

GIGABYTE™

W775-V10

BMC User Guide

Insyde Web GUI Interface for Firmware Version 23.08.xx

User Manual

Rev. 1.0

Copyright

© 2026 Giga Computing Technology CO., LTD., All rights reserved.

The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of Giga Computing.

Changes to the specifications and features in this manual may be made by Giga Computing without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without Giga Computing's prior written permission.

Documentation Classifications

In order to assist in the use of this product, Giga Computing provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use of this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents.

For More Information

For related product specifications, the latest firmware and software, and other information please visit our website at <http://www.gigabyte.com/Enterprise>

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email: marketing@giga-computing.com

For Playbooks - <https://build.nvidia.com/station>

For DGX Station Development Guide - <https://docs.nvidia.com/dgx/dgx-station-development-guide/>

Table of Contents

Chapter 1	Getting Started.....	6
1-1	Software Requirement	6
1-2	Gigabyte Management Console Network Configuration	6
1-3	Log In Gigabyte Management Console.....	7
1-3-1	Required Browser Settings:	7
1-4	Quick Button and Logged-in User	7
1-5	Menu Bar.....	9
Chapter 2	Enter Gigabyte Management Console.....	11
2-1	Overview	11
2-2	Dashboard.....	12
2-3	Logs	15
2-3-1	System Event Log.....	15
2-3-2	Post code.....	16
2-3-3	SOL Log.....	17
2-3-4	BIOS Log	18
2-3-5	Host Video Recorder	19
2-3-6	System diagnostics.....	20
2-4	Hardware status	20
2-4-1	System Information.....	21
2-4-2	FRU Information	21
2-4-3	CPU Information	22
2-4-4	DDR Information.....	23
2-4-5	Inventory and LEDs	23
2-4-6	Sensors Readings	24
2-4-7	NIC Information (BIOS).....	25
2-4-8	NVMe/HDD Information (BIOS)	25
2-4-9	System Components	26
2-4-10	SMBIOS.....	27
2-5	Operations.....	28
2-5-1	Factory Reset	28
2-5-2	KVM	29
2-5-3	Firmware.....	38
2-5-4	Reboot BMC	39
2-5-5	SOL Console	39
2-5-6	Server power operations.....	40
2-5-7	Virtual front panel.....	41

2-5-8	Virtual Media	42
2-5-9	Boot Config	44
2-6	Settings	45
2-6-1	Alert	45
2-6-2	Alert policies	57
2-6-3	Alert Email	58
2-6-4	Date and Time	60
2-6-5	Networks	61
2-6-6	VLAN	64
2-6-7	SOL	65
2-6-8	SNMP	67
2-6-9	iKVM and virtual media	68
2-6-10	Dynamic DNS	69
2-6-11	Syslog settings	70
2-6-12	Backup restore	72
2-6-13	Power restore policy	73
2-7	Security and access	74
2-7-1	Current users	74
2-7-2	LDAP	74
2-7-3	RADIUS	85
2-7-4	TACACS+	86
2-7-5	Users	86
2-7-6	Policies	88
2-7-7	Certificate management	89
2-7-8	Kerberos authentication	90
2-7-9	Security settings	91
2-7-10	IP access control	93
2-8	Resource Management	96
2-8-1	Power	96
2-8-2	Power Statistics	96
2-8-3	Power Schedule	97
2-9	BIOS (Insyde BIOS joint feature)	98
2-9-1	Main	98
2-9-2	Advanced	98
2-9-3	Boot	100
3-1	Appendix A - Assertion Condition (BIT EVENT) References	101
3-1-1	Sensor type: Temperature, Voltage, Current, Fan	101
3-1-2	Sensor type: Physical Security	101
3-1-3	Sensor type: Processor	101
3-1-4	Sensor type: Power supply	102
3-1-5	Sensor type: Other Units-based Sensor	102

3-1-6	Sensor type: Memory.....	102
3-1-7	Sensor type: Event Logging Disabled.....	102
3-1-8	Sensor type:Critical Interupt	103

Chapter 1 Getting Started

1-1 Software Requirement

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in video/keyboard/mouse functionality.

Supported Browsers

- Chrome latest version.
- Edgelatest version
- Firefox (with limited support).



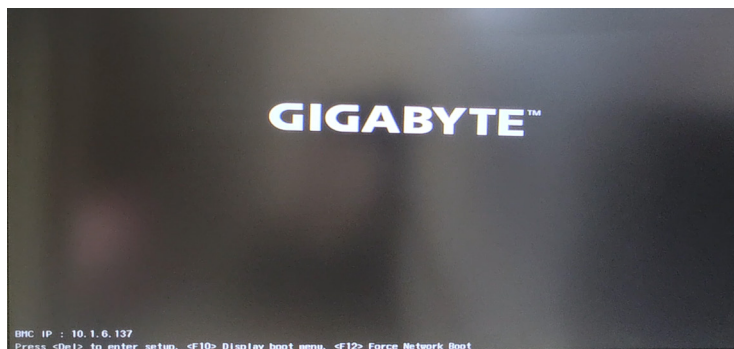
Note: It is advisable to use Chrome or IE for H5Viewer since Firefox has its own memory limitations.

1-2 Gigabyte Management Console Network Configuration

Follow the instruction to enable the console redirection function.

Option 1: Gather the IP

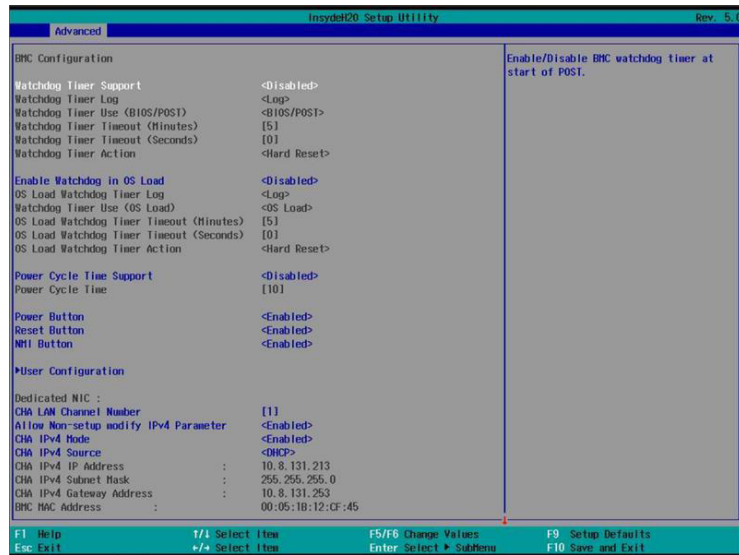
The BMC IP address is displayed in the lower-left corner during POST.



Option 2: View the IP Address via BIOS Setup Menu

If the screen flashes too quickly or uses a static fallback, you can alternatively find the address through the BIOS configuration:

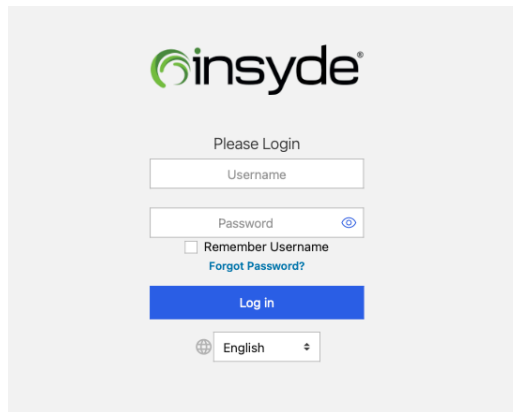
1. Go to the BIOS setup menu.
2. Navigate to: Select Setup Utility → Advanced → H2O IPMI Configuration → BMC Configuration.
3. The BMC IP Address will appear on the CHA IPv4 IP address parameter.



4. Save the configuration and exit BIOS setup menu.

1-3 Log In Gigabyte Management Console

To access the Gigabyte Management Console, the Insyde utility will prompt you to enter the User Name and Password.



The fields are explained as follows:

For basic login to the Insyde UI, use the following login:

- **Username:** root
- **Password:** OpenBmc



NOTE! The first character is the number "0", not the letter "O".

- **US - English:** Changes the interface language.

Remember Username: Check this option to remember your login credentials.

Forgot password: If you forget your password, you can generate a new one using this link.

Enter the user name, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

1-3-1 Required Browser Settings:

Allow file download from this site: For Internet Explorer, Choose **Tools ->Internet Options ->Security Tab**, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click **Custom level**

In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click **OK** to the entire dialog boxes.

For all Other Browsers, accept file download when prompted.

Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.

Enable cookies for this site: The icon indicates whether the cookies setting are enabled in browser.



NOTE!

Cookies must be enabled in order to access the website.

1-4 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web GUI. A screenshot of the logged-in user information is shown below.



Power: This option shows Server power status and click the power icon to the Server power operations page.

Refresh: Click the icon to reload the current page.

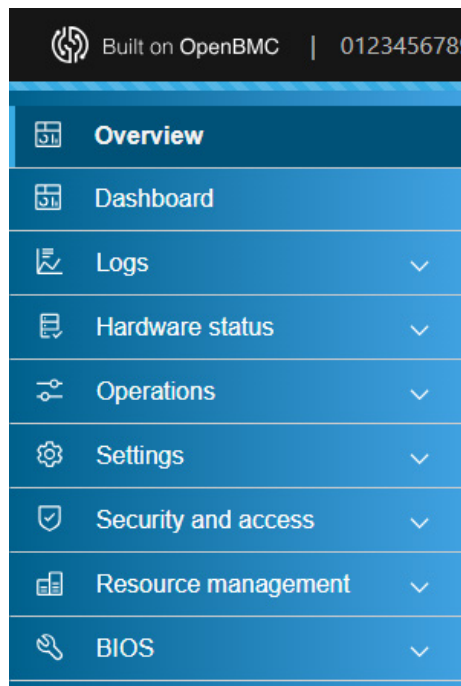
root

The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions:

Profile setting: Click the root icon to change Profile settings.

1-5 Menu Bar

The menu bar displays the following:



Dashboard • Virtual Front Panel • Date & Time • Current Users • Virtual Media • Screen Preview • System Information • Network • Temperature • Voltage • System Event Log • Power Statistics	Settings • Alerts • Alerts Policies • Alerts Email • Date & Time • Networks • VLAN • SOL • SNMP • Ikm & Virtual Media • Dynamic DNS • Syslog Settings • Backup restore • Power restore policy
Logs • System Event Log • POST code • SOL log • BIOS log • Host Video Recorder • System diagnostics	Security and access • Current Users • LDAP • RADIUS • TACACS+ • Users • Policies • Certificate management • Kerberos authentication • Security Settings • IP Access Control
Hardware status • System information • FRU information • CPU Information • DDR information • Inventory and LEDs • Sensor Readings • NIC information(BIOS) • NVMe/HDD information(BIOS) • System Component • SMBIOS	Resource Management • Power • Power statistics • Power schedule
Operations • Factory reset • KVM • Firmware • Reboot BMC • SOL console • Server power operations • Virtual Front Panel • Virtual Media • Boot config	BIOS • Main • Advanced • Security • Power • Boot

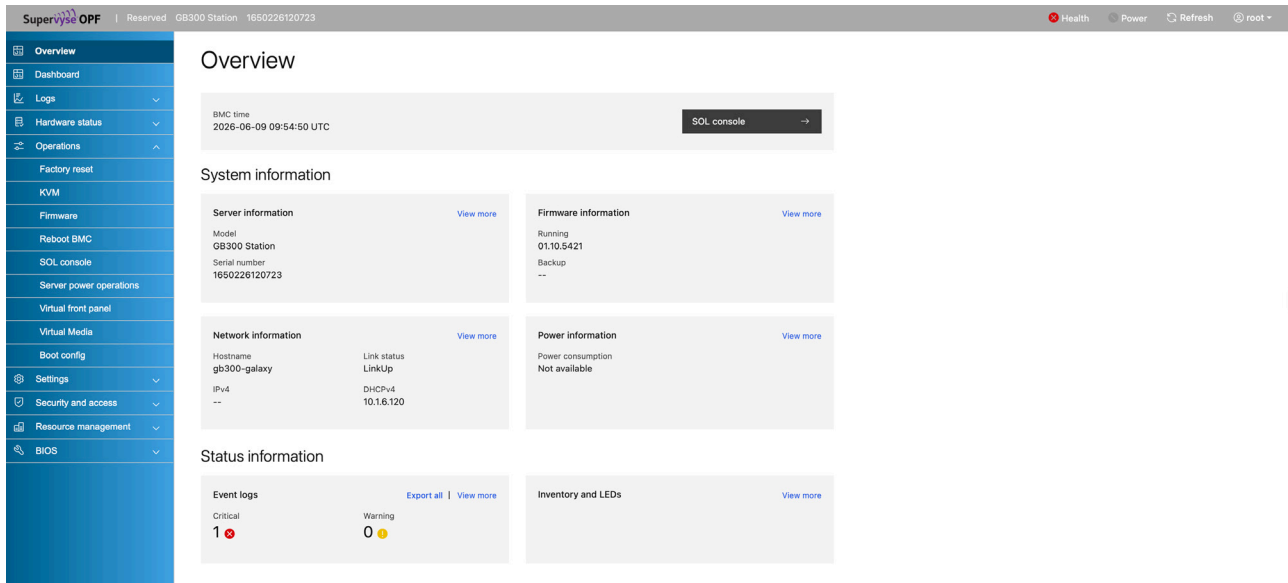
Chapter 2 Enter Gigabyte Management Console

2-1 Overview

Usage

Overview used to show the overall/important Host status in single page.

To open the Overview page, click **Overview** from the menu bar. It displays the following:



Overview includes the following information:

- System information
- Status information

Click the "**View more**" to display detailed information.

2-2 Dashboard

The Dashboard page gives the overall information about the status of a device.
To open the Dashboard page, click **Dashboard** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

OverviewDashboardLogsHardware statusOperationsSettingsAlertsAlert policiesAlert emailDate and timeNetworksVLANSOLSNMPIKVM and virtual mediaDynamic DNSSyslog settingsBackup restorePower restore policySecurity and accessCurrent usersLDAPRADIUSTACACS+UsersPoliciesCertificate managementKerberos authenticationSecurity settingsIP access controlResource managementBIOS

Dashboard

Virtual front panel

Power

Date and time

2026/06/17

Wednesday

17:24

UTC

Current users

User Name	Type	IP Address
root (me)	Web (HTTPS)	10.8.133.57

Virtual media

Device 1	No disk emulation set
Device 2	No disk emulation set
Device 3	No disk emulation set
Device 4	No disk emulation set
Device 5	No disk emulation set

Screen preview

System information

BMC Uptime :	2 days 6 hours 44 minutes 7 seconds
Active BMC Firmware Build Time :	Fri, Jun 05, 2026, 15:24:59
Active BMC FW Rev :	01.10.5421
BMC Chipset :	AST2600-A3

Networks

Dedicated NIC (1)

IP Address	10.1.6.83
Gateway	10.1.6.253
Subnet Mask	255.255.255.0
IPv6 Static Address	["..."]
IPv6 Dynamic Address	["..."]
MAC Address	4c-bb-47-c6-87-e1

Temperature

Healthy	Name
OK	BMC_0_Temp_0
OK	CX8_0_Temp_0
OK	M0_Air_Temp_0
OK	M0_Air_Temp_1
OK	M0_PCB_Temp_0

Voltage

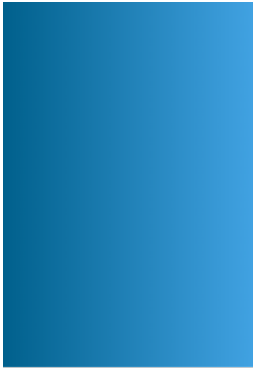
Healthy	Name
OK	GPU_0_Voltage_0
Unknown	VOLT_LEAK1
Unknown	VOLT_LEAK2
Unknown	VOLT_LEAK3
Unknown	VOLT_LEAK4

Fan

Healthy	Name
OK	TACH_PUMP_FAN1
OK	TACH_PUMP_FAN2
OK	TACH_REAR_FAN1
OK	TACH_REAR_FAN2
OK	TACH_REAR_FAN3

System event log

Event ID	Time Stamp	Sensor Name	Controller	Severity	Sensor Type	Description
62	Tue Jun 16 18:04:10 2026	#00	BIOS	Information	System Event	OEM System Boot Event - Asserted
61	Tue Jun 16 17:52:00 2026	#22	BIOS	Information	BaseOSBoot/InstallationStatus	boot completed - boot device not specified - Asserted
60	Tue Jun 16 17:50:39 2026	#00	BIOS	Information	System Event	OEM System Boot Event - Asserted



Power statistics 

Subsystem	Current Watt
Entire Platform	1999.564
CPU	[1999.564]
GPU	[0]



Dashboard

A brief description of the Dashboard page is given below.

Virtual Front Panel

Displays Status LED, Chassis LED, and Power LED.

Date & Time

Displays BMC Date and Time.

Current Users

Displays connections status, included User Name, Connect Type, IP Address.

Virtual Media

Displays KVM screen.

Screen Preview

Displays Virtual Media devices.

System Information

Displays the technical information for the system.

Network

Displays Dedicated NIC and Shared NIC Network configurations (IP Address, Gateway, Subnet Mask, IPv6 Static Address, IPv6 Dynamic Address, MAC Address).

Temperature

Displays Host Temperature sensors Healthy and Name.

Voltage

Displays Power Voltage Healthy and Name.

System event log

Displays the list of event logs occurred by the different sensors on this system.

Power statistics

Displays current power consumption reading and power cap enabled status.

2-3 Logs

2-3-1 System Event Log

Supervise OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Settings

Security and access

Resource management

BIOS

System event log

BMC SEL

BMC Audit Log

Event logs

Select event log category

All Events

Start2026/06/0900:00End2026/06/0923:59Search0 itemsClear

Save Log

BMCBIOSSystem Software

Save event logs generated by the BMC, BIOS, System Software.

Clear LogRefresh All Logs

121/11

Total Event Log: 129 event entries

Event ID	Time Stamp	Sensor Name	Controller	Severity	Sensor Type	Description
129	Tue Jun 09 09:37:10 2026	ACPL_PWR	BMC	Information	OEM	S4/S5 soft-off - Asserted
128	Mon Jun 08 17:39:29 2026	#22	BIOS	Information	BaseOSBoot/InstallationStatus	boot completed - boot device not specified - Asserted
127	Mon Jun 08 17:39:09 2026	ACPL_PWR	BMC	Information	OEM	S0/G0 working - Asserted
126	Mon Jun 08 17:38:06 2026	#00	BIOS	Information	System Event	OEM System Boot Event - Asserted
125	Mon Jun 08 17:37:45 2026	ACPL_PWR	BMC	Information	OEM	S0/G0 working - Asserted
124	Mon Jun 08 17:37:41 2026	ACPL_PWR	BMC	Information	OEM	S0/G0 working - Asserted
123	Mon Jun 08 17:37:34 2026	PWR_BUTTON	BMC	Information	Button/Switch	Power Button pressed - Asserted
122	Mon Jun 08 17:19:06 2026	ACPL_PWR	BMC	Information	OEM	S4/S5 soft-off - Asserted

BMC SEL

This page displays the list of event logs occurred by the different sensors on this device.

Select event log category

The category could be either All Events, BMC Generated Events, BIOS Events, System Software Generated Events, SMI Handler Events, System Management Software Events, OEM Events, Remote Console Software Events, Terminal Mode Remote Console Software Event.

Severity category

- Information:** This category includes non-critical events that provide general information about the system's operation.
- Warning:** Events in the warning category indicate potential problems that may not require immediate attention.
- Critical:** Critical logs represent serious problems that usually require immediate attention. These events may indicate system failure, hardware failure

Save Log

Click on the Save Log button to save all Log entries.

Clear Log

Click on the Save Log button to remove all Log entries.

Refresh Log

Click on the Refresh Log button to redisplay all of the current set of event records. The Log does not automatically refresh, in order to allow review of the entries.



Support circular mode only. The circular mode means older SELs will be automatically cleared when the SEL is almost full.

BMC Audit Log

Audit Log page will display all the system events occurred in this device that has been already configured.

Save Log

Click on the Save Log button to save all Log entries.

Clear Log

Click on the Save Log button to remove all Log entries.

Refresh Log

Click on the Refresh Log button to redisplay all of the current set of event records. The Log does not automatically refresh, in order to allow review of the entries.

2-3-2 Post code

Supervyse OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Settings

Security and access

Resource management

BIOS

POST code

Time Style: Offset

Previous Boot

Current Boot

Boot Time

2026-06-16 01:49:24

Time	Code	Description
00:00.000	01000000000001C000	Hardware QSPI FW Flash Init
00:00.012	01000000000001C100	FW Boot on BRBCT Load
00:00.025	01000000010001C101	FW Boot on Boot Chain Select #1
00:00.084	01000000020001C100	FW Boot on BR Exit Done
00:00.251	01000000050001C102	FW Boot on MB1 Start #2
00:00.296	01000000010001C000	Hardware QSPI Data Flash Init
00:00.321	01000000020001C002	Hardware QSPI #2
00:00.921	01000000000002C010	Hardware UPHY Init #16
00:01.036	01000000000002C011	Hardware UPHY Init #17
00:01.153	01000000000002C00A	Hardware UPHY Init #10
00:01.264	01000000000002C013	Hardware UPHY Init #19
00:01.366	01000000000002C014	Hardware UPHY Init #20

Boot Time

2026-06-16 17:50:13

Time	Code	Description
00:00.000	01000000000001C000	Hardware QSPI FW Flash Init
00:00.013	01000000000001C100	FW Boot on BRBCT Load
00:00.025	01000000010001C101	FW Boot on Boot Chain Select #1
00:00.087	01000000020001C100	FW Boot on BR Exit Done
00:00.248	01000000050001C102	FW Boot on MB1 Start #2
00:00.593	01000000010001C000	Hardware QSPI Data Flash Init
00:00.621	01000000020001C002	Hardware QSPI #2
00:00.908	01000000000002C010	Hardware UPHY Init #16
00:01.022	01000000000002C011	Hardware UPHY Init #17
00:01.140	01000000000002C00A	Hardware UPHY Init #10
00:01.250	01000000000002C013	Hardware UPHY Init #19
00:01.350	01000000000002C014	Hardware UPHY Init #20

Time Style:

A drop-down menu that allows users to switch the format of the timestamp display (e.g., Offset time or absolute date/time).

Previous Boot

Displays the boot start timestamp and the corresponding chronological table of POST codes, execution offsets, and detailed step descriptions from the last completed boot cycle.

Current Boot

Displays the boot start timestamp and the live or most recent chronological table of POST codes, execution offsets, and step descriptions for the ongoing or active boot cycle.

2-3-3 SOL Log

Supervyse OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Settings

Security and access

Resource management

BIOS

SOL log

RefreshSave SOL LogClear SOL Log

Dxe/DEBUG/NorFlashDxe.dll 0x7C3AF60000

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/NorFlashDxe/NorFlashDxe/DEBUG/NorFlashDxe.dll

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/NorFlashDxe/NorFlashDxe/DEBUG/NorFlashDxe.dll

add-symbol-file /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/CapsuleUpdatePolicyDxe/CapsuleUpdatePolicyDxe/DEBUG/CapsuleUpdatePolicyDxe.dll 0x7C3AF10000

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/CapsuleUpdatePolicyDxe/CapsuleUpdatePolicyDxe/DEBUG/CapsuleUpdatePolicyDxe.dll

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/CapsuleUpdatePolicyDxe/CapsuleUpdatePolicyDxe/DEBUG/CapsuleUpdatePolicyDxe.dll

add-symbol-file /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/EepromDxe/Eeprom/DEBUG/EepromDxe.dll 0x7C39D08000

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/EepromDxe/Eeprom/DEBUG/EepromDxe.dll

Cvm Eeprom data validation failed

Populated dummy Cvm Eeprom data

Cvb Eeprom data validation failed(Success)

add-symbol-file /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/NvSecureBootProvisionDxe/NvSecureBootProvisionDxe/DEBUG/NvSecureBootProvisionDxe.dll 0x7C39CFC000

Image - /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Silicon/NVIDIA/Drivers/NvSecureBootProvisionDxe/NvSecureBootProvisionDxe/DEBUG/NvSecureBootProvisionDxe.dll

add-symbol-file /out/nvidia/bootloader/uefi/Server_RELEASE/Build/Server/RELEASE_GCC5/AARCH64/Armpk

Refresh

Click this button to reload and update the latest SOL log entries on the screen.

Save SOL Log

Click this button to download and save the current SOL log text file to your local storage.

Clear SOL Log

Click this button to erase and clear all the current log entries from the display and buffer.

2-3-4 BIOS Log

Supervyse OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Settings

Security and access

Resource management

BIOS

BIOS log

«<1234>»

ExportExport All

[Tue Jun 16 09:50:20 2026]enable uphy3_pll10_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy3_pll0_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy2_pll10_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy2_pll0_mgmt

[Tue Jun 16 09:50:20 2026]enable up

hy1_pll10_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy1_pll0_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy0_pll10_mgmt

[Tue Jun 16 09:50:20 2026]enable uphy0_pll0_mgmt

[Tue Jun 16 09:50:20 2026]enable xusb_core_dev

[Tue Jun 16 09:50:20 2026]enable i2c3

[Tue Jun 16 09:50:20 2026]enable xusb_ss

[Tue Jun 16 09:50:20 2026]initialized clk_mach_post

[Tue Jun 16 09:50:20 2026]initialized regulator_post

[Tue Jun 16 09:50:20 2026]initialized pwrmodel

[Tue Jun 16 09:50:20 2026]initialized pwrmodel_mrqr

[Tue Jun 16 09:50:20 2026]initialized profile

[Tue Jun 16 09:50:20 2026]initialized mrqr

[Tue Jun 16 09:50:20 2026]initialized extras_post

[Tue Jun 16 09:50:33 2026]c2c_link_init part_bitmap 0x3 0xff

Pagination Buttons

Allows users to navigate through multiple pages of log records (e.g., page 1, 2, 3, 4, or skipping to the first/last page).

