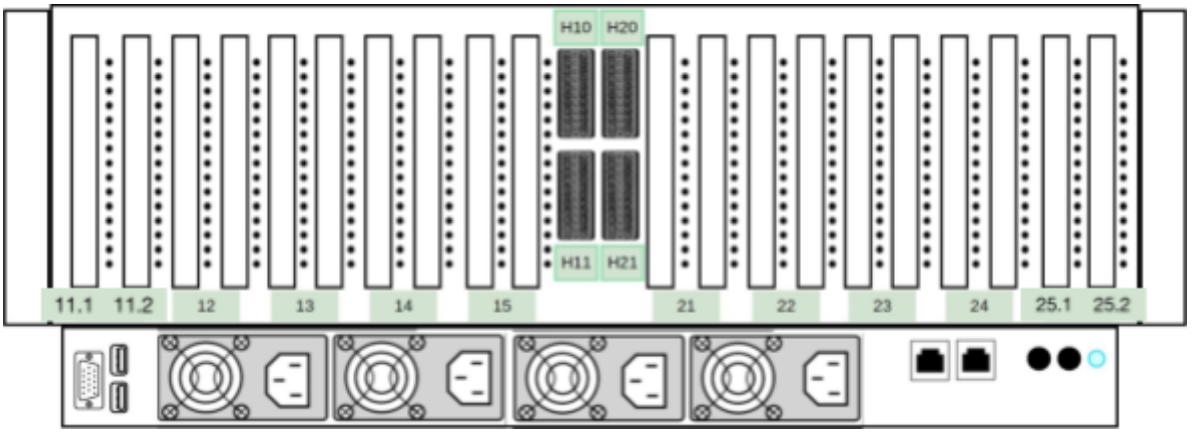


Figure 4. Images of PCIe Gen5 GPU box port number by different application scenarios

Chapter 2.
Installation and Boot-Up Guide

2.1 Confirm Label and Product Match

This procedure provides the steps to verify the Falcon 5012 system's configuration to ensure it matches your requirements. The process includes identifying the SKU, confirming the PSU model, and verifying that the selected mode (Standard (std) or Advanced (adv)) aligns with your requested configuration and included accessories.

About this Task

To ensure the system is configured correctly, you will:

1. Identify the application scenarios: Determine whether the system is configured for 10 GPUs (SKU A) or 8 GPUs + 4 NICs (SKU B).
2. Verify the mode: Confirm whether the system is in Standard (std) or Advanced (adv) mode by checking the included accessories (Retimers and CDFP Cables).
3. Confirm the PSU model: Verify that the installed PSU matches the power requirements (2100W or 3200W).

Notes: Ensure that all accessories match the configuration type indicated by the SKU before proceeding.

Tools and Materials

You will need:

- Access to the SKU label on the external packaging.
- Access to the system chassis for internal verification.

Procedures

Step 1. Identifying the SKU

A. Locate the SKU label on the external packaging (refer to Figure 21).

Figure 21. SKU Label on the Carton (Early & Current Version)

B. Use the following elements in Table 24 to interpret the SKU label:

Table 24. PN Elements and Interpretations for Falcon 5012

PN Elements		Interpretations
Early version	Current version	
"PRPF5012"	"PRG5"	Product - Falcon 5012 (PCIe Gen5 Chassis)
"10" or "08"	"2" or "4"	Application scenarios (SKU): - 10 GPUs (SKU A - 2 Cable CEMs) - 8 GPUs + 4 NICs (SKU B - 4 Cable CEMs)
"STD" or "ADV"	"2" or "4"	- Standard mode (2 host retimers and cables) - Advanced mode (4 host retimers and cables)
"2100" or "3200"	"2" or "3"	PSU rating 2100W or 3200W
N/A	"3" or later	Chassis version (This digit will change as the chassis version is updated)

Step 2. Verify SKU Configuration: Open the chassis and check the expansion cable set (Cable CEMs) count (refer to Figure 22):

- 10 GPU (SKU A): Requires 2 expansion cable sets.
- 8 GPUs + 4 NICs (SKU B): Requires 4 expansion cable sets.

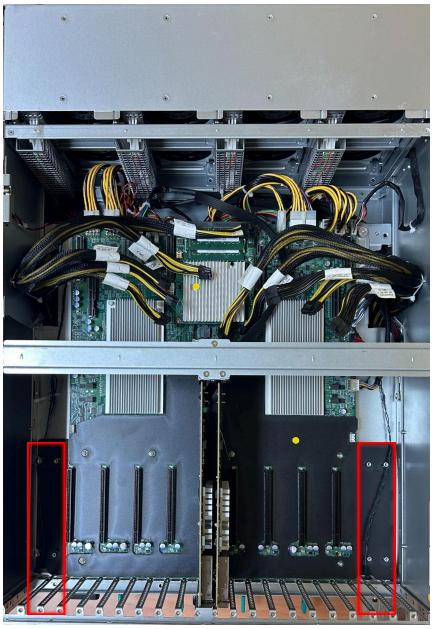


Figure 22. 10 GPUs with 2 expansion cable sets (cable CEMs)

Step 3. Confirming the Standard (std) and Advanced (adv) Mode Accessories

A. Check the included accessories according to Table 25 to ensure they match your configuration:

Table 25. Accessory Comparison Between Standard (std) and Advanced (adv) Modes

Configuration	Host Retimers	CDFP Cables
Standard (std)	2	2
Advanced (adv)	4	4

B. Verify the following:
   - Standard Mode: Confirm the presence of 2 Retimers and 2 CDFP Cables.
   - Advanced Mode: Confirm the presence of 4 Retimers and 4 CDFP Cables.

C. Compare the received accessories with the table above to confirm consistency.

Step 4. Confirming the PSU Model

A. Open the chassis and locate the installed PSU.

B. Verify that the PSU matches one of the supported models:

    - 2100W
    - 3200W

Results

- If the SKU, PSU model, and included accessories match your requested configuration, the system is ready for installation.
- If discrepancies are identified, contact technical support for further assistance.

2.2 Hardware Setup and Power-On Preparation

Set up the Falcon 5012 system by connecting peripherals and preparing the hardware for power-on.

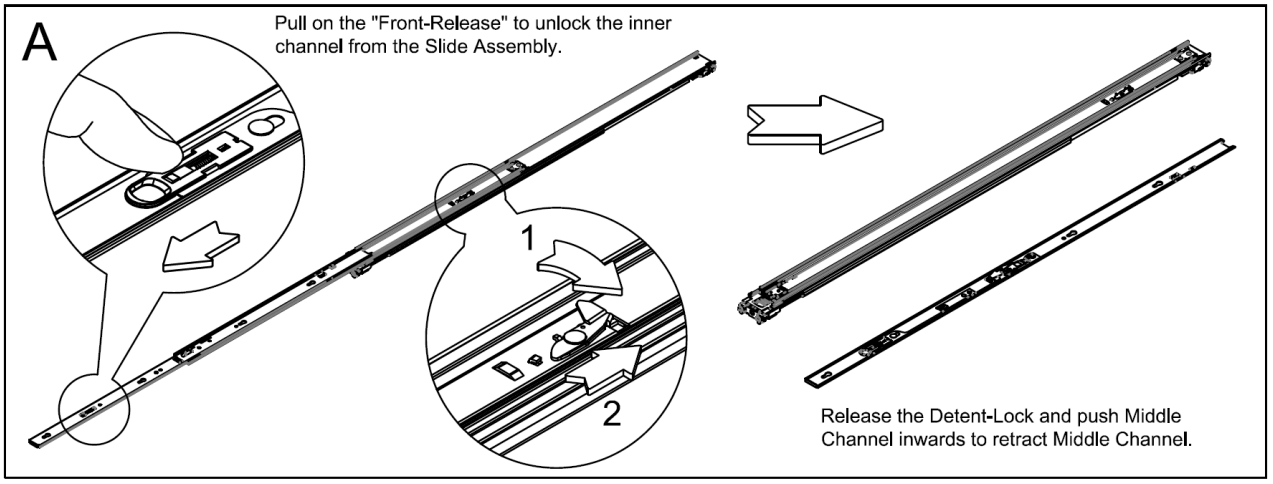
About this task

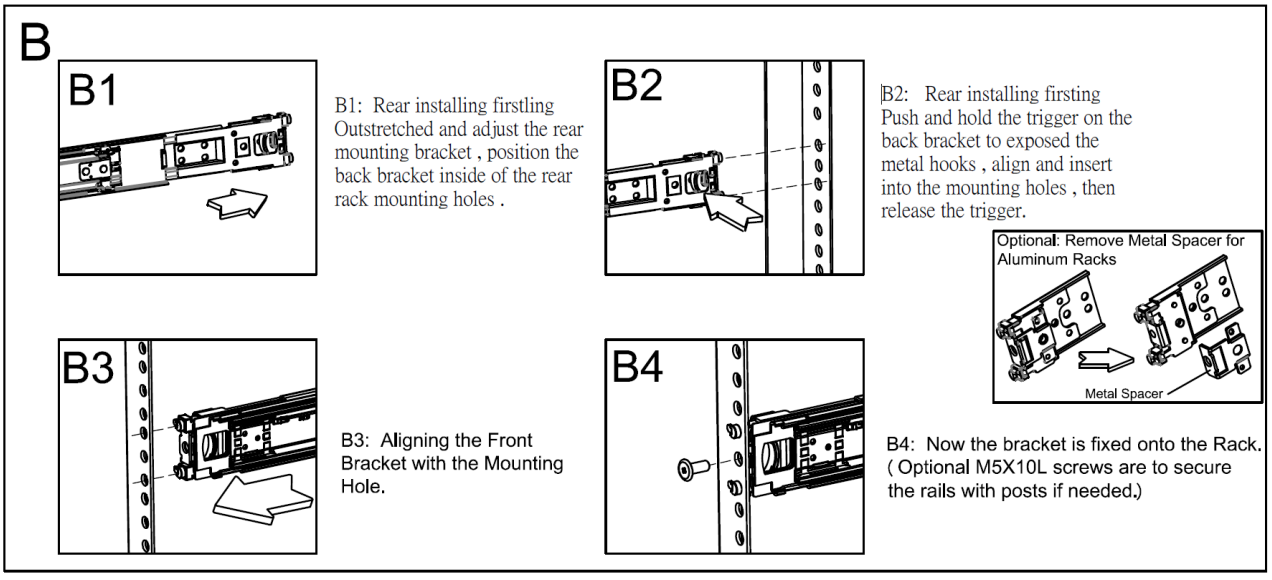
This task involves connecting necessary components and ensuring the system is ready for initialization.

Procedures:

Step 1. Install the System into the Rack (Tool-less Installation)

Refer to Figure 7: Tool-less Rack Rail Installation





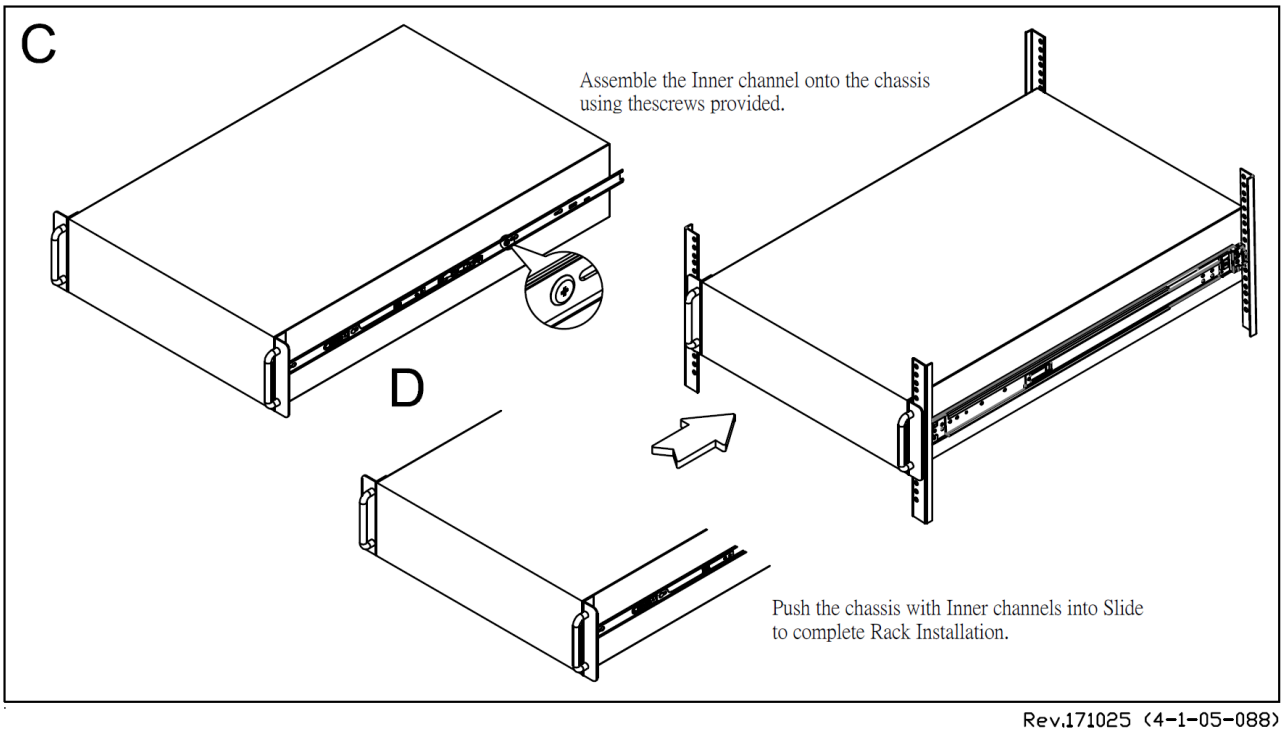


Figure 7. Tool-less Rack Rail Installation

Step 2. Connect the following peripherals (refer to Figure 8)

- Monitor via VGA port.
- Keyboard via USB port.
- LAN cables for GUI and BMC access.

Attention:
Ensure the LAN port indicator light is illuminated after connecting the network cable. This confirms successful communication.

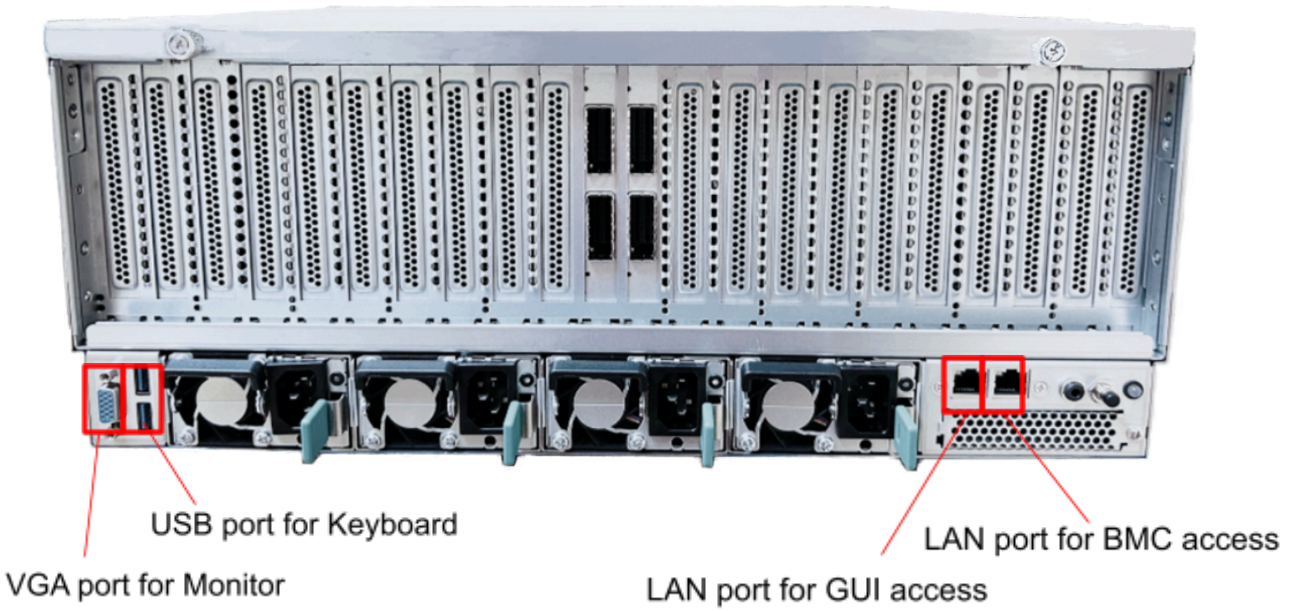


Figure 23. Rear Panel Connections for VGA, USB, and LAN Ports

---

Step 2. Plug in the Power Cord

Connect the power cord to the system (refer to Figure 24 and observe the UID light (refer to Figure 25):

A. The UID light should blink twice and then turn off.
B. Press the Power button to power on the system.

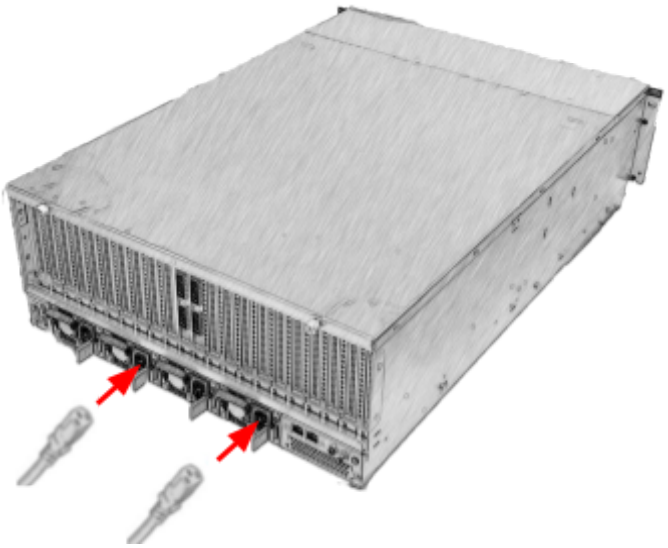


Figure 24. Plugging in Power Cords

Figure 25. UID Light Blinks Twice Before System Power-On

Attention: If the system does not power on (e.g., the screen remains unresponsive or black):

1. Perform an AC power cycle by unplugging and re-plugging the power cord.
2. Repeat Step 2 to confirm the system powers on.
3. If the issue persists, report the problem to the technical support team.

