Veeam hardened repository installation guide for Nexsan VHR-Series Appliance

Submitted for the Veeam Ready Appliance Certification

July 22, 2025

Contents

Alliance Partner	NEXSAN
Alliance Product	NEXSAN VHR-Series Appliance
Program Category	Veeam Ready – Appliance
Category Description	Appliances are officially validated for Veeam deployments using the Veeam Appliance ISO, with compatibility confirmed through testing and accompanied by documented best practices and configuration screenshots.
Article ID	NEXSAN VHR-Series
Features and attributes	Hardened repository Immutability
Publication Date	July 22, 2025
Last modified date	July 22, 2025
Product details	
Product name and Version	NEXSAN VHR-Series Appliance
Product firmware version	

Vendor recommended configuration

Readers are strongly encouraged to review the following links to properly configure the NEXSAN VHR-Series as a Veeam Hardened Repository. This document also includes relevant screenshots and step-by-step guidance to support the setup process.

How to perform a firmware upgrade

Firmware updates are to be carried out by Supermicro only if a firmware-related issue has been identified through Supermicro Support. Support links can be found here:

Global Support Email: support@nexsan.com

UK Office:

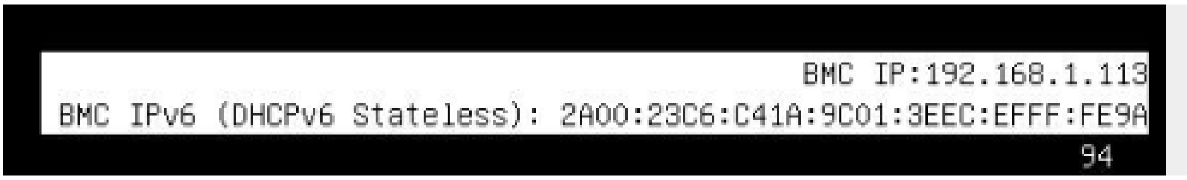
- Phone: +44 (0)1332 596 900
- Email: sales@nexsan.com

North America:

- Toll-free: +1 866-263-9726
- Phone: +1 760-690-1111
- Email: sales@nexsan.com

BMC IP address appears in the bottom right during POST

IP address located in 'IPMI > BMC Network Configuration' in the BIOS



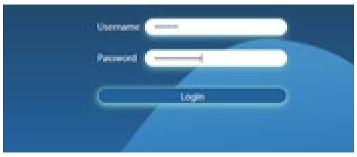
```
                                          BMC IP:192.168.1.113
BMC IPv6 (DHCPv6 Stateless): 2A00:23C6:C41A:9C01:3EEC:EFFF:FE9A
                                                            94
```

At this stage the server is ready for you to control remotely.

<u>Connecting to the server</u>

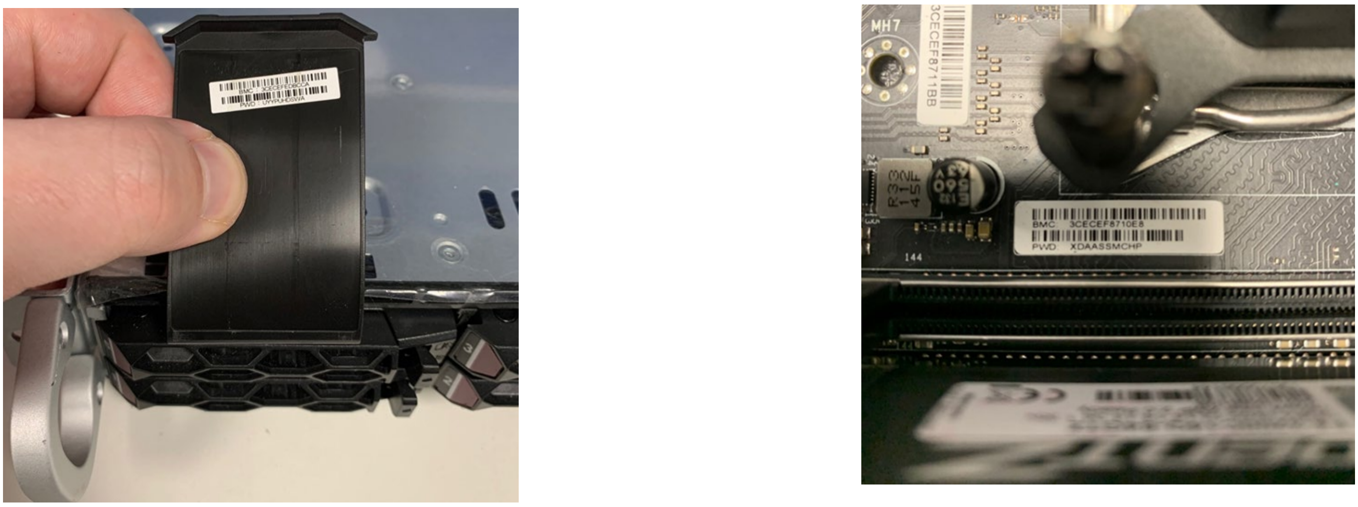
Connecting to the BMC interface using the IPMI Web Interface.