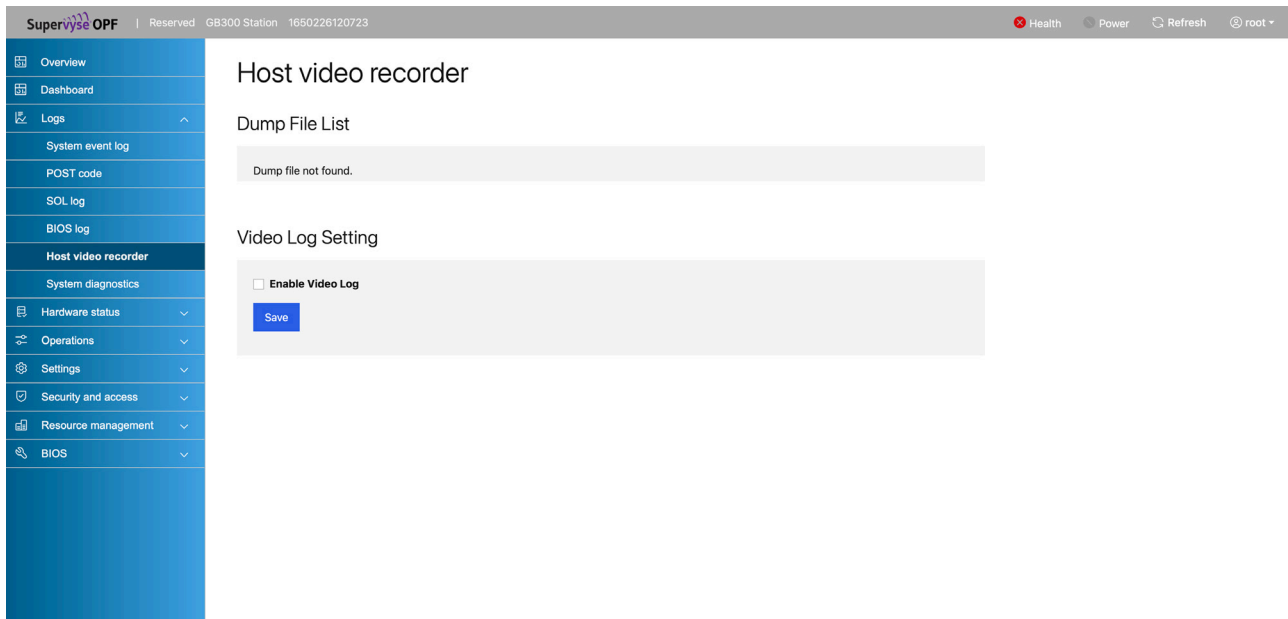
Export

Click this button to download and save the log entries of the current page.

Export All:

Click this button to download and save the complete history of all BIOS log entries.

2-3-5 Host Video Recorder



Dump File List

This page displays dump file list.

Video Log Setting

Enable Video Log

Toggle to enable/disabled host video recorder feature.

Video Quality

Select the video quality as Low, High, and Normal from the Video Quality drop-down list.

Video Trigger

Video Trigger Settings is used to configure the events that will trigger auto video recording function. Event List shows the list of available events to be configured. The events are:

- Watchdog Timer Event
- Chassis Power Off Event
- Chassis Reset
- Host Crash Event (CATERR/IERR for Intel, CPER for Nvidia, and RAS error for AMD ...etc)

Pre-Event Video Recording

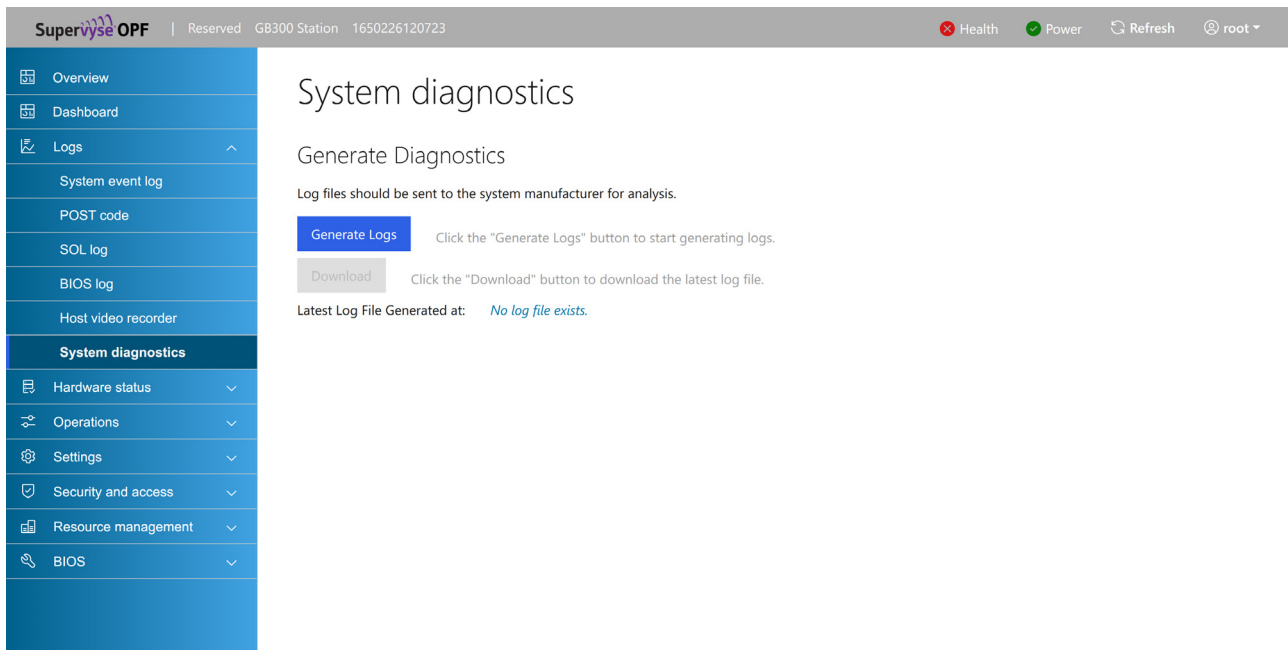
Pre-Event Video Recording is to edit the Pre-Event video recording configurations.

- **Maximum Dumps:** Enter the pre-event maximum dumps of the video.
- **Duration (Sec):** Select the duration in seconds (10-60) from the drop-down list.

Enabled Remote Storage

Check to enable the Remote Video Support. NOTE: By default, video files will be stored in the local path of BMC. If remote video support is enabled, then the video files will be stored only in the remote path, not within BMC.

2-3-6 System diagnostics



Generate Logs

Click this button to trigger the system to start compiling the latest diagnostics and log bundles.

Download

Click this button to save the newly compiled diagnostics archive file to your local workspace. This button is only active after a log file has been successfully generated.

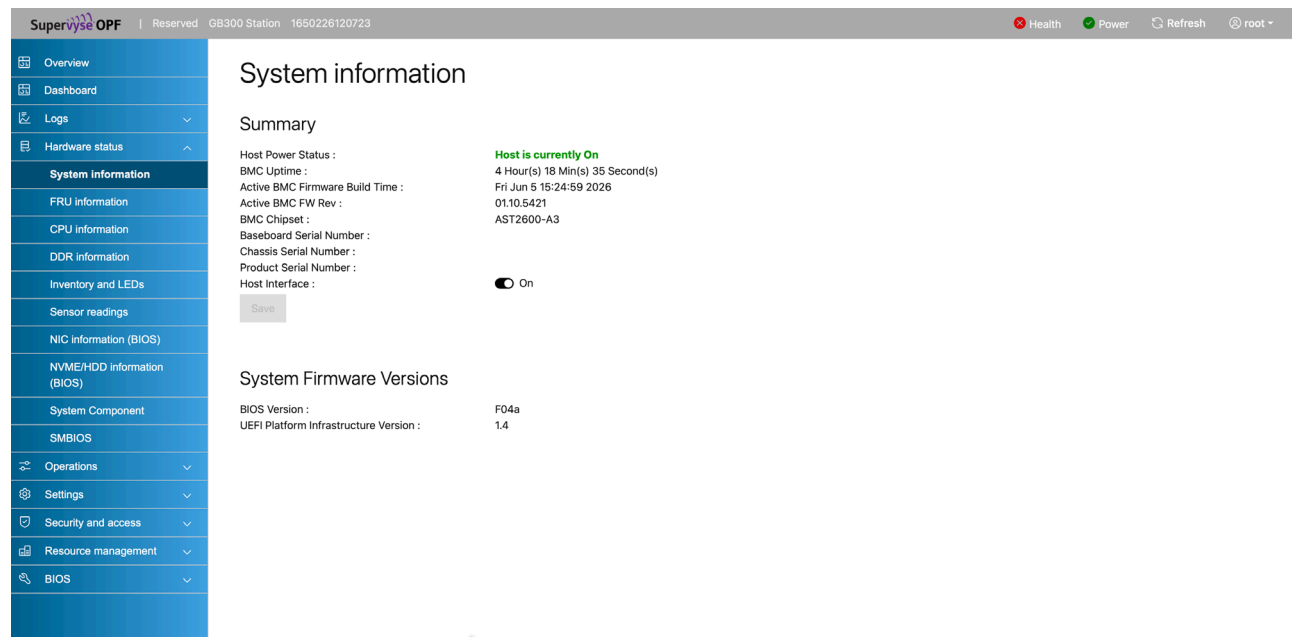
2-4 Hardware status

The Hardware Status page displays the following information:

- System Information
- FRU information
- CPU information
- DDR information
- Inventory and LEDs
- Sensor readings
- NIC Information (BIOS)
- NVMe/HDD information (BIOS)
- System Component
- SMBIOS

2-4-1 System Information

This page displays information about system information.
To open the System Information page, click **System Information** from the menu bar. It displays the following:



2-4-2 FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information.
To open the FRU Information page, click **FRU Information** from the menu bar. It displays the following:

Supervyze OPF

GB300 Station 1650226120723

Health

Power

Refresh

root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

FRU information

DeviceBMC_FRU

Product Information

AssetTag :

FRUFileId :v0.1

Manufacturer :NVIDIA

Name :P3809-BMC

PartNumber :699-13809-0503-600

Serial :

Version :AE.1s

Board Information

Manufacturer :NVIDIA

ManufacturerDateTime2025-11-25T03:17:00+00:00

:

Name :P3809

PartNumber :699-13809-0503-600

Serial :

FRUDeviceID :0

Language :English

Extra

Extra 1:01

Extra 2:

Device

Select to display FRU0 or FRU1 information.

2-4-3 CPU Information

This page displays installed CPU information.

To open the CPU Information page, click **CPU Information** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1650226120723

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

CPU information

CPU_0

Id: CPU_0

Manufacturer: NVIDIA

Model: Grace A02P

Speed: 3.321 GHz

Voltage: -12.8 V

Socket Type: None

Status: Populated, CPU Enabled

Asset Tag: GQG4P6712A0002

PartNumber: W775-V10-L01

Processor Signature: 0x0000001203680241

L1Cache: 9 MB

L2Cache: 72 MB

L3Cache: 114 MB

ProcessorType: CPU

SerialNumber: 0x00000001784112422000000002010040

Socket: G10.0

Number of Cores: 72

TotalThreads: 72

GPU_0

Id: GPU_0

Manufacturer: NVIDIA

Model: NVIDIA GB300

PartNumber: 31C2-893-A1

ProcessorType: GPU

SerialNumber: 1650226120897

2-4-4 DDR Information

This page displays installed DDR information.

To open the DIMM Information page, click **DDR information** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1650226120723

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

DDR information

Search

3 items

Slot Number	Size	Type	Speed	Manufacturer	Asset Tag	Serial Number	Part Number
GPU_0_DRAM_0	256703 MB	HBM	0 MHz	--	--	--	--
--	507904 MB	LPDDR5_SDRAM	6400 MHz	Micron Technology	--	18446744072516987982	699-23830-0000-400
LP5x_0	--	--	--	--	--	--	--

2-4-5 Inventory and LEDs

This page displays Inventory and LEDs information.

To open the this page, click **Inventory and LEDs** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1650226120723

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

Inventory and LEDs

LED light control

Power status On

Quick links to hardware components

System

BMC manager

Chassis

2-4-6 Sensors Readings

This page displays Sensor Readings information.

To open the this page, click **Sensor Readings** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1650226120723

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

Sensor readings

Use this page to see the sensor readings and their thresholds.

Select a sensor owner BMC

Select a sensor type category All Sensors

Auto Refresh(sec) 60

Refresh Show thresholds

Sensor Readings: 39 sensors

Healthy	Name	Status	Current value	Line chart	View chart
OK	ACPI_PWR	S0/G0 working	0x0180		
OK	BMCmgmtHealth	Normal	0x0080		
OK	BMC_BOOT_UP	Initiated by power up	0x0180		
OK	BMC_CPU_Util	Normal	53 percent		
OK	BMC_Mem_Util	Normal	53 percent		
OK	PWR_BUTTON	Normal	0x0080		
OK	System_Event	Normal	0x0080		
OK	System_Event_Log	Log Area Reset/Cleared	0x0480		
OK	BMC_0_Temp_0	Normal	32 degrees C		
Unknown	RTX_0_Power	Not Available	No Reading		

Sensor owner

Displays the Sensor Owner information.

Select a Sensor Type Category

- All Sensors
- System ACPI Power State
- Management Subsystem Health

- Button / Switch
- System Event
- Event Logging Disabled
- Temperature Sensors
- Other Unites-based Sensor
- Watchdog2
- Fan
- Voltage
-

Auto Refresh(sec)

Select the Auto Refresh time by drop-down list. Option available: 5/ 10/ 15/ 30/ 60/ 150/ 300/ Never

Refresh

Click on the Refresh button to refresh the page.

Show Thresholds

Click on the Show Thresholds button to view non-critical, critical and non-recoverable thresholds.

2-4-7 NIC Information (BIOS)

This page displays all detected NICs on this device. It allows you to on-board NICs, add-on NICs. To open the this page, click **NIC Informatiion (BIOS)** from the menu bar. It displays the following:

Supervise OPF

Reserved GB300 Station 1660226120723

Health

Power

Refresh

root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVMe/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

NIC information (BIOS)

Segment	Port	Class	Component	Device	Vendor	DeviceId	VendorId	SubsystemId
01	03:00.0	Network controller	SoC	Device 1023	Mellanox Technologies	0x1023	0x15B3	0x21D5
01	03:00.1	Network controller	SoC	Device 1023	Mellanox Technologies	0x1023	0x15B3	0x21D5
01	06:00.0	Network controller	SoC	Device 04C0	Aquantia Corp.	0x04C0	0x1D6A	0x21D5

2-4-8 NVMe/HDD Information (BIOS)

This page displays all detected NVMe device and other hard drive devices in this system. To open this page, click **NVMe/HDD information (BIOS)** from the menu bar. It displays the following:

Supervise OPF | Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

NVME/HDD information (BIOS)

Device Count: 4

▼	HFS1T9GEJ8X176N Port: 0 MediaType: SSD
▼	HFS1T9GEJ8X176N Port: 0 MediaType: SSD
▼	HFS1T9GEJ8X176N Port: 0 MediaType: SSD
▼	HFS1T9GEJ8X176N Port: 0 MediaType: SSD

2-4-9 System Components

This page displays information about the system components, including the System-on-Chip (SoC) and available expansion slots in this system. To open this page, click System Component from the menu bar. It displays the following items:

- SoC: Click to expand and view specific processor or chipset-level configurations and details.
- Slot1 ~ Slot9: Click on individual slot identifiers to expand and view information about the devices installed in the corresponding PCIe or expansion slots.

Supervise OPF | Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

System Component

- ▶ SoC
- ▶ Slot1
- ▶ Slot2
- ▶ Slot3
- ▶ Slot4
- ▶ Slot5
- ▶ Slot6
- ▶ Slot7
- ▶ Slot8
- ▶ Slot9

2-4-10 SMBIOS

To enable this function, turn on the host and wait for the BIOS to upload the relevant data.
Display the SMBIOS.

Save: Click to save the settings.

Reset: Click to reset the changes.

Supervise OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NVME/HDD information (BIOS)

System Component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

SMBIOS

Type: 0

Type: 1

Type: 2

Type: 3

Type: 4

Type: 7

Type: 8

Type: 9

Type: 10

Type: 11

Type: 13

Type: 16

Type: 17

Type: 19

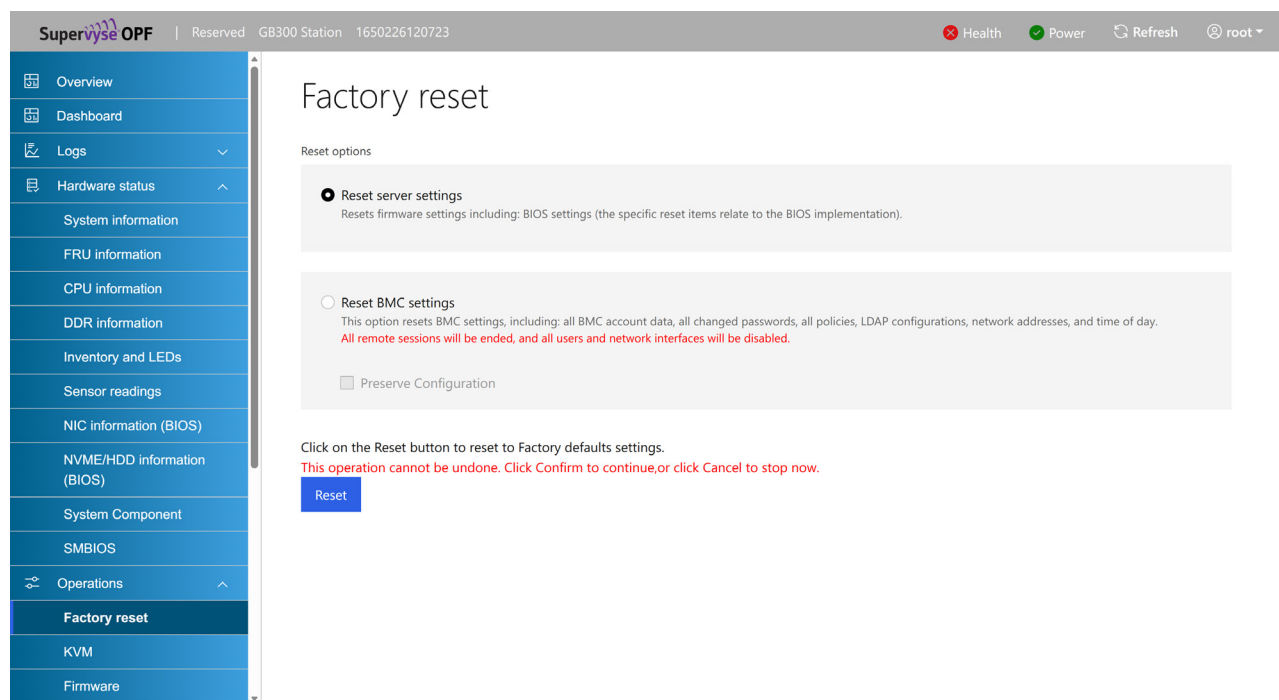
2-5 Operations

2-5-1 Factory Reset

In Web GUI, this option is used to reset the factory defaults of the device firmware, BIOS settings, BMC settings.

Warning: Please note that after entering reset factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within a few minutes.

To open Factory Reset page, click Operations > Factory Reset from the menu bar. A sample screenshot of the Factory Reset Defaults Page is shown below.



Preserve Configuration: Select the settings to be preserved.

Reset: Click on the Reset button to reset factory settings.

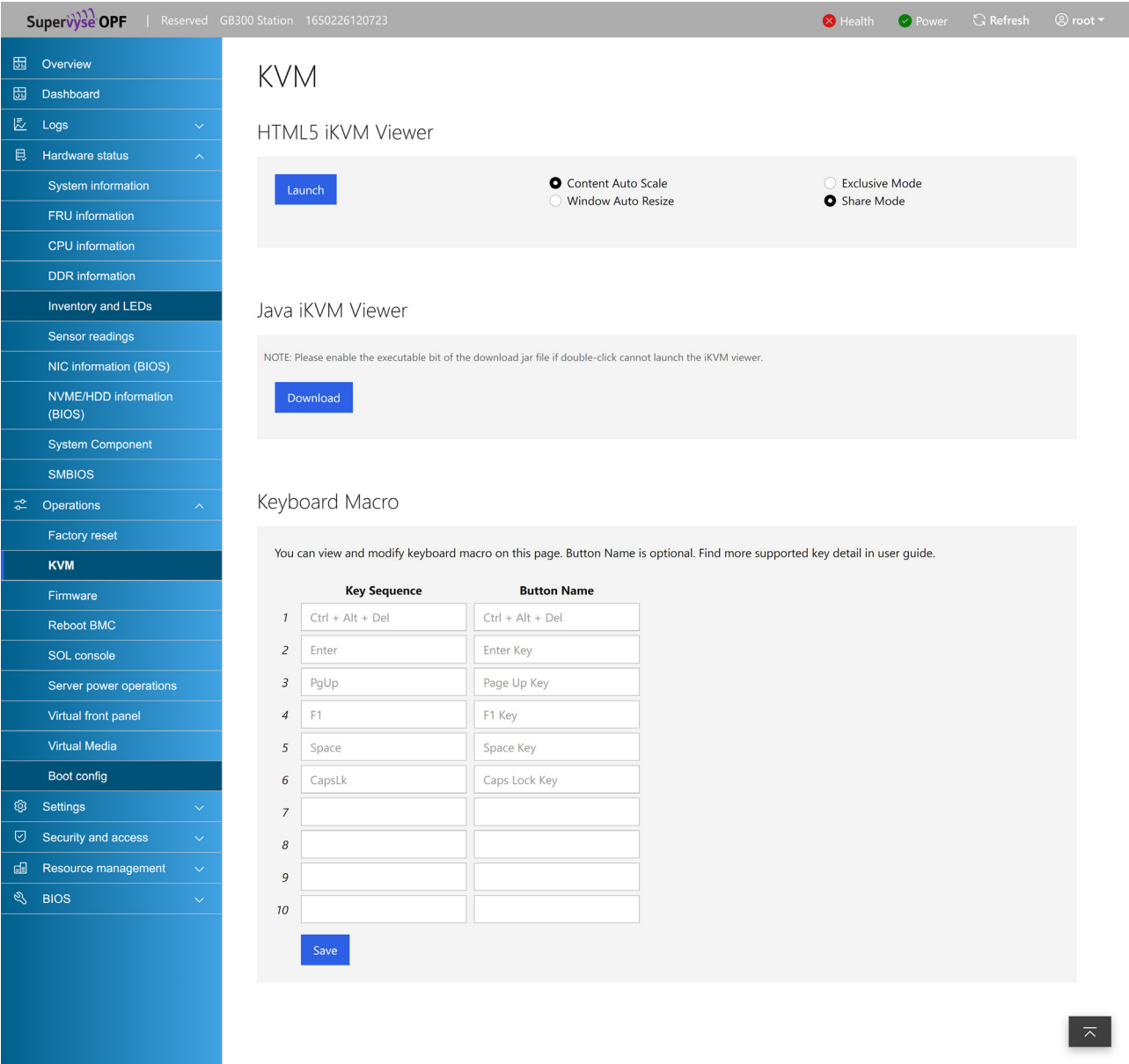
2-5-2 KVM

The system and browser requirements for Remote Control are given below.

System Requirements

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be a lag in the video/keyboard/mouse functionality.

To open KVM, click Operations > KVM from the menu bar. A sample screenshot of the KVM Page is shown below.



A detailed description of the menu items is given below.

HTML5 iKVM Viewer

Click the **Launch** button to launch the H5viewer window.

Java iKVM Viewer

Click the **Download** button to download the Java iKVM Viewer jar file.

Keyboard Marco

You can view and modify keyboard macro on this page. Button Name is optional.

iKVM Setting Panel

- **Content Auto Scale**

If this function is enabled, the iKVM display area will be scaled to fit the window automatically.

- **Window Auto Resize**

If this function is enabled, the window size will be resized to the size of iKVM display area automatically.

- **Share Mode**

If this function is enabled, the iKVM Server should try to share the desktop by leaving other clients connected.

- **Exclusive Mode**

If this function is enabled, the iKVM Server should give exclusive access to this client by blocking all other clients.

Exclusive Mode rule

1. Only the first connection can activate Exclusive mode.
2. If the second connection or other enable Exclusive mode, they can't eject other connection.
3. Some of client can not connect due to Exclusive mode, the viewer should show the reason.

Click "**Launch**" to open the HTML5 iKVM Viewer, as shown below.



1. Client Mode status (Share Mode or Exclusive Mode)
2. Host resolution
3. iKVM update frame per second
4. Current virtual keyboard layout

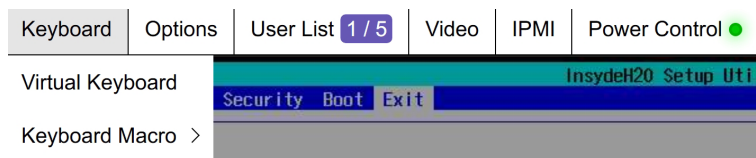
NOTE! If it shows **(View Only)** in front of the title indicator, which means the user can not control mouse, keyboard, power control menu, ipmi menu, keyboard menu and option menu.

Remote Mouse

- Control the host remotely via mouse.
- Supported mouse operations: left click, right click, middle click, move, drag and drop, mouse wheel.

Remote Keyboard

- Control the host remotely via a keyboard.
- Supported keys: all keys on a standard keyboard.



Virtual Keyboard

- Virtual Keyboard is an on-screen keyboard.
- Click the button **Keyboard** -> **Virtual Keyboard** to launch the virtual keyboard.
- The language layout of the virtual keyboard can be changed.
 1. Right click on the virtual keyboard to open the language layout menu.
 2. Select a language to change the keyboard layout.
- Winkey usage: It depends on host OS.
 1. WinKey + <other key>: WinKey Shortcuts
 2. Double-click WinKey: Open and close the Start Screen or Start Menu

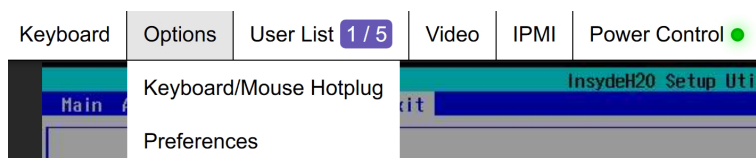
Keyboard Macro

- This feature provides many hotkeys, shortcuts, and macros for use with a keyboard.

Go to **Keyboard** -> **Keyboard Macro**

 1. Keyboard Macro list
 - Default Macro
 - Ctrl+Alt+Del
 - Alt+Tab
 - Alt+Esc
 - Ctrl+Esc
 - Alt+Space
 - Alt+Enter
 - Alt+Hypen
 - Alt+F4
 - Alt+PrntScn
 - PrntScn
 - F1
 - Alt+F1
 - Pause
 - Custom Macro: Users can define at web > Remote Control > Keyboard Macros page
 2. Hold key: When the hold key is enabled, it will emulate when the user presses a key.

Options

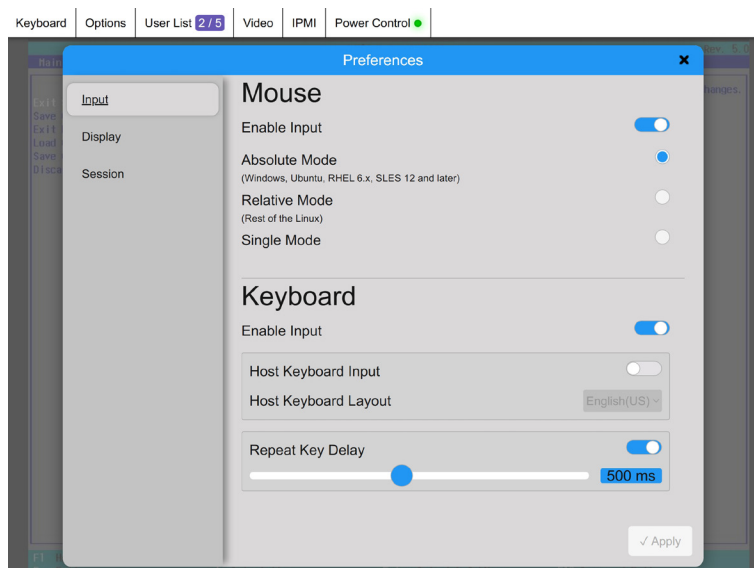


Keyboard Mouse Hotplug

Click to activate Keyboard Mouse Hotplug.