2.3 Retrieve GUI IP for System Boot-Up

Boot into the Linux operating system to retrieve the Management system GUI and BMC IP addresses needed for system operation and chassis management.

About this task

This step is critical for accessing the GUI, finalizing the initial setup, and ensuring efficient system management.

Procedures:

1. Log in to the mCPU console using (refer to Figure 11):
    - Username: admin
    - Password: h3

Figure 11. Linux Login Screen for mCPU Console Access

2. Retrieve the Chassis LAN port IP for connecting to the system's management interface.
    - Enter the command (refer to Figure 12):

```
Unset
ip a
```

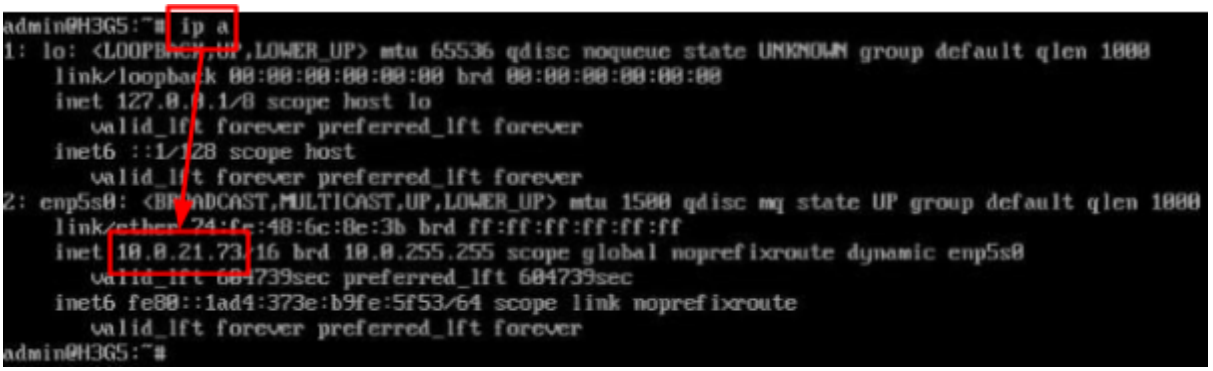


Figure 12. Retrieving Chassis LAN Port IP Address in Linux Interface

3. Retrieve the BMC port IP for connecting to the BMC management interface.
    - Enter the command (refer to Figure 13):

Unset

```
ipmitool lan print
```

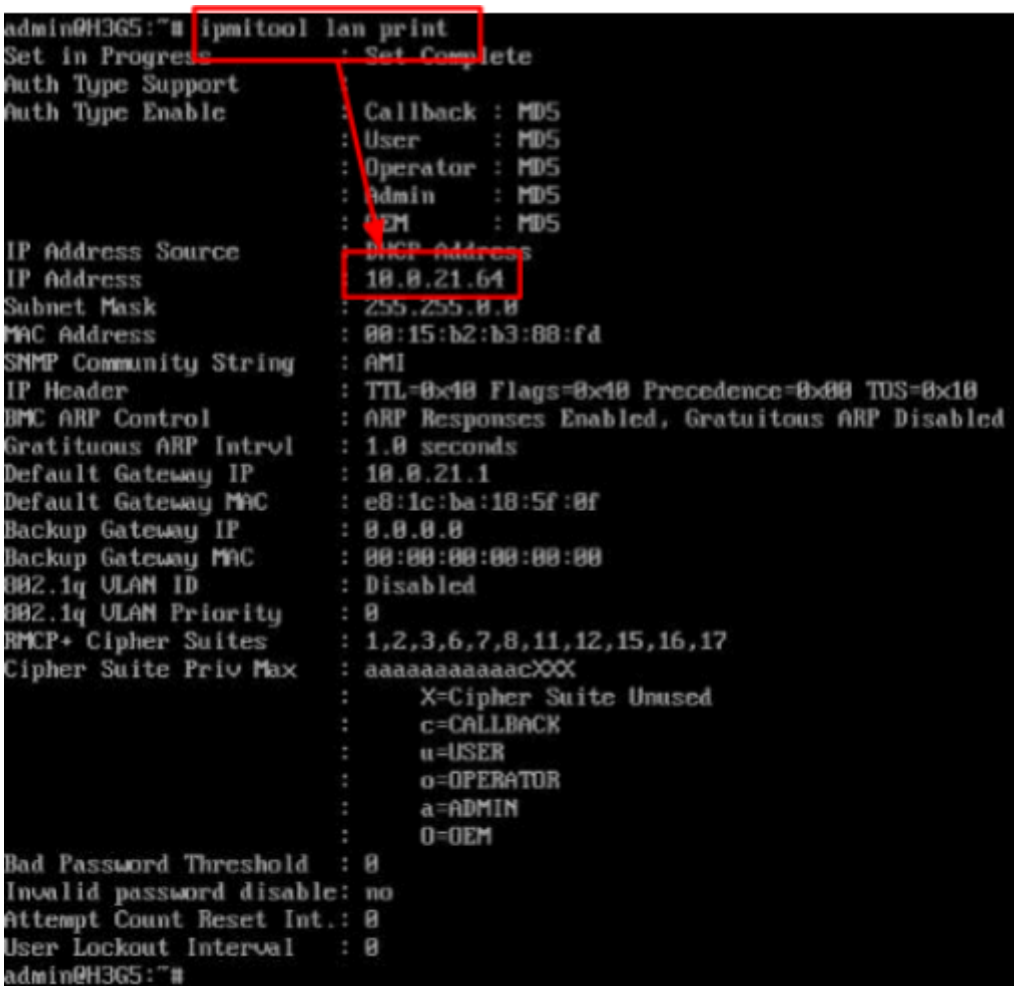


Figure 13. Retrieving BMC port IP Address in Linux Interface

4. Record both IP addresses for further tasks.

Note: For detailed instructions on BMC login, system power control via BMC, CPLD firmware update, and BMC firmware update, refer to Section 3: Common BMC Operations Guide (Page 56).

If the BMC IP is inaccessible:

- Verify the network connection and IP configuration.
- Contact our technical support team for assistance if the issue persists.

2.4 Complete Initial Setup for Falcon 5012 Management GUI

Access the Falcon 5012 Management GUI via the LAN port IP address to configure essential initial settings. These settings include creating an administrator account, configuring network settings, setting the system date and time, and ensuring the GUI is up-to-date.

About this task:
This task is crucial to prepare the system for operation and management. Completing the initial settings ensures seamless integration and functionality for subsequent resource management.

Procedures:
Step1. Access the Management GUI:

- Open a web browser on a device connected to the same network as the chassis.
- Enter the default IP address in the browser's address bar to access the system management interface.

GUI/API Default Address: **http://169.254.100.200**

Note:

- If two systems need to access the GUI for initial setup at the same time, make sure to complete the setup on one system before switching to the next. This prevents IP conflicts.
- Make sure your computer is on the same network as the device. Connect the network cable to the laptop, configure the network settings, verify GUI accessibility, and proceed with the initial setup via the GUI.

Step 2. Complete the Initial Setting Steps:

A. Set Administrator Account (refer to Figure 26):

1. Create and confirm a strong password for the administrator account.
2. Click Next to proceed to the next step of the setup.

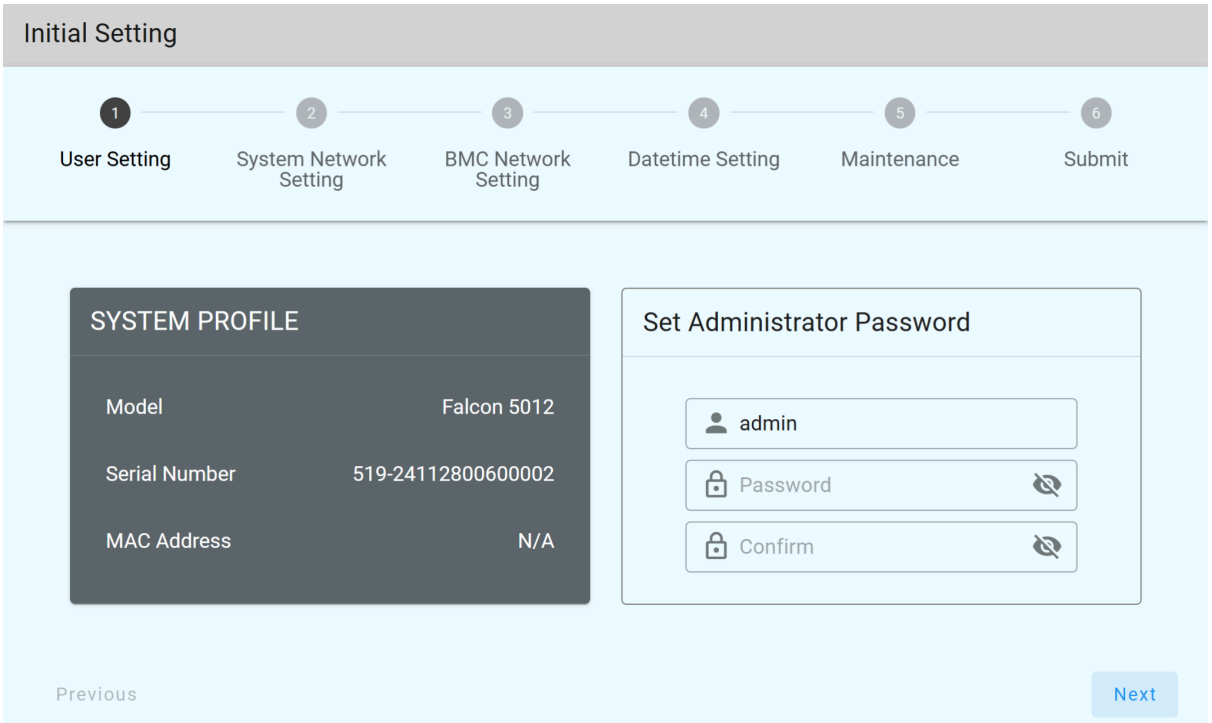


Figure 26. Setting the Administrator Password During Initial Setup

B. Configure System Network Settings (refer to Figure 27)

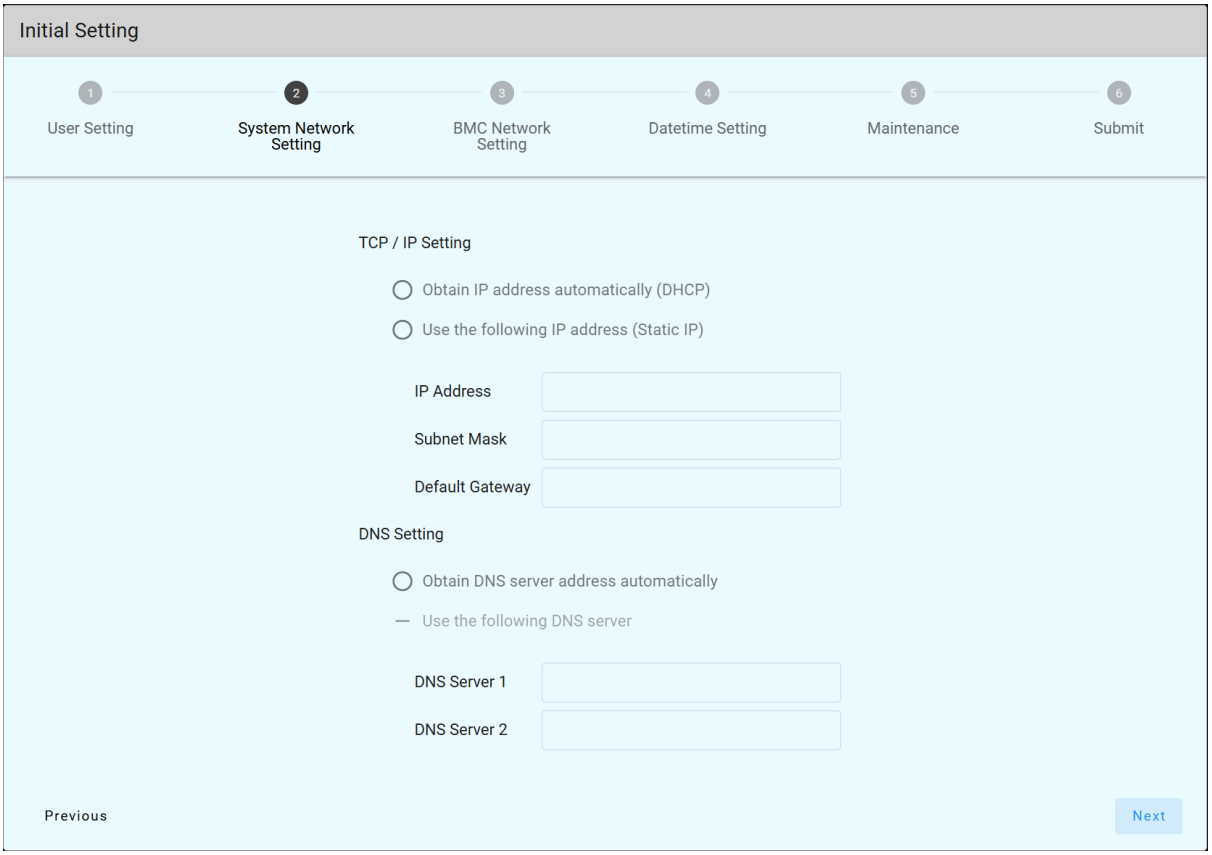


Figure 27. Configuring TCP/IP and DNS Settings in System Network Setting

C. Select IP Configuration Method:
Option 1: Select Obtain IP address automatically (DHCP) to use a dynamically assigned IP address from the network.

> **Important:** DHCP-assigned IP addresses are dynamic and may change. If the IP address expires or changes, you will need to return to the Linux OS to obtain the new DHCP IP address.

Option 2: Select Use the following IP address (Static IP) to manually configure a fixed IP address to avoid address changes.

Input Network Details (if using a Static IP):

a. IP Address: Enter the desired static IP address.
b. Subnet Mask: Input the appropriate subnet mask for your network.
c. Default Gateway: Provide the default gateway address for network communication

D. Select DNS Configuration Method:
Option 1: Select Obtain DNS server address automatically to use DNS settings provided by the network.

Option 2: Select Use the following DNS server and manually input:

a. DNS Server 1: Primary DNS server address.
b. DNS Server 2: Secondary DNS server address (optional).

Save and Confirm:

a. Review all entered information to ensure accuracy.
b. Click Next to save the settings and proceed to the next configuration step.

Note:

- DHCP IP addresses are suitable for temporary setups but may lead to connectivity issues if they change.
- Using a static IP is recommended for stable and long-term configurations to maintain consistent access to the GUI.
- Always ensure the selected IP address (static or dynamic) does not conflict with other devices on the network.

Step 3. Configure BMC Network Settings

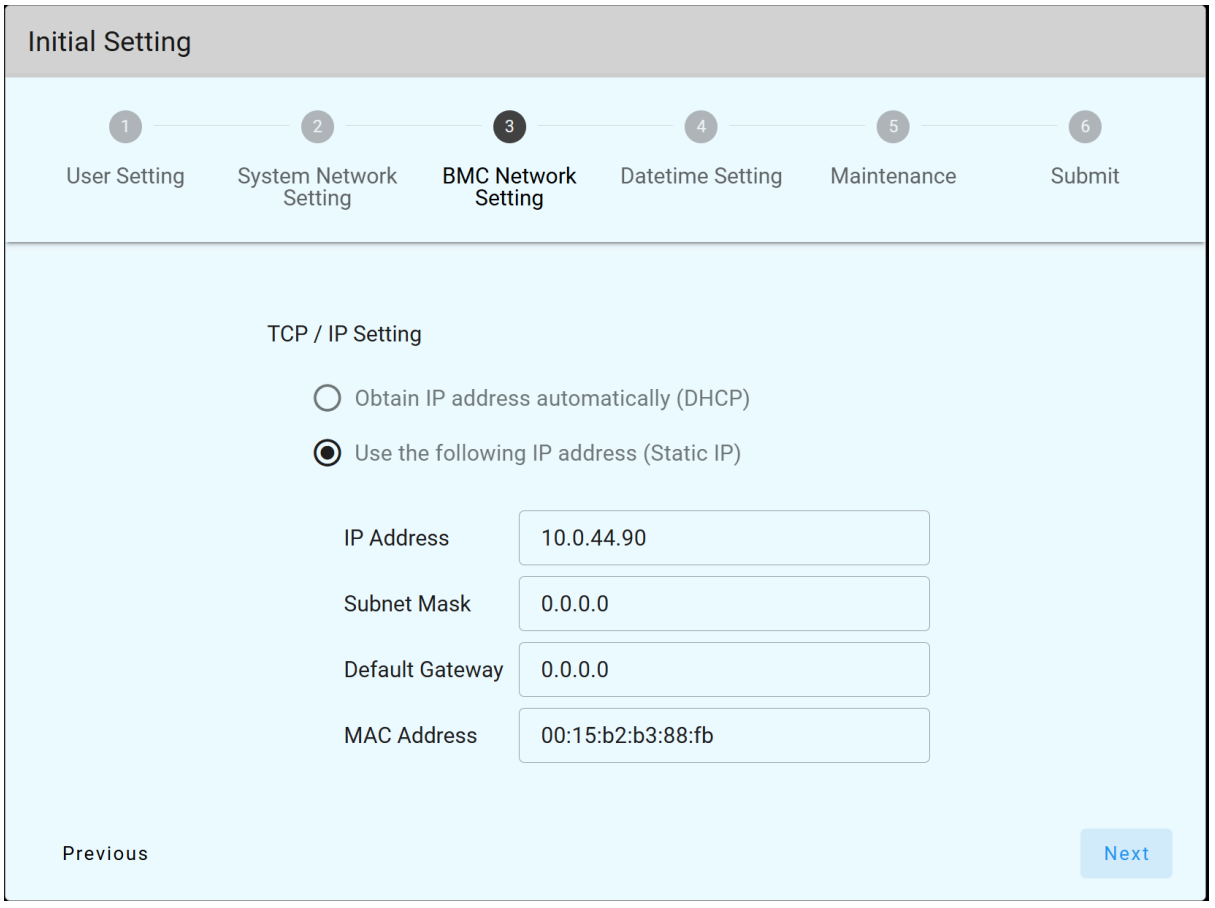


Figure 28. Configuring BMC Network Settings with TCP/IP Options

A. Select BMC IP Configuration Method:

Option 1: Dynamic IP Address (DHCP):

- Select Obtain IP address automatically (DHCP) to allow the network to assign an IP address dynamically.