If you are on the same or a routable network to that which the BMC is connected to, you can simply open a web browser and type in the IP address and you will be presented with the screen below.



IPMI login screen

By default, the username is ADMIN. The unique password can be located on the pull-out server tag, usually located on the front of the server. It is also printed on the motherboard in the form of a sticker with a barcode.

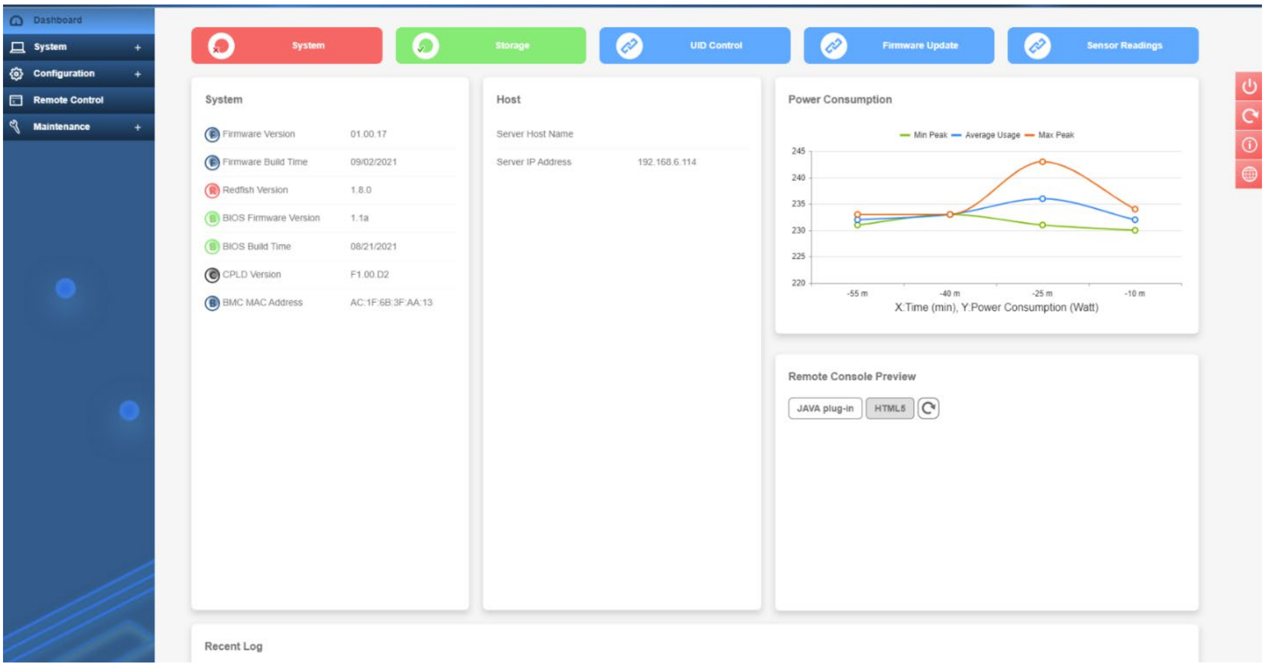


Server service tag showing BMC MAC address and unique password or IPMI MAC address and unique password printed on the Motherboard