Preferences

Click to open preferences.



Input

Mouse

- Allow different modes of mouse to be set on the BMC, so that the client can use the mouse control correctly.
 - If enabling mouse input, it will send mouse events from client to host, and vice versa.
- Mouse mode (depends on the host OS).
 - **Absolute mode** - use the absolute location on screen to address.
 - **Relative mode** - use the bias value to move Host cursor (Ex: X axis +1 means move to left a unit).
 - **Single mode** - behavior like Relative mode. But the client cursor is hidden to avoid user confusion with Host cursor image.

NOTE!

- Use **absolute mode** first. When **absolute mode** not work, use candidate **relative/single mode** to move the cursor. (eg: bios environment)
- **Single mode** can be regarded as enhanced **relative mode**. It provides a better user experience.
- Enter and Exit single mode
 - **Enter**: Click the viewer GUI to enter.
 - **Exit**: press **esc** or combo key **ctrl+6** to leave.

Keyboard

- Host keyboard input switch:
 - Host keyboard input switch is used to make client keyboard layout(Not virtual keyboard) mapping host keyboard layout.
 - For example, If client keyboard layout is JP and the host keyboard layout is US, and then you press "=" on the client keyboard, the host will display "^" character.
- Host keyboard Layout:
 - Set Host keyboard Layout's language.

- Provide multi language keyboard layouts to be used, as well as setting the key press repeating timeout period.
 - If enabling keyboard input, it will send keyboard events from the client to host, and vice versa.
 - Change virtual keyboard layout.
 - Adjust key down repeat delay. Range is 0 - 1000 ms.

Display

Image Quality

Control the host screen Quality. The more, the sharper the screen becomes.



Session

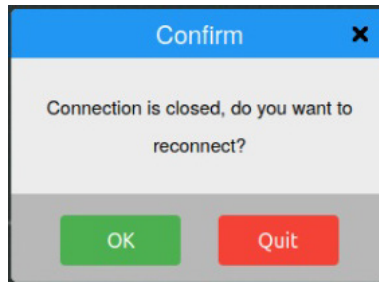


Timeout

- The "Session Timeout" contains two options:
 1. Enable Session Timeout:
 - Enable or disable session timeout
 2. Set Session Timeout:
 - Set the value of the session timeout.
 - The value of session timeout is between 1 to 99999 minutes.

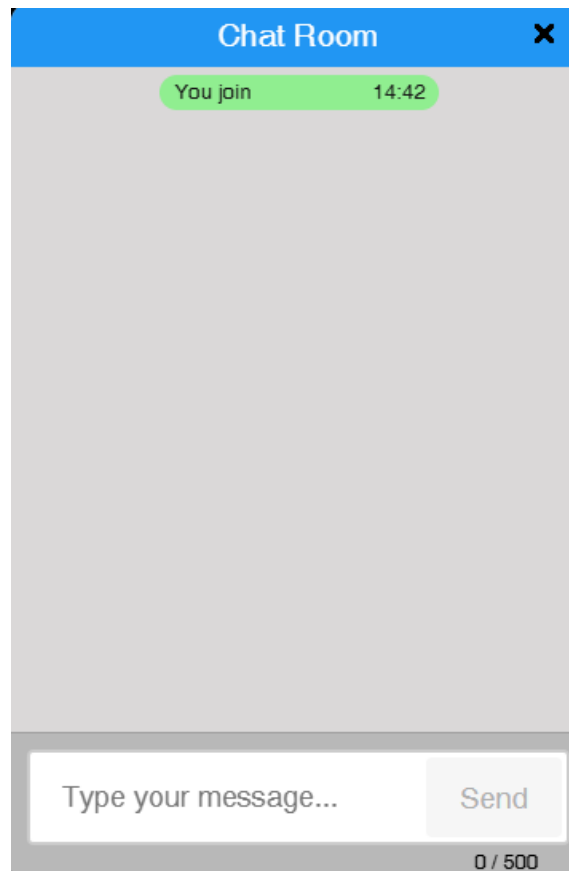
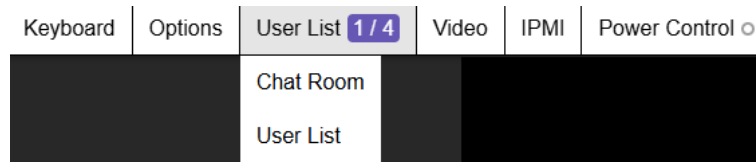
Additional Confirmation Window

- If the network is disconnected for some reason, this dialog will appear to notify user.
- This dialog user can chose the reconnect or not



User List

Chat Room

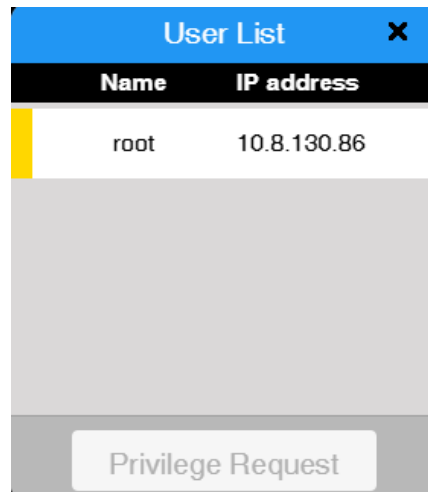


1. Click to open chatroom.
2. Greet message. Include user joined and leave.

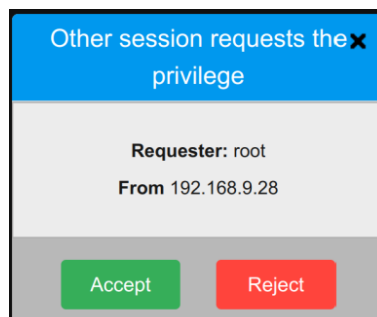
3. Normal message bubble. Show the user name, ip address and time.
4. Whisper message bubble.
5. Input message area. Press "Enter" key or click "Send" button to send message.
 - How to whisper other user
 - You can also send whisper messages by using the format on the message @<username> <message>
 - Notice: Currently, the maximum size of message is 500 words.

User List

- Click to open the userlist.

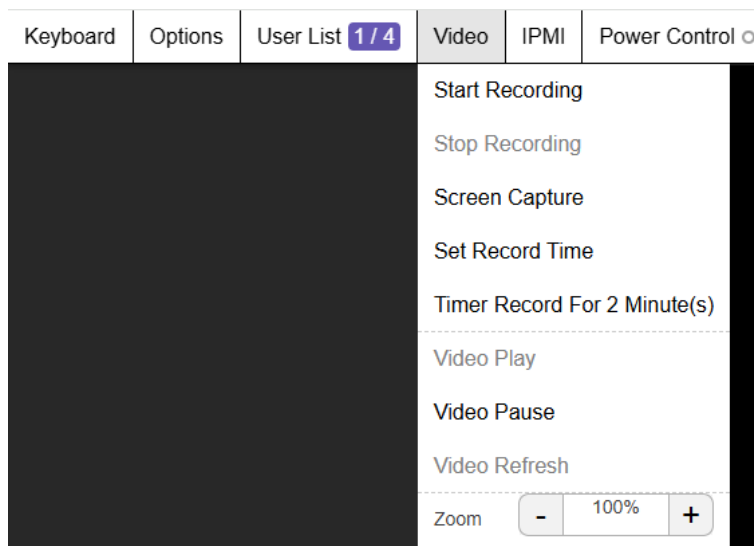


1. Show number of users who are using iKVM.
 2. Click to open userlist window
 3. 3Drag area
 4. iKVM users, the yellow head bar is current privilege owner who can control ikvm, and the grey head is not.
- The user can click the Privilege Request button to request iKVM control privileges.
 - The user who has control privileges will receive the privilege request from the (Video only) user.



Video

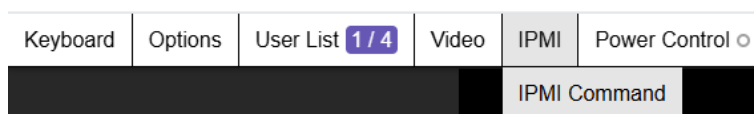
- Click to open record functions.



1. Start to record video of iKVM. The video format is webm.
2. Stop the video recording then save file to local filesystem. Capture the screen of iKVM then save PNG file to local filesystem.
3. Setup recording time for timer recording function, default value is 1 minute. Maximum is 180 minutes.
4. This is will be displayed as Timer recording for x minute(s) which x depends on recording time. Clicking this function will record video for x minutes. User can use the "Stop recording" function to save
5. the video before timeout.
6. Play the host display
7. Pause the host display
8. Refresh the host display
9. Zoom in/out the host display

IPMI

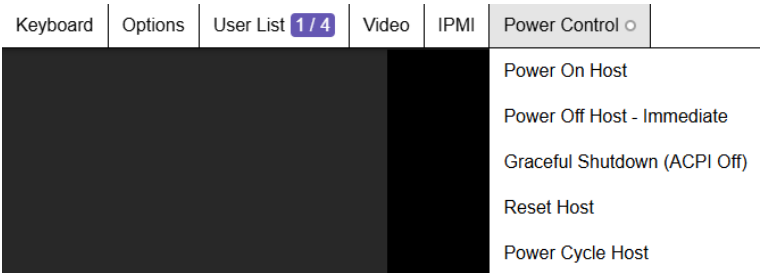
- Click to open ipmi window.



10. Enter the ipmi command to input field and press "Enter" key to send.
11. The ipmi request command.
12. The ipmi response command.
 - NOTE: So far, the maximum size of command is 500 words.

Power Control

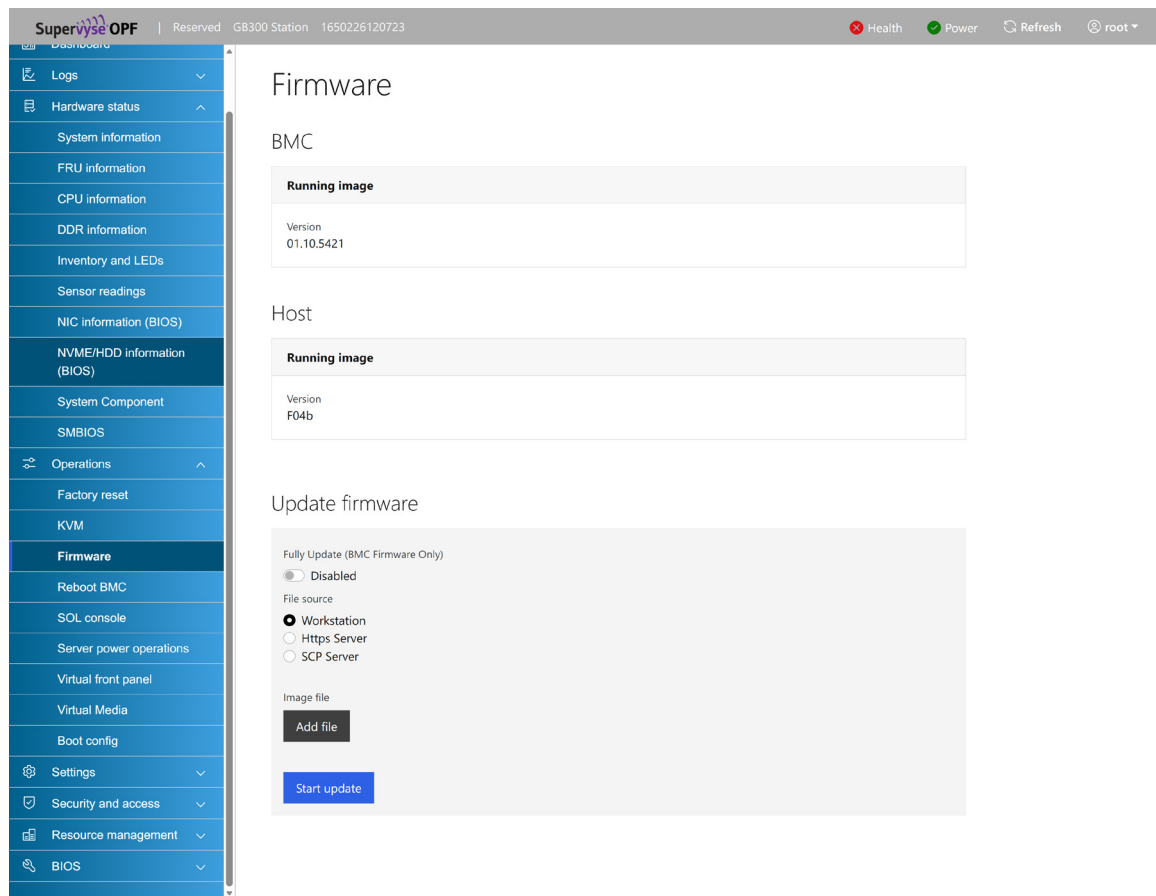
- Click to open power control function.



1. A.C. Power On the Host CRB Board
2. A.C. Power Off the Host CRB Board
3. Emulates OS Software Shutdown
4. A.C. Power reset Host CRB Board
5. A.C. Power Cycle Host CRB Board

2-5-3 Firmware

This page takes you through the process of firmware up gradation. A reset of the box will automatically follow if the upgrade is completed or canceled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.



Update Firmware

File Source

Select the file source:

- Workstation: Upload the firmware file directly from your local computer.
- TFTP Server: Download the firmware file from a remote server over the network using TFTP.

Firmware Type

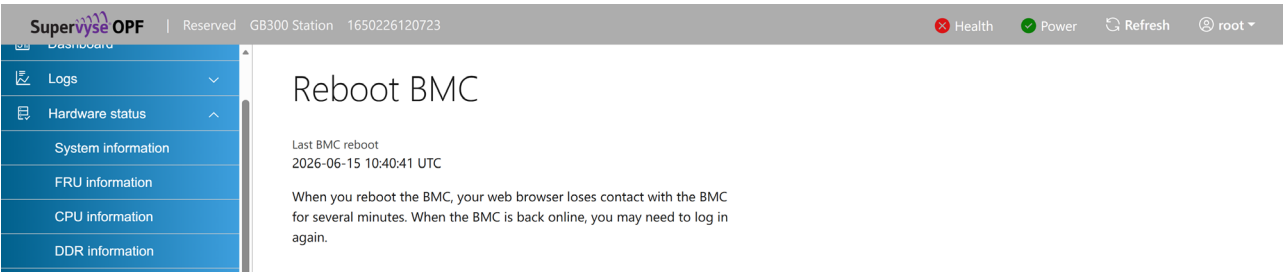
- BMC
 - Active
- BIOS
 - Active

Select the firmware type by the drop-down list. Click **Add file** and Click **Start update** button to process the firmware update.

NOTE! Firmware images are required to be in the .tar file format.

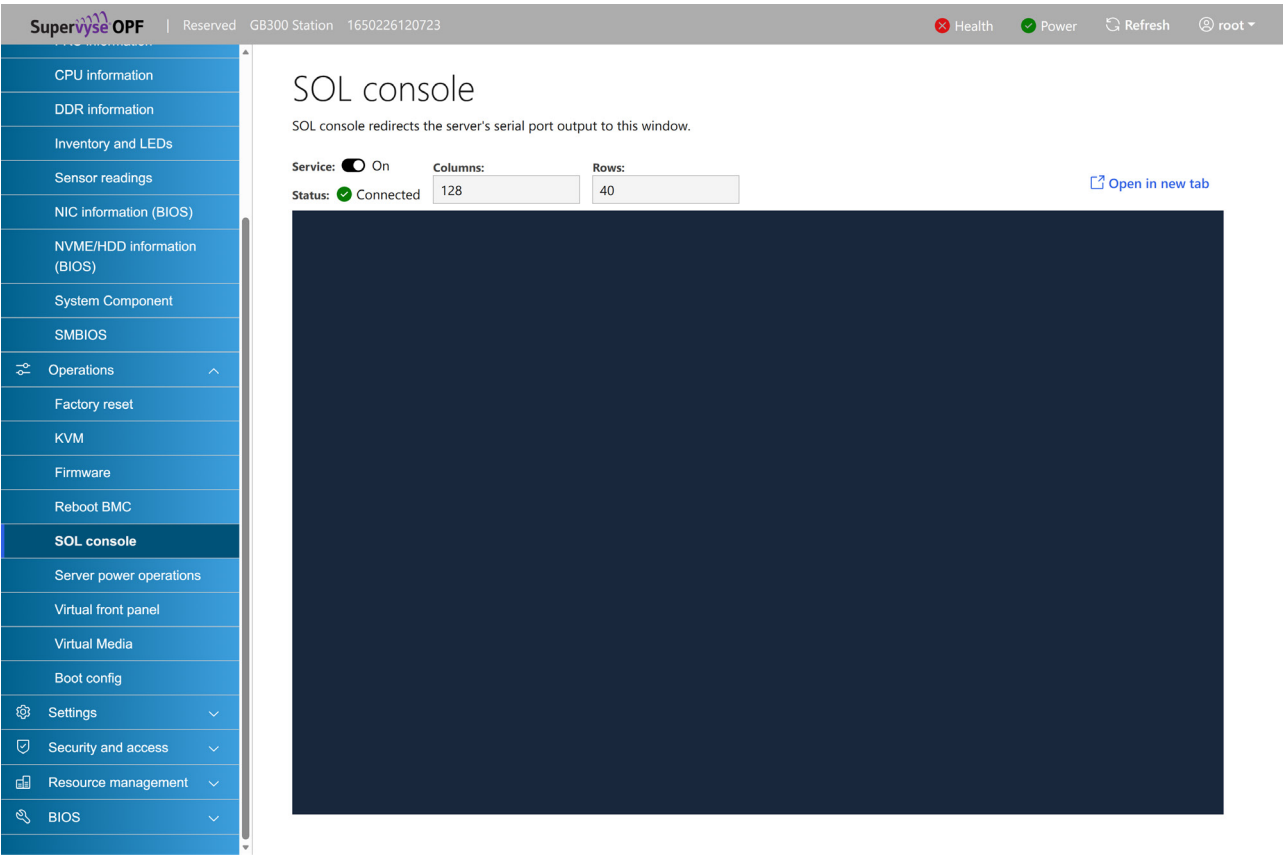
2-5-4 Reboot BMC

Click Reboot BMC to process BMC rebooting.
When you reboot the BMC, your web browser loses contact with the BMC for several minutes. When the BMC is back online, you may need to log in again.



2-5-5 SOL Console

To open SOL Page page, click Operations > SOL Console from the menu bar. A sample screenshot of the SOL COnsole Page is shown below.



Service: Configure the SOL service state (Enable/Disable).
NOTE! The activation process requires approximately 20–22 seconds before the service becomes fully operational. Recommended to set a large value for Rows.

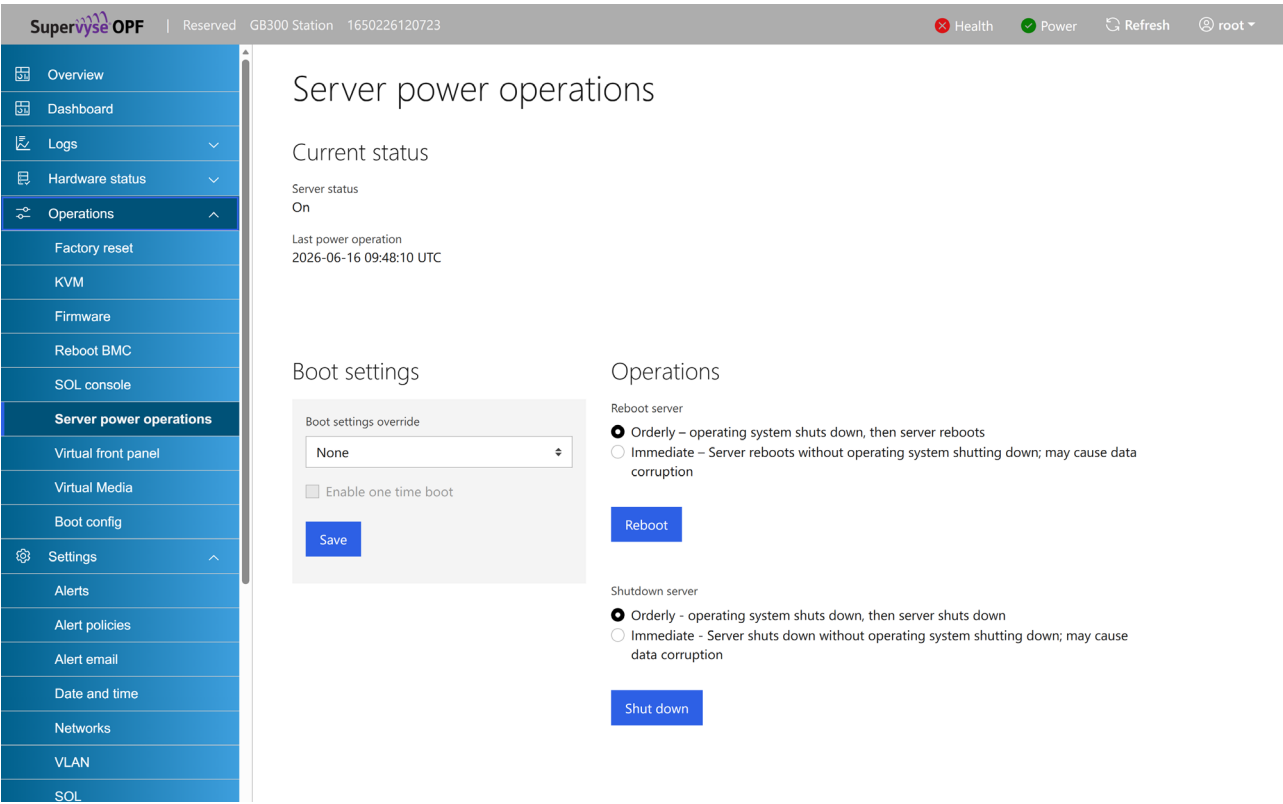
Status: Displays the connection status.

Columns: This setting defines the horizontal resolution of the console display.

Rows: This setting defines the vertical resolution of the console display.
NOTE! Set a larger value is recommended.

2-5-6 Server power operations

This page allows you to view and control the power of your server.
To open Server power operations, click Operations > Server power operations from the menu bar. A sample screenshot of Server power operations is shown below.

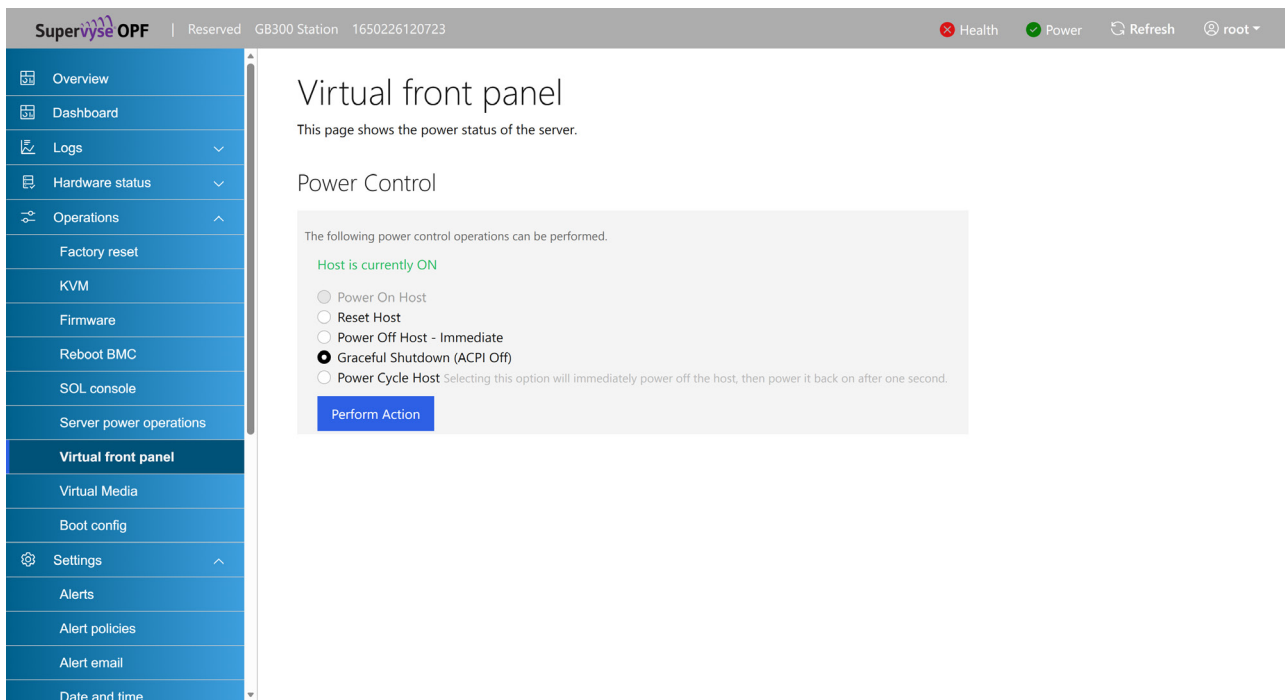


Current Status: Display server power operations.
Operations: Click to the button to process the power operation.

2-5-7 Virtual front panel

This page shows the power status of the server.

To open Virtual front panel, click Operations > Virtual front panel from the menu bar. A sample screenshot of Virtual front panel is shown below.



Power Control

This page shows the power status of the server. The following power control operations can be performed:

Power On Host

Selecting this option will power on the host.

Reset Host

Selecting this option will hard reset the host without powering off.

Power Off Host - Immediate

Selecting this option will immediately power off the host.

Graceful Shutdown (ACPI Off)

Selecting this option will soft power off the host.

Power Cycle Host

Selecting this option will immediately power off the host, then power it back on after one second.

NOTE! All power control actions are done through the BMC and are immediate actions. It is suggested to gracefully shutdown the operating system via the iKVM interface or other interface before initiating power actions.

Perform Action

Click to execute the selected remote power command.

2-5-8 Virtual Media

This page enables the mounting of remote NFS/HTTPS images and exposes them to the system as local storage. To open Virtual Media, click Operations > Virtual Media from the menu bar. A sample screenshot of Virtual Media is shown below.