> **Note:** DHCP-assigned IP addresses are dynamic and may change over time. If the BMC IP changes, you will need to return to the Linux OS to retrieve the new address.

Option 2: Static IP Address: Select Use the following IP address (Static IP) to manually assign a fixed IP address.

B. Input Static IP Details (if selected): Enter the following information:
   - **IP Address:** The desired static IP address for the BMC.
   - **Subnet Mask:** The appropriate subnet mask for your network.
   - **Default Gateway:** The default gateway address for the BMC network.

C. Review and Save Settings:
   1. Verify the entered information for accuracy and alignment with your network configuration.
   2. Click Next to save the settings and proceed to the next configuration step.

> **Important Notes:**
> - For DHCP Users:
>   DHCP is suitable for temporary setups or dynamic environments. Be aware that IP addresses may change, requiring you to retrieve the new BMC IP address from the Linux OS if access is lost.
> - For Static IP Users:
>   A static IP ensures stable and consistent access to the BMC. Ensure the assigned IP does not conflict with other devices on the network.
> - General Precautions:
>   - Verify that the IP address, subnet mask, and gateway belong to the same subnet.
>   - Avoid leaving the gateway field blank, as it may cause connectivity issues.

Step 4. Set Datetime:

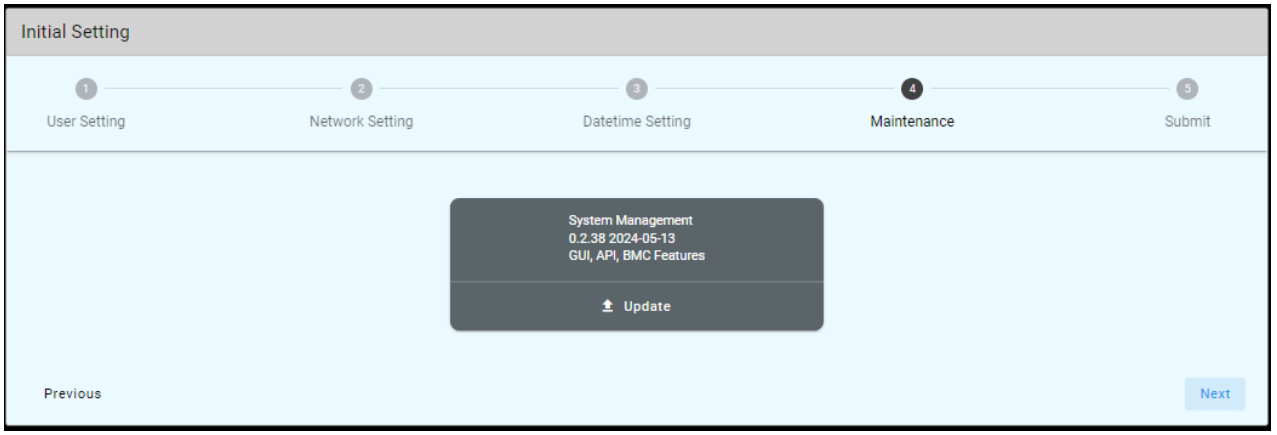
- Adjust the system date and time to ensure accuracy.

Step 5. Perform Maintenance Updates

A. Download the Latest Firmware:

1. Access the H3 Platform support page:
   - Navigate to Support → Knowledge Base → Download on the H3 Platform website.
   - Alternatively, visit the following URL directly: https://www.h3platform.com/knowledge-base/document
2. Select the appropriate options:
   - Product Type: Composable GPU Chassis.
   - Model Type: Falcon 5012.
3. Download the latest System Management Firmware file.

B. Upload the Firmware to the System:



1. On the Maintenance screen: Click the Update button under the System Management section.
2. Select the downloaded firmware file: Confirm the file is correct and click Update.

Important: Uploading the firmware cannot be cancelled once you click the Update button.

3. Verify the upload process:
   a. Wait for the system to process the firmware update.
   b. A success message will be displayed:
      "System firmware update successful. Please proceed to the next step."

C. Complete the Maintenance Step:

1. After the firmware upload is complete: Click Submit to finalize the Maintenance step.
2. Proceed to the next steps in the Initial Setting process.

D. Restart the System (Post-Setup):
    1. Complete all steps in the Initial Setting process.
    2. After entering the GUI system, the system will prompt for a restart.
    3. Restart the system to apply the firmware update.

Notes:
- File Compatibility: Ensure the downloaded firmware matches the Falcon 5012 model to prevent errors.
- Stable Upload Environment: Do not power off or interrupt the system during the firmware upload process.
- Firmware Application: The updated firmware will only take effect after completing the Initial Setting process and restarting the system.

Step 6. Submit the Configuration:

After completing all settings, click Submit to save the changes and proceed to the GUI dashboard for system management.

2.5 Device Installation in Falcon 5012 System

This task outlines installing GPUs and other PCIe devices into the Falcon 5012 system. It includes accessing the chassis, installing and securing GPUs, and connecting power cables. Follow the steps precisely to ensure system stability and performance.

About this task:
Proper GPU installation is critical to maintain system integrity and ensure optimal performance. This task includes safety precautions, required tools, and step-by-step instructions for installing dual-width and single-width PCIe devices.

Procedures:

Step 1. Preparation for GPU Installation:

A. Safety Precautions:
   1. Power off the system and disconnect it from all power sources.
   2. Use an ESD wrist strap to prevent electrostatic discharge damage.
   3. Verify the GPU's compatibility with the system's PCIe slot and power cables.

B. Required Tools:
   1. Screwdriver for stabilization plate and PCIe slot screws.
   2. GPU power cables (refer to Figure 34 for cable descriptions).

Important:
Always use an ESD wrist strap to protect the system from static damage. Ensure that the system is completely powered off before proceeding.

Step 2: Accessing the Chassis:

A. Opening the Chassis:
   1. Loosen the hand screws securing the top cover.
   2. Slide the cover backward to expose internal components (refer to Figure 29).

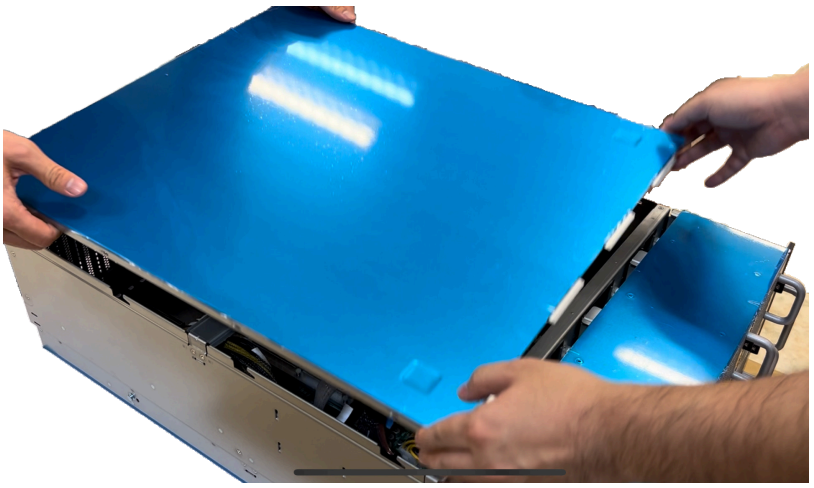


Figure 29. Removing the Top Cover to Access the Internal Components

B. Removing the Stabilization Plate:
    1. Unscrew the screws on both sides of the stabilization plate.
    2. Carefully lift and remove the plate (refer to Figure 30).

Figure 30. Removing the Stabilization Plate for Internal Component Access

---

Step 3: Installing Dual-Width GPUs:

A. Preparing the PCIe Slot: loosen and remove the two brackets adjacent to the target PCIe slot.

B. Inserting the GPU:

Important: Be cautious of onboard components during the installation process to avoid accidental collisions.

1. Align the GPU connector with the PCIe slot.
2. Press the GPU vertically into the slot until it is securely seated (refer to Figure 31).

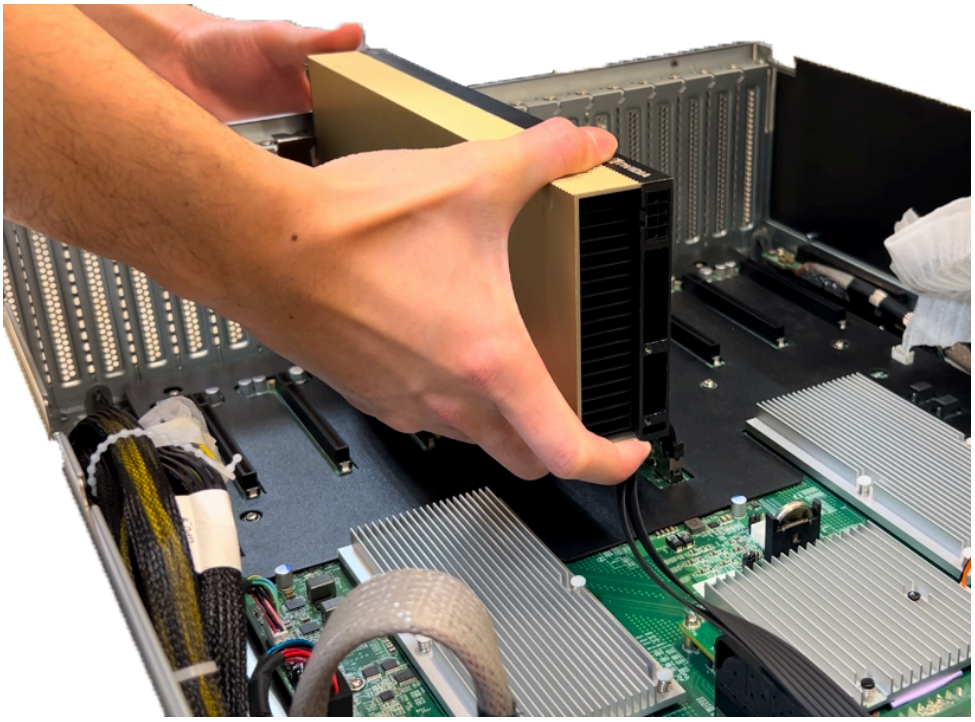


Figure 31. Inserting a Dual-Width GPU into the PCIe Slot

C. Securing the GPU: Use screws to secure the GPU in place.

Note:
Ensure the rear gold fingers are properly seated in the PCIe slot. Misalignment may cause system errors or physical damage.

Step 4: Connecting GPU Power Cables:

A. Power Cable Mapping: Use the appropriate GPU power cables and connect them according to the following mapping (refer to Figure 33):
   - Left-side short cables (GPU_1, GPU_2, GPU_3): PCIe slots 11, 12, 13.
   - Left-side long cables (GPU_4, GPU_5): PCIe slots 14, 15.
   - Right-side long cables (GPU_6, GPU_7): PCIe slots 21, 22.
   - Right-side short cables (GPU_8, GPU_9, GPU_10): PCIe slots 23, 24, 25.

Note: Connect the GPU power cables as indicated by the labels on the cables. Refer to Figure 32 for an example of the label format, which displays the corresponding GPU number (e.g., GPU_4, GPU_5) for accurate identification.

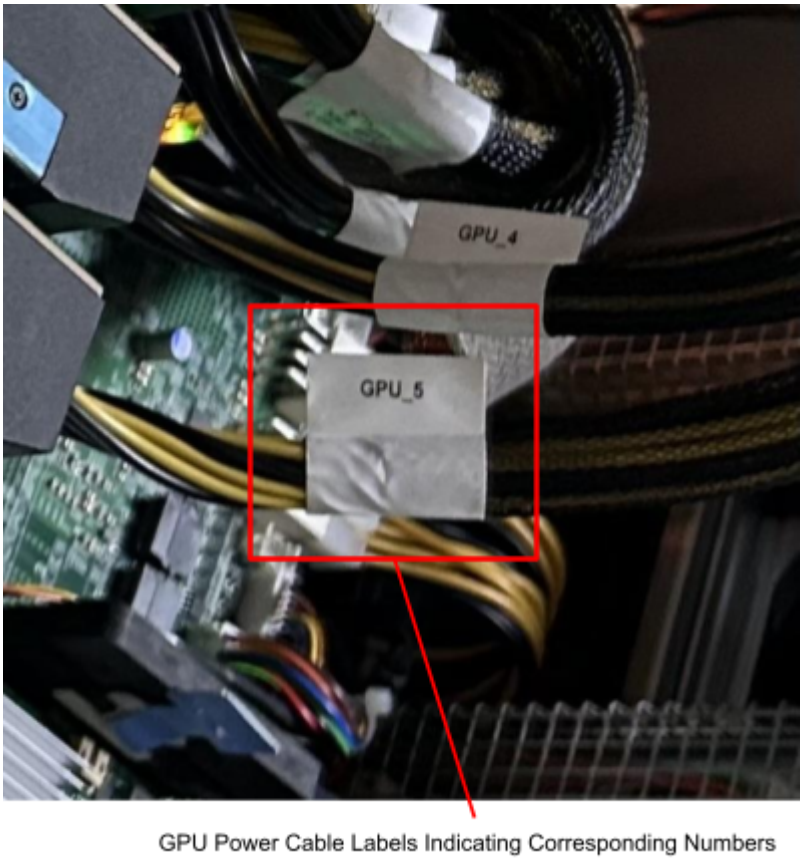


Figure 32. GPU power cables are labeled with corresponding numbers (e.g., GPU_4, GPU_5) to ensure accurate connections.

Important: Connect the GPU power cables to the corresponding PCIe slots as indicated. The figure below illustrates the slot numbers for each connection.

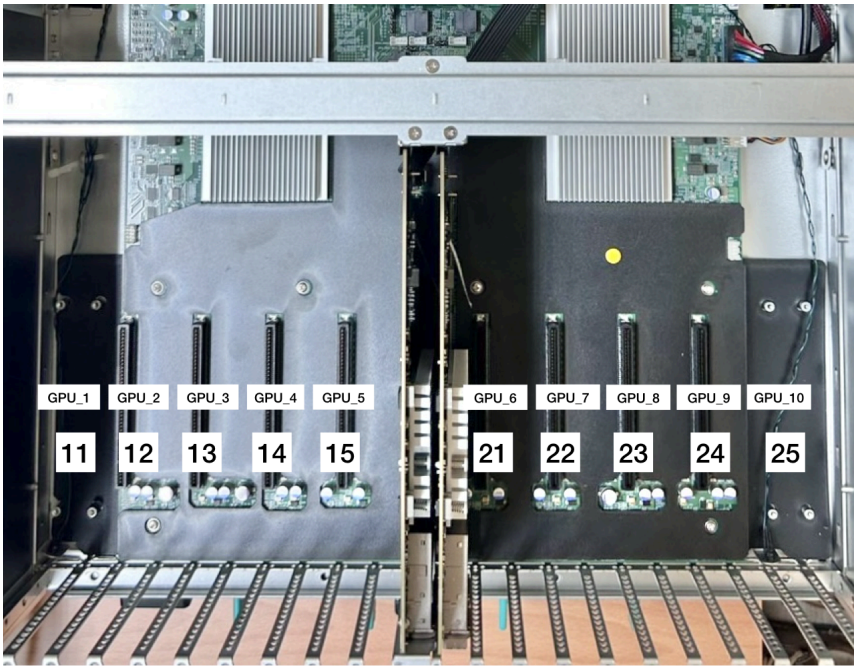


Figure 33. PCIe Slots with Corresponding Numbers

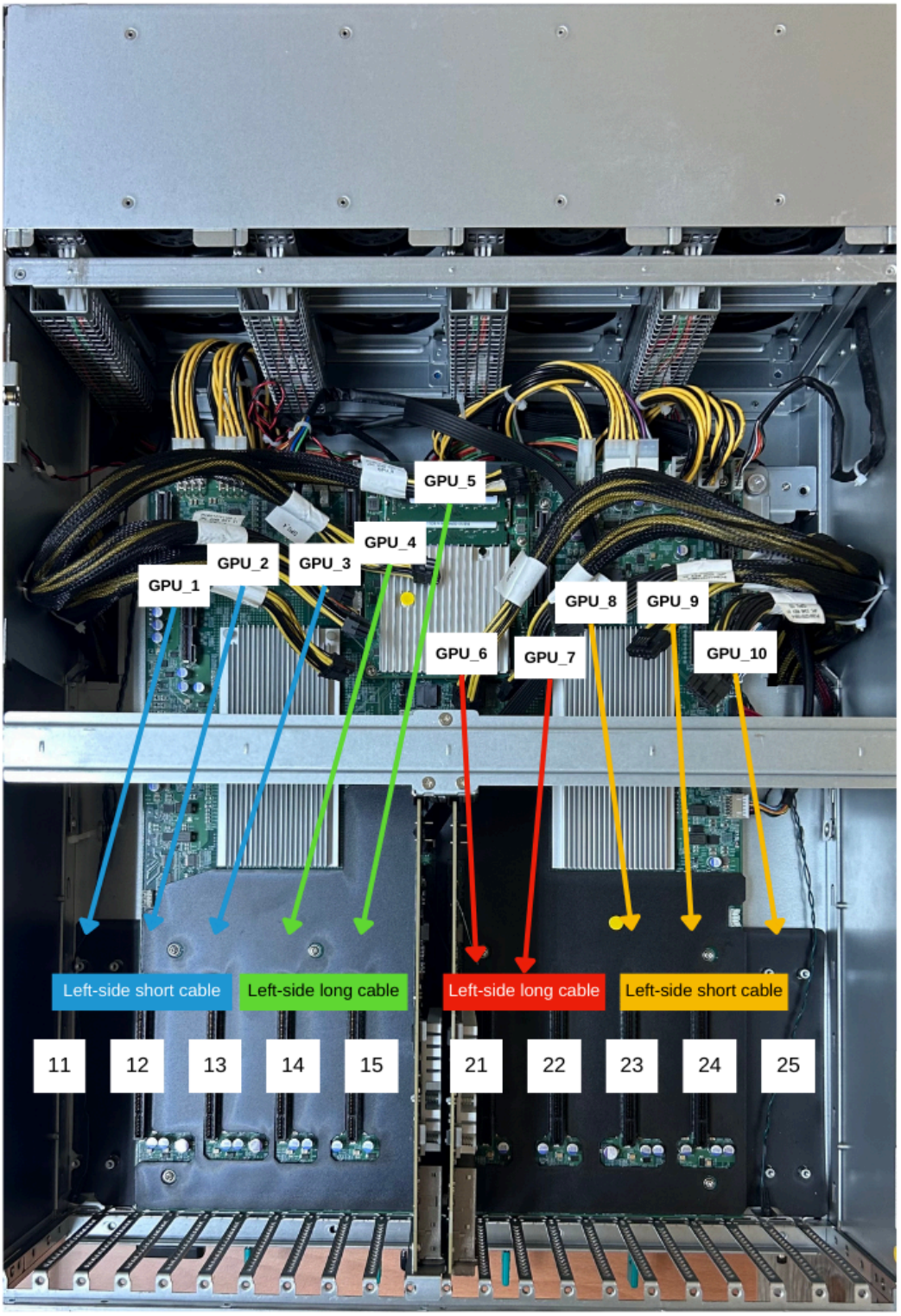


Figure 34. GPU Power Cable Connections and Label Mapping

B. Securing Connections: Ensure all power cables are securely connected.

Caution: Use only model-specific power cables to avoid damage. Ensure that each power cable is connected to its corresponding GPU for proper one-to-one mapping.