IPMI MAC address and unique password printed on the Motherboard

<u>The Web GUI</u>

Once logged in, the start page is the **Dashboard**, which provides a summary of the server's status along with quick access to key features. Shortcut links at the top of the screen take you directly to sections such as **System**, **Storage**, **UID Control**, **Firmware Update**, and **Sensor Readings**.



System

Firmware Version	01.00.17
Firmware Build Time	09/02/2021
Redfish Version	1.8.0
BIOS Firmware Version	1.1a
BIOS Build Time	08/21/2021
CPLD Version	F1.00.D2
BMC MAC Address	AC:1F:6B:3F:AA:13

Host

Server Host Name	
Server IP Address	192.168.6.114

The Dashboard

While in the **Dashboard**, you'll find a range of useful system information, including **BIOS and IPMI firmware revisions**, **IP and MAC addresses**, and the **host name**. The dashboard also provides a summary and graphical overview of **recent power consumption**, along with a **log of recent system events** for quick diagnostics.

There is also direct access to launch the **Remote Console**, which includes a small live preview of the server's current screen. This console provides full **KVM (Keyboard, Video, Mouse)** control over the server — a feature we'll explore in more detail later. You can choose between the **Java-based console** or the **HTML5 version**. In practice, the **HTML5 console** tends to launch more quickly, delivers a smoother experience, and doesn't require Java installation on your local machine — an advantage often preferred in secure IT environments.

At the top of the Dashboard, you'll also find **shortcut links** to commonly used sections of the interface. These, along with the complete navigation menu on the left-hand side, will be covered in the next section.

RAID controller configuration

Operating system boot device(s)

- **RAID card description:** SuperMicro **AOC-S3916L-H16IR (-32DD)**
  - The RAID 1 OS boot device consists of two enterprise-grade 480 GB SSDs installed in bays 0 and 1, housed in Gen4 3.5-inch conversion chassis. This configuration is automatically provisioned by Nexsan's deployment automation.

Backup storage drives "Version-S"

- **Cache policy:** 8 GB flash-backed write cache (50% read / 50% write)
- **Strip size used:** 256 KiB
- **Data protection method:** RAID 6 (1 sets of 10 RAID 6)

Considerations for LUN configuration

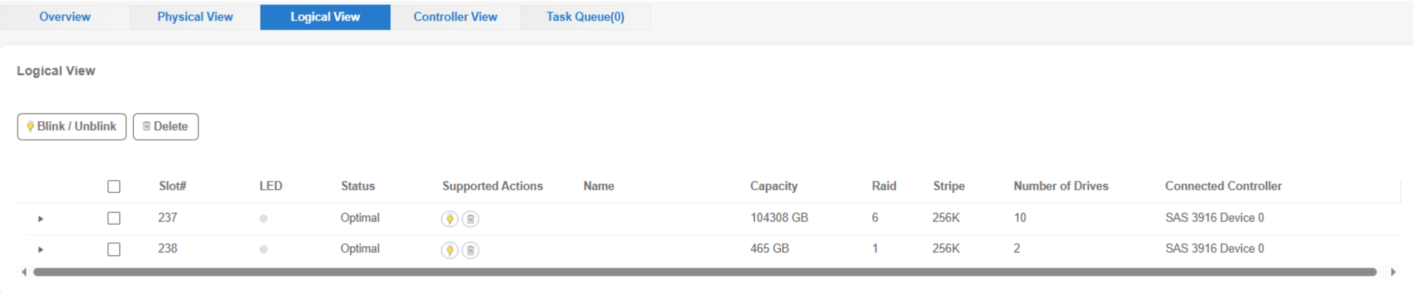
- Default initialization method—Full. Use this method; otherwise, the initialization will complete slowly in the background, impacting performance for days.
- Assign 50% of the controller cache to read.
- **Number of logical volumes:**

  Nexsan recommends using the entire array capacity for a single logical volume.