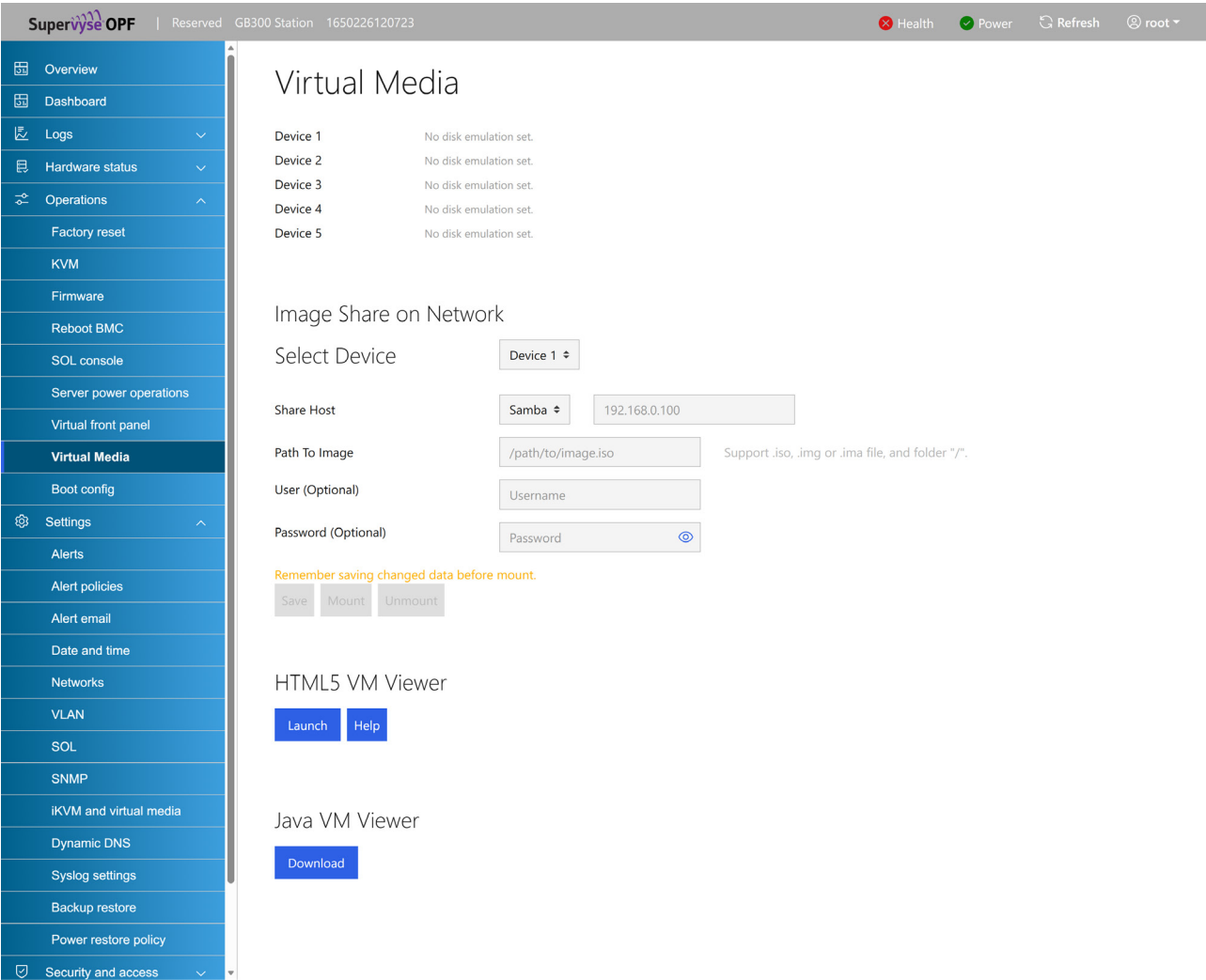


Image Share on Network

Select Device: Select virtual media Device.

Share Host: Select the host.

Path To Image: Enter the path to image. Note: Support .iso, .img or .ima file, and folder "/".

User (Optional): Enter the User account.

Password (Optional): Enter the Password.

Actions

- **Save**

Click on the Save button to save the settings.

- **Mount**

Click on the Mount button to mount the image file.

- **Unmount**

Click on the Unmount button to unmount the image file.

- **Test Steps**

1. Prepare a file server such as Samba, HTTPS or NFS. We will share media from the network.
2. Select Device: Select a device you want to use.
3. Share Host: Choose which file server you want to use for sharing media: Samba, HTTPS, or NFS. And enter ip address of file server.
4. Path To Image: Enter the path to the file you want to share from the file server.
5. User: Enter the user, if access to the file requires authentication.
6. Password: Enter the password, if access to the file requires authentication.
7. Save: Must be click on the Save button before click on the Mount button.
8. Mount: Mount the image file.
9. Unmount: Unmount the image file.

HTML5 VM Viewer

Click 'Launch' button to launch the Virtual Media window.

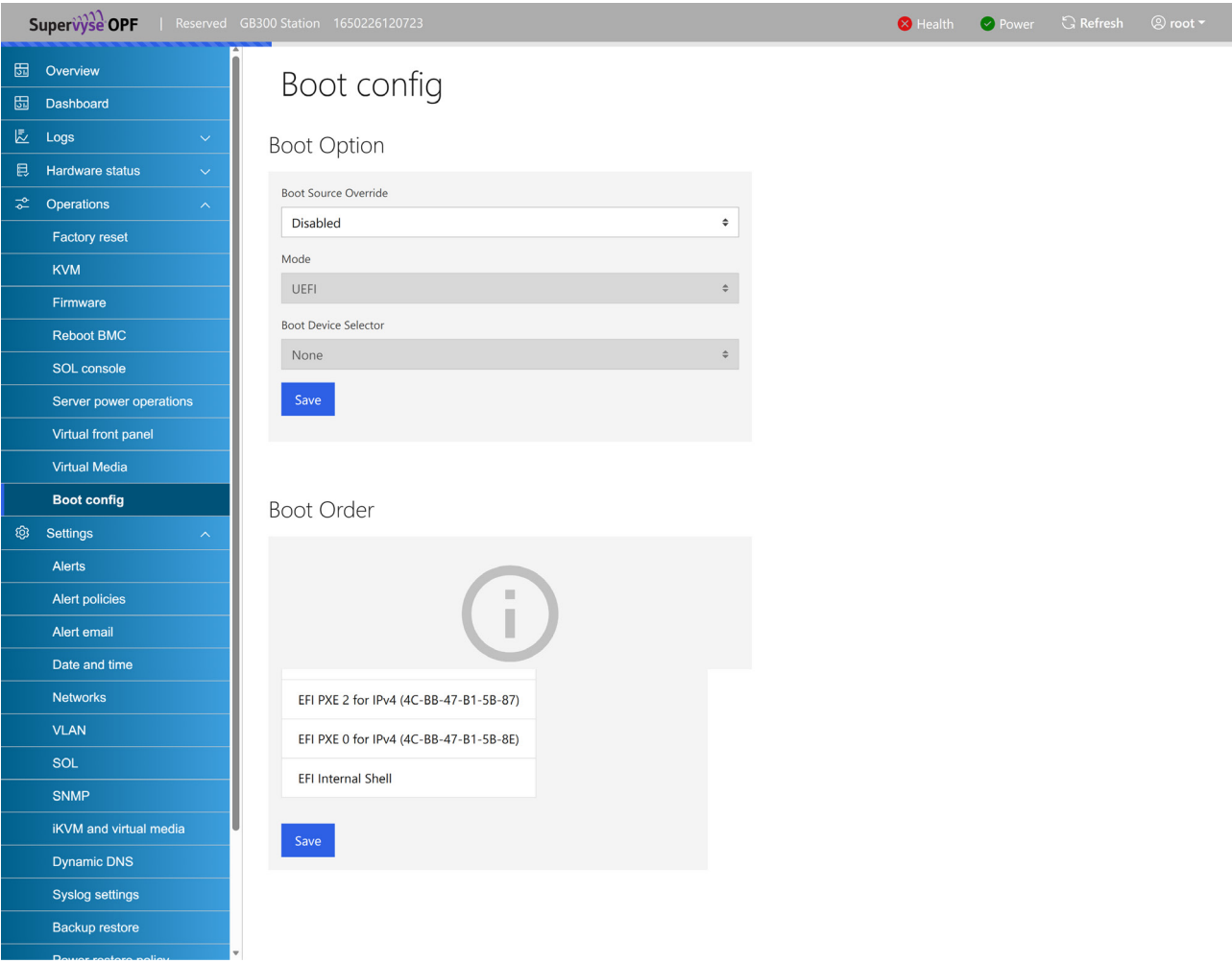
Java VM Viewer

Click 'Download' button to download the VMviewer (.jar) file.

2-5-9 Boot Config

This page Display boot configuration information.

To open Boot Config, click Operations > Boot Config from the menu bar. A sample screenshot of Boot Config is shown below.



Boot Option: Select the device to boot.

Boot Order: Priority the Boot Order.

Actions

Save: Click on the Save button to save the option settings.

2-6 Settings

2-6-1 Alert

This page displays alerts information.
To open Alert page, click Settings > Alert from the menu bar. A sample screenshot of the Alert Page is shown below.

SupervyseOPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

Hardware status

Operations

Factory reset

KVM

Firmware

Reboot BMC

SOL console

Server power operations

Virtual front panel

Virtual Media

Boot config

Settings

Alerts

Alert policies

Alert email

Date and time

Networks

VLAN

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Backup restore

Power restore policy

Security and access

Resource management

BIOS

Alerts

PEF

To configure the global PEF configuration, please click [here](#)

No.	PEF Enable	Policy Set	Sensor Type	Sensor Name	Assertion Condition	PEF Actions
1	Yes	1	Temperature	Match All	state:0,2,4,7,9,11	Alert; edit
2	Yes	1	Voltage	Match All	state:0,2,4,7,9,11	Alert; edit
3	Yes	1	Current	Match All	state:0,2,4,7,9,11	Alert; edit
4	Yes	1	Fan	Match All	state:0,2,4,7,9,11	Alert; edit

SNMP Trap

LAN ChannelDedicated NIC (1)

SNMP Trapv1v2cv3

Community Stringpublic

Save

Alert Destination

LAN ChannelDedicated NIC (1)

Enable Alerting

Alert Destination #1

SNMPSend SNMP Alerts to IPIP:default port 162

EmailSend Email tomail@example.com

Alert Destination #2

SNMPSend SNMP Alerts to IPIP:default port 162

EmailSend Email tomail@example.com

Alert Destination #3

SNMPSend SNMP Alerts to IPIP:default port 162

EmailSend Email tomail@example.com

Alert Destination #4

SNMPSend SNMP Alerts to IPIP:default port 162

EmailSend Email tomail@example.com

Alert Destination #5

SNMPSend SNMP Alerts to IPIP:default port 162

EmailSend Email tomail@example.com

SaveSend Test Alert

2-6-1-1 PEF Configuration

Platform Event Filter (PEF) provides a configurable mechanism that enables the BMC to **determine and execute predefined system actions** in response to both externally received and internally generated event messages. Supported actions **shall include** system power-off, system reset, and the initiation of alert generation. The PEF configuration shall consist of a global configuration section and up to **28 individually defined event filter entries**, each of which **must specify** event-matching conditions and the corresponding system response.

Supervise OPF | Reserved GB300 Station 1650226120723 Health Power Refresh root

Overview Dashboard Logs Hardware status Operations Factory reset KVM Firmware Reboot BMC SOL console Server power operations Virtual front panel Virtual Media Boot config

Alerts

PEF

To configure the global PEF configuration, please click [here](#)

No.	PEF Enable	Policy Set	Sensor Type	Sensor Name	Assertion Condition	PEF Actions
1	Yes	1	Temperature	Match All	state:0,2,4,7,9,11	Alert; Edit
2	Yes	1	Voltage	Match All	state:0,2,4,7,9,11	Alert; Edit
3	Yes	1	Current	Match All	state:0,2,4,7,9,11	Alert; Edit
4	Yes	1	Fan	Match All	state:0,2,4,7,9,11	Alert; Edit

Navigate to Alerts Page: Find the PEF section.

Global PEF Configuration:

PEF Enable: This setting controls whether the entire PEF system is active.

- Options: Enable / Disable

Log Event on Filter Action: This setting determines whether events should be logged when a filter action is triggered.

- Options: On / Off

PEF Actions: These are the actions that can be taken when a filter is triggered. Multiple actions can be selected.

- Options: Alert, Power Off, Reset, Power Cycle, Graceful Shutdown, Diagnostic Interrupt

Configuring Event Filters:

- You can configure up to 28 event filters, each with its own settings.
- Event Filter Enable: This setting controls whether the specific event filter is active.
 - Options: On / Off

Alert: This setting determines whether an alert should be sent when the filter is triggered.

- Options: On / Off

Event Filter Action: These are the actions that will be taken when the filter is triggered. Multiple actions can be selected.

- Options: Alert, Power Off, Reset, Power Cycle, Graceful Shutdown, Diagnostic Interrupt

Policy Set: An option allows you to specify a set of actions that should be taken when this event filter is triggered.

Sensor Type: This setting specifies the type of sensor to monitor. You can choose a specific type or select "Match All" to include all sensors of that type.

- Example:** Temperature, Voltage, Fan, etc.
- Match All:** Select this option to include all sensors type.

Sensor Name: This setting specifies the name of the sensor to monitor. You can choose a specific sensor or select

"Match All" to include all sensors under the specified type.

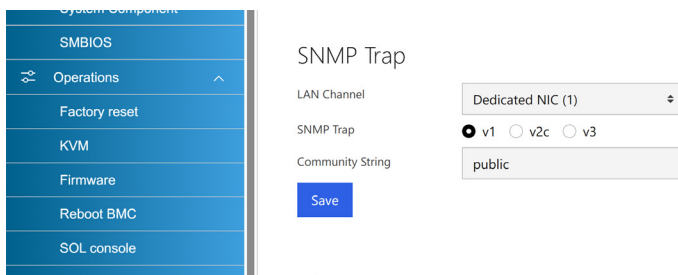
- **Example:** Sensor1, Sensor2, etc.
- **Match All:** Select this option to include all sensors under the specified type.

Assertion Condition (BIT EVENT): This setting specifies the conditions under which the event filter will be triggered. You can select multiple conditions.

Save the Settings: Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.

2-6-1-2 SNMP Trap Configuration

SNMP (Simple Network Management Protocol) TRAPs allow the system to send notifications to a network management system when specific events occur.



Navigate to Alerts Page: Go to the Settings Alerts and find the SNMP Trap sections.

Configure SNMP TRAP:

LAN Channel Selection: Choose between Shared NIC or Dedicated NIC for SNMP TRAP.

Note: Each LAN Channel's settings are saved separately, but only one set of settings can be saved at a time.

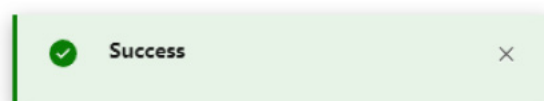
SNMP Version: Select the SNMP version to use:

SNMP v1/v2c:

- Enter the community string.

SNMP v3:

- **Authentication Protocol:** Choose the authentication protocol (e.g., MD5, SHA).
- **Authentication Passphrase:** Enter the authentication passphrase.
- **Security Level:** Select the security level:
 - **authNoPriv:** Authentication without privacy.
 - **authPriv:** Authentication with privacy, which requires additional settings:
 - **Privacy Protocol:** Choose the privacy protocol (e.g., DES, AES).
 - **Privacy Passphrase:** Enter the privacy passphrase.
 - **SNMP TRAP Destination:** Enter the SNMP TRAP destination IP address.
 - **Severity Level:** Set the severity level of events to be trapped.
- **Save the Settings:** Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.



2-6-1-3 Alert Destination

The screenshot displays the 'Alert Destination' configuration interface. On the left, a sidebar lists various system settings, with 'Alerts' currently selected. The main panel is titled 'Alert Destination' and contains the following elements:

- LAN Channel:** A dropdown menu showing 'Dedicated NIC (1)'.
- Enable Alerting:** A toggle switch that is currently turned on.
- Alert Destination #1 to #5:** Five identical configuration blocks. Each block has:
 - SNMP:** A selected radio button, a label 'Send SNMP Alerts to IP', and an input field containing 'IP:default port 162'.
 - Email:** An unselected radio button, a label 'Send Email to', and an input field containing 'mail@example.com'.
- Buttons:** 'Save' and 'Send Test Alert' buttons at the bottom.

Navigate to the Alert Page: Find the Alert Destination section.

LAN Channel Selection:

Select LAN Channel:

- **Select LAN Channel:** Choose either Dedicated NIC or Shared NIC from the dropdown menu. Each NIC has its own separate configuration.
- **Enable Alerting:** Toggle the switch to enable or disable alerting for the selected NIC.
- **StartTLS Enable:** Enable or disable StartTLS for the SMTP connection.

Configure Destinations:

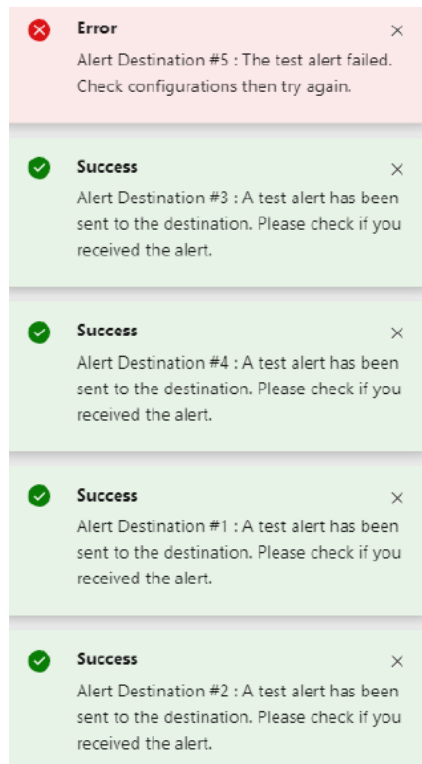
You can configure up to 5 alert destinations. For each destination, you can choose between SNMP and Email.

- **Alert Destination #1 to #5:**
 - **SNMP:**
 - **Select SNMP:** Choose the SNMP option to send SNMP alerts.
 - **Enter IP Address:** Provide the IP address and port for SNMP alerts in the format 192.168.1.1:1234. If no port is specified, the default port 162 will be used.
 - **Email (SMTP):**
 - **Select Email:** Choose the Email option to send alerts via email.
 - **Enter Email Address:** Provide the email address to which alerts should be sent.

Save the Settings: Click the Save button to save your configurations for the selected NIC.

Send Test Alert: You can click the Send Test Alert button to test the alert settings.

- The system sequentially dispatches alert messages to each configured destination and automatically bypasses any entries with undefined parameters (i.e., missing IP address or email address).
- During the test procedure, the system generates a diagnostic email or SNMP trap containing no operational data; its sole purpose is to validate the alert configuration and verify network connectivity between the host system and the designated SNMP server.
- For each transmission attempt, the interface displays either a success or failure status, as illustration below:



- If an alert transmission fails, verify that the selected NIC has proper network reachability to the target SNMP or SMTP server, and ensure that the SMTP email parameters are correctly configured.

2-6-1-4 Alert Example

- Enter the string you want to display.
 - Real sensor events can be directly selected in the PEF configuration via the WebUI by specifying the sensor type and name.
 - Virtual sensor events, such as those generated by the BIOS, cannot be directly selected and require specific settings.
- Since System Event Log (SEL) entries generated by the BIOS or by virtual sensors are not associated with any physical BMC sensors, the PEF alert mechanism cannot match them using standard sensor identifiers. To enable PEF alert handling for these SELs, configure the Sensor Type and Sensor Name fields to “Match All”, and specify the appropriate Assertion Condition bits required for the intended event-trigger behavior.
- If the event is from a real sensor on the BMC, please refer to examples **System Event Log Cleared** and **All Temperature sensor** upper threshold. For BIOS or Virtual Sensor Events, refer to examples **BIOS Event (Example of Critical Interrupt: PCIe AER Error)** and **BIOS Event(Example of Memory: Correctable ECC & Uncorrectable ECC)**.

The table below lists the BIOS events and virtual sensor events:

From	Sensor Type	Assertion Condition bit(s)
BMC	Memory	0,1,4
BMC	Critical Interrupt	4,5

2-6-1-5 System Event Log Cleared

1. Go to **Setting->Alert email** and **SMTP** setup page.

The screenshot shows the 'Alert email' configuration page in the Supervise OPF interface. The left sidebar contains a menu with options: Overview, Dashboard, Logs, Hardware status, Operations, Factory reset, KVM, Firmware, Reboot BMC, and SOL console. The main content area is titled 'Alert email' and contains an 'SMTP' section. The SMTP configuration fields are: SMTP Server (Domain/IPv4/IPv6 Address), Sender Email Address, SMTP User, SMTP Password (with a toggle for visibility), SMTP Server Port Number (set to 25), and SMTP SSL/TLS Enable (with radio buttons for On and Off, currently set to Off).

2. Go to **Setting->Alert ->** and **Alert Destination** setup page. Save the settings, and then click Send Test Alert. You will receive a email intended for testing purposes only, containing no real information.

The screenshot shows the 'Alert Destination' configuration page in the Supervise OPF interface. The left sidebar contains a menu with options: Server power operations, Virtual front panel, Virtual Media, Boot config, Settings, Alerts, Alert policies, Alert email, Date and time, Networks, VLAN, SOL, SNMP, iKVM and virtual media, Dynamic DNS, Syslog settings, Backup restore, and Power restore policy. The main content area is titled 'Alert Destination' and contains a 'LAN Channel' dropdown (set to 'Dedicated NIC (1)'), an 'Enable Alerting' toggle (set to On), and five 'Alert Destination' entries. Each entry has radio buttons for 'SNMP' (selected) and 'Email', and fields for 'Send SNMP Alerts to IP' (set to 'IP:default port 162') and 'Send Email to' (set to 'mail@example.com'). A 'Send Test Alert' button is visible on the right side of the page.

Event that generated this alert:

RID:FFFE TS:12/31/1969 23:59:59 SN:Test Trap ST:Platform Alert ED:Platform Event trap generated ET: EC:OK

RID:FFFE RT:00 TS:65920B5A GID:0040 ER:03 ST:24 S#:00 ET:6F ED:02 80 00 EX:00 00 00 00 00 00 00 00

3. Set up the PEF and save the configuration. In the following example, the SEL cleared is used to illustrate the procedure.

Modify PEF Configuration ×

Enter the information for the alert below and press Save.

Event Filter Enable

☒

Alert

☒

Event Filter Action

☐ Power Off ☐ Reset ☐ Power Cycle

☐ Graceful Shutdown ☐ Diagnostic Interrupt

Policy Set

1

Sensor Type

Event Logging Disabled

Sensor Name

SEL

Assertion Condition

☐ bit0 Correctable Memory Error Logging Disabled

☐ bit1 Event 'Type' Logging Disabled.

☒ bit2 Log Area Reset/Cleared

☐ bit3 All Event Logging Disabled

☐ bit4 SEL Full.

☐ bit5 SEL Almost Full.

☐ bit6 Correctable Machine Check Error Logging Disabled

4. Go to **Alert Policies** Page, set up the Policies.

Policy Table ×

Group Number

1

Enable

☒

Action

always send alert to this destination

LAN Channel

Shared NIC (2)

Destination Selector

1

Event Specific Alert String

☐

Alert String Key

1

Cancel

Save

5. Set up Alert String Key

Strings Table ×

No.

1

Alert String Key

alert string example

Cancel

Save

6. Go to **System Event Log** Page and clear log.

Supervise OPF

Reserved GB300 Station 1650226120723

Health

Power

Refresh

root

Overview

Dashboard

Logs

Hardware status

Operations

Factory reset

KVM

Firmware

Reboot BMC

SOL console

Server power operations

Virtual front panel

Virtual Media

Boot config

Settings

Alerts

Alert policies

Alert email

Date and time

Networks

VLAN

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Syslog settings

Use this page to collect system debug information about the server.

Basic Setting

Enable Syslog

Syslog Level

Kernel Log

Kernel Log Level

Save

Log to Remote Server

Redirect Syslog to Remote Server

Remote Syslog Server Address

Protocol

Remote Facility

Save

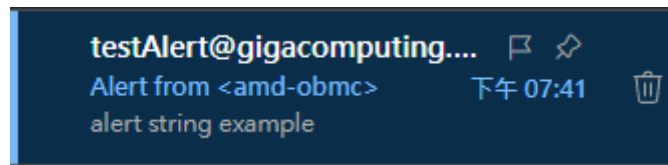
Reset to Default

Click button to reset all syslog settings to default value.

Warning: This action will clean remote server and all filters.

Reset

7. Check mailbox.



2-6-1-6 All Temperature sensor upper threshold

- After configuring the PEF settings, save the configuration. In the following example, the Upper Threshold of the All Temperature Sensors group is used to illustrate the procedure.

Modify PEF Configuration

Enter the information for the alert below and press Save.

Event Filter Enable

Alert

Event Filter Action

Policy Set

Sensor Type

Sensor Name

Assertion Condition

Power Off

Reset

Power Cycle

Graceful Shutdown

Diagnostic Interrupt

1

Temperature

Match All

bit0 (LNC going low for threshold)

bit1 (LNC going high for threshold)

bit2 (LC going low for threshold)

bit3 (LC going high for threshold)

bit4 (LNR going low for threshold)

bit5 (LNR going high for threshold)

bit6 (UNC going low for threshold)

bit7 (UNC going high for threshold)

bit8 (UC going low for threshold)

bit9 (UC going high for threshold)

bit10 (UNR going low for threshold)

bit11 (UNR going high for threshold)

Cancel

Save

2. When Sensor Name is set to Match All, the Assertion Condition field does not display a description of the corresponding event, as each sensor type may have different event definitions and settings. For instance, in the case of a temperature sensor, bit 7 and bit 9 typically represent “UNC Going High” and “UC Going High”, respectively.
3. Go to **Alert Policies** Page, set up the Policies.

Policy Table

×

Group Number

1

Enable

☒

Action

always send alert to this destination

LAN Channel

Shared NIC (2)

Destination Selector

1

Event Specific Alert String

☒

Alert String Key

1

Cancel

Save

4. Raise the temperature to above the threshold.
5. Check mailbox.
 - In the following example, shows two Temperature sensor crossed the threshold.
 - CPU0_TEMP
 - VDDCR_0_P0_TMP

Event that generated this alert:

RID:0004 TS:08/06/2024 01:23:56 SN:CPU0 TEMP ST:Temperature ED:Upper Non-critical - going high ET:Asserted EC:Non-Critical

RID:0004 RT:02 TS:66B17B2C GID:0020 ER:04 ST:01 S#:01 ET:01 ED:57 5F EX:01 FF FF FF FF FF FF

Event that generated this alert:

RID:0007 TS:08/06/2024 01:28:55 SN:VDDCR 0 P0 Temperature ST:Temperature ED:Upper Critical - going high ET:Asserted EC:Critical

RID:0007 RT:02 TS:66B17C57 GID:0020 ER:04 ST:01 S#:0E ET:01 ED:59 3B EX:02 FF FF FF FF FF FF

2-6-1-7 BIOS Event (Example of Critical Interrupt: PCIe AER Error)

Modify PEF Configuration

Enter the information for the alert below and press Save.