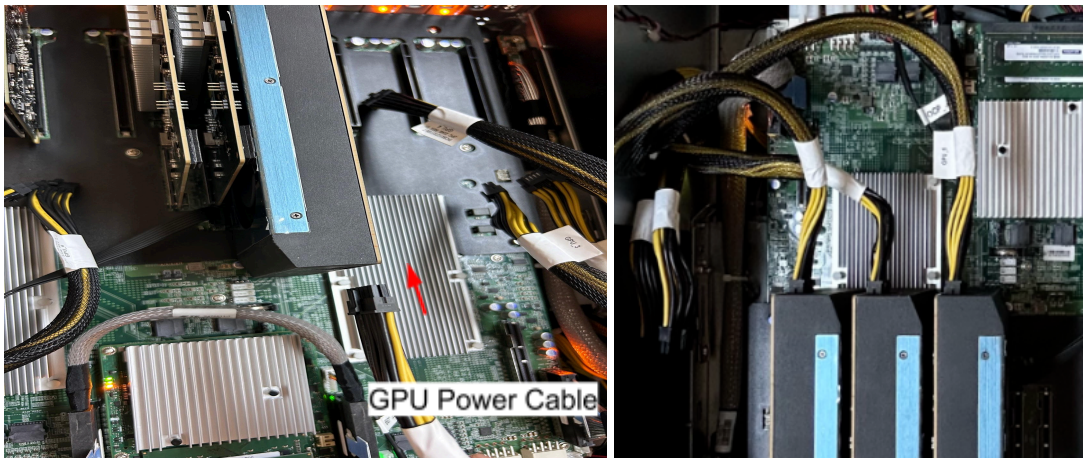


Figure 35. Securing GPU Power Cable Connections

Step 5. Installing Single-Width PCIe Devices:
Installation Steps:

Important: Be cautious of onboard components during the installation process to avoid accidental collisions.

A. Remove the bracket nearest to the target PCIe slot
B. Insert the single-width device (e.g., NIC card or single-width GPU) into the PCIe slot (refer to Figure 36)

Figure 36. Installing a Single-Width Device into the PCIe Slot

C. Secure the device with screws.

Important: Ensure PCIe slots can accommodate the device's width and follow installation guidelines to avoid connection errors.

2.6 Retimer Installation and Host Configuration

Retimer cards are required to maintain PCIe Gen5 signal integrity between the host server and the expansion chassis. This section focuses on installing and configuring retimer cards in host-side (server-side) deployments, where the card is installed directly into a PCIe Gen5 x16 slot on the server.

Two types of retimer cards are supported: C01 and D01. Each requires specific DIP switch settings to ensure proper link control and system compatibility when installed on the host.

> **Note:** For advanced configurations where retimer cards are installed inline within the Falcon 5012 chassis-side expansion cabling, refer to Chapter 7 – Supplementary Notes for additional instructions and supported topologies.

About the Task

To configure a retimer card for host-side installation:

1. Identify the card variant:
    - C01: Single SW1 switch
    - D01: 3-bit DIP switch (CH1–CH3)
2. Set DIP switch positions:

   C01
    - SW1 = ON
    - SW2 = HLL
3. D01
    - SW1:
        - PERST = ON
        - I2C_SDA = OFF
        - I2C_SCL = OFF
    - SW2 = HLH
4. Install the card into the designated PCIe Gen5 x16 slot on the host server.
5. Connect the CDFP cable between the retimer and the expansion chassis.

Prerequisites

Before proceeding with the installation, ensure the following:

- The host system has an available PCIe x16 slot with installation space of 150 mm length and 68.85 mm height (see Table 26).

Table 26. Retimer Installation Requirements

Requirement	Description
Installation Space	PCIe x16 socket, with 150 mm length and 68.85 mm height.

- The Retimer is ready for installation.
- Proper electrostatic discharge (ESD) precautions are taken to prevent damage to components.

Refer to Section 2.4.2 for the hardware information of the Retimer.

Procedures

Step 1. Configure Retimer Switches

Before installing the retimer card, configure the DIP switches properly. C01 and D01 variants have different switch layouts and behavior.

For C01 Host Adapter:

- Set SW1 = ON for server-side installation.
  Refer to Figure 37 for switch orientation.
- Set SW2 = HLL, which corresponds to I2C address 0xE8
  This is the default setting and typically does not require change.

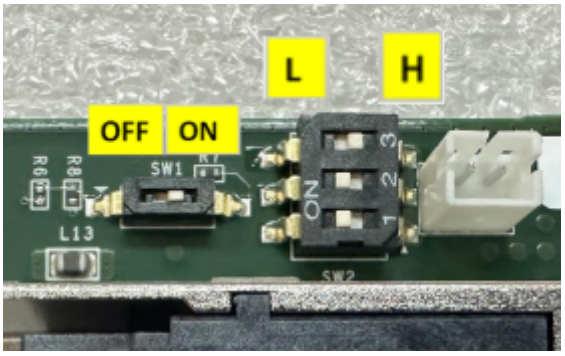


Figure 37. SW1 and SW2 DIP Switch Settings for C01 Host-Side Installation

---

For D01 Host Adapter:

- Configure SW1 (3-bit DIP switch) as follows for host-side use:
  - PERST switch = ON → Allow PERST from host to JBOX

- I2C_SDA switch = OFF → Block I2C_SDA from host
- I2C_SCL switch= OFF → Block I2C_SCL from host
- Refer to Figure 39 for DIP switch layout.

- Set SW2 = HLH, which corresponds to I2C address 0xEA

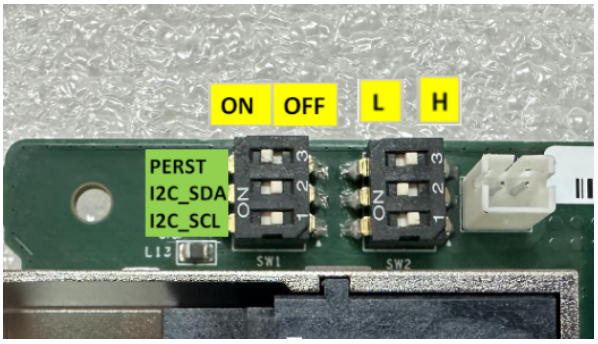


Figure 38. SW1 and SW2 DIP Switch Settings for D01 Host-Side Installation

---

Step 2. Install the Retimer Card

A. Insert the retimer card into the designated PCIe Gen5 x16 slot on the host server.
B. Verify that the card is fully seated and secured using the chassis retention mechanism.

Step 3. Connect the CDFP Cable

A. Use certified CDFP cables to connect the retimer card to the expansion chassis.
B. Ensure both ends are properly seated and locked to avoid signal loss.

Caution: Ensure the CDFP cable is securely connected. Failure to properly lock the connector can result in system malfunctions and potential damage to the Falcon 5012.

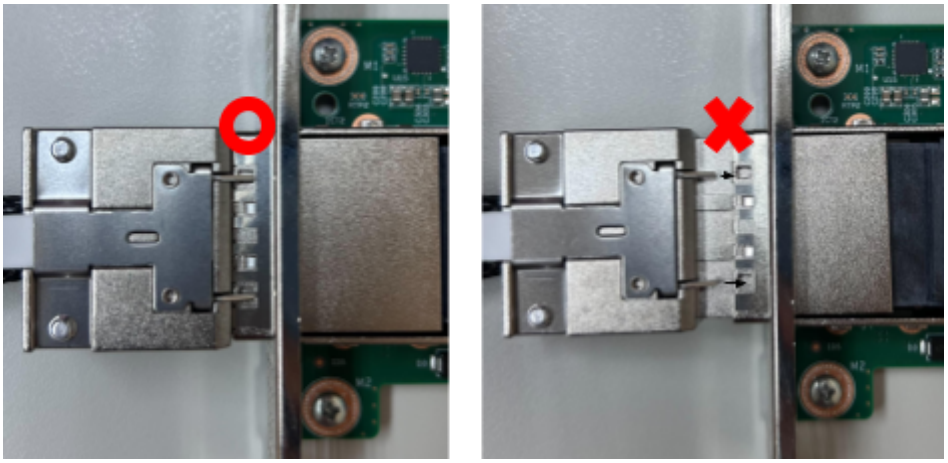


Figure 39. Picture of properly connecting the CDFP cable with the CDFP connector

Note: For JBox-side deployments, refer to Chapter 7 – Supplementary Notes for the appropriate DIP switch configuration.

2.7 GPU Assign and Unassign

This task explains how to assign or unassign GPUs to hosts using the Resource Management interface in the GUI.

Attention: The mode switch between Standard Mode and Advanced Mode must be synchronized across all PCIe switches.

- It is not possible to have mixed modes (e.g., some switches in Standard Mode and others in Advanced Mode).
- Ensure that all switches are set to the same mode to avoid operational conflicts.

About this task:

In Standard Mode, each PCIe switch is fixedly assigned to a single host, and the GPUs connected to that switch are automatically allocated to the host.

In Advanced Mode, one PCIe switch can connect to multiple hosts, enabling users to dynamically assign or unassign GPUs based on specific host requirements. This mode offers greater flexibility for resource allocation.

Procedures

Step 1. Assign GPUs in Advanced Mode:

A. Navigate to the Resource Management interface in the GUI.

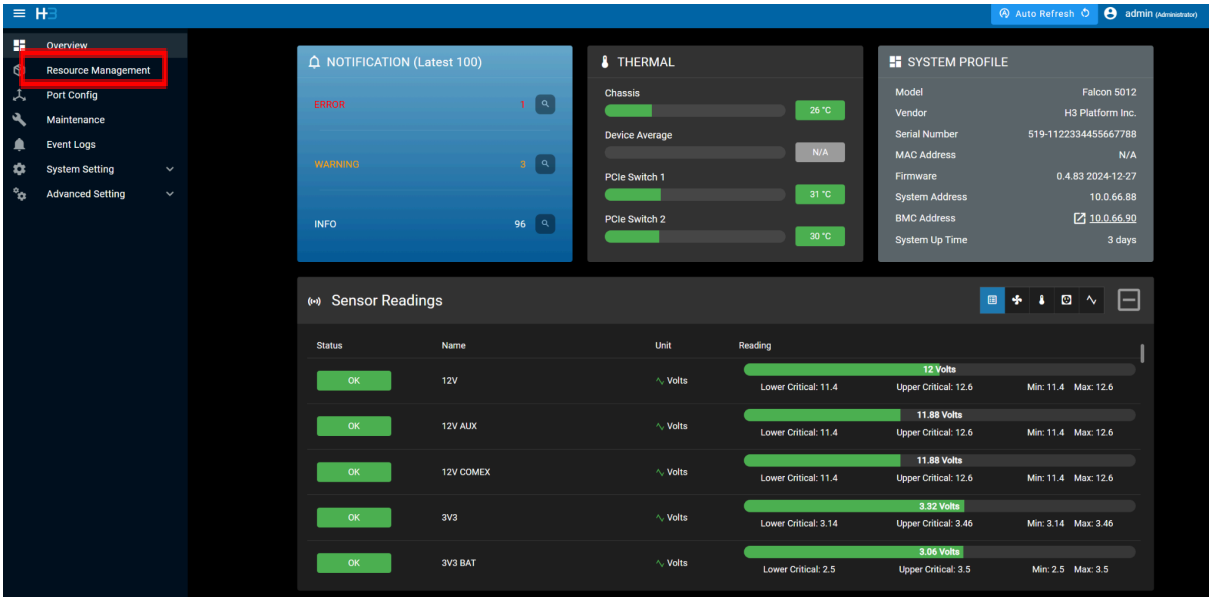


Figure 40. Accessing the Resource Management Interface on GUI

B. Select the host to which you want to assign GPUs.

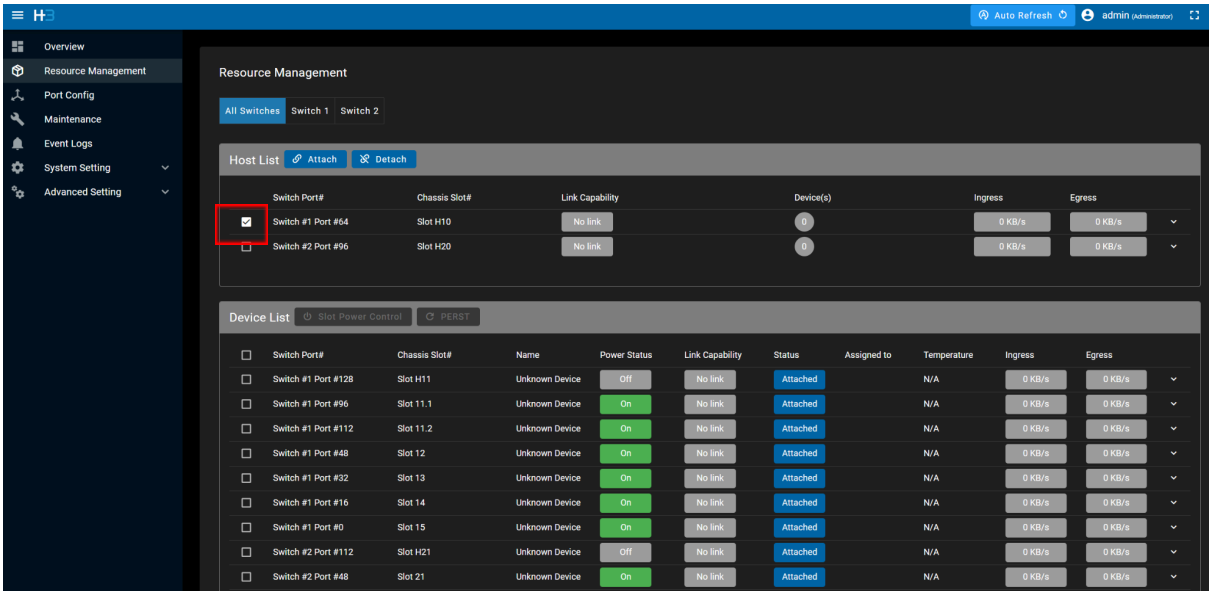


Figure 41. Selecting a Host for GPU Assignment in Resource Management

C. Click the Attach tab to access the GPU allocation page.

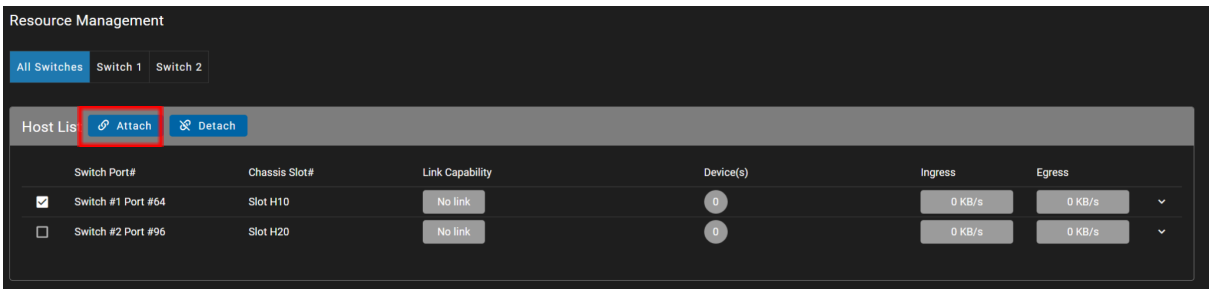


Figure 42. Accessing the GPU Allocation Page via the Attach Tab

D. Perform the following steps:

1. From the displayed GPU list, select the GPUs you want to assign.

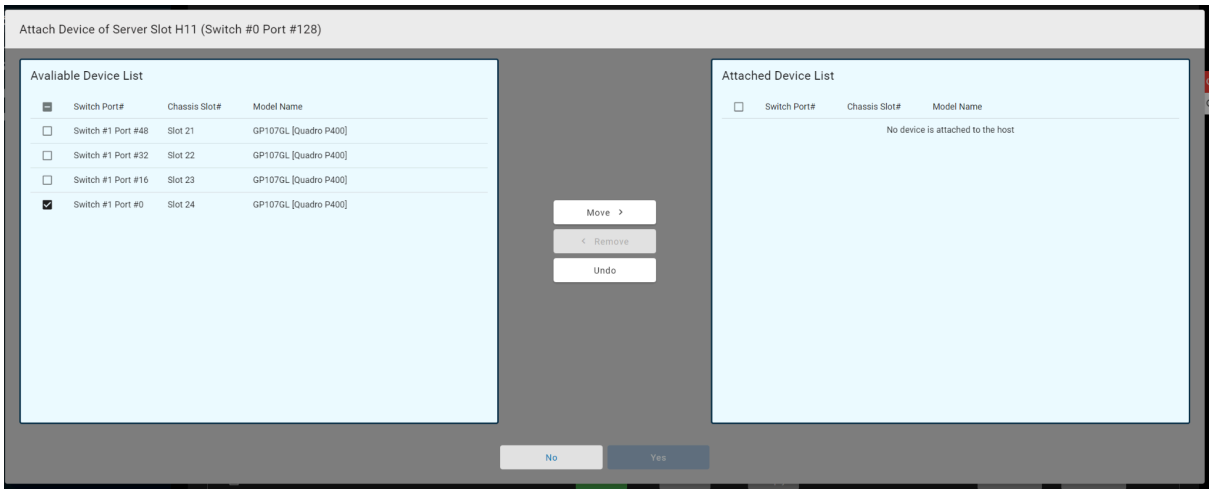


Figure 43. Selecting GPUs from the Available Device List

2. Click Move to transfer the selected GPUs to the Attached GPUs column.

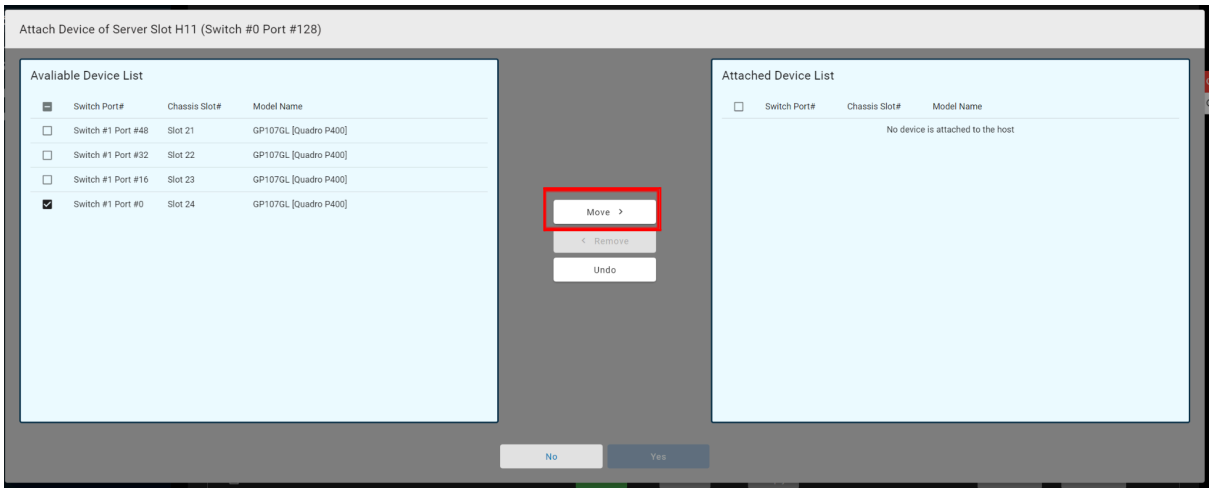


Figure 44. Moving GPUs from the Available Device List to the Attached Device List

E. Confirm the selection by clicking Yes to complete the GPU assignment.

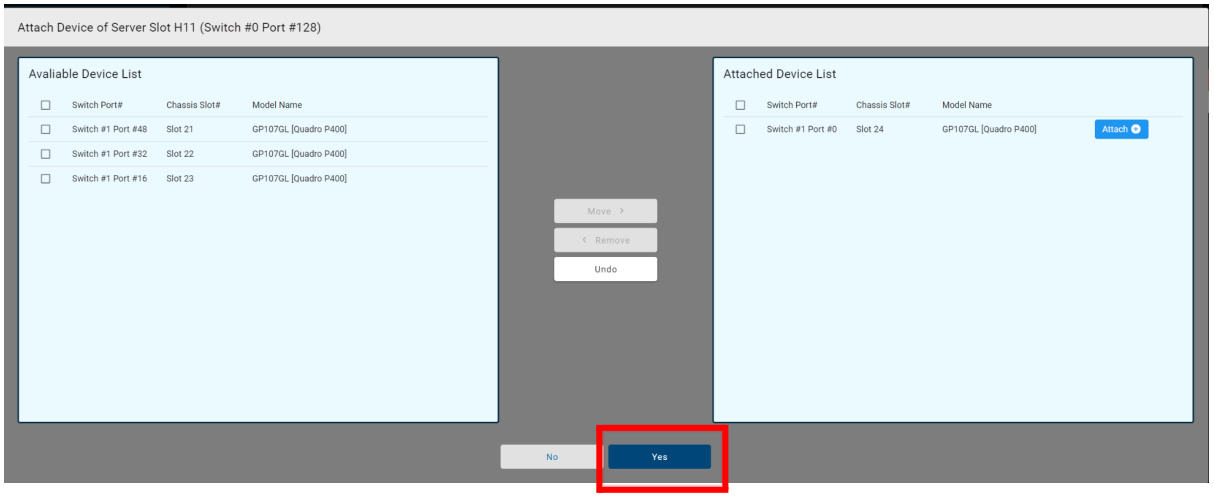


Figure 45. Confirming GPU Assignment by Clicking "Yes"

Step 2. Unassign GPUs in Advanced Mode (if needed):

A. Navigate to the Resource Management interface in the GUI.

B. Select the host from which you want to unassign GPUs.

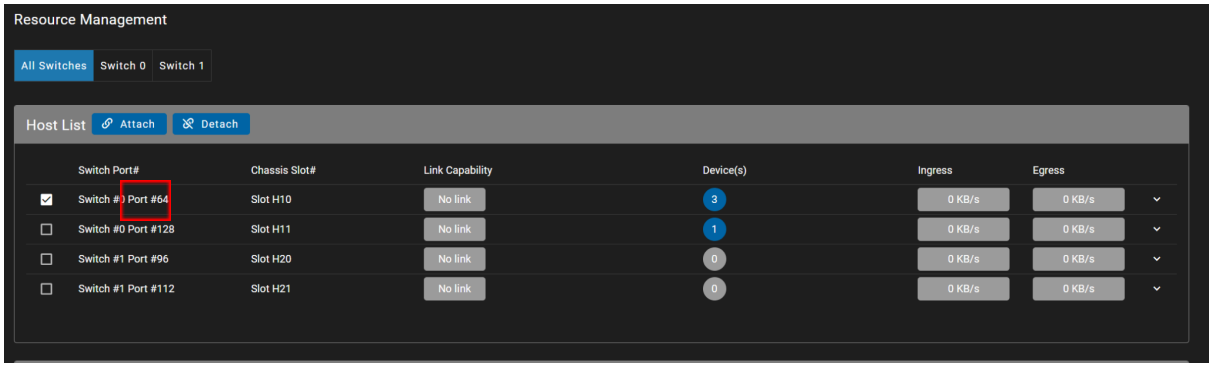


Figure 46. Selecting Host for GPU Unassignment on GUI

C. Click the Detach tab to access the unassignment page.

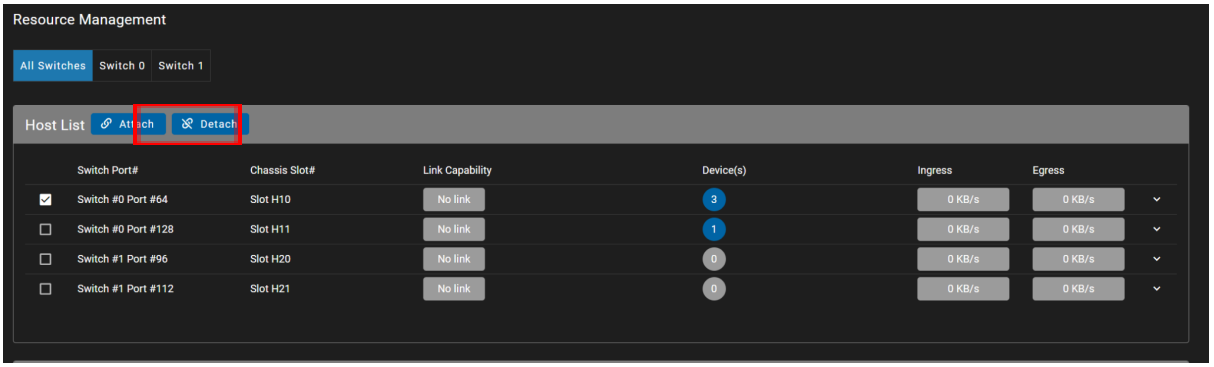


Figure 47. Accessing the Unassignment Page via the Detach Tab

D. Perform the following steps:

1. From the Attached GPUs column, check the GPUs you want to unassign.

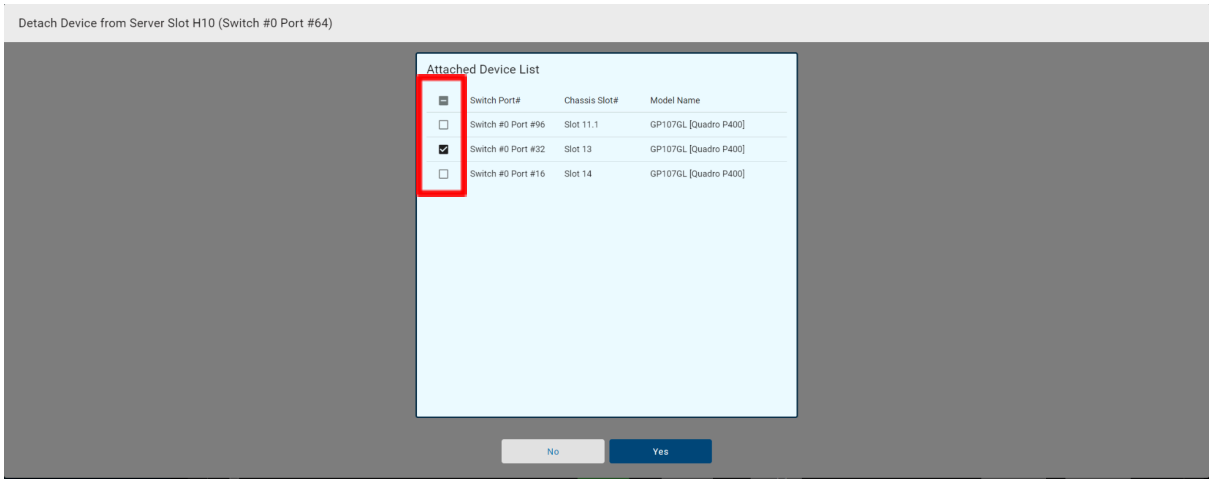


Figure 48. Checking the GPUs for Detachment

2. Click Yes to detach the selected GPUs back to the Available GPUs column.

Step 3. Verify Connections:

A. Ensure that the CDFP cable is securely connected between the chassis and host (refer to Figure 49). Connect the corresponding ports with CDFP cables as shown in Figure 50.
B. Confirm that GPUs are properly assigned to their respective hosts in the GUI.
C. After verifying all connections and assignments, proceed to power on the server.

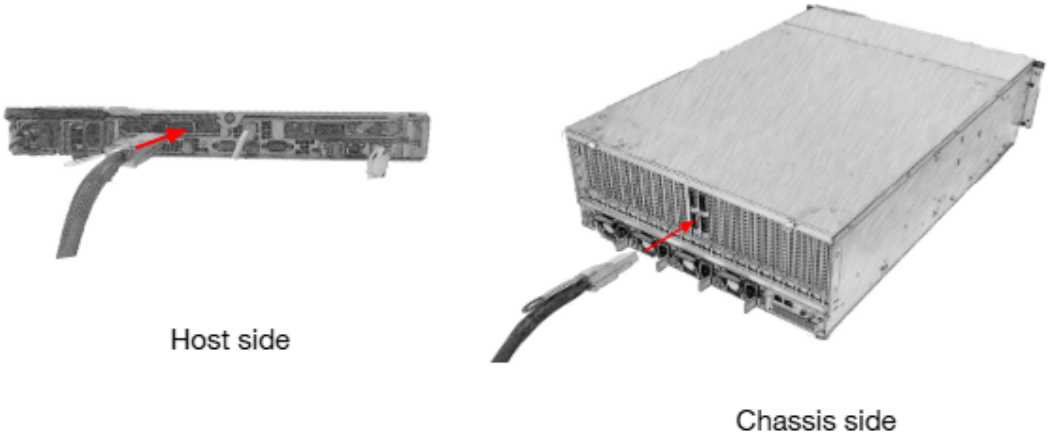


Figure 49. Host and Chassis Connections Using CDFP Cables

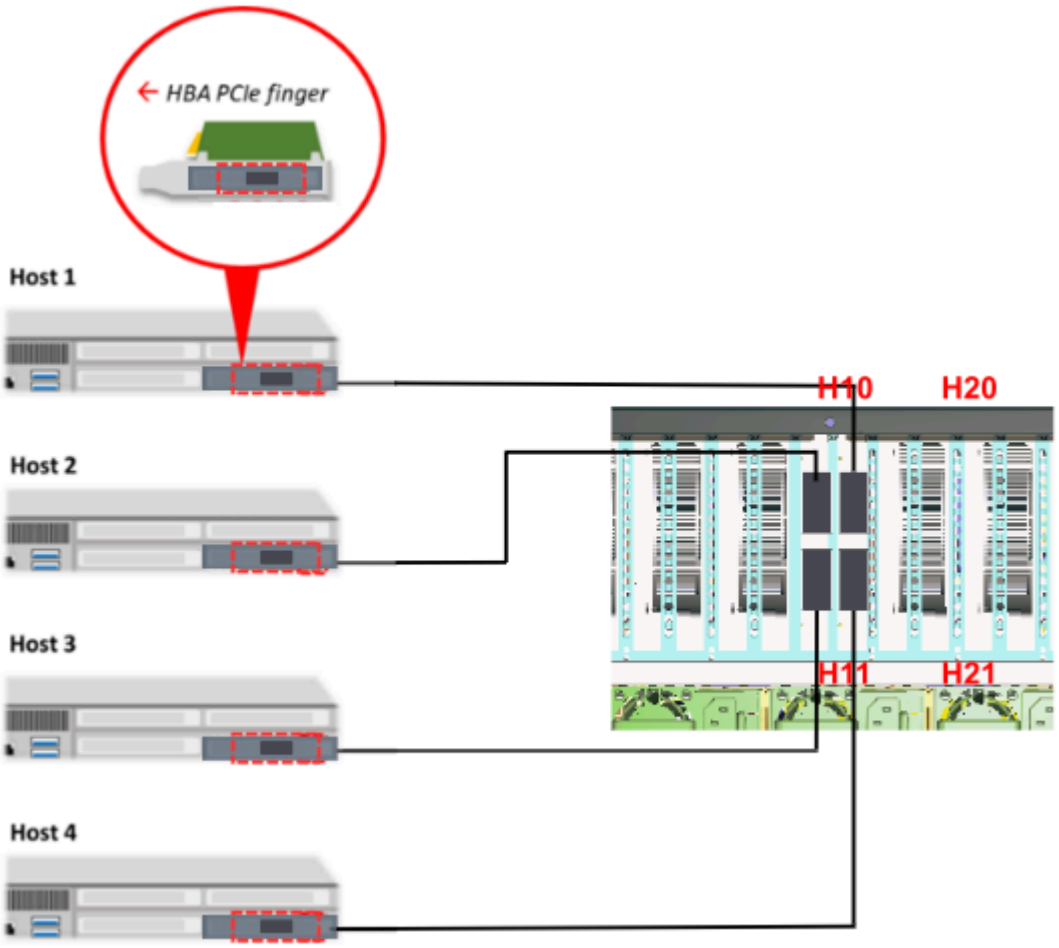


Figure 50. CDFP Cable Mapping Between Hosts and Chassis Ports

2.8 Verifying GPU Resource Assignment or Unassignment on the Host

This procedure outlines how to verify GPU assignment or unassignment on the host system, ensuring GPUs are correctly mapped, detected, and operational through server commands and GUI checks.

About this task

After assigning or unassigning GPU resources, the following verifications are necessary:

1. Ensure GPUs are properly mapped in the PCIe tree structure on the server.
2. Confirm the total number of GPUs matches the expected configuration.
3. Verify that the host GUI reflects the correct PCIe link capability and recognizes all assigned GPUs.

Procedures

Step 1. Verify PCIe Tree Structure on the Server

A. On the server, open a terminal and run the following command lspci -vt:

```
None

lspci -vt
```

B. Review the output to confirm GPU assignments.

Step 2. Verify Total GPUs on the Server

A. Run the following command nvidia-smi to check the total number of NVIDIA GPUs on the server:

```
None

nvidia-smi
```

B. Verify that the total GPU count matches the expected number.

Step3. Verify GPU Status on the Host via GUI

A. Access the system's Web GUI and navigate to the Resource Management panel.

B. Confirm the following:

- Link Capability: Ensure PCIe links are displayed with the correct specifications (e.g., Gen4x16 or Gen5x16).
- Device(s): Verify the assigned GPUs are listed and operational. For example, if the Device(s) field displays "4," it indicates that four GPUs are correctly assigned and connected.

Results

When the procedure is successfully completed:

- The server recognizes the assigned GPUs in the PCIe tree and displays the correct count.
- The host GUI confirms accurate PCIe link capability and GPU assignments.

If any discrepancies are identified, contact technical support for further diagnostics and solutions.

2.9 Updating Firmware

This procedure provides instructions for updating the firmware on Falcon 5012 using the GUI. The system automatically detects the type of firmware being updated, such as BMC or PCIe switch firmware. Ensure all host machines are disconnected before proceeding.

About this Task

To update the firmware, you will:

1. Download the appropriate firmware file from the support team.
2. Access the Falcon 5012 GUI and navigate to the Maintenance section.
3. Upload the firmware file and initiate the update process.
4. Reboot the system to complete the update.

Tools and Materials

You will need:

- A PC with access to the Falcon 5012 GUI.
- The firmware file (.img format) provided by support@h3platform.com.

Procedures

Step 1. Obtain the Firmware File

A. Download the Firmware:
   - Access the H3 Platform support page:
     - Navigate to Support → Knowledge Base → Download on the H3 Platform website.
     - Alternatively, visit the following URL directly: https://www.h3platform.com/knowledge-base/document.
   - Select the appropriate options:
     - Product Type: Composable GPU Chassis.
     - Model Type: Falcon 5012.
   - Download the following firmware files:
     - PCIe Switch 1 Firmware (SwitchA)
     - PCIe Switch 2 Firmware (SwitchB)
     - System Management Firmware

B. Contact H3 Platform Support:
   - Email support@h3platform.com to request the latest firmware file.

Note: The system includes two PCIe switches, each requiring a separate firmware update. Ensure that the correct firmware is applied to each switch to maintain system stability and functionality.