Event Filter Enable

Alert

Event Filter Action

Power Off

Reset

Power Cycle

Graceful Shutdown

Diagnostic Interrupt

Policy Set

1

Sensor Type

Match All

Sensor Name

Match All

Assertion Condition

bit0 assertion event

bit1 assertion event

bit2 assertion event

bit3 assertion event

bit4 assertion event

bit5 assertion event

bit6 assertion event

bit7 assertion event

bit8 assertion event

bit9 assertion event

bit10 assertion event

bit11 assertion event

bit12 assertion event

bit13 assertion event

bit14 assertion event

Cancel

Save

Event that generated this alert:

RID:000B TS:08/06/2024 01:40:36 SN:Bios Event ST:Critical Interrupt ED:Front Panel NMI / Diagnostic Interrupt ET:Asserted EC:Critical
RID:000B RT:02 TS:66B17F14 GID:0001 ER:04 ST:13 S#:21 ET:6F ED:00 FF EX:02 00 00 00 00 00 00

Event that generated this alert:

RID:0010 TS:08/06/2024 01:47:48 SN:Bios Event ST:Critical Interrupt ED:PCI SERR(PCI Bus=0x0 Dev=0xA Func=0x0) ET:Asserted EC:Critical
RID:0010 RT:02 TS:66B180C4 GID:0003 ER:04 ST:13 S#:08 ET:6F ED:A5 00 50 EX:02 00 00 00 00 00 00

2-6-1-8 BIOS Event(Example of Memory: Correctable ECC & Uncorrectable ECC)

As described in the BIOS Event section, BIOS-generated events do not correspond to actual BMC sensors. Therefore, for PEF configuration, both Sensor Type and Sensor Name should be set to “Match All”, and all relevant Assertion Condition bits should be selected in this example.

Modify PEF Configuration

Enter the information for the alert below and press Save.

Event Filter Enable

Alert

Event Filter Action

Policy Set

Sensor Type

Sensor Name

Assertion Condition

Power Off

Reset

Power Cycle

Graceful Shutdown

Diagnostics Interrupt

1

Match All

Match All

☒ bit0 assertion event

☒ bit1 assertion event

☒ bit2 assertion event

☒ bit3 assertion event

☒ bit4 assertion event

☒ bit5 assertion event

☒ bit6 assertion event

☒ bit7 assertion event

☒ bit8 assertion event

☒ bit9 assertion event

☒ bit10 assertion event

☒ bit11 assertion event

☒ bit12 assertion event

☒ bit13 assertion event

☒ bit14 assertion event

Cancel

Save

Event that generated this alert:

RID:0010 TS:08/06/2024 01:47:48 SN:Bios Event ST:Critical Interrupt ED:PCI SERR(PCI Bus=0x0 Dev=0xA Func=0x0) ET:Asserted EC:Critical

RID:0010 RT:02 TS:66B180C4 GID:0003 ER:04 ST:13 S#:08 ET:6F ED:A5 00 50 EX:02 00 00 00 00 00 00

Event that generated this alert:

RID:0004 TS:08/15/2024 15:18:48 SN:Bios Event ST:Memory ED:Uncorrectable ECC / other uncorrectable memory error(DIMM_F0) ET:Asserted EC:Critical

RID:0004 RT:02 TS:66BE1C58 GID:0003 ER:04 ST:0C S#:08 ET:6F ED:A1 00 50 EX:02 00 00 00 00 00 00

Please refer **Appendix** for **Assertion Condition (BIT EVENT) References**

Gigabyte Server Management Console

- 57 -

2-6-2 Alert policies

This page allows administrators to configure and manage alert policies, defining specific action rules, transmission channels, and custom string keys for system event notifications.

To open this page, click Alert policies under the Settings section from the menu bar. It displays the following sections:

2-6-2-1 Policies

This table displays the list of defined alerting rules (up to 20 entries). Click the Edit icon (pencil) at the end of each row to modify the policy.

2-6-2-2 Alert String Key

This section displays a list of customizable text entries (up to 40 entries) used to map event messages to user-defined strings. Click the Edit icon (pencil) to configure or modify the string contents for each index.

Supervyse **OPF**

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Overview

Dashboard

Logs

Hardware status

Operations

Factory reset

KVM

Firmware

Reboot BMC

SOL console

Server power operations

Virtual front panel

Virtual Media

Boot config

Settings

Alerts

Alert policies

Alert email

Date and time

Networks

VLAN

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Backup restore

Alert policies

Policies

Policy Table: 20 entries

No.	Group Number	Enable	Action	LAN Channel	Destination Selector	Event Specific Alert String	Alert String Key
1	1	Yes	always send alert to this destination	1	1	No	N/A
2	1	Yes	always send alert to this destination	1	2	No	N/A
3	1	Yes	always send alert to this destination	1	3	No	N/A

For the options marked with an asterisk: if alert to previous destination was successful, do not send alert to this destination.

Alert String Key

Strings Table: 40 entries

No.	Strings
1	
2	
3	
4	

2-6-3 Alert Email

Display alert email information.

Supervise OPF | Reserved GB300 Station 1650226120723 Health Power Refresh root

Alert email

SMTP

SMTP Server Domain/IPv4/IPv6 Address

Sender Email Address

SMTP User

SMTP Password

SMTP Server Port Number

SMTP SSL/TLS Enable ☐ On ☒ Off

STARTTLS Enable ☐ On ☒ Off

Authentication Method ☐ On ☐ Manual ☒ Off

Navigate to the Alert Email Page: Find the Alert Email section.

Configure SMTP Settings:

- **SMTP Server Domain/IPv4/IPv6 Address:** Enter the domain name or IP address (IPv4/IPv6) of the SMTP server.
- **Sender Email Address:** Provide the email address that will appear as the sender of the alert emails
- **SMTP User:** Enter the username for the SMTP server authentication.
- **SMTP Password:** Enter the password for the SMTP server authentication.
- **SMTP Server Port Number:** Specify the port number used by the SMTP server (commonly 25, 465, or 587).
- **SMTP SSL/TLS Enable:** Enable or disable SSL/TLS encryption for the SMTP connection.
 - Options: On / Off
- **StartTLS Enable:** Enable or disable StartTLS for the SMTP connection.
 - Options: On / Off
- **Authentication Method:** Choose the method of authentication for the SMTP server.
 - Options: On / Manual / Off
 - On: The system will automatically handle authentication.
 - Manual: If selected, choose one of the following methods:
 - PLAIN: Simple base64-encoded authentication.
 - CRAM-MD5: Challenge-response authentication mechanism.
 - EXTERNAL: Use an external mechanism for authentication.
 - LOGIN: Two-step authentication with separate username and password steps.
 - Off: No authentication will be used.

Important Notes:

Click **Save** button to save all configurations.

- **SSL/TLS and STARTTLS:** Only one of these should be enabled at a time. If both are enabled, STARTTLS will typically be used.
 - **SSL/TLS:** Provides encryption from the start of the connection on a dedicated port (commonly port 465).
 - **STARTTLS:** Begins as an unencrypted connection and then switches to encryption after the STARTTLS command is issued (commonly used on ports 25 or 587).
- **Authentication Method:** If "Off" is selected for Authentication Method, SSL/TLS and STARTTLS settings will

not be used.

Save the Settings: Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.

2-6-4 Date and Time

Supervise OPF | Reserved GB300 Station 1650226120723 Health Power Refresh root

Reboot BMC
SOL console
Server power operations
Virtual front panel
Virtual Media
Boot config
Settings
Alerts
Alert policies
Alert email
Date and time
Networks
VLAN
SOL
SNMP
iKVM and virtual media
Dynamic DNS
Syslog settings
Backup restore

Date and time

To change how date and time are displayed (either UTC or browser offset) throughout the application, visit [Profile Settings](#)

NTP

☐ NTP Enable

☐ Use NTP servers (DHCP)

Primary NTP Server Secondary NTP Server

Date 24-hour time (UTC)

YYYY-MM-DD HH:MM

2026-06-17 14:28

Save Sync from RTC

Time Zone

The time zone setting will valid after BMC reboot.

NTP Enable

Enable/disable NTP service.

Primary NTP Server

Secondary NTP Server

Date (YYYY-MM-DD)

Time (24-hour)(HH:MM)

NOTE: The date and time can not be set more than Tue Jan 19 03:14:07 2038 .

Sync from RTC

Click the 'Sync from RTC' button to Synchronize BMC system time from BMC RTC time.

Save

Click the 'Save' button to save the new Date Time configuration.

If NTP is enable, just only update BMC system time.

If NTP is disable, update BMC system time and BMC RTC time.

2-6-5 Networks

This page provides configure IPMI Lan Channel settings for the BMC.

Supervise OPF | Reserved GB300 Station 1650226120723 Health Power Refresh root

Reboot BMC
SOL console
Server power operations
Virtual front panel
Virtual Media
Boot config
Settings
Alerts
Alert policies
Alert email
Date and time
Networks
VLAN
SOL
SNMP
iKVM and virtual media
Dynamic DNS
Syslog settings
Backup restore

Networks

Configure IPMI LAN Channel settings for the BMC

LAN Channel

MAC address

Hostname

Save settings

IPv4 Network Settings

IPv6 Network Settings

- Lan Failover
 - Enable: Bind all interfaces together.
 - Disable: Each interface has its own configuration.
- Lan channel: Select LAN channel to configure.
- MAC address: Set MAC address.
- Hostname: Set host name.
- IPv4 Network Settings
- IPv6 Network Settings

IPv4 Network Settings

Network interface

- Link Disabled: This option disables the network interface.
- Static IP Address: This option allows you to manually configure the network settings by assigning a fixed IP address, subnet mask, and gateway.
- DHCP Enabled: This option enables the network interface to automatically obtain an IP address, subnet mask, and gateway from a DHCP server.

Gateway

When using a static IP, you manually set the gateway; with DHCP, it's provided automatically.

IP Address

An IP address is a unique identifier assigned to each device on a network.

Subnet mask

A subnet mask defines the network and host portions of an IP address, allowing devices to identify which network they belong to.

DNS Server

The Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or any

resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

Note

1. An IPv4 address consists of 32 bits, divided into four groups (or blocks) of 8 bits each, written in decimal and separated by dot (".").
2. Each group ranges from 0 to 255
3. First group must not be 0 (IP address range 0.0.0.0/8 is reserved exclusively as a source address).
4. When the network source changes from DHCP to Static, the Static IP, Subnet Mask, and Gateway settings remain the same as those provided by the DHCP source.

IPv6 Network Settings

Network interface

- **Link Disabled:** This option disables the network interface.
- **Link Enabled:** This option enables the network interface.

Gateway (Static)

This setting allow you to manually configure a gateway for the network, even if DHCPv6 or SLAAC (Stateless Address Autoconfiguration) is enabled. When a static gateway address is set, it takes precedence over any dynamically assigned gateway address provided by DHCPv6/SLAAC. This means that even if DHCPv6/SLAAC is enabled and assigns a dynamic gateway address, the system will prioritize the static gateway address for network routing.

Gateway (Dynamic)

This setting allow user to configure a gateway dynamically. It dynamically configures ipv6 address using DHCP (Dynamic Host Configuration Protocol).

Link-local address

Link-local address is a type of IPv6 address that is automatically configured and used for communication within a local network segment. These addresses are not routable across the broader internet and are only valid within a single network link. They start with the prefix fe80::/10, and each device on a network segment uses a unique Link-local address to communicate directly with other devices on the same link.

DHCPv6/IPv6 DHCPv6/SLAAC

IPv6 DHCPv6 and SLAAC can be set to either enable or disable to control how an IPv6 address is assigned to a device. DHCPv6 and SLAAC are enabled simultaneously, where SLAAC assigns the address, and DHCPv6 provides additional network configuration like DNS servers.

If this option is enabled, dynamic IP address and its prefix length will be displayed.

IP Address

A static IPv6 address that is manually assigned and does not change over time. When a static IPv6 address is configured, it takes priority over any dynamically assigned IP addresses (from DHCPv6 or SLAAC). Even if the device also receives a dynamic address, the static address will be preferred for outbound communication, routing, or any services bound to it.

DNS Server

As same as ipv4 DNS Server settings but using ipv6 address.

Note

1. Unlike IPv4, an IPv6 interface can have multiple addresses, such as link-local, global, and unique local addresses.
2. You can setup only one static ipv6 address.
3. An IPv6 address consists of 128 bits, divided into eight groups (or blocks) of 16 bits each, written in hexadecimal

and separated by colons (":"). For example 2001:0db8:85a3:0000:0000:8a2e:0370:7334

4. Each block represents 16 bits, and leading zeros in each block can be omitted for brevity. Additionally, consecutive blocks of zeros can be replaced with "::" once in an address.

Save settings

Click the 'Save settings' button to save the new Date Time configuration.

2-6-6 VLAN

This page is used to configure BMC VLAN settings.

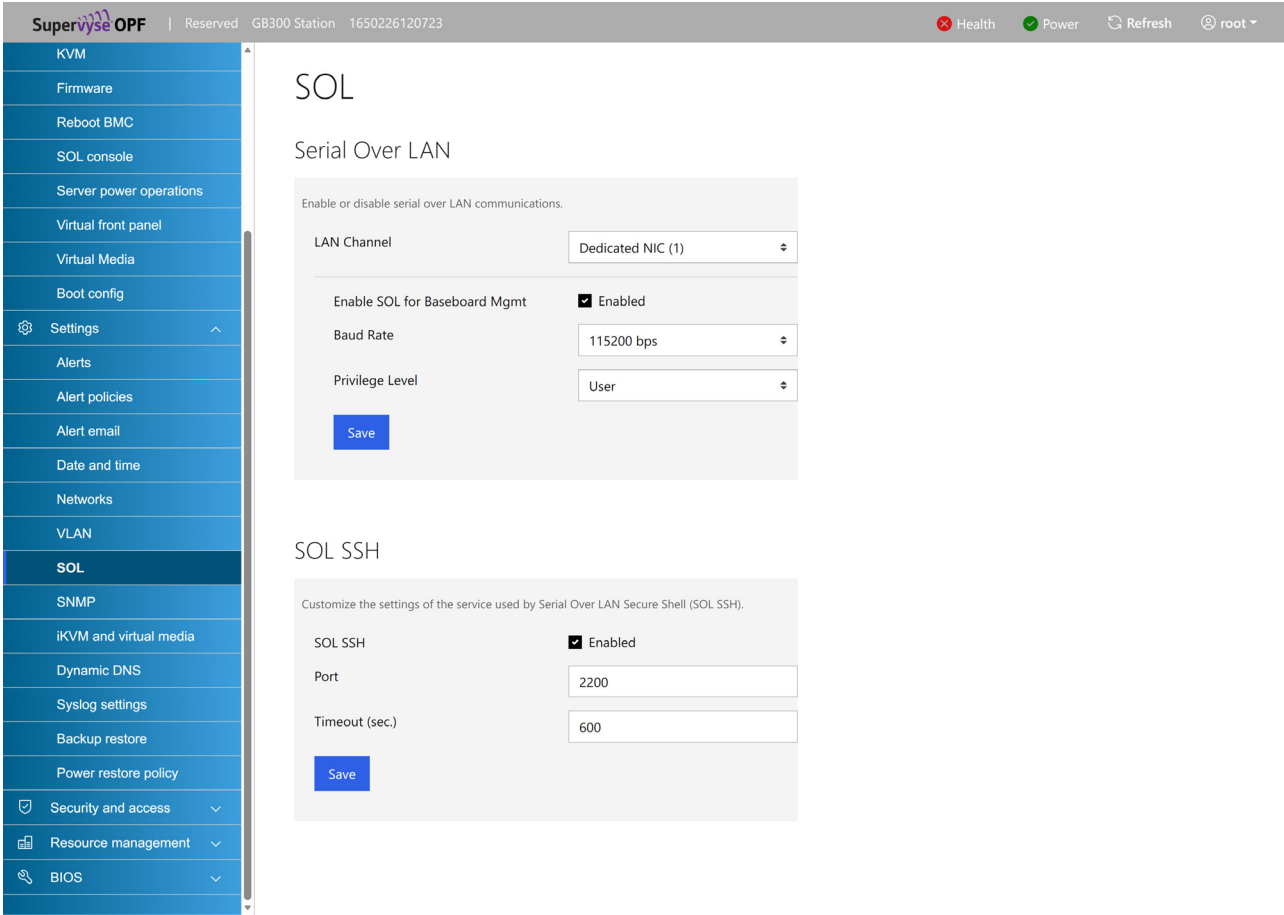
The screenshot shows the Supervise OPF web interface. The top header includes the logo, system information (Reserved GB300 Station 1650226120723), and status indicators for Health (red X), Power (green checkmark), Refresh, and a user dropdown (root). A left sidebar contains a menu with items like Reboot BMC, SOL console, Server power operations, Virtual front panel, Virtual Media, Boot config, Settings (selected), Alerts, Alert policies, Alert email, Date and time, Networks, VLAN (highlighted), SOL, SNMP, iKVM and virtual media, Dynamic DNS, Syslog settings, and Backup restore. The main content area is titled 'VLAN' and includes a description: 'Use this page to configure an 802.1Q VLAN private network on the specified LAN channel.' Below this, there are configuration fields: 'LAN Channel' with a dropdown menu showing 'Dedicated NIC (1)', 'Enable VLAN' with a toggle switch, 'VLAN ID' with a text input field containing '0', and 'VLAN Priority' with a text input field containing '0'. A blue 'Save' button is located at the bottom left of the configuration area.

- Lan channel: Select LAN channel to configure.
- Enable VLAN: Enable/disable VLAN.
- VLAN ID: 1-4094
- VLAN Priority: 0-7

Save

Click the 'Save' button to save the VLAN configuration.

2-6-7 SOL



Serial Over LAN

Enable or disable serial over LAN communications.

Enable or disable Serial Over LAN for each LAN channel.

LAN Channel

Select which LAN Channel.

Enable SOL for Baseboard Mgmt

Click for enable or disable SOL for Baseboard Mgmt.

Baud Rate

9600 bps/19200 bps/38400 bps/57600 bps/115200 bps can be selected.

Flow Control

The options are None, RTS/CTS, and XON/XOFF.

Privilege Level

The options are User/Operator and Administrator.

SOL SSH

Customize the settings of the service used by Serial Over LAN Secure Shell (SOL SSH).

Allows changing the settings about service enable/disable, timeout and port used by the SOL (Serial Over LAN) SSH. Changing this setting will immediately terminate all the sessions which are using SOL SSH service.

SOL SSH

Checking/Unchecking the checkbox to enable/disable SOL SSH service.

Port

Port range is 1 ~ 65535.

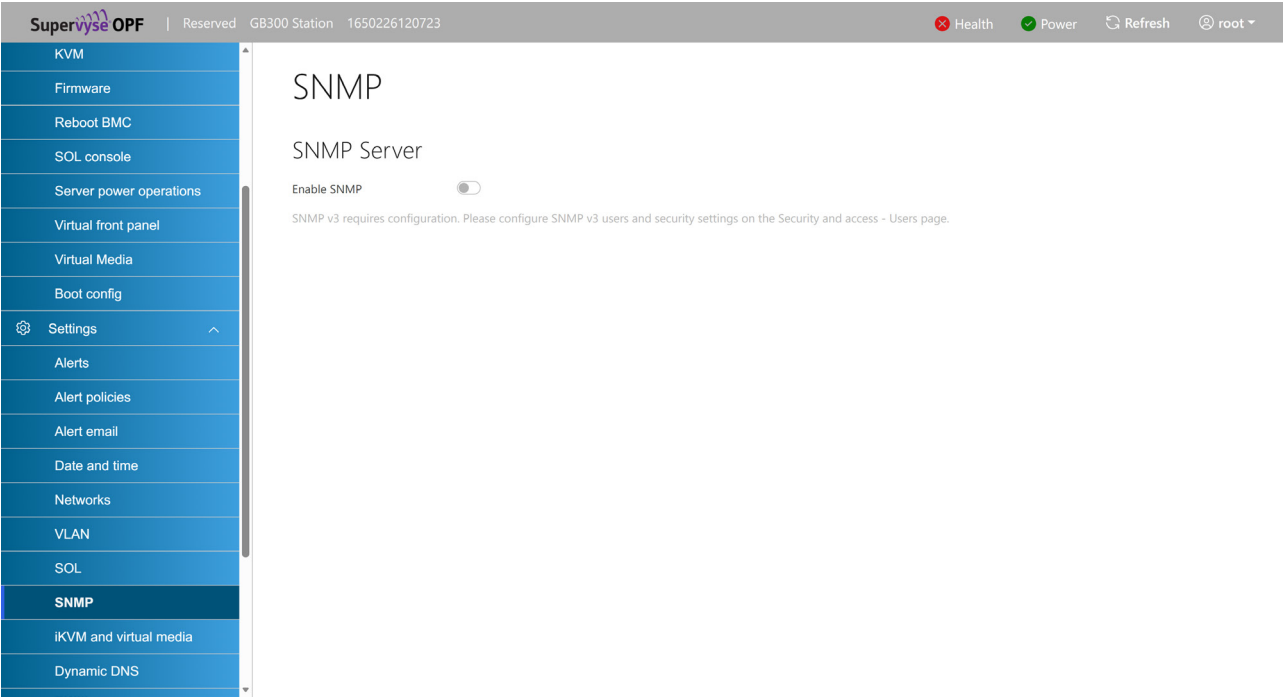
Timeout (sec.)

Timeout used for the idle sessions. (Units: seconds, default: 600, Range: 60-65535).

Save

Click the 'Save' button to save the SOL SSH configuration.

2-6-8 SNMP



SNMP Server

Enable SNMP

Enable/disable SNMP Server.

Enable SNMP V1/V2

Enable/disable SNMP Server.

Read-Only Community String

Set read-only Community "public"

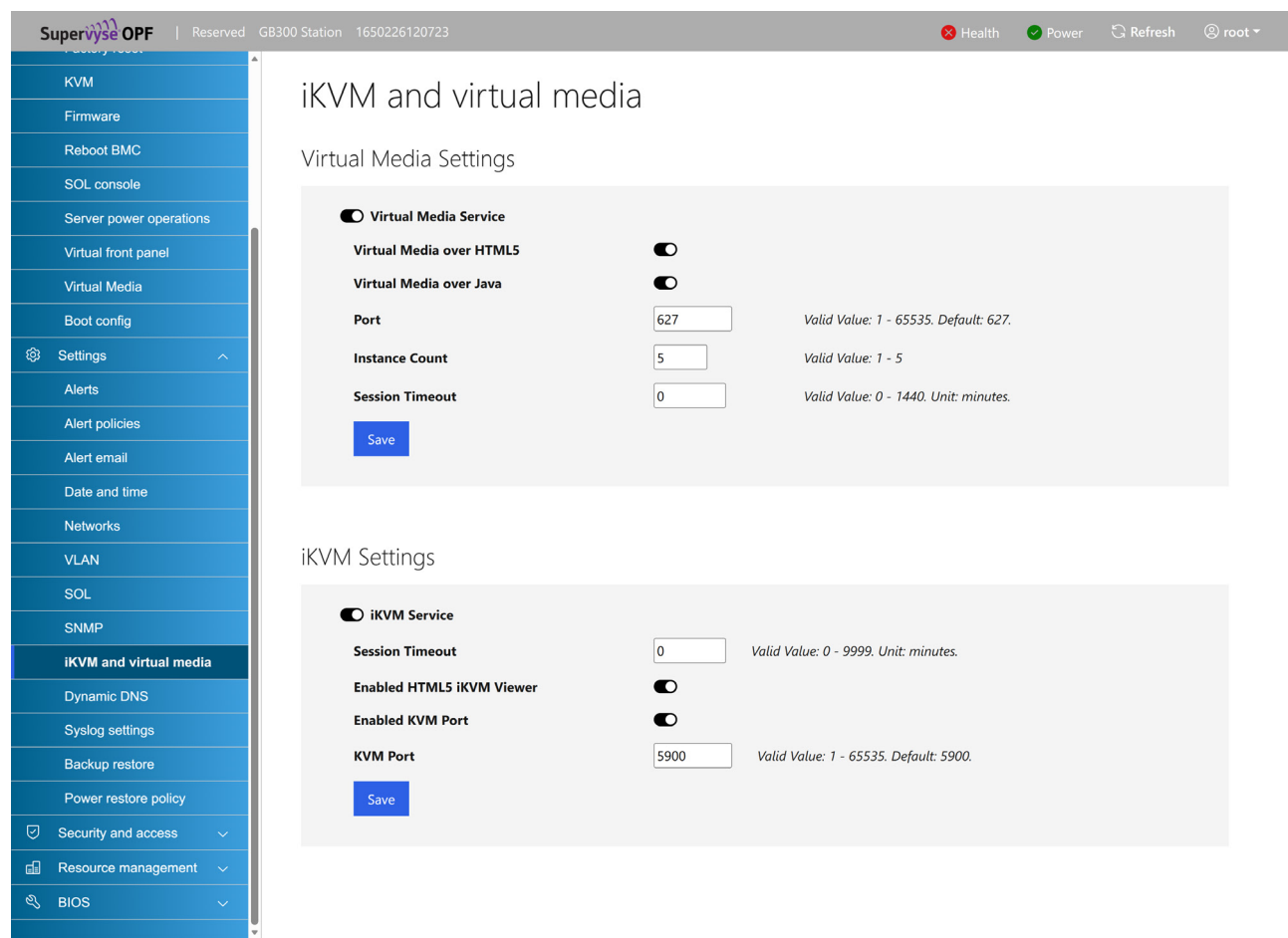
Read-Write Community String

Set read-write Community "public"

Save

Click the 'Save' button to save the configuration.

2-6-9 iKVM and virtual media



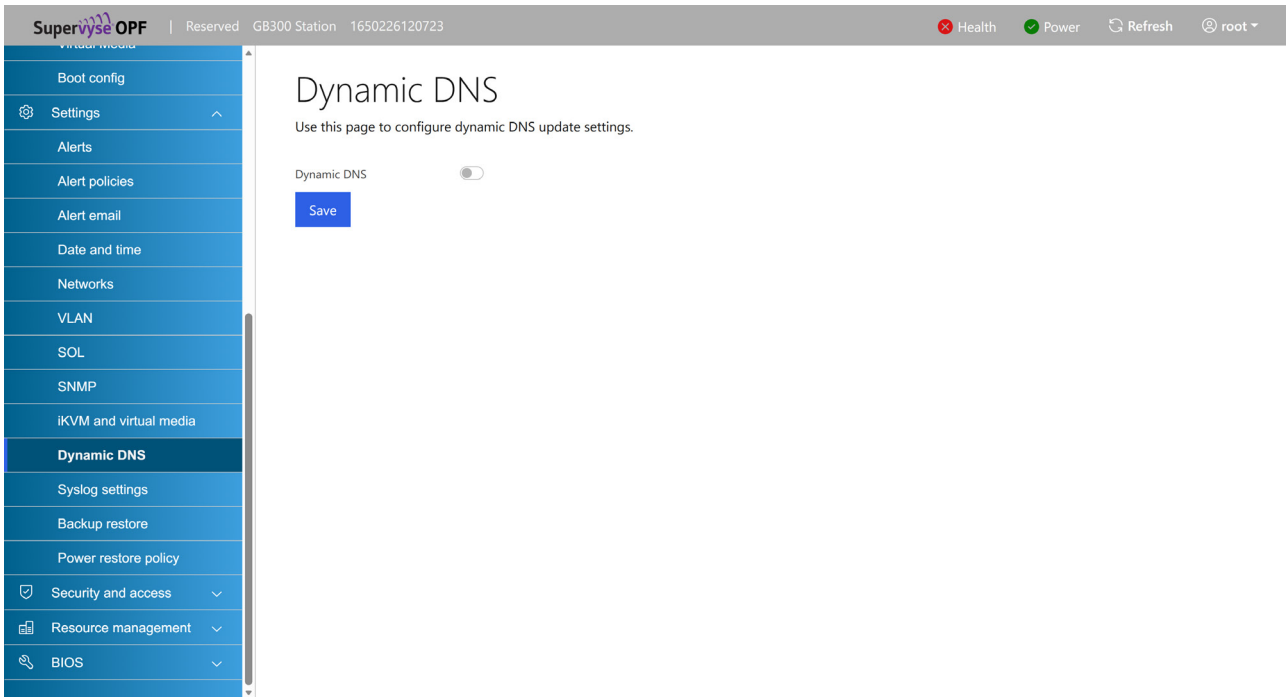
Virtual media settings

Display iKVM and Virtual Media.