- Switch 1 firmware is typically labeled as SwitchA and follows the naming convention:
  h3-pcifw-aicSwitchA_YYYYMMDDHHMM.fw.h3.signed
- Switch 2 firmware is labeled as SwitchB and follows the naming convention:
  h3-pcifw-aicSwitchB_YYYYMMDDHHMM.fw.h3.signed

Before proceeding with the update, verify the firmware file names to confirm they correspond to the correct switch. Applying incorrect firmware may result in system errors or unexpected behavior.

Step 2. Access the Maintenance Page

A. Log in to the Falcon 5012 GUI:
   - Enter the system's IP address in your web browser.
   - Log in using your credentials.

B. From the left navigation menu, click Maintenance to access the firmware update tools (refer to Figure 81).

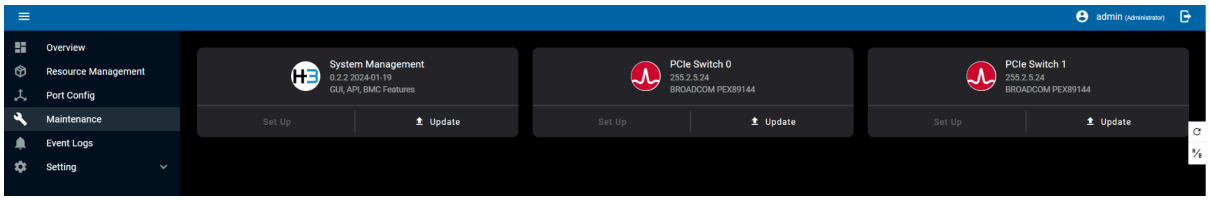


Figure 81. Firmware Update Tools on the Maintenance Page

Step 3. Upload the Firmware File

A. On the Maintenance page, click the Upload/Install button.

B. Select the system management firmware file (.img format) from your device and upload it (refer to Figure 82).

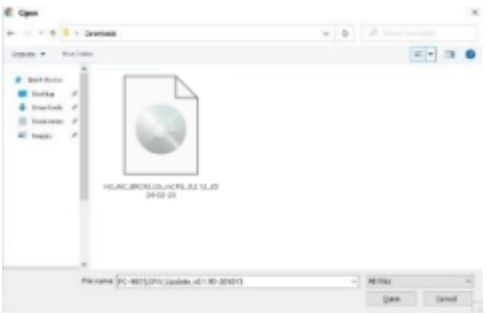


Figure 82. Selecting the Firmware File from the Download Location

C. A confirmation message will appear:
   - Verify the file name and file size of the firmware file you selected.

- Click Yes to proceed with the update (refer to Figure 83).

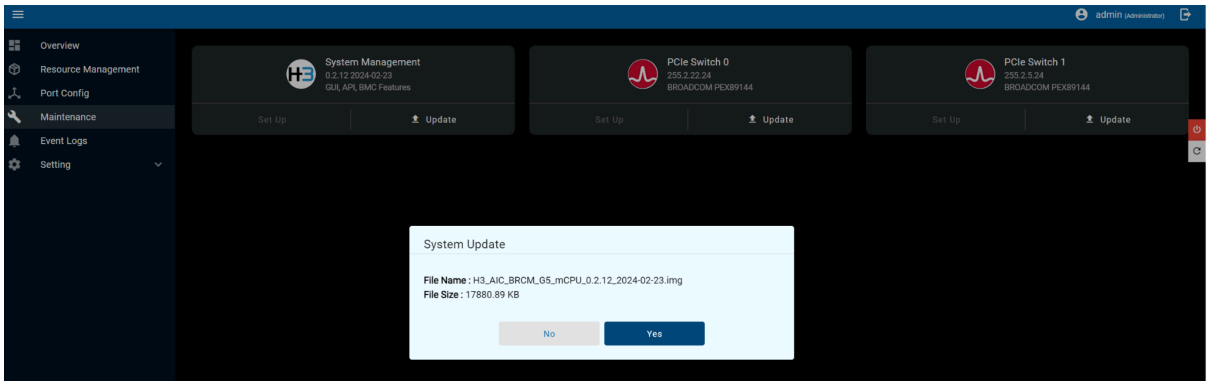


Figure 83. Confirmation Message for Firmware Update

Step 4. Firmware Update and System Reboot

A. Wait for the update to complete.
B. Before clicking Restart Now, ensure that all connected servers are powered off to proceed safely with the operation.
C. Once the update finishes, click Restart Now to reboot the system (refer to Figure 84).

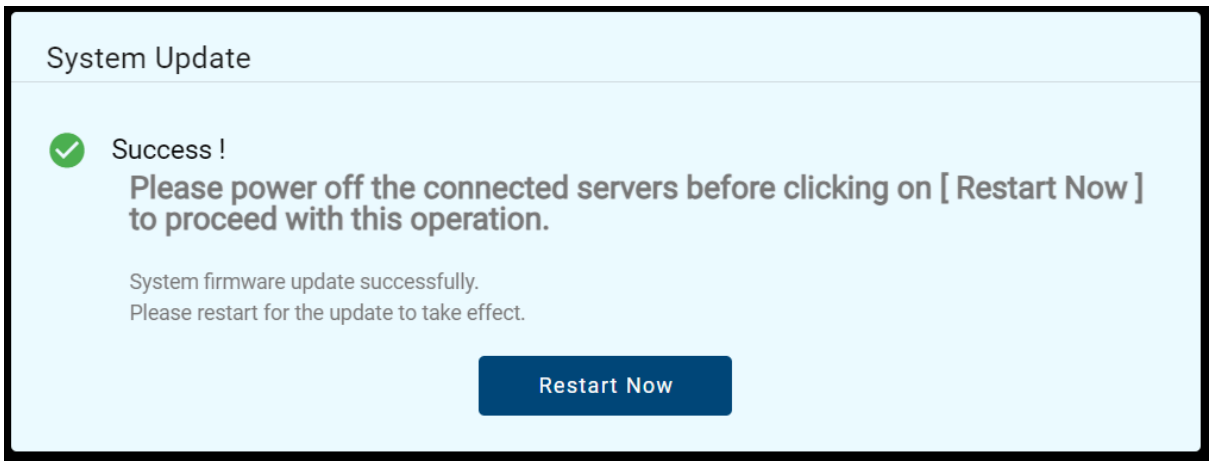


Figure 84. Firmware Update Success Prompt with Restart Now Option

---

Step 5. Post-Update Validation

A. After rebooting, the firmware update is complete.
B. If another user logs in or opens a new GUI session after the update, a reminder message will appear next to the Maintenance menu on every page (refer to Figure 85).

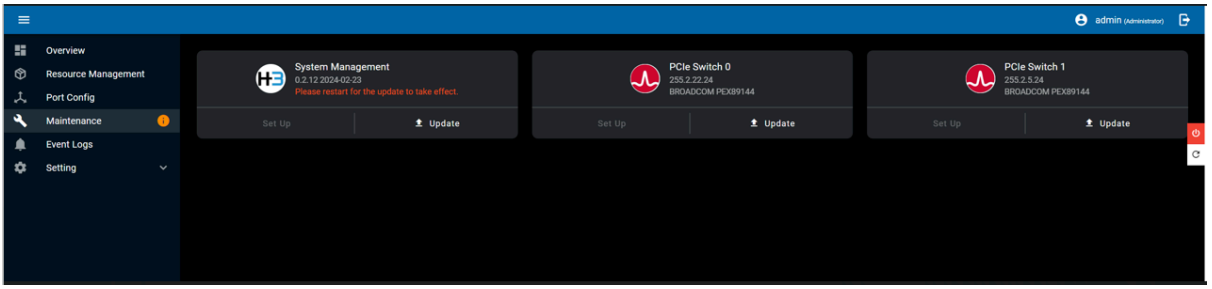


Figure 85. Post-Update Reminder Prompt in Maintenance Menu

C. To finalize the update, click the Restart button as prompted.

Notes:

- Ensure all host machines are disconnected during the update to prevent disruptions.
- If issues arise during the update, contact technical support at support@h3platform.com.

Chapter 3.

Common BMC Operations Guide

The Baseboard Management Controller (BMC) GUI provides a comprehensive interface for system monitoring, remote management, and firmware updates. This chapter outlines key procedures, including logging into the BMC, remotely controlling power states, and updating firmware components such as BMC, CPLD, and retimer firmware.

For detailed guidance on BMC operations, refer to The Falcon 5012 BMC User Manual available on the H3 Platform website:

- Navigate to Product → GPU Chassis → Falcon 5012 → Resource
- Alternatively, navigate to Support → Knowledge Base → Download on the H3 Platform website.
    - Alternatively, visit the following URL directly: https://www.h3platform.com/knowledge-base/document
- Select the appropriate options:
    - Product Type: Composable GPU Chassis.
    - Model Type: Falcon 5012.
- Download the latest BMC user manual.

By following the instructions in this chapter, users can ensure secure access, efficient power management, and proper firmware maintenance for optimal system performance.

3.1 BMC GUI Log-in

To access the BMC GUI, follow these steps:

1. Open a supported web browser.
2. Enter the BMC IP address in the URL bar. (Refer to the previous section 3.3 Retrieve GUI IP for System Boot-Up for instructions on retrieving the BMC IP address.)
3. When prompted, log in using the default login credentials (see Figure 99).

Default Login Credentials:

- **Username:** admin
- **Password:** 12345678

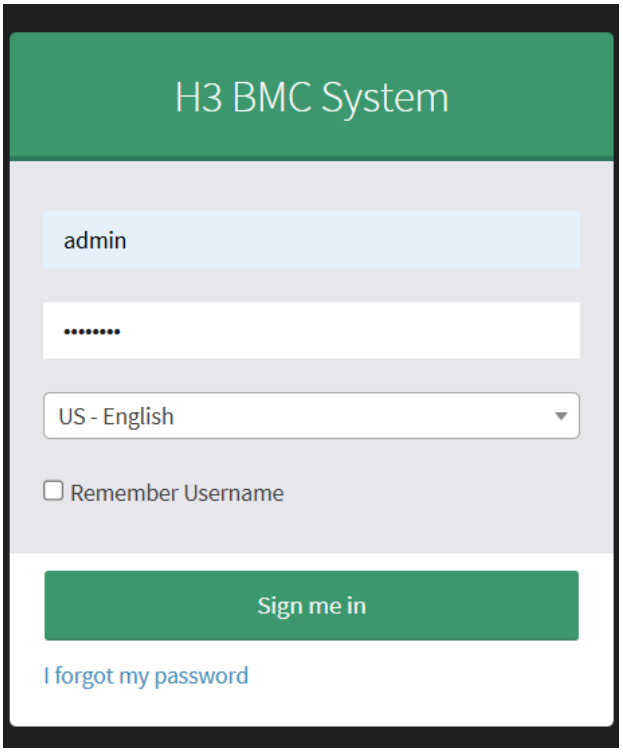


Figure 99. BMC System Log-in page

For security purposes, it is recommended to change the default password after the first login.

Note: If one password does not work, try the alternative password: admin.

3.2 Remote Powering On/Off Using BMC

This procedure provides instructions for using the BMC (Baseboard Management Controller) GUI to remotely manage the power states of the system. By accessing the Remote Control section and launching the H5Viewer, users can utilize the Power menu to execute actions such as resetting, shutting down, or powering on the server.

About this Task

To remotely manage the system's power state, you will:

1. Access the BMC GUI and navigate to the Remote Control section.
2. Launch the H5Viewer to open the KVM interface.
3. Use the Power menu to execute desired actions.

Procedures

Step 1. Navigate to Remote Control

A. After logging in, locate the Remote Control tab in the left navigation bar (refer to Figure 100).

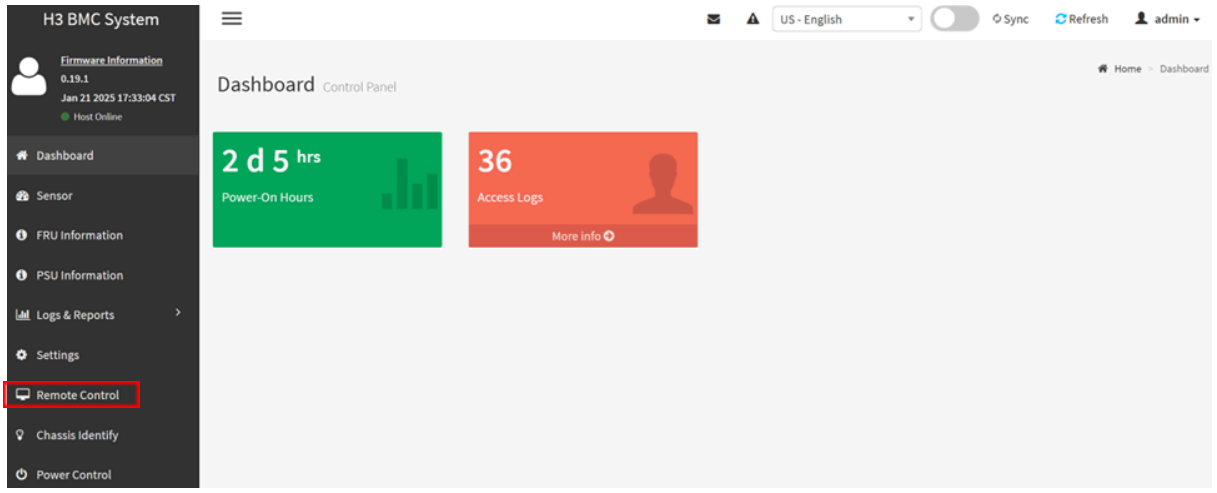


Figure 100. Locating the Remote Control Tab in the BMC GUI Navigation Bar

B. Click on Launch H5Viewer to access the KVM interface (refer to Figure 101).

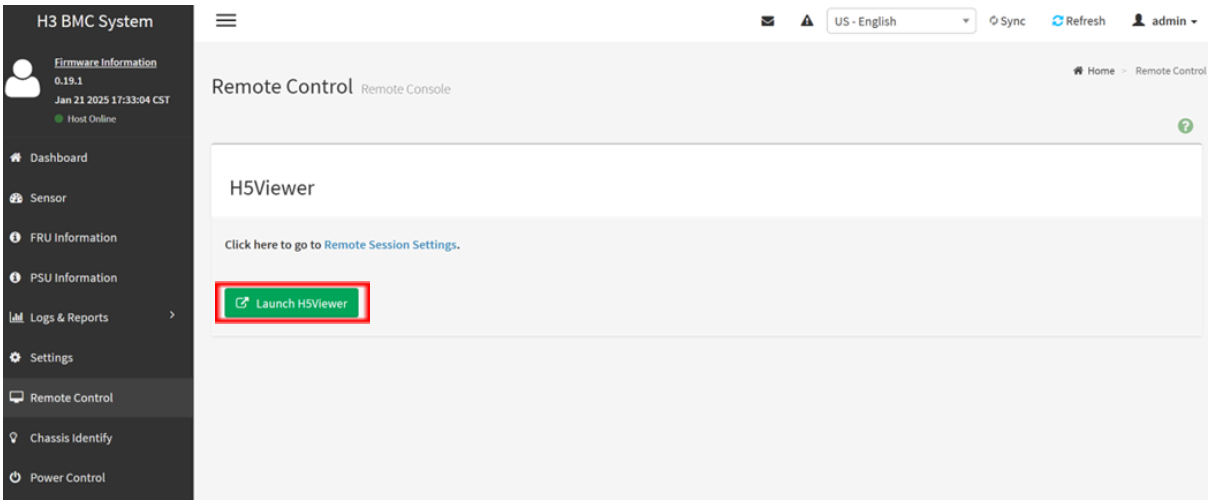


Figure 101. Launching H5Vi1ewer from the Remote Control Tab

Step 2. Use the Power Menu

A. In the KVM interface, locate the Power menu in the top navigation bar (refer to Figure 102).

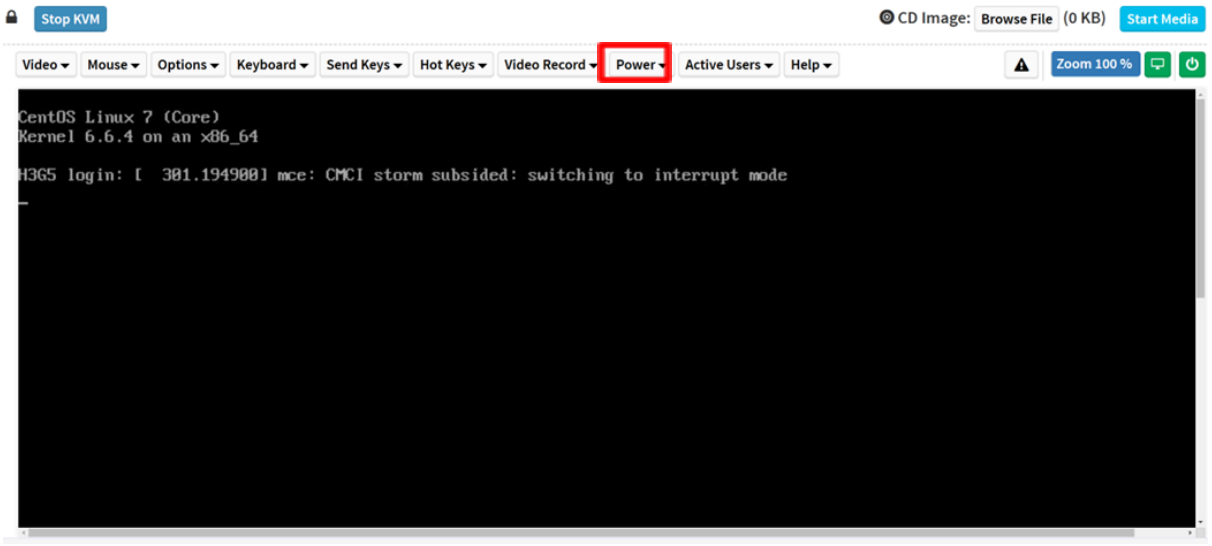


Figure 102. Locating the Power Menu in the KVM Interface Navigation Bar

B. From the Power menu (refer to Figure 103), select the desired action:

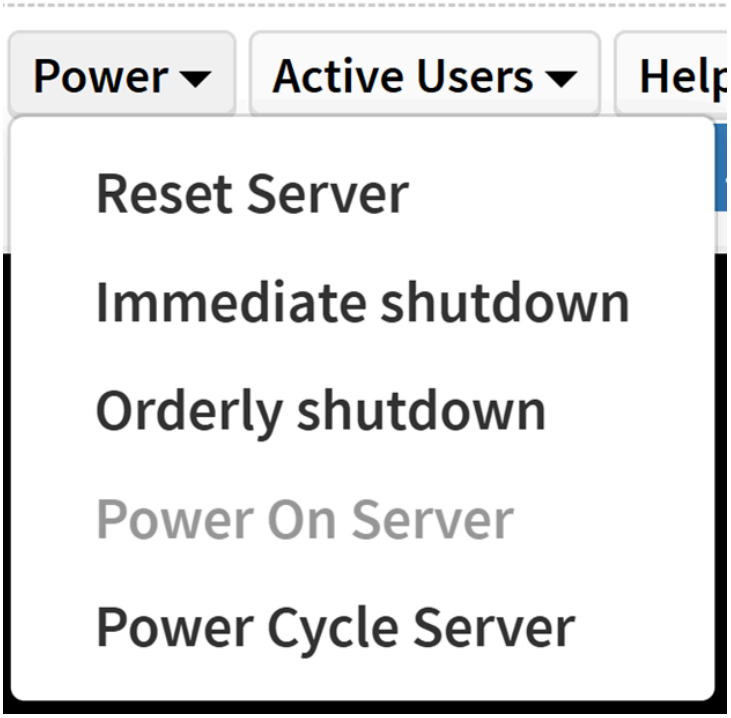


Figure 103. Power Menu Options in the KVM Interface

- Reset Server: Reboot the system.
- Immediate Shutdown: Instantly powers off the system.
- Orderly Shutdown: Initiates a graceful system shutdown.
- Power On Server: Turns the server on remotely.
- Power Cycle Server: Restarts the system by cutting and restoring power.

C. Confirm your selection to execute the chosen power action.

Results

- The selected power action is executed successfully.
- The system reflects the updated power state.

Notes

- Ensure proper network connectivity between the BMC and your management machine.
- Use Immediate Shutdown only when necessary, as it may not allow the system to save its state.
- For routine operations, prefer Orderly Shutdown for a graceful power-off process.

3.3 Updating BMC Firmware

The BMC firmware update is an essential maintenance task designed to ensure optimal system performance, enhanced security, and the availability of new features for the Falcon 5012 GPU chassis. This process involves updating the Baseboard Management Controller (BMC), which serves as the core for system management functions such as hardware monitoring and remote administration.

Users are advised to refer to the Falcon 5012 BMC User Manual for a comprehensive step-by-step guide. The manual provides detailed instructions on firmware preparation, upload, validation, and finalization procedures. Follow these guidelines to ensure a successful update and to minimize system downtime.

About the Task

The BMC firmware update requires the following key considerations:

- Purpose: To enhance system functionality by addressing known firmware issues, improving compatibility, and incorporating the latest security patches.
- Preconditions: Ensure the system is stable, critical data is backed up, and all necessary update files are available.
- Key Steps:
    1. Access the Falcon 5012 BMC interface via a secure connection.
    2. Upload the firmware package, which must be obtained from a verified source.
    3. Follow the firmware validation and installation instructions provided in the manual.
    4. Restart and verify the BMC firmware version after the update process is complete.

Reference Guide

For a detailed walkthrough of the BMC firmware update process, refer to the Falcon 5012 BMC User Manual:

- Path:
  Navigate to the H3 Platform website using the following steps:
  Product → GPU Chassis → Falcon 5012 → Resource → Falcon 5012 → BMC User Manual.

- Direct URL: https://drive.google.com/file/d/1y47HJo2CnhJFhwqODxwvuWUHyaiDresN/view

Ensure to follow the safety and preparatory instructions outlined in the manual. For additional assistance, contact H3 Platform Support at support@h3platform.com.

3.4 Updating CPLD Firmware Using BMC

This procedure provides step-by-step instructions to update the CPLD Firmware using the BMC interface. The process includes selecting the firmware file, initiating the update, and completing an AC power cycle.

About this Task

To update the CPLD firmware, you will:

1. Access the CPLD Firmware Utility from the Maintenance section of the BMC GUI.
2. Select the appropriate CPLD firmware file for the update.
3. Execute the firmware update and complete the process with a power cycle.

Tools and Materials

You will need:

- The CPLD firmware file (.jed format) stored on your computer.
- Network access to the BMC.
- Supported web browser (e.g., Firefox or Chrome).

Procedures

Step 1. Access CPLD Firmware Utility

A. Open a supported browser and enter the BMC IP address in the URL bar.
B. Log in to the BMC GUI using your credentials:
    - Default Username: admin
    - Default Password: 12345678

Note: If one password does not work, try the alternative password provided.

C. From the navigation bar on the left, select Maintenance (refer to Figure 104).

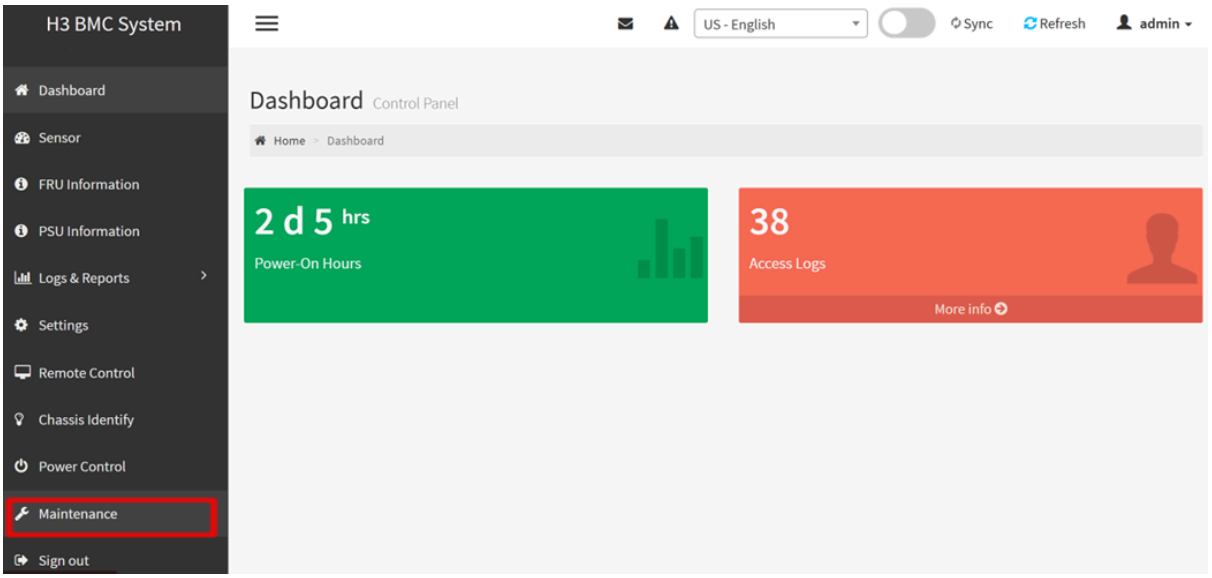


Figure 104. Navigating to the **Maintenance** section.

Step 2. Select the CPLD Firmware Utility

A. Under the Maintenance section, click on CPLD Firmware Utility (refer to Figure 105).

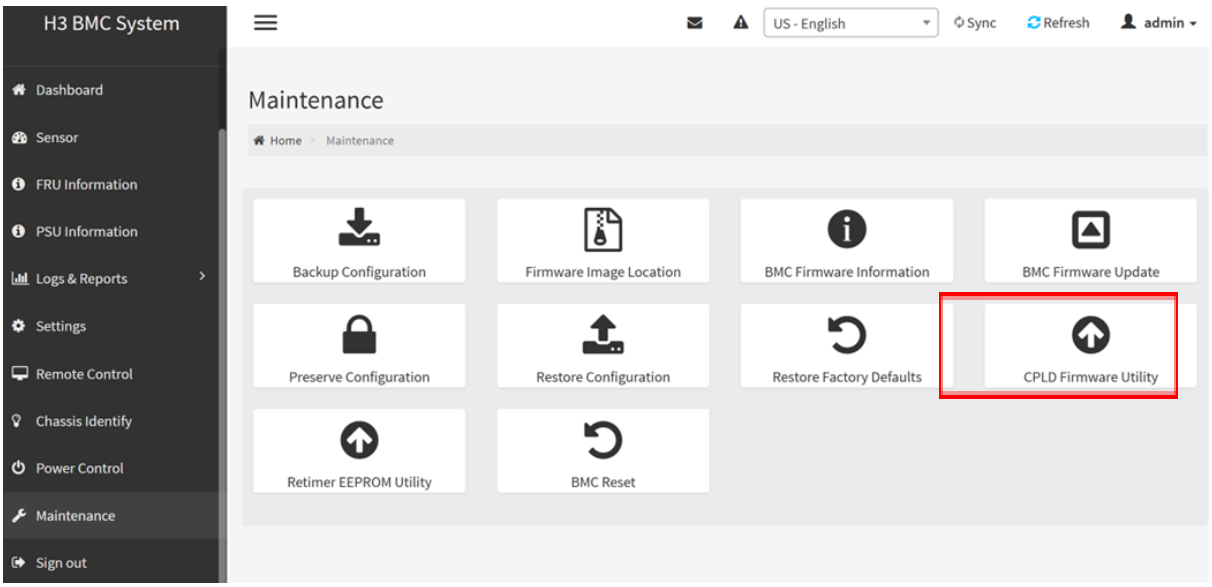


Figure 105. Accessing the CPLD Firmware Utility page.

B. On the CPLD Firmware Utility page, review the current CPLD IDs, Bus, and Firmware Version.

Step 3. Perform a Remote System Shutdown Using BMC

A. Refer to the Remote Power On/Off Using BMC section for detailed instructions.
B. Access the Power Control option under the Remote Control section in the BMC interface.
C. Select Immediate Shut Down to safely shut down the system remotely.
D. The screen will suddenly black out, indicating that the system has successfully powered off.

Step 4. Update CPLD Firmware

A. Click the Select CPLD firmware file button and upload the firmware file (.jed format) from your computer.
B. Click the Start Update button to initiate the update process (refer to Figure 106)

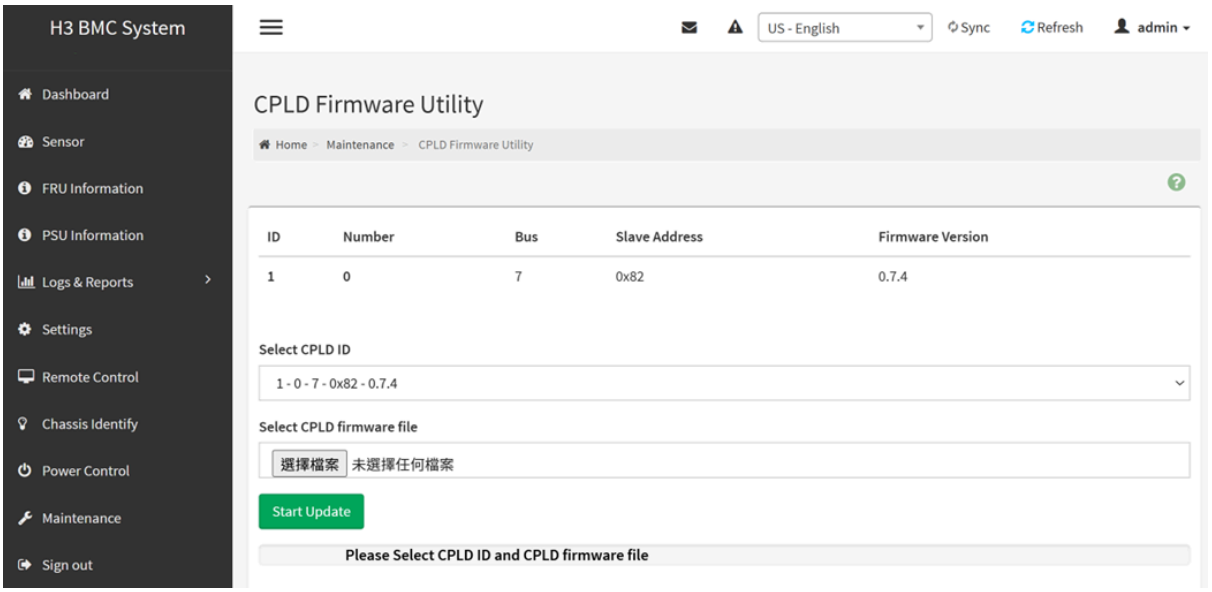


Figure 106. Selecting and starting the CPLD Firmware update.

C. During the update, a Processing message will appear, indicating the progress percentage (refer to Figure 107).

Figure 107. Processing During CPLD Firmware Update

Step 5. Confirm Update Completion

A. After the update, a notification will appear: Update Completed (Please unplug and replug the power cable) (refer to Figure 108).

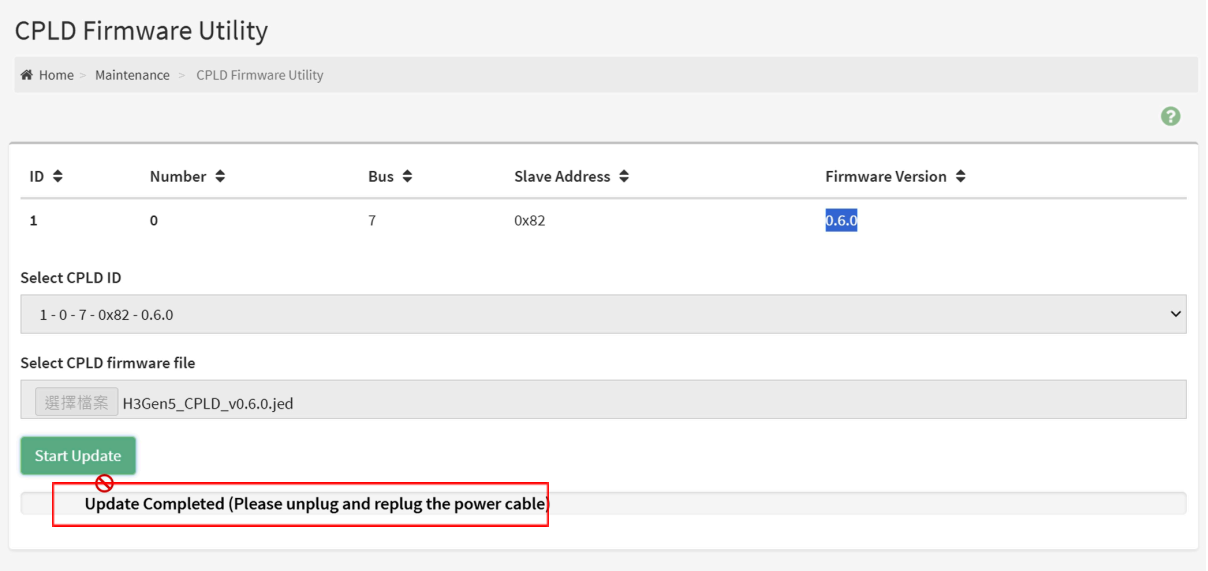


Figure 108. Firmware update completion notification.

B. Disconnect the power cable to perform an AC power cycle.
C. Access the BMC interface to verify whether the CPLD version has been successfully updated.

Notes

- Ensure the correct CPLD firmware file is selected to avoid compatibility issues.
- Performing the AC power cycle is mandatory for the firmware update to take effect.

3.5 Updating Host Adapter (Retimer) Firmware

This section provides instructions for updating the firmware on the Host Adapter (Retimer) installed in Falcon 5012 that supports PCIe expansion. The update procedure uses the BMC Retimer EEPROM Utility. Host Adapter (Retimer) modules C01 and D01 are supported.

About this task

This procedure describes how to update the firmware on the Host Adapter (Retimer) using the BMC Retimer EEPROM Utility. This utility provides an interface to upload firmware images, select individual Host Adapter (Retimer), and perform controlled updates. Follow all instructions precisely to avoid incorrect flashing.

To update the firmware:

- Identify the Host Adapter (Retimer) module type.
- Power on the system and log in to the BMC Web Interface.
- Download the correct firmware version from the H3 Platform website.
- Use the Retimer EEPROM Utility to upload and apply the firmware image.
- Verify the version after a full power cycle.

Procedures

Step 1. Preparing for Host Adapter (Retimer) Firmware Update

A. Power off the server system.
B. Host adapters must be installed into Falcon 5012 on the Slots 12~15, and 21~24 (except the Slots 11 and 25) to perform firmware updates.