Save

Click the 'Save' button to save the configuration.

2-6-10 Dynamic DNS



Use this page to configure dynamic DNS update settings. To open this page, click Dynamic DNS under the Settings section from the menu bar. It displays the following items:

Dynamic DNS

A toggle switch to enable or disable the Dynamic DNS (DDNS) feature on the system.

Save

Click this button to apply and save the configured Dynamic DNS settings.

2-6-11 Syslog settings

Syslog settings

Use this page to collect system debug information about the server.

Basic Setting

Enable Syslog: ☐

Syslog Level: 4 - Error (default)

Kernel Log: ☐

Kernel Log Level: 1 - Emergency (default)

Save

Log to Remote Server

Redirect Syslog to Remote Server: ☐

Remote Syslog Server Address: Please input IPv4 address

Protocol: ☒ UDP ☐ TCP
Syslog service will redirect log message to remote server port UDP:514 or TCP:618.

Remote Facility: 1 - user (default)

If remote log is disabled, the facility will be set as the user (default)

Save

Reset to Default

Click button to reset all syslog settings to default value.

Warning: This action will clean remote server and all filters.

Reset Restore syslog default settings.

Configuration File

Import File: 選擇檔案 沒有選擇檔案
Import: Select a valid DBG configuration file.

Export File: **Export** Press the button to export DBG configure file.

Use this page to collect system debug information about the server. To open this page, click Syslog settings under the Settings section from the menu bar. It displays the following sections

Basic settings

- **Enable Syslog:** A toggle switch to enable or disable the system log collection service.
- **Syslog Level:** A drop-down menu to select the logging severity level for the system (e.g., 4 - Error (default)).
- **Kernel Log:** A toggle switch to enable or disable specific kernel-level logging.
- **Kernel Log Level:** A drop-down menu to select the logging severity level for kernel events (e.g., 1 - Emergency).
- **Save:** Click this button to apply and save the configuration in the Basic Setting section.

Log to Remote Server

- **Redirect Syslog to Remote Server:** A toggle switch to enable or disable forwarding log messages to a remote

server.

- Remote Syslog Server Address: Enter the IPv4 address of the target remote Syslog server.
- Protocol: Select the transport protocol (UDP or TCP) used for forwarding logs. The service will redirect log messages to remote server port UDP:514 or TCP:618.
- Remote Facility: A drop-down menu to define the Syslog facility type (e.g., 1 - user (default)). If remote log is disabled, the facility will be set as the user (default).
- Save: Click this button to apply and save the configuration in the Log to Remote Server section.

Reset to Default

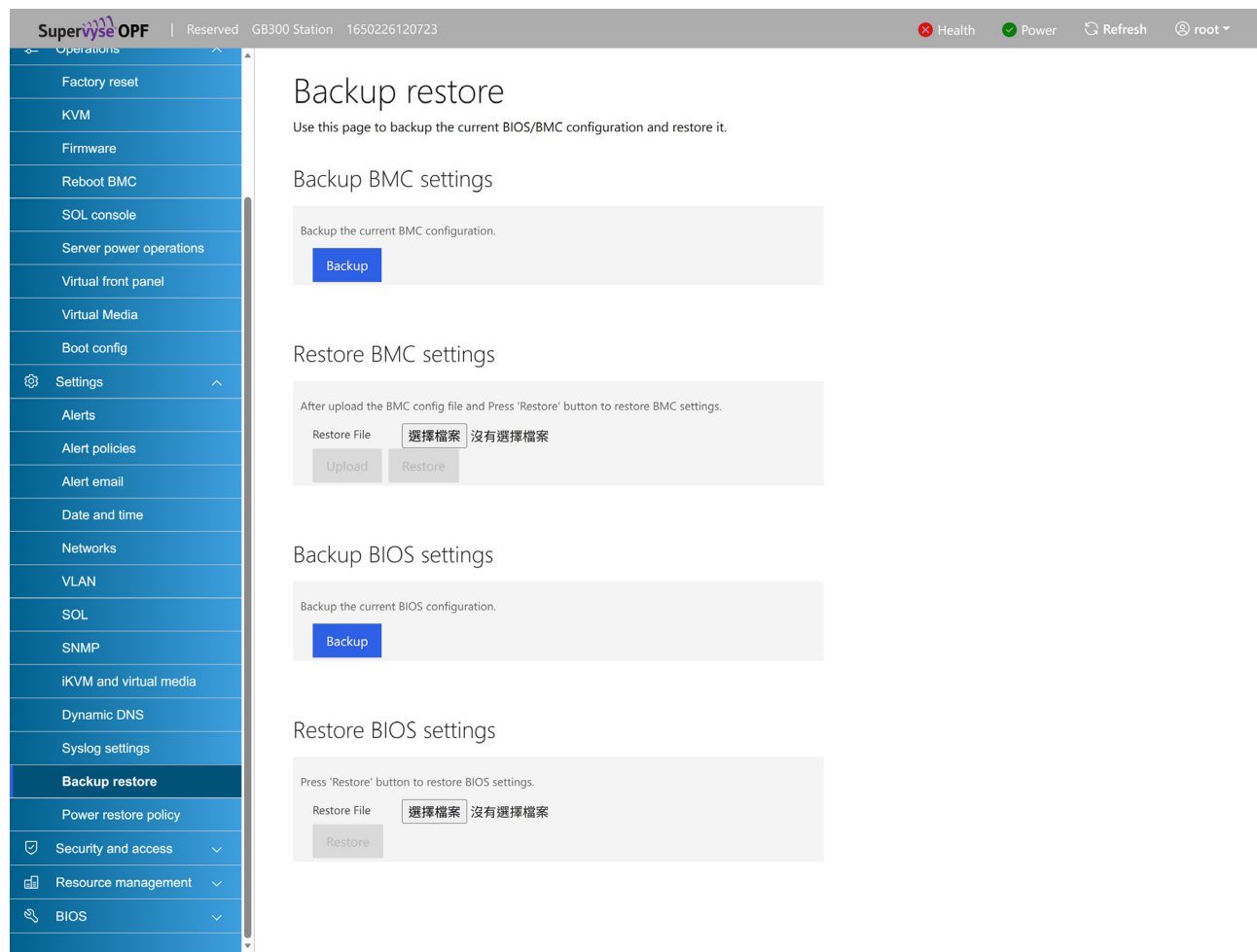
- Reset: Click this button to restore all syslog configurations back to their default values.
- Warning: This action will clean the remote server configuration and all filters.

Configure File

- Import File: Click 選擇檔案 (Choose File) to select a valid DBG configuration file from your local workspace, then click Import to upload and apply it.
- Export File: Click the Export button to download and save the current DBG configuration file to your local workspace.

2-6-12 Backup restore

Use this page to backup the current BIOS/BMC configuration and restore it.



Backup BMC settings

Click the 'Backup' button to backup the current BMC configuration.

Restore BMC settings

Click the 'Restore' button to restore BMC settings.

Backup BIOS settings

Click the 'Backup' button to backup the current BIOS configuration.

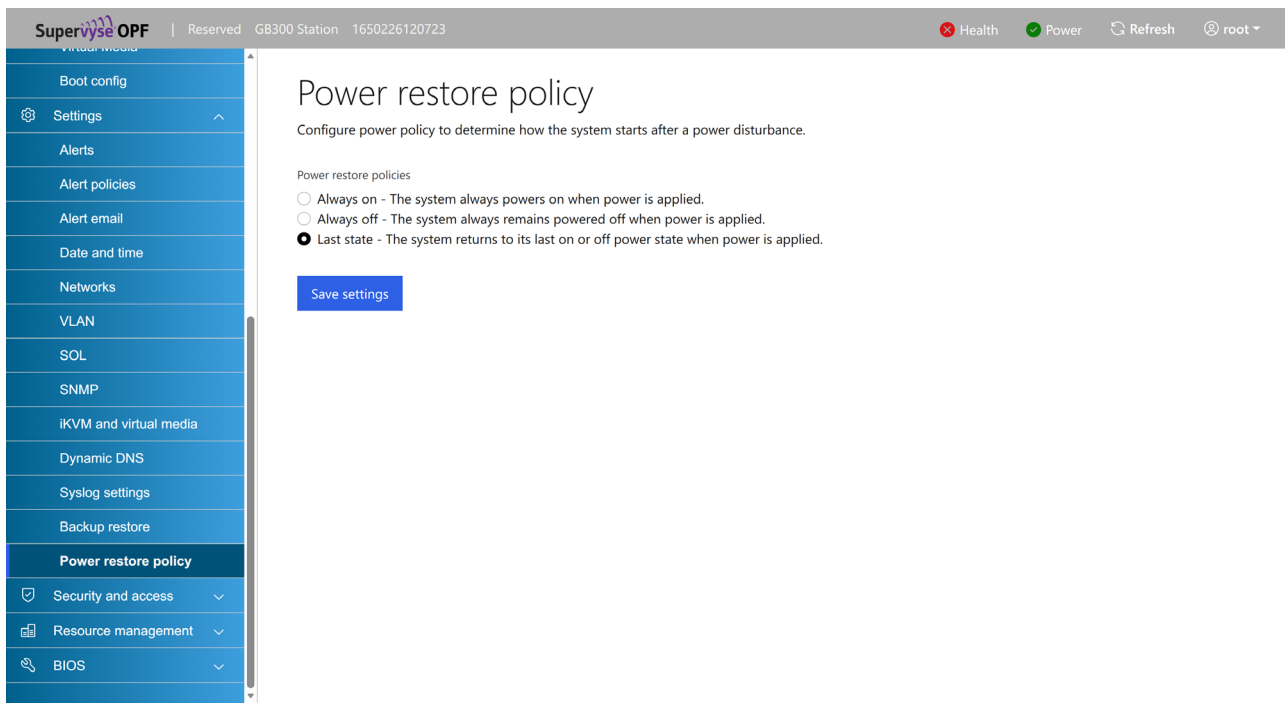
Restore BIOS settings

Click the 'Restore' button to restore BIOS settings.

2-6-13 Power restore policy

This page allows administrators to configure the power policy to determine how the system starts after a power disturbance or unexpected power loss event.

To open this page, click Power restore policy under the Settings section from the menu bar. It displays the following options:



Power restore policies

Select one of the following radio buttons to define the system recovery behavior when AC power is applied or restored.

- **Always on:** The system automatically powers on immediately when power is applied.
- **Always off:** The system remains powered off when power is applied, requiring a manual power-on command.
- **Last state:** The system automatically restores and returns to its last active power state (either on or off) before the power interruption occurred.

Save settings

Click this button to apply and save the selected power restore policy configuration to the system..\\

2-7 Security and access

2-7-1 Current users

This page is used to display Current Users.

SupervyseOPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Backup restore

Power restore policy

Security and access

Current users

LDAP

RADIUS

TACACS+

Users

Policies

Certificate management

Kerberos authentication

Security settings

IP access control

Resource management

Current users

Search sessions

1 item

	Username	Type	IP address	Kill session
☐	root (me)	Web (HTTPS)	10.8.133.57	Disconnect

20

Items per page

<

1

>

Web Session Timeout

30 Min(s)

Save

2-7-2 LDAP

The **Lightweight Directory Access Protocol (LDAP)/E-Directory** Settings is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

In Web GUI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the BMC. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group based policies to control access.

Supervise OPF

Reserved GB300 Station 1650226120723

Health Power Refresh root

Boot config

Settings

Alerts

Alert policies

Alert email

Date and time

Networks

VLAN

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Backup restore

Power restore policy

Security and access

Current users

LDAP

RADIUS

TACACS+

Users

Policies

Certificate management

Kerberos authentication

Security settings

IP access control

Resource management

BIOS

LDAP

Configure LDAP settings and manage role groups

Settings

LDAP authentication

Enable

Secure LDAP using SSL

A CA certificate and an LDAP certificate are required to enable secure LDAP

Enable

CA Certificate valid until

--

LDAP Certificate valid until

--

Manage SSL certificates

Service type

OpenLDAP

Active Directory

Server 1

Server URI

ldap://

Bind DN

Bind password

Leave empty to keep the pr

Base DN

User ID attribute - optional

Group ID attribute - optional

Save settings

Role groups

LDAP authentication must be enabled to modify role groups.

Add role group

Group name	Group privilege	Group domain
No items available		

Role groups

LDAP authentication must be enabled to modify role groups.

Add role group

Group name	Group privilege	Group domain
No items available		

2-7-2-1 Configuring on BMC server (Active Directory Login)

Settings

- Service type: Active Directory/OpenLDAP
- Server URI: Your AD server IP
- Bind DN: (AD user name)@(AD domain name)
 - e.g. good@adtest.local.com
- Bind password: AD user password
- Base DN: AD domain name
 - e.g. dc=adtest,dc=local,dc=com

Note: User ID and Group ID is optional and could keep empty

Gigabyte Server Management Console

- 76 -

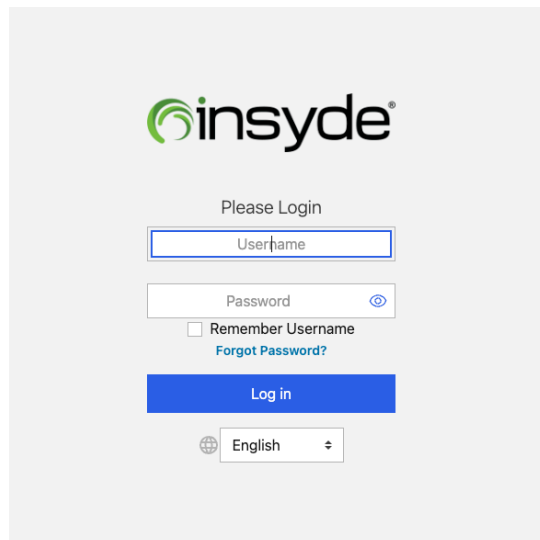
- Add role group
- Group name: Your AD user primary group
 - e.g. davidtest

Note: If you didn't setup AD user's primary group, default primary group will be Domain Users

- Group privilege: Select login access ability
 - e.g. Administrator

Active Directory Login

Web GUI login screen with AD user and password



OpenLDAP

Environment setup

Prompt when installing:

OS : Ubuntu 20.04

```
# sudo apt-get install slapd ldap-utils gnutls-bin ssl-cert
```

1. Administrator password => admin (Please input your LDAP admin password)
2. Confirm password => admin

Configuring slapd

In Ubuntu, there is a terminal UI to reconfigure slapd.

```
# sudo dpkg-reconfigure slapd Follow the steps below to set your environment:
```

1. Omit OpenLDAP server configuration? => No

2. DNS domain name => sc1.test (Domain name will be your base DN)
3. Organization name => bmc
4. Administrator password => admin (Please input your LDAP admin password)
5. Confirm password => admin
6. Do you want the database to be removed when slapd is purged => No
7. Move old database => yes

LDAP Browser/Editor After configuring LDAP is finished, reviewing or editing the LDAP tree can be done through the LDAP browser/editor application. We will use phpldapadmin for the following example:

1. Install phpldapadmin for LDAP management
sudo apt-get install phpldapadmin
2. Edit phpldapadmin configurations
sudo vi /etc/phpldapadmin/config.php

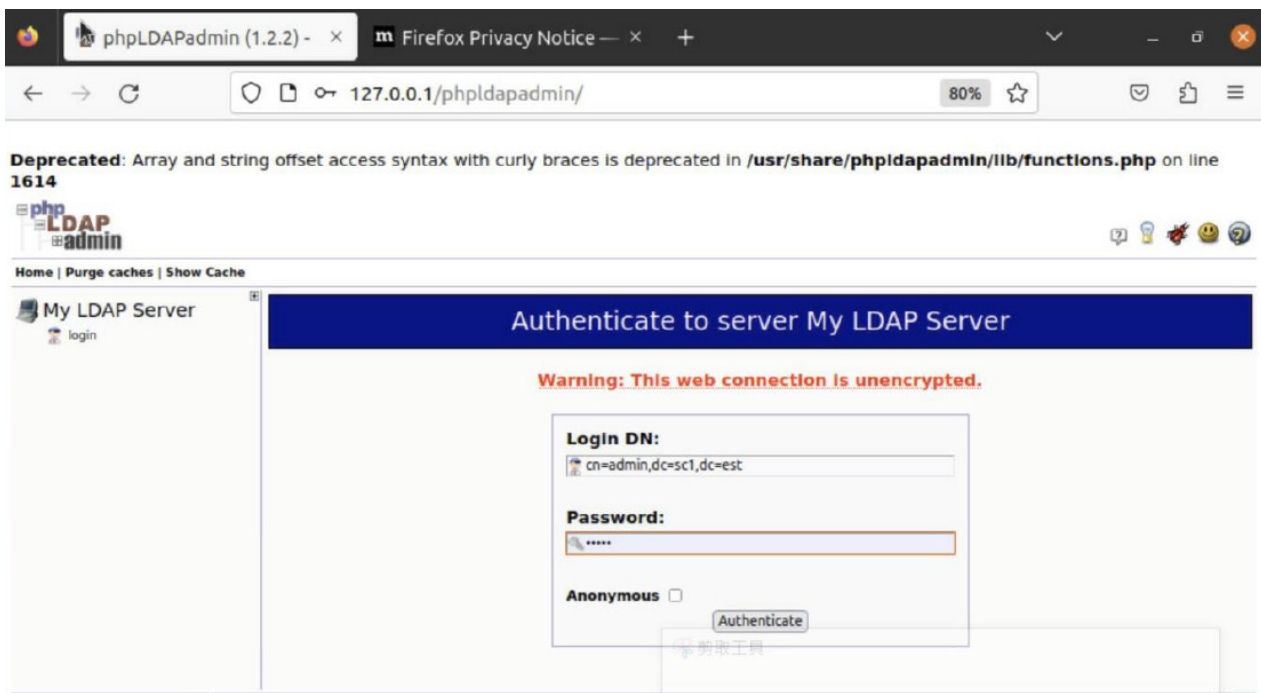
```
auto-detect it for you. */
$servers->setValue('server','base',array('dc=sc1,dc=test'));

/* Five options for auth_type:
1. 'cookie': you will login via a web form, and a client-side cookie will
store your login dn and password
```

```
$config->custom->appearance['hide_template_warning'] = true;
# $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');

/* Your LDAP password. If you specified an empty bind_id above, this MUST also
```

Login to phpLDAPadmin to set LDAP users
<http://localhost/phpldapadmin>



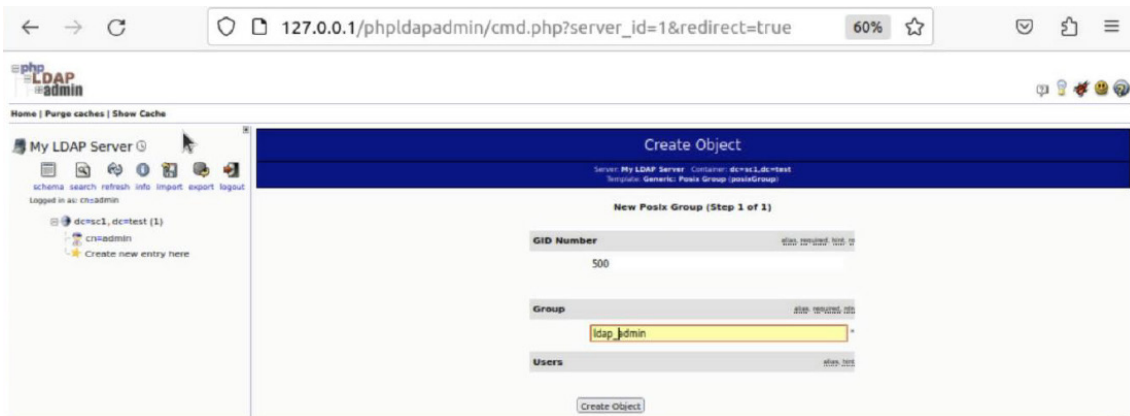
Login DN: cn=admin,dc=sc1,dc=test

Login password: admin

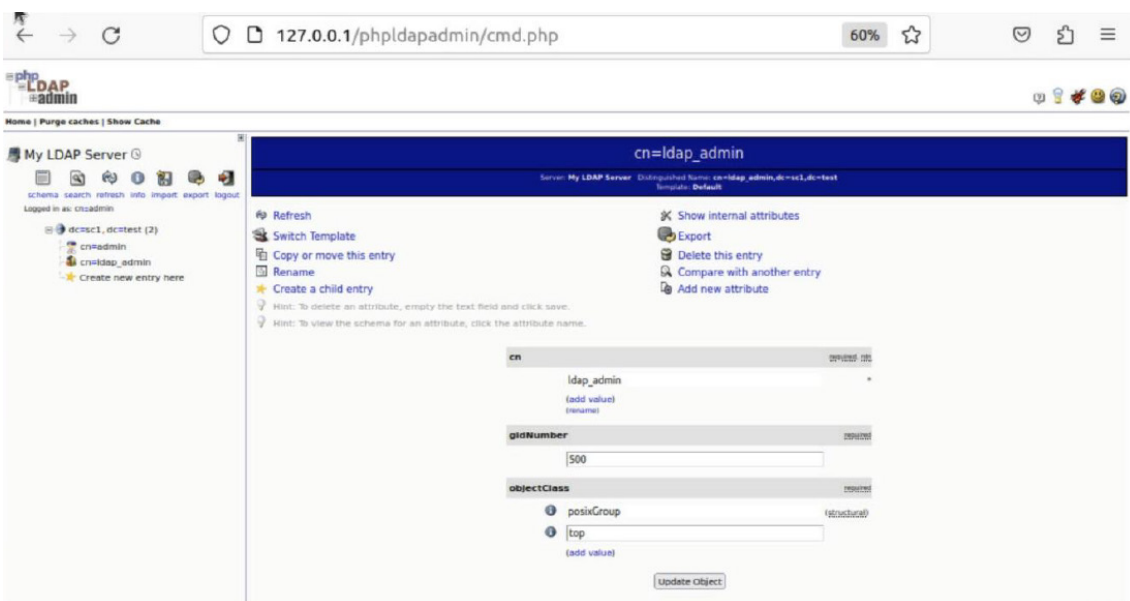
Setting on LDAP server



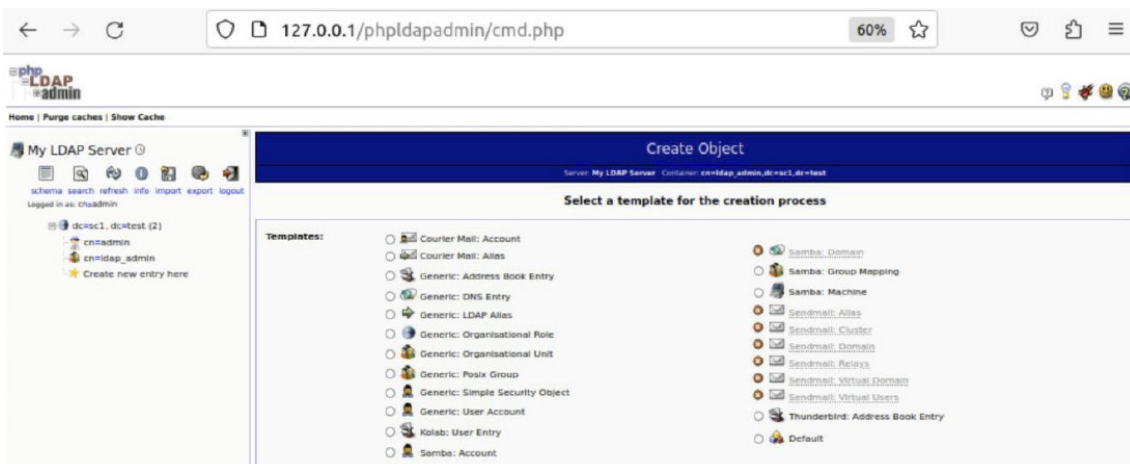
1. Click Create a child entry
2. Click Generic: Posix Group



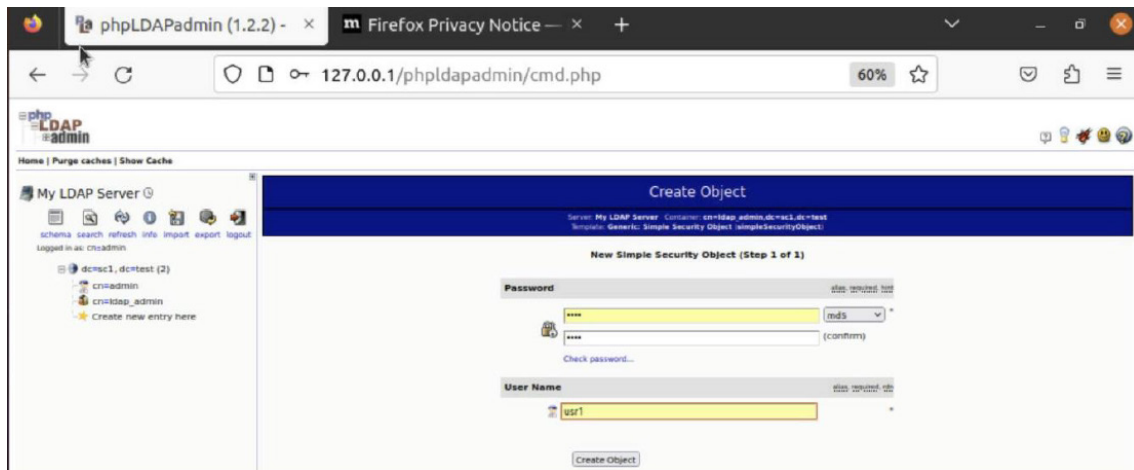
3. Input ldap_admin and click Create object