- C01 DIP switch settings must be configured as follows (see Figure 109):
  -
  - SW1: ON (Right)
  - SW2: HLL (Right, Left, Left)

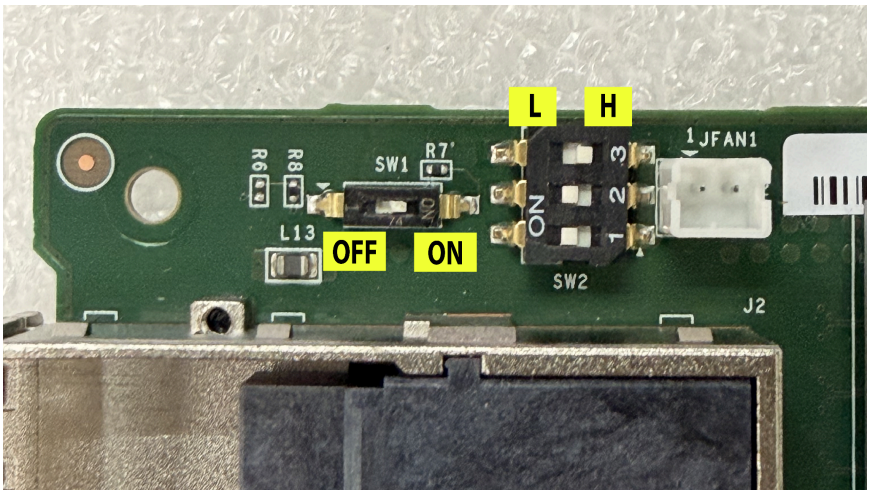


Figure 109. Host Adapter (C01) DIP Switch Settings for Firmware Update at Falcon side

- D01 DIP switch settings must be configured as follows(see Figure 110):
  -
  - SW1: ON, ON, ON (Left, Left, Left)
  - SW: HLH (Right, Left, Right)

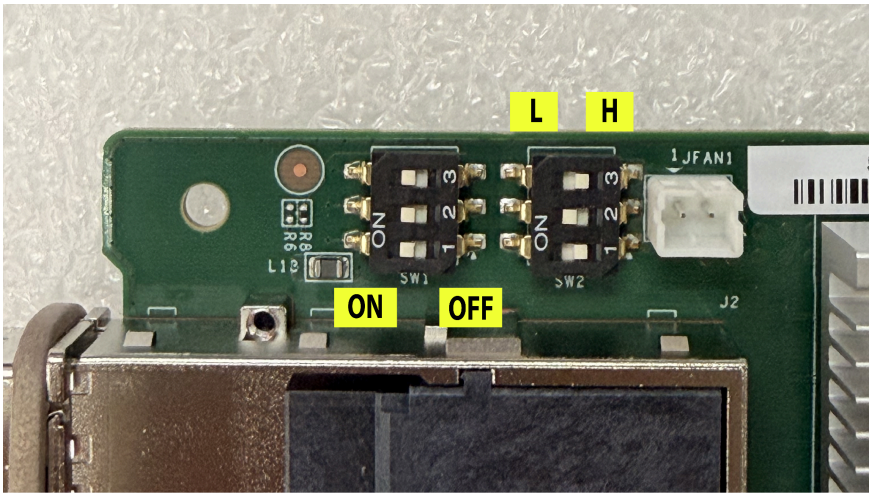


Figure 110. Host Adapter (D01) DIP Switch Settings for Firmware Update at Falcon side

---

Step 2. Accessing the BMC Interface

A. Power on the system.
B. Log in to the BMC Web Interface.
C. Navigate to the Maintenance tab (see Figure 111).

D. Select the Retimer EEPROM Utility option (see Figure 112).

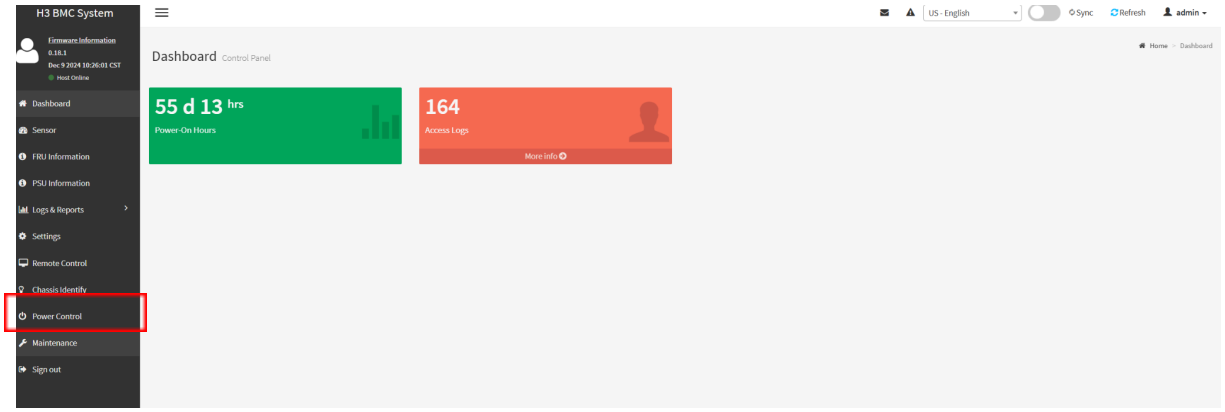


Figure 111. Navigating to the **Maintenance** section.

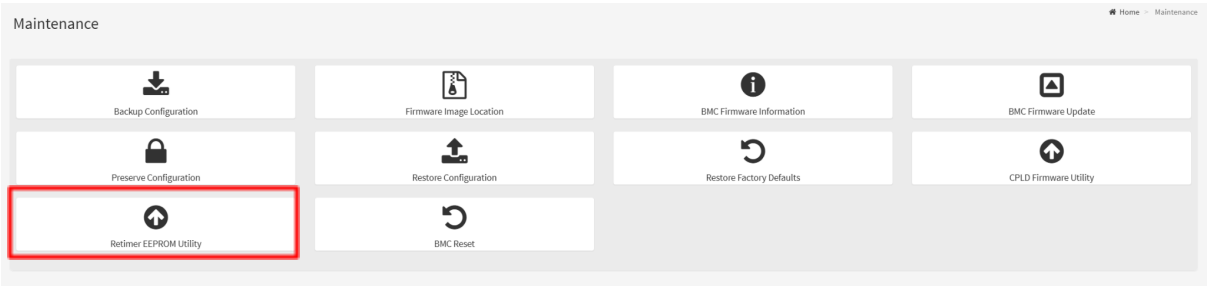


Figure 112. Navigating to the Retimer EEPROM Utility section.

Step 3. Downloading the Host Adapter (Retimer) Firmware File

A. Go to the H3 Platform support site: https://www.h3platform.com/knowledge-base/document
B. Navigate to: **Support → Knowledge Base → Download.**
C. Select:
    - **Product Type:** Composable GPU Chassis
    - **Model Type:** Falcon 5012

D. Download the latest Host Adapter (Retimer) firmware file.

Step 4. Performing the Update

The Retimer EEPROM Utility lists all Host Adapter (Retimer) modules detected in the system (see Figure 113). Displayed details include:

- Slot ID: Logical ID mapped to the physical chassis or host slot.

- Link Width: PCIe channel configuration (e.g., x1, x4).
- Bus Address / Device ID: Indicates I2C control interface.
- EEPROM Version: Displays current firmware revision.

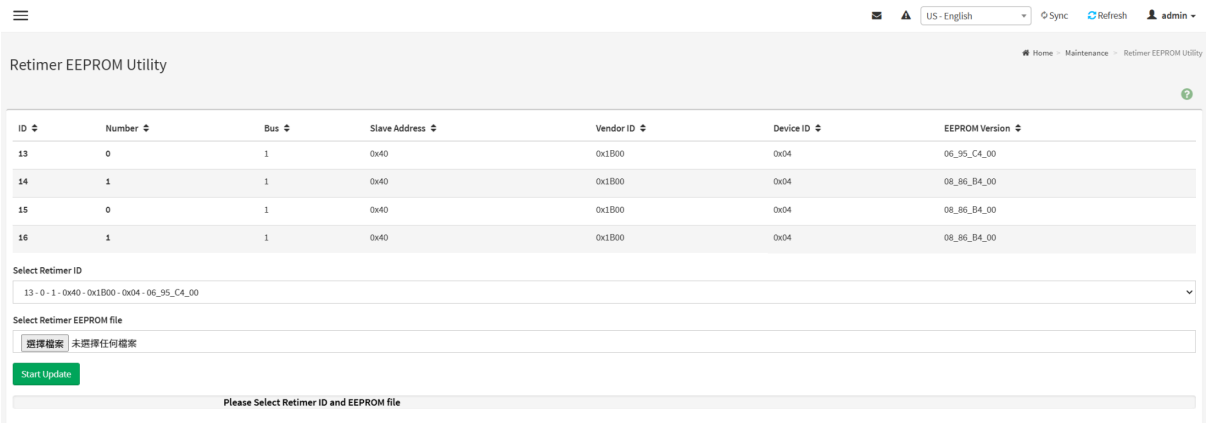
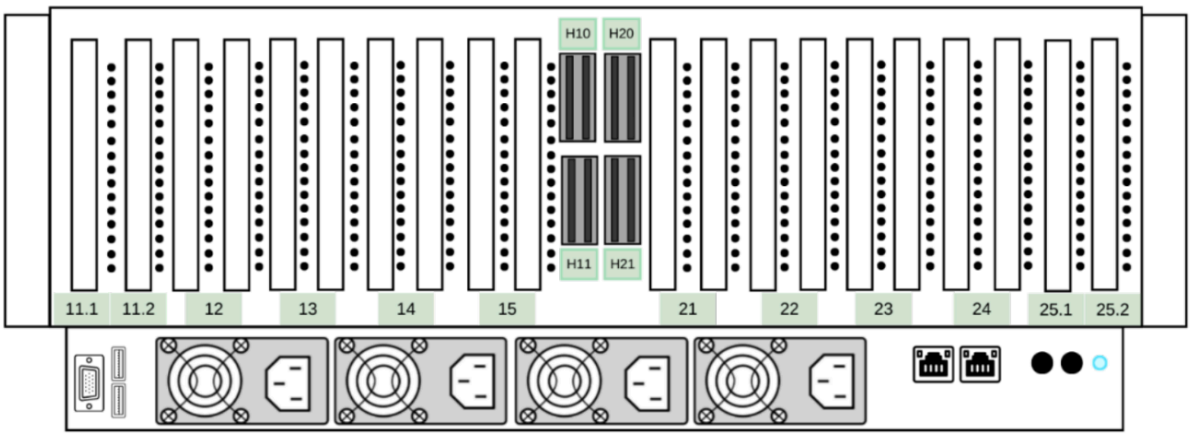


Figure 113**.** Retimer EEPROM Utility Interface

The table in Figure 114 is a reference for host ports and slot IDs . Please use the Slots 12~15, and 21~24 (except the Slots 11 and 25).



Slot	ID
H11	13
H10	14
H21	15
H20	16

Figure 114. Physical slot to Slot ID mapping for chassis modules

To begin the update:

1. Select the correct Slot ID. Verify it corresponds to the installed Host Adapter (Retimer) to prevent misflashing.
2. Click Select Retimer EEPROM File and choose the firmware file.
3. Click Start Update.
4. Monitor the status via the progress bar (see Figure 115).

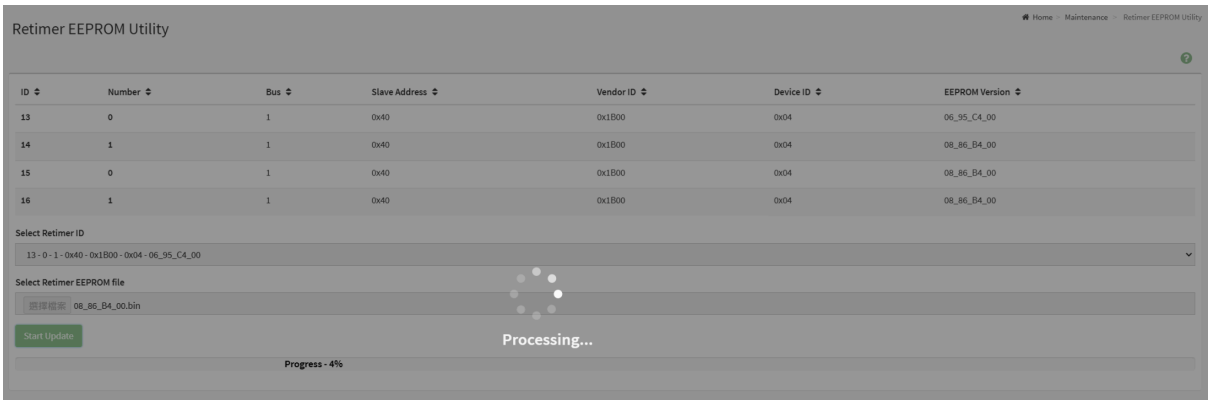


Figure 115. Firmware update progress status

Step 5. Verifying the Update

A. The firmware version may not immediately appear in the EEPROM Utility after update.
B. Perform a full power cycle by unplugging and reconnecting the system's power cord.
C. Reconnect to the BMC Web Interface to verify the updated version.
D. If the updated version is still not shown, contact H3 Technical Support for assistance.

The Falcon 5012 installation and initial set-up are completed. Please see the Falcon 5012 User Manual for more operation details.

Warranty

H3 Platform offers free 2-year limited warranty service on our products. If the standard warranty period is not enough, H3 Platform offers optional purchase extended warranty service coverage that will provide warranty for 1, 2, or 3 additional years.

Limited Warranty

H3 Platform warrants its products against defects in material and workmanship. Under normal use and service, every hardware portion of the products will be free from physical defects in material and workmanship during the warranty period, or the product will be repaired or replaced as determined solely by H3 Platform. H3 Platform provides a limited warranty for its products only to the person or entity that originally purchased the product from H3 Platform or its authorized distributor or retailer. H3 Platform's products are PCI switches, and H3 Platform makes no warranty of the devices installed, or warranty on compatibility of all PCIe devices. H3 Platform will not be liable in any way for the loss of data stored on H3 Platform products and any damage caused by this.

Extra warranty period might be provided by H3 Platform's worldwide dealers/distributors. Please contact dealers/ distributors to purchase the extended warranty.

If a product does not operate as warranted above during the applicable warranty period, H3 Platform shall, at its option and expense (except for shipping cost), repair the defective product or part, deliver to the customer an equivalent product or part to replace the defective item. All products that are replaced will become the property of H3 Platform. Replacement products may be new or reconditioned.

Warranty does not apply, if:

1. The warranty period is expired,
2. The warranty label is broken or removed,
3. The serial number label is missing or unrecognizable,
4. The product has been modified or repaired by any unauthorized service center or personnel.
5. The defect was subject to abuse, improper use not conforming to product manual instructions, or environment conditions more severe

than those specified in the manual and specification.

6. The defect was subject to Force Majeure, such as acts of God, flood, lighting, earthquake, war, vandalism, theft, brownouts or sags (damage due to low voltage disturbances)
7. Consumables, such as batteries
8. Routine cleaning, or normal cosmetic and mechanical wear
9. Damage caused by misuse, abuse, or neglect
10. Damage caused by parts that were not manufactured or sold by H3 Platform
11. Damage caused by installing devices not on the compatible list
12. Damage caused when warranted parts were repaired or replaced by an organization other than H3 Platform or by a service provider not authorized by H3 Platform.

If the customer's product is not covered under warranty, H3 Platform may offer Repair Services under the customer's payment.

Software Limited Warranty

Except as provided in the applicable software end-user license or program license agreement, including any software products or the operating system preinstalled by H3 Platform are provided “as is” and with all faults, and H3 Platform hereby disclaims all other warranties and conditions, either express, implied, or statutory, including, but not limited to, warranties of title and non- infringement, any implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, and of lack of viruses. Some states/jurisdictions do not allow exclusion of implied warranties or limitations on the duration of implied warranties, so the above disclaimer may not apply to you in its entirety. To the maximum extent permitted by applicable law, in no event shall H3 Platform or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy arising out of or in any way related to the use of or inability to use the software product, even if H3 Platform or any supplier has been advised of the possibility of such damages and even if the remedy fails of its essential purpose. H3 Platform is not responsible for any interoperability or compatibility issues. Some states/jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

H3 Platform warrants all pre-installed H3 Platform software will execute its programming instructions when all files are properly installed. H3 Platform does not warrant that the software will be uninterrupted or error free. In the event H3 Platform software fails to execute its programming instructions during the warranty period, the customer's remedy will be either (1) replacement of the H3 Platform software or (2) a refund upon return of the product and all copies of software as well as installation instructions.

Compatibility

We have tested and verified the compatibility of third-party products and peripherals on the H3 Platform Compatibility List. Please note that the tests conducted in H3 Platform labs may not have covered every aspect and that changes to firmware or hardware may affect device compatibility and stability. H3 Platform does not guarantee the compatibility with third-party products and peripherals on the List and reserves the right to update the List at any time without prior notice.

Repair Service

Warranty and out of warranty service should be obtained by contacting the system integrator/dealer/retailer/e-retailer or distributor where the customer purchased the product. When requesting for service, the proof of purchase and the product serial number must be provided. The return of the defective product should be strictly through the original route of purchase, and the customers shall pack the product appropriately to prevent the returned product from suffering in the transportation.

There are no user serviceable parts inside the product. Do not allow any unauthorized service center or personnel to repair or modify the product. If the original channel is no longer in business or unavailable, the customer may contact H3 Platform Technical Support for international RMA services. In this case, the customer will be charged for handling fee, $50 (USD), and all fees incurred, including two ways freight, duties, taxes and brokerage fee.

It is customer's sole responsibility to back up his/ her data. Before allowing any service from H3 Platform or its service provider, including remote login check and repairing service, the customer must back up the data and remove any of the customer's confidential, proprietary or personal information. Neither H3 Platform nor its service provider will be liable for any damage, loss and exposure of confidential or private information or data contained in any product, hardware, software or media.

Notice of Warranty Claims

All warranty claims must be made during the applicable warranty period. Any claim made after that time will not be eligible for warranty service but may be serviced under a separate H3 Platform support contract covering the product.

DISCLAIMER OF WARRANTY

H3 Platform does not warrant uninterrupted or error-free operation of an H3 Platform product. If the customer transfers an H3 Platform product to another user, warranty service is NOT available to that user for the remainder of the warranty period.
Consumables, such as batteries and PCIe power cables have no warranty. The above warranties will not apply to products from which serial numbers have been removed or to defects resulting from misuse (including operation of a H3 Platform product without covers and incorrect input voltage), unauthorized modification, operation or storage outside the environmental specifications for the product, in-transit damage, improper maintenance, or defects resulting from use of third-party software, accessories, media, supplies, consumables, or such items not designed for use with the product. The H3 Platform Software Product Limited Warranty does not apply to software used with products not covered by any of the H3 Platform limited warranties offered as part of your purchase of an H3 Platform product.

TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND H3 PLATFORM SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

Some Countries, states or provinces do not allow limitations on the duration of an implied warranty, so the above limitation or exclusion might not apply to you. The warranty gives you specific legal rights and you might also have other rights that vary from country to country, state to state or province to province.

Limitation of liability and Remedies.

In no event will H3 Platform or its affiliates, subcontractors, or suppliers be liable for any of the following:

1. Damages for loss of data, or software restoration;

2. Damages relating to Customer's procurement of substitute products or services (i.e., "cost of cover");
3. Incidental, special, or consequential damages (including lost profits, loss of use, Customer downtime, cost of data recovery/re-creation), even if H3 Platform is informed of their possibility;
4. Third-party claims against Customer for losses or damages.
5. H3 Platform PCIe Switches are not specifically designed, manufactured or intended for sale as parts, components or assemblies for the planning, construction, maintenance, or direct operation of a nuclear facility. Customer is solely liable if Products or Support purchased by Customer are used for these applications.

TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL H3 PLATFORM OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE.

Some countries, states or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

THE WARRANTY TERMS CONTAINED HERE, EXCEPT TO THE EXTENT LAWFULLY PERMITTED, DO NOT EXCLUDE, RESTRICT OR MODIFY AND ARE IN ADDITION TO THE MANDATORY STATUTORY RIGHTS APPLICABLE TO THE SALE OF THIS PRODUCT TO YOU.