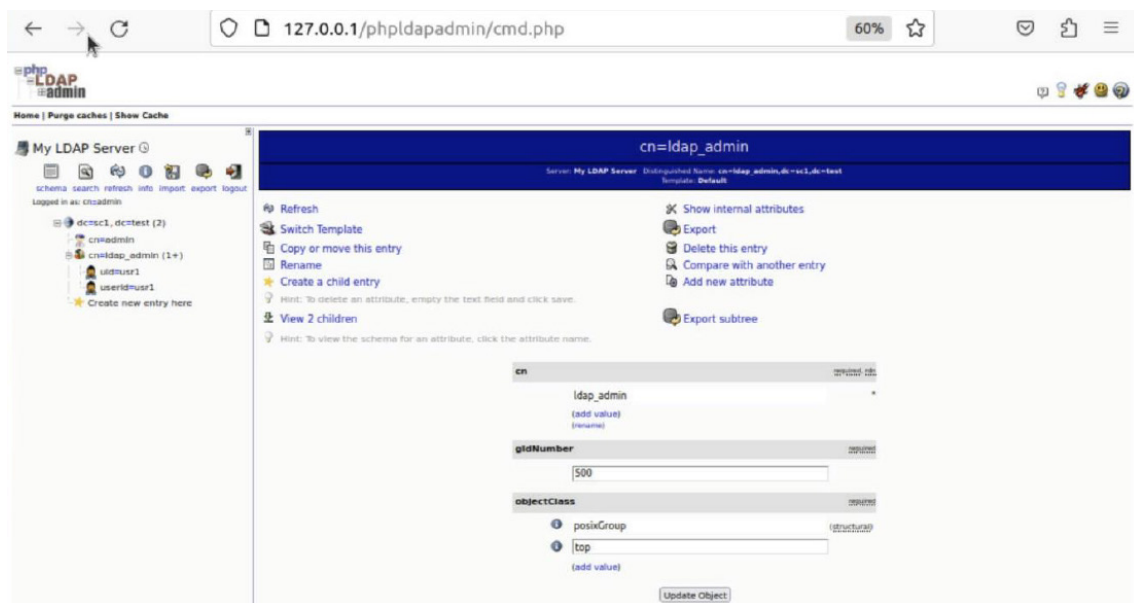
4. Input ldap_admin and click Create a child entry



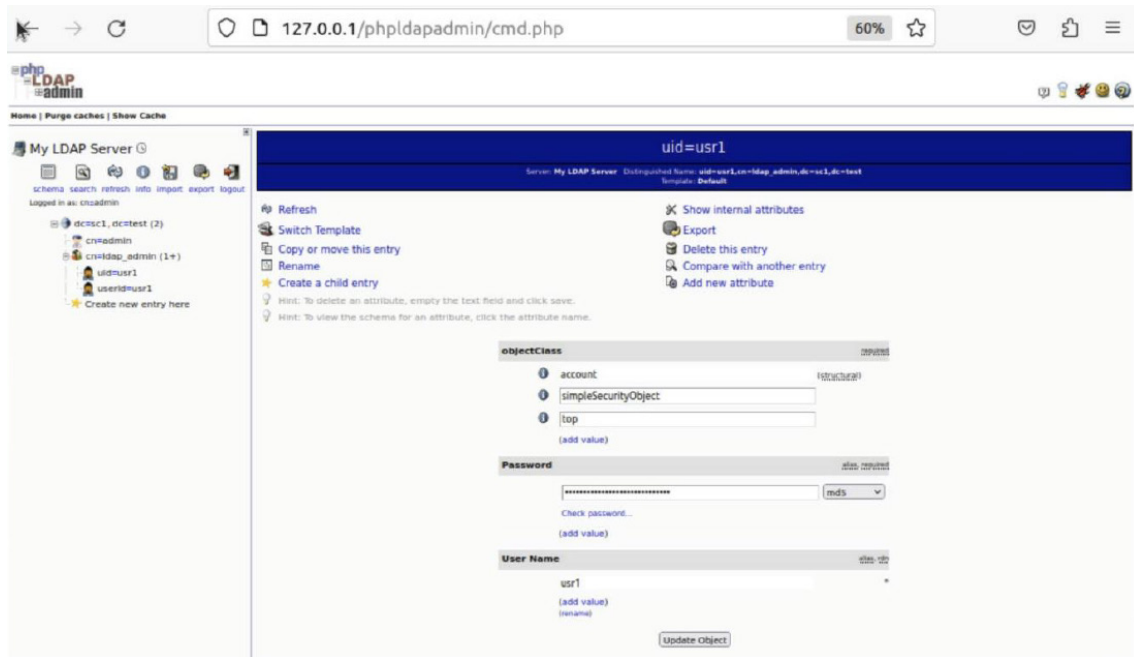
5. Click Generic: Simple Security Object



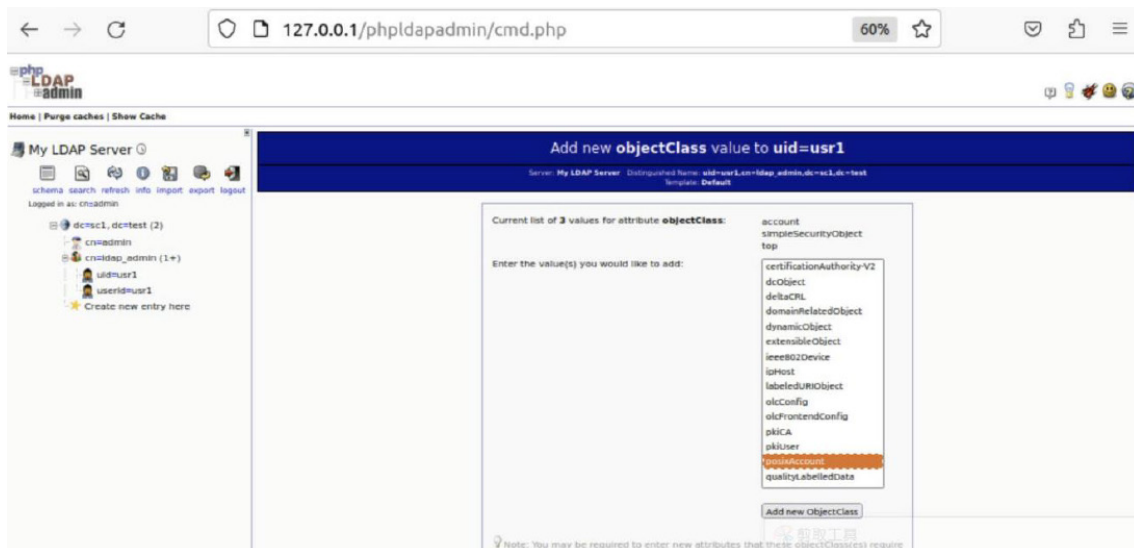
6. Input password pwd1 and User Name usr1



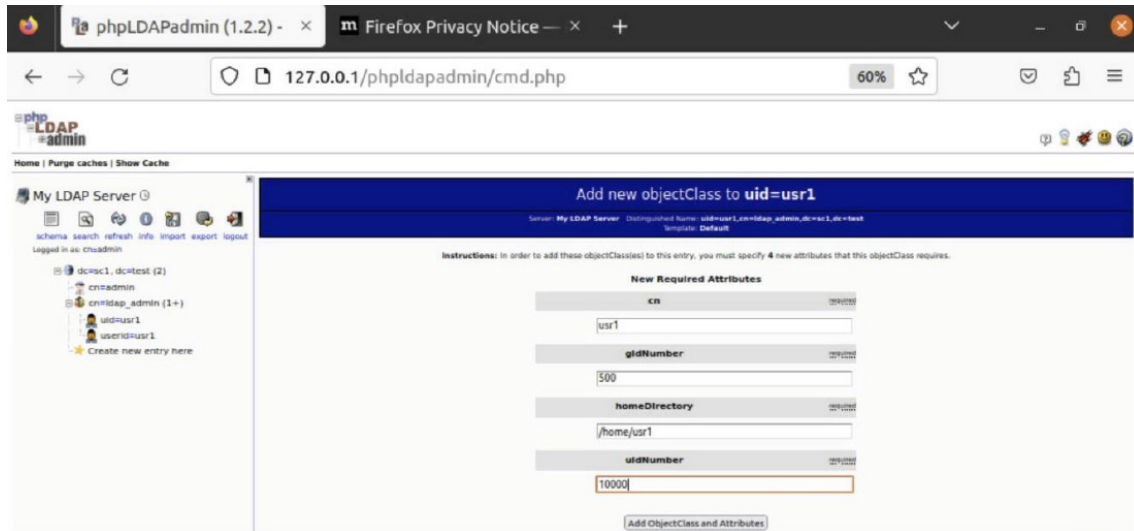
7. Click cn=ldap_admin and check the gid, it's 500 in this example



8. Click userid=usr1 and add value to attribute objectClass

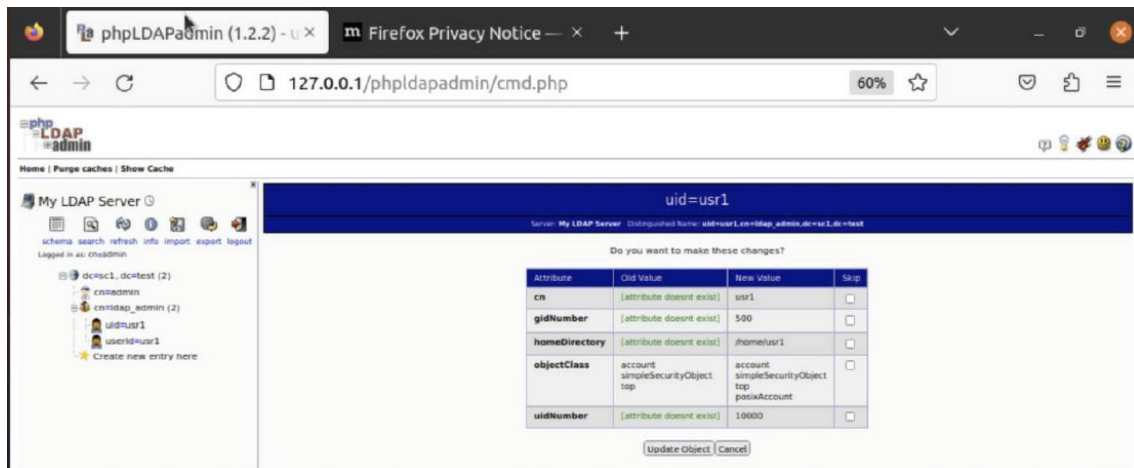


9. Select posixAccount



10. Input attribute

- cn is usr1
- gidNumber is the gid of ldap_admin, it's 500 in this example
- homeDirectory is /home/usr1 (no effect)
- uidNumber is 10000 (no effect)



2-7-2-2 Configuring on BMC server (OpenLDAP)

To enable/disable LDAP, check or uncheck the "Enable LDAP Authentication" checkbox respectively.

Supermicro OPF | Reserved GB300 Station 1650226120723

Health Power Refresh root

LDAP

Configure LDAP settings and manage role groups

Settings

LDAP authentication

☐ Enable

Secure LDAP using SSL
A CA certificate and an LDAP certificate are required to enable secure LDAP

☐ Enable

CA Certificate valid until
--

LDAP Certificate valid until
--

[Manage SSL certificates](#)

Service type

☒ OpenLDAP
☐ Active Directory

Server 1

Server URI ⓘ
ldap://

Bind DN

Bind password
Leave empty to keep the pr ⓘ

Base DN

User ID attribute - optional

Group ID attribute - optional

Save settings

Settings

Web login -> Security and access Page -> LDAP page.

- Enable LDAP authentication
- Choose Service type **OpenLDAP**
- Enter LDAP Server URI
- Bind DN is **cn=admin,dc=sc1,dc=test**
- Bind Password is **admin**
- Bind DN is **dc=sc1,dc=test**
- User ID attribute is **cn**
- Group ID attribute is **gidNumber**
- Click Save settings, then you can add role group

Role groups

			+ Add role group	
☐	Group name	Group privilege		
☐	ldap_admin	Administrator		

Click “Add role group”

- Group name is **ldap_admin**
- Group privilege **Administrator**
- Click Add

Active Directory Login



Please Login

Username

Password

☐ Remember Username

[Forgot Password?](#)

Log in

English

Login in WebUI successfully

Supervise OPF | Reserved GB300 Station 1650226120723

Health Power Refresh root

Dashboard

Virtual front panel

Power

Date and time

2026/06/17
Wednesday

17:24
UTC

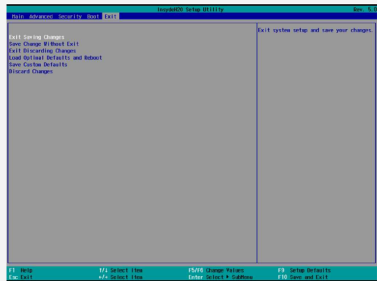
Current users

User Name	Type	IP Address
root (me)	Web (HTTPS)	10.8.133.57

Virtual media

Device	Status
Device 1	No disk emulation set
Device 2	No disk emulation set
Device 3	No disk emulation set
Device 4	No disk emulation set
Device 5	No disk emulation set

Screen preview



System information

BMC Uptime :	2 days 6 hours 44 minutes 7 seconds
Active BMC Firmware Build Time :	Fri, Jun 05, 2026, 15:24:59
Active BMC FW Rev :	01.10.5421

Networks

Dedicated NIC (1)

IP Address	10.1.6.83
Gateway	10.1.6.253
Subnet Mask	255.255.255.0

Overview

Dashboard

Logs

Hardware status

Operations

Settings

Alerts

Alert policies

Alert email

Date and time

Networks

VLAN

SOL

SNMP

iKVM and virtual media

Dynamic DNS

Syslog settings

Backup restore

Power restore policy

Security and access

Current users

LDAP

RADIUS

TACACS+

Users

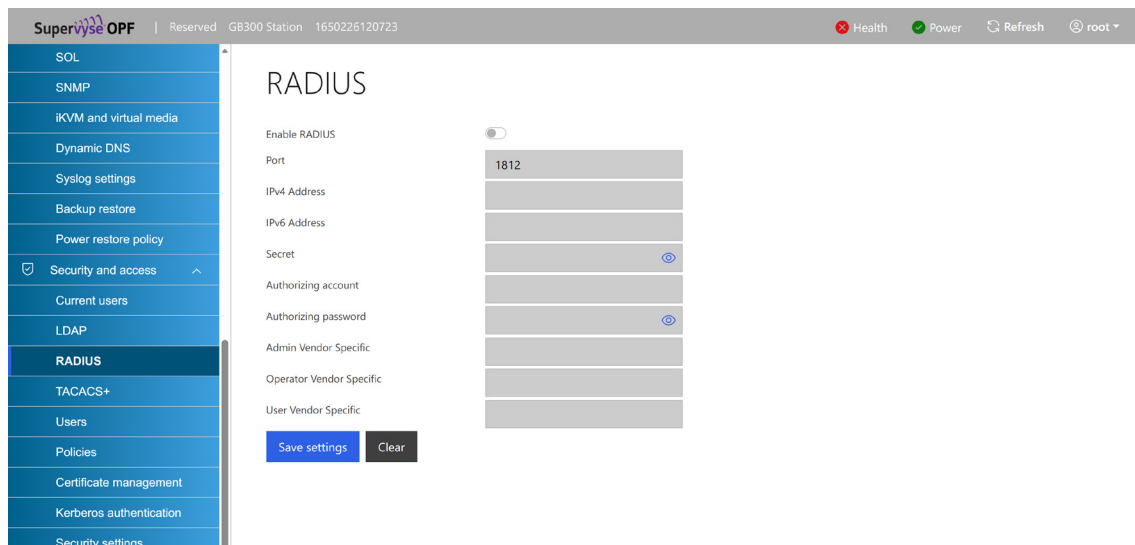
Policies

Certificate management

Login Web test

Now you can login with LDAP user **usr1** with password **pwd1**

2-7-3 RADIUS

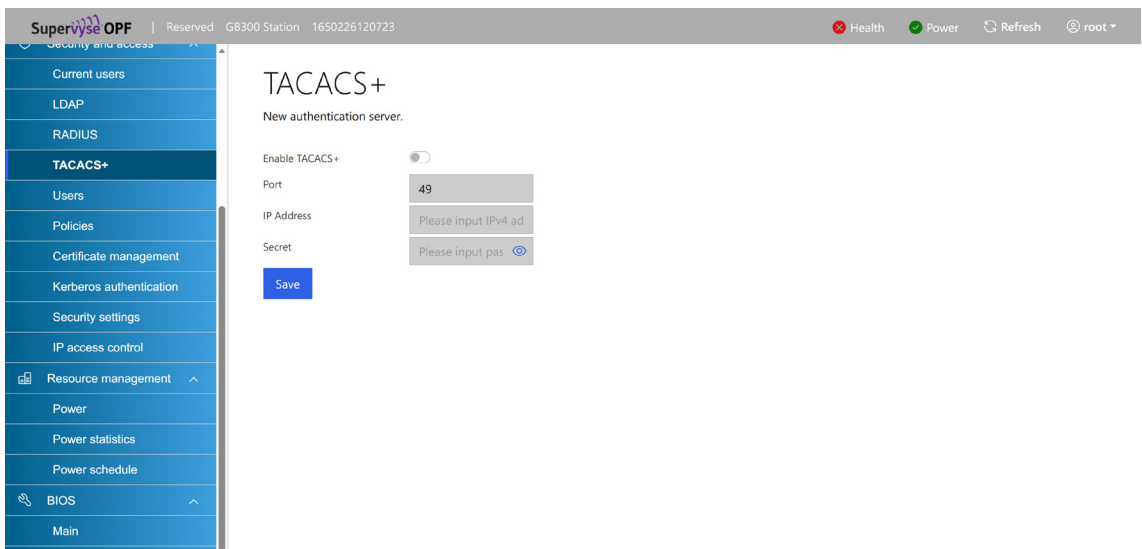


This page allows administrators to configure Remote Authentication Dial-In User Service (RADIUS) settings for centralized authentication, authorization, and accounting management.

To open this page, click RADIUS under the Security and access section from the menu bar. It displays the following fields and options:

- **Enable RADIUS:** A toggle switch to enable or disable the RADIUS authentication service on the system.
- **Port:** Enter the port number used for RADIUS authentication server communication (default is 1812).
- **IPv4 Address:** Enter the IPv4 address of the RADIUS server.
- **IPv6 Address:** Enter the IPv6 address of the RADIUS server.
- **Secret:** Enter the shared secret key used for encrypting communication between the system and the RADIUS server. Click the Eye icon to toggle the visibility of the secret characters.
- **Authorizing account:** Enter the service account name used for RADIUS server authorization requests.
- **Authorizing password:** Enter the password corresponding to the authorizing account. Click the Eye icon to toggle the visibility of the password characters.
- **Admin Vendor Specific:** Configure the Vendor-Specific Attribute (VSA) configuration string mapping for Administrator privilege level.
- **Operator Vendor Specific:** Configure the Vendor-Specific Attribute (VSA) configuration string mapping for Operator privilege level.
- **User Vendor Specific:** Configure the Vendor-Specific Attribute (VSA) configuration string mapping for Common User privilege level.
- **Save settings:** Click this button to apply and save the configured RADIUS infrastructure settings.
- **Clear:** Click this button to discard current inputs and reset the text input fields.

2-7-4 TACACS+



This page allows administrators to configure Terminal Access Controller Access-Control System Plus (TACACS+) settings to establish a new authentication server for remote access management.

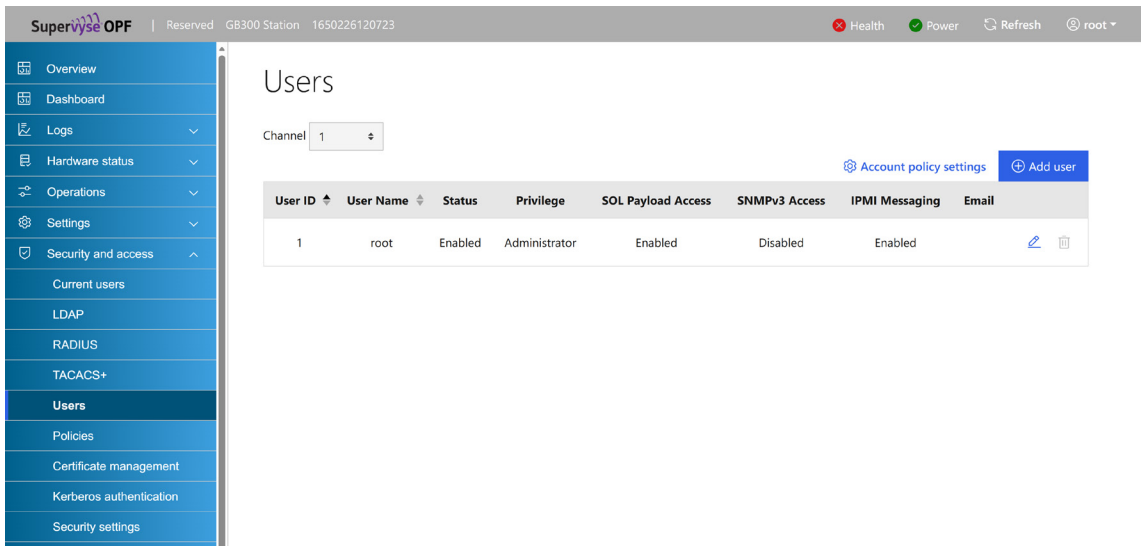
To open this page, click TACACS+ under the Security and access section from the menu bar. It displays the following fields and options:

- **Enable TACACS+:** A toggle switch to enable or disable the TACACS+ authentication service on the system.
- **Port:** Enter the port number used for TACACS+ server communication (default is 49).
- **IP Address:** Enter the IPv4 address of the target TACACS+ authentication server.
- **Secret:** Enter the shared secret key used for encryption between the system and the TACACS+ server. Click the Eye icon to toggle the visibility of the secret characters.
- **Save:** Click this button to apply and save the configured TACACS+ server settings.

2-7-5 Users

In Web GUI, the User page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click **Security and access > Users** from the menu bar. A sample screenshot of User Management Page is shown below.



Click "Add user" for advanced configuration.

Fill in related the new user information and click 'Save user' to create a user.

Add user

User ID

2

User Name

Password

Confirm Password

Email

Network Privilege

Administrator

User Enabled

Enabled

SOL Payload Access

Disabled

Password Expiration Day

0

☐ SNMPv3 Access

SNMPv3 Access Level

ReadOnly

SNMPv3 Authentication Protocol

HMAC_MD5

SNMPv3 Authentication Passphrase

SNMPv3 Privacy Protocol

CFB128_AES128

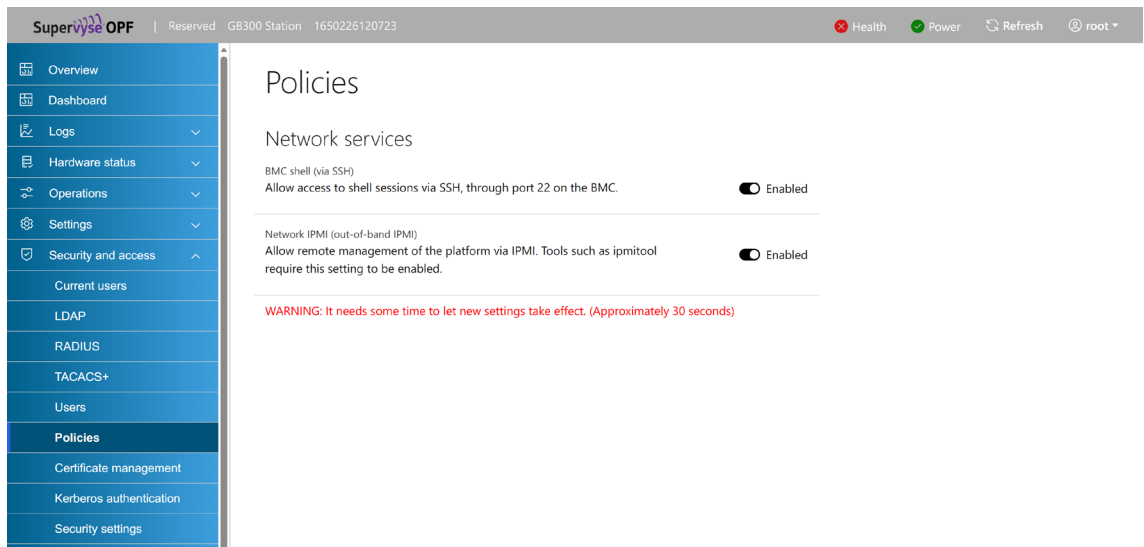
SNMPv3 Privacy Passphrase

Cancel

Add user

2-7-6 Policies

This page is used to configure Policies.



Network services

- BMC shell (via SSH)
- Network IPMI (out-of-band IPMI)

BMC shell (via SSH)

Allow access to shell sessions via SSH, through port 22 on the BMC.

Network IPMI (out-of-band IPMI)

Allow remote management of the platform via IPMI. Tools such as ipmitool require this setting to be enabled.

Add user

User ID

2

User Name

Password

Confirm Password

Email

Network Privilege

Administrator

User Enabled

Enabled

SOL Payload Access

Disabled

Password Expiration Day

0

☐ SNMPv3 Access

SNMPv3 Access Level

ReadOnly

SNMPv3 Authentication Protocol

HMAC_MD5

SNMPv3 Authentication Passphrase

SNMPv3 Privacy Protocol

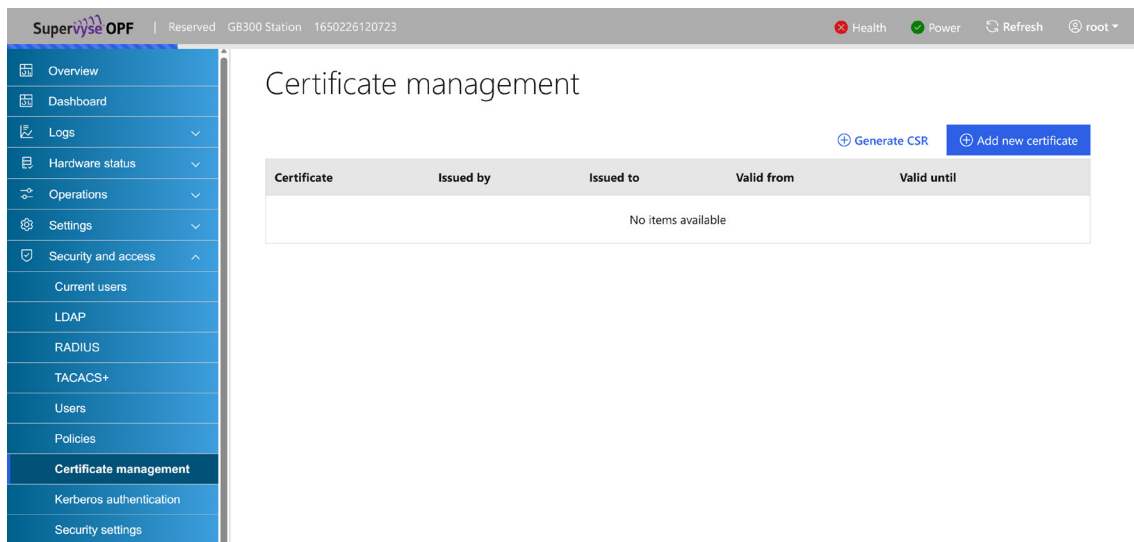
CFB128_AES128

SNMPv3 Privacy Passphrase

Cancel

Add user

2-7-7 Certificate management



This page allows administrators to manage the system's SSL/TLS certificates, view certificate details, generate signing requests, and upload new credentials to secure communication channels.

To open this page, click Certificate management under the Security and access section from the menu bar. It displays the following components:

- **Generate CSR:** Click this text link button to create a Certificate Signing Request (CSR) required when applying for a new certificate from a Certificate Authority (CA).
- **Add new certificate:** Click this button to upload and install a newly issued SSL/TLS certificate or private key to the system.
- **Certificate List Table:** Displays a structured overview of all currently installed certificates. If no certificates are uploaded, it shows No items available. The table columns include:
 1. **Certificate:** Displays the filename or alias identifier of the certificate.
 2. **Issued by:** Identifies the Certificate Authority (CA) that generated and signed the certificate.
 3. **Issued to:** Specifies the common name (CN) or entity domain name to which the certificate belongs.
 4. **Valid from:** Indicates the beginning timestamp of the certificate's validity period.
 5. **Valid until:** Indicates the expiration timestamp of the certificate's validity period.

2-7-8 Kerberos authentication

Supervyse OPF | Reserved GB300 Station 1650226120723

Health Power Refresh root

Overview
Dashboard
Logs
Hardware status
Operations
Settings
Security and access
Current users
LDAP
RADIUS
TACACS+
Users
Policies
Certificate management
Kerberos authentication
Security settings

Kerberos authentication

Enable Kerberos Authorization ☐

Kerberos Realm

Kerberos KDC Server Domain/IPv4/IPv6

Kerberos KDC Server Port

Keytab file 沒有選擇檔案

This page allows administrators to configure Kerberos authentication settings to establish network identity verification via a Key Distribution Center (KDC).

To open this page, click Kerberos authentication under the Security and access section from the menu bar. It displays the following fields and options:

- **Enable Kerberos Authorization:** A toggle switch to enable or disable the Kerberos authorization service on the system.
- **Kerberos Realm:** Enter the domain name of the Kerberos realm (e.g., EXAMPLE.COM).
- **Kerberos KDC Server Domain/IPv4/IPv6:** Enter the domain name, IPv4 address, or IPv6 address of the target Kerberos Key Distribution Center (KDC) server.
- **Kerberos KDC Server Port:** Enter the port number used for communicating with the KDC server (default is 88).
- **Keytab file:** Click 選擇檔案 (Choose File) to select a valid keytab file containing Kerberos principals and keys from your local workspace, and click the Upload button to save it.
- **Save settings:** Click this button to apply and save the configured Kerberos text field entries.

2-7-9 Security settings

You can view and modify the security settings on this page.

Supervise OPF | Reserved GB300 Station 1650226120723 Health Power Refresh root

Overview
Dashboard
Logs
Hardware status
Operations
Settings
Security and access
Current users
LDAP
RADIUS
TACACS+
Users
Policies
Certificate management
Kerberos authentication
Security settings
IP access control
Resource management
BIOS

Security settings

You can view and modify the security settings on this page.

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode allows an administrator to get or set the system SSL cipher mode.

SSL Cipher Mode **Advanced**

Save

IP Blocking Settings

Configuring the bad password threshold and the login failed attempts interval time of the remote client before that is login blocked out and how long the remote client login blocked out will be expired and the remote client can re-login again.

IP Blocking ☒

Failed Login Attempts (1 - 255)

Failed Login Attempts Interval Time (sec)

Remote Client Lockout Time (sec)

Save Restore

Port Settings

Set the port used for https (default: 443) web sessions. Changing this setting will immediately terminate all current web sessions. Port range is 1 ~ 65535.

HTTPS (Secure) Port

Save Restore

Optional Network Services

IPMI over LAN ☒ Enable/Disable the RMCP/RMCP+ service.

Save

Network services

- BMC shell (via SSH)
- Network IPMI (out-of-band IPMI) IPMI over LAN

BMC shell (via SSH)

Allow access to shell sessions via SSH, through port 22 on the BMC.

Network IPMI (out-of-band IPMI)

Allow remote management of the platform via IPMI. Tools such as ipmitool require this setting to be enabled.

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode allows an administrator to get or set the system SSL cipher mode. Select the SSL Cipher Mode and click 'Save' to save the configuration.

IP Blocking Settings

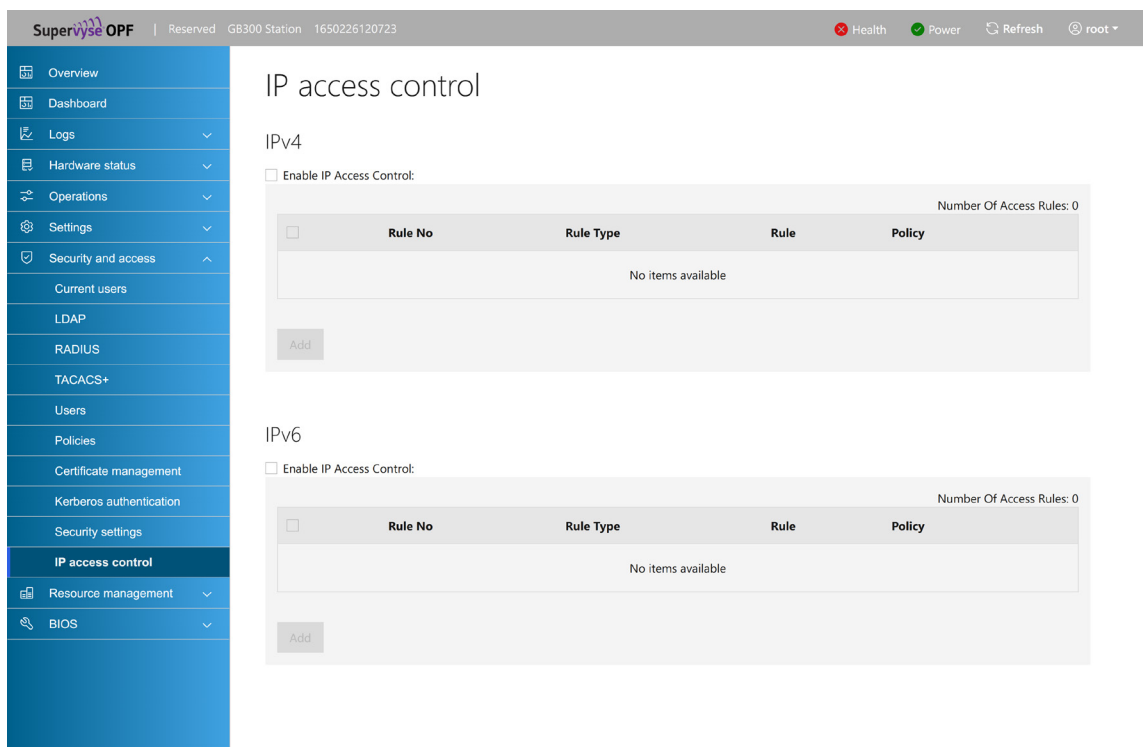
Configuring the bad password threshold and the login failed attempts interval time of the remote client before that is login blocked out and how long the remote client login blocked out will be expired and the remote client can re-login again.

Optional Network Services

- IPMI over LAN: Enable or disable the RMCP/RMCP+ service. Click 'Save' to save the configuration.

2-7-10 IP access control

Use this page to add, edit or remove IP access rules.



IPv4 Enable IP Access Control

- Click for enable or disable IP Access Control policy.

IPv4 Add Rule ×

Rule No

1

Policy

Accept

Rule Type

IP/Mask

IP/Mask:

192.168.2.0/24

Cancel

Add Rule

Add

Add a new rule.

Insert

Insert a new rule.

Modify

Modify the existed rule.

Delete

Delete the existed rule.

Rule No

Show current Rule No.

Policy

- accept
- drop

Rule Type

- ipMask: Enter IP/Mask.
- ipRange: Enter IP Range Start and End.
- Mac: Enter mac address
- Port: Enter tcp/udp protocol

Add Rule

Click on the Add button to add new rule.

IPv6

Enable IP Access Control

Click for enable or disable IP Access Control policy.

IPv4 Add Rule

×

Rule No

1

Policy

Accept

Rule Type

IP/Mask

IP/Mask:

192.168.2.0/24

Cancel

Add Rule

Add

Add a new rule.

Insert

Insert a new rule.

Modify

Modify the existed rule.

Delete

Delete the existed rule.

Rule No

Show current Rule No.

Policy

- accept
- drop

Rule Type

- ipMask: Enter IP/Mask.
- ipRange: Enter IP Range Start and End.
- Mac: Enter mac address
- Port: Enter tcp/udp protocol

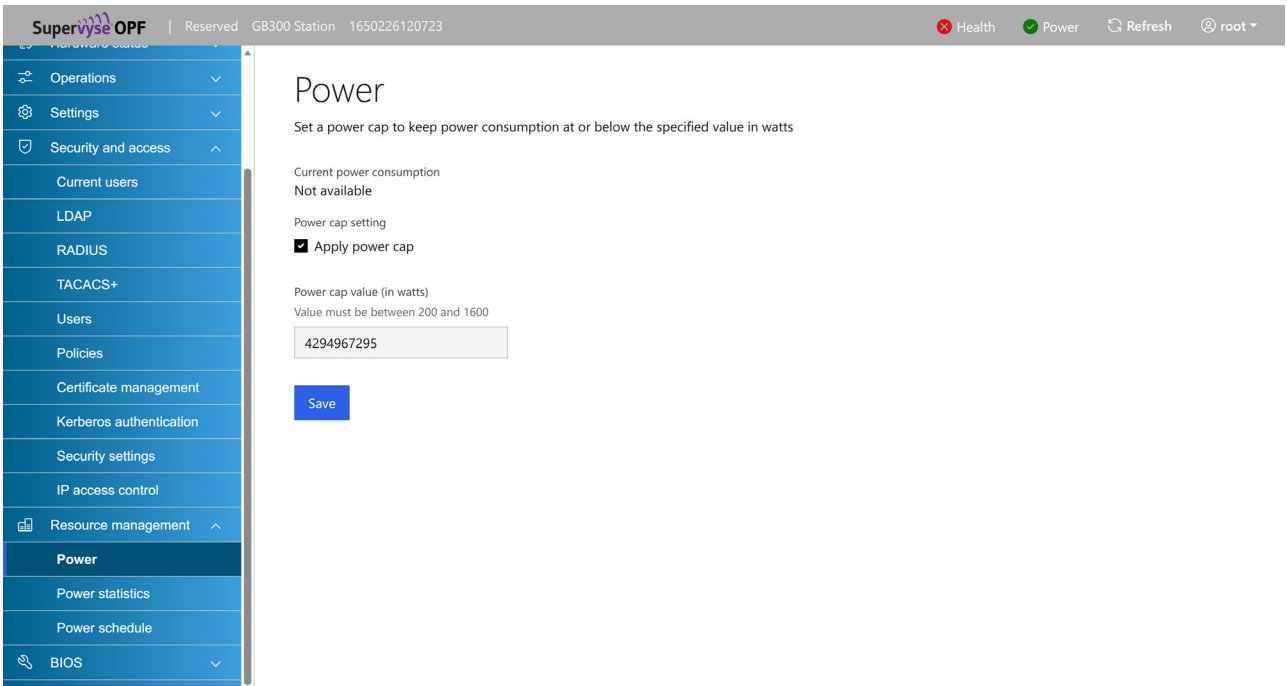
Add Rule

Click on the Add button to add new rule.

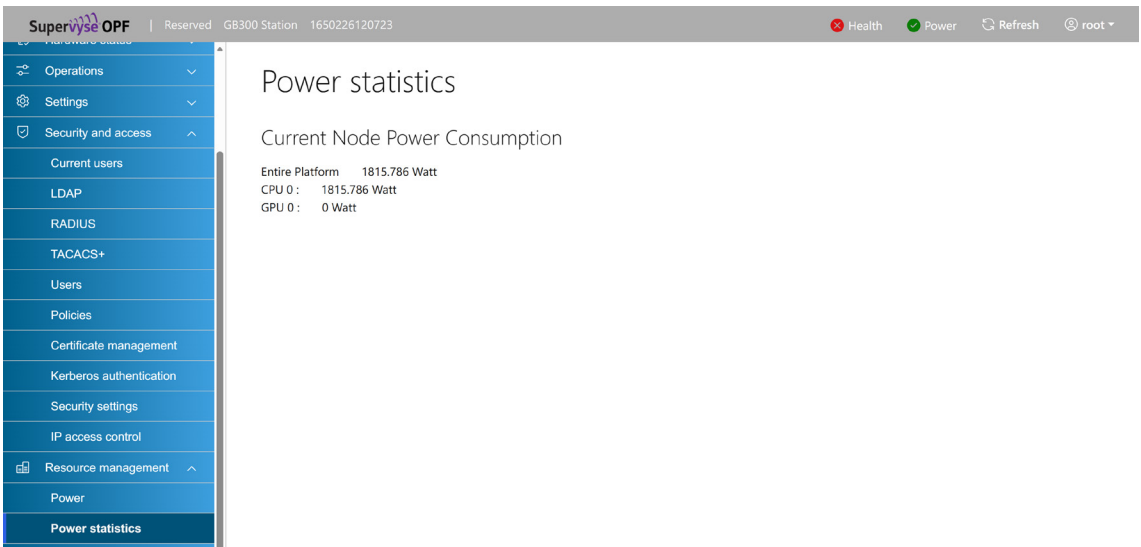
2-8 Resource Management

2-8-1 Power

Displays system power information.



2-8-2 Power Statistics



This page displays the real-time power consumption statistics of the server node, allowing administrators to monitor power distribution across primary hardware subsystems.

To open this page, click Power statistics under the Resource management section from the menu bar. It displays the following section:

Current Node Power Consumption

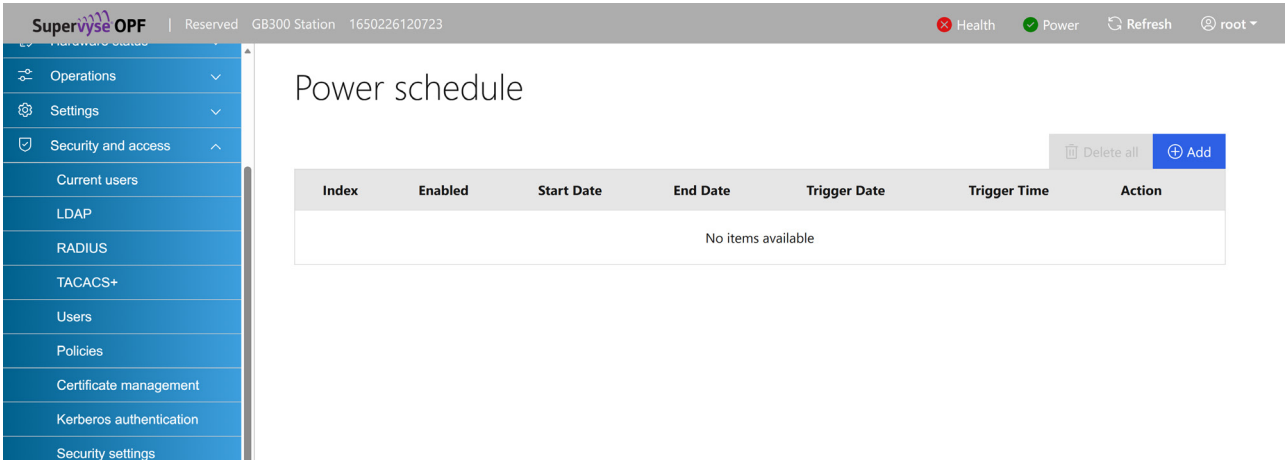
This section provides live readings of the system's power consumption metrics measured in Watts:

- **Entire Platform:** Displays the total power consumption accumulated by the entire server chassis and its active integrated components.
- **CPU 0:** Displays the specific real-time power draw consumed by the first central processing unit (CPU 0).

- **GPU 0:** Displays the specific real-time power draw consumed by the first graphics processing unit (GPU 0).

2-8-3 Power Schedule

Displays power schedule.



Delete all

Click on the Delete all button to delete all data.

Add

Click on the Add button to add new data. Add Schedule window pops up. Enter values and click 'Save' to add a new power schedule.

Add Schedule

Task

1

Enabled

Enabled

Action

Power Off Host - Immediate

Schedule

Time

00

:

00

Date

Specific

2025-12-03

Cancel

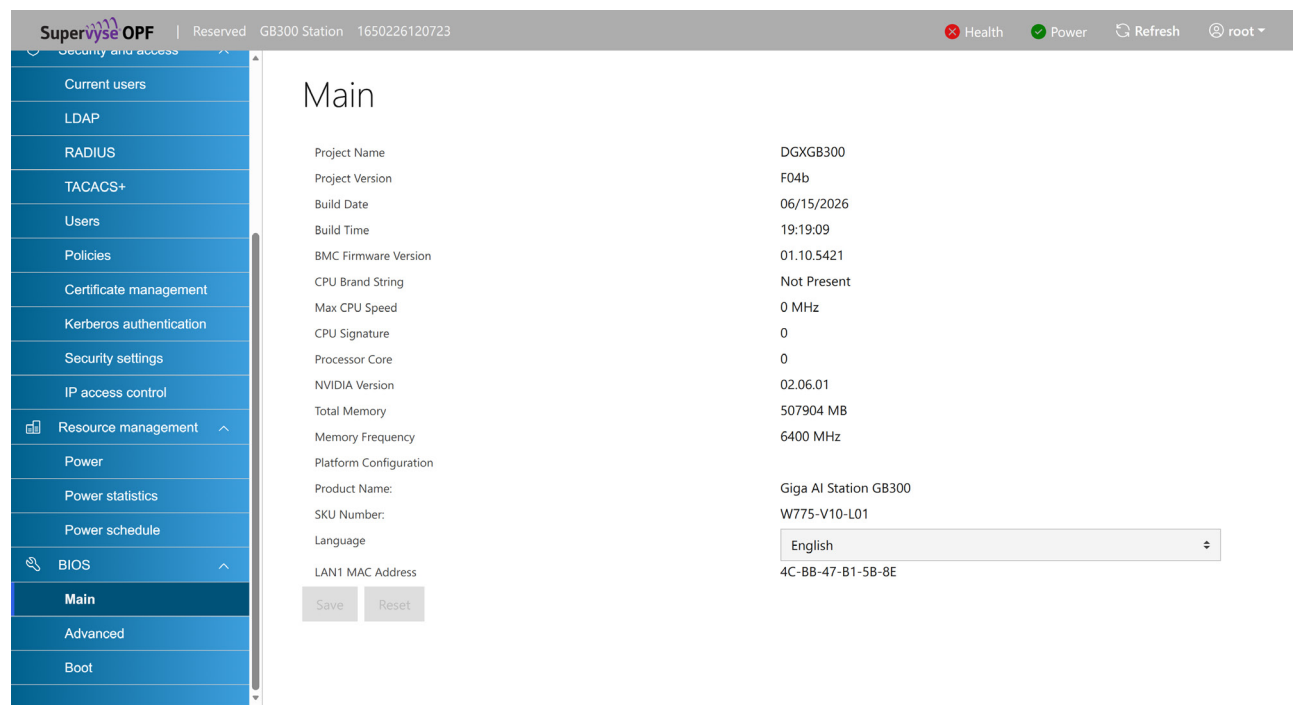
Add

2-9 BIOS (Insyde BIOS joint feature)

This is Insyde BIOS joint feature. You should turn on the host and wait for the BIOS to upload the relevant data.

2-9-1 Main

The page show all BIOS configurations.



Save

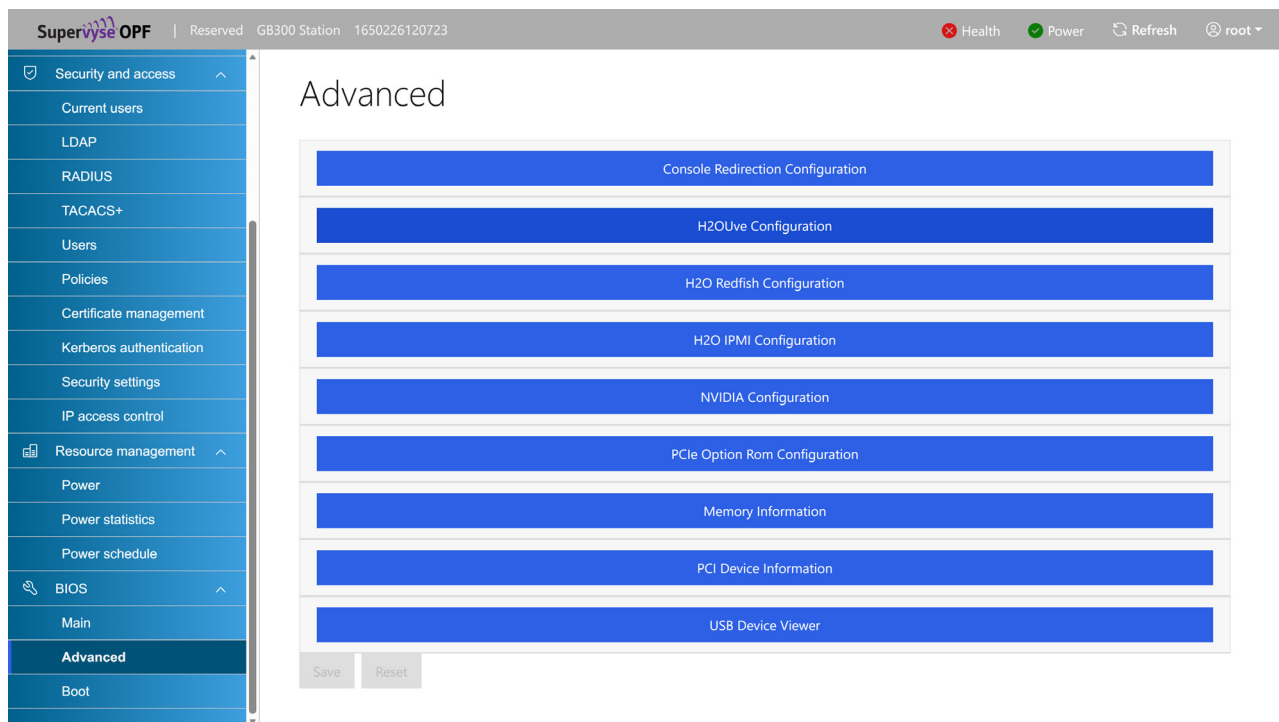
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-2 Advanced

The page shows all BIOS advanced page configurations.



Save

Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-3 Boot

Displays BIOS boot information and provides items for configuration of the boot sequence.

Supervyse OPF

Reserved GB300 Station 1650226120723

HealthPowerRefreshroot

Security and access

Current users

LDAP

RADIUS

TACACS+

Users

Policies

Certificate management

Kerberos authentication

Security settings

IP access control

Resource management

Power

Power statistics

Power schedule

BIOS

Main

Advanced

Boot

Boot

Quick Boot

Quiet Boot

Network Stack

PXE Boot Capability

HTTP/HTTPS Boot Capability

PXE/ HTTP Boot Retry Policy

Add Boot Options Policy

USB Boot

Timeout

Automatic Failover

Group Boot Options

Sync Order

Adjust Non-BIOS Boot Options

Group Auto Boot Order

Device Type in Boot Manager

SaveReset

Enabled

Enabled

Enabled

UEFI:IPv4

Disabled

(0x2)2

Auto

Enabled

(0x0)0

Enabled

Grouped

Disabled

Enabled

Disabled

Enabled

Save

Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

3-1 Appendix A - Assertion Condition (BIT EVENT) References

3-1-1 Sensor type: Temperature, Voltage, Current, Fan

- bit0. Lower Non-critical - going low
- bit1. Lower Non-critical - going high
- bit2. Lower Critical - going low
- bit3. Lower Critical - going high
- bit4. Lower Non-recoverable - going low
- bit5. Lower Non-recoverable - going high
- bit6. Upper Non-critical - going low
- bit7. Upper Non-critical - going high
- bit8. Upper Critical - going low
- bit9. Upper Critical - going high
- bit10. Upper Non-recoverable - going low
- bit11. Upper Non-recoverable - going high

To open the Overview page, click **Overview** from the menu bar. It displays the following:

3-1-2 Sensor type: Physical Security

- bit0. General Chassis Intrusion
- bit1. Drive Bay intrusion
- bit2. I/O Card area intrusion
- bit3. Processor area intrusion
- bit4. LAN Leash Lost (system is unplugged from LAN)
- bit5. Unauthorized dock
- bit6. FAN area intrusion

3-1-3 Sensor type: Processor

- bit0. IERR
- bit1. Thermal Trip
- bit2. FRB1/BIST failure
- bit3. FRB2/Hang in POST failure

bit4. FRB3/Processor Startup/Initialization failure (CPU didn't start)
bit5. Configuration Error
bit6. SM BIOS 'Uncorrectable CPU-complex Error'
bit7. Processor Presence detected
bit8. Processor disabled
bit9. Terminator Presence Detected
bit10. Processor Automatically Throttled
bit11. Machine Check Exception (Uncorrectable)
bit12. Correctable Machine Check Error

3-1-4 Sensor type: Power supply

bit0. Presence detected
bit1. Power Supply Failure detected
bit2. Predictive Failure
bit3. Power Supply input lost (AC/DC)[2]
bit4. Power Supply input lost or out-of-range
bit5. Power Supply input out-of-range, but present
bit6. Configuration error
bit7. Power Supply Inactive (in standby state)

3-1-5 Sensor type: Other Units-based Sensor

bit0. Lower Non-critical - going low
bit1. Lower Non-critical - going high
bit2. Lower Critical - going low
bit3. Lower Critical - going high
bit4. Lower Non-recoverable - going low
bit5. Lower Non-recoverable - going high
bit6. Upper Non-critical - going low
bit7. Upper Non-critical - going high
bit8. Upper Critical - going low
bit9. Upper Critical - going high
bit10. Upper Non-recoverable - going low
bit11. Upper Non-recoverable - going high

3-1-6 Sensor type: Memory

bit0. Correctable ECC / other correctable memory error
bit1. Uncorrectable ECC / other uncorrectable memory error
bit2. Parity
bit3. Memory Scrub Failed (stuck bit)
bit4. Memory Device Disabled
bit5. Correctable ECC / other correctable memory error logging limit reached
bit6. Presence detected
bit7. Configuration error
bit8. Spare
bit9. Memory Automatically Throttled
bit10. Critical Overtemperature

3-1-7 Sensor type: Event Logging Disabled

bit0. Correctable Memory Error Logging Disabled
bit1. Event 'Type' Logging Disabled
bit2. Log Area Reset/Cleared
bit3. All Event Logging Disabled
bit4. SEL Full (SEL is in circular mode, so this event will not be triggered.)

bit5. SEL Almost Full (SEL is in circular mode, so this event will not be triggered.)
bit6. Correctable Machine Check Error Logging Disabled

3-1-8 Sensor type:Critical Interupt

bit0. Front Panel NMI / Diagnostic Interrupt
bit1. Bus Timeout
bit2. I/O channel check NMI
bit3. Software NMI
bit4. PCI PERR
bit5. PCI SERR
bit6. EISA Fail Safe Timeout
bit7. Bus Correctable Error
bit8. Bus Uncorrectable Error
bit9. Fatal NMI (port 61h, bit 7)
bit10. Bus Fatal Error
bit11. Bus Degraded (bus operating in a degraded performance state)