Backup storage drives configuration

Version-S

- Create one RAID 6 set consisting of 10 drives. This configuration Uses 56 drives, 2 parity per set. A single RAID controller will manage the RAID 6 volume — using the AOC-S3916L-H16IR — which features 16 PCIe lanes and an 8 GB cache.

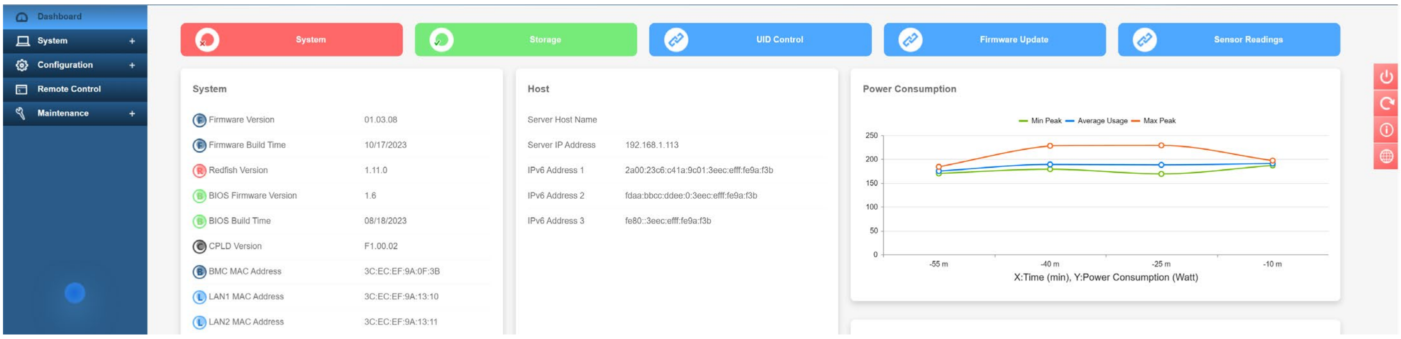


Logical View

	Slot#	LED	Status	Supported Actions	Name	Capacity	Raid	Stripe	Number of Drives	Connected Controller
□	237	●	Optimal			104308 GB	6	256K	10	SAS 3916 Device 0
□	238	●	Optimal			465 GB	1	256K	2	SAS 3916 Device 0

Creating the OS Raid 1 and Data Raid 6 volumes

Select the Storage Tab



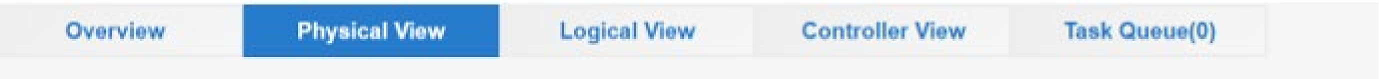
System

Firmware Version	01.03.08
Firmware Build Time	10/17/2023
Redfish Version	1.11.0
BIOS Firmware Version	1.6
BIOS Build Time	08/18/2023
CPLD Version	F1.00.02
BMC MAC Address	3C:EC:EF:9A:0F:3B
LAN1 MAC Address	3C:EC:EF:9A:13:10
LAN2 MAC Address	3C:EC:EF:9A:13:11

Host

Server Host Name	
Server IP Address	192.168.1.113
IPv6 Address 1	2a00:23c6:c41a:9c01:3eec:efff:fe9a:f3b
IPv6 Address 2	fdaa:bbcc:ddee:0:3eec:efff:fe9a:f3b
IPv6 Address 3	fe80::3eec:efff:fe9a:f3b

Select the "Physical View" within the interface to verify the status and configuration of all physical disks.



Select the "Controller View" in the management interface.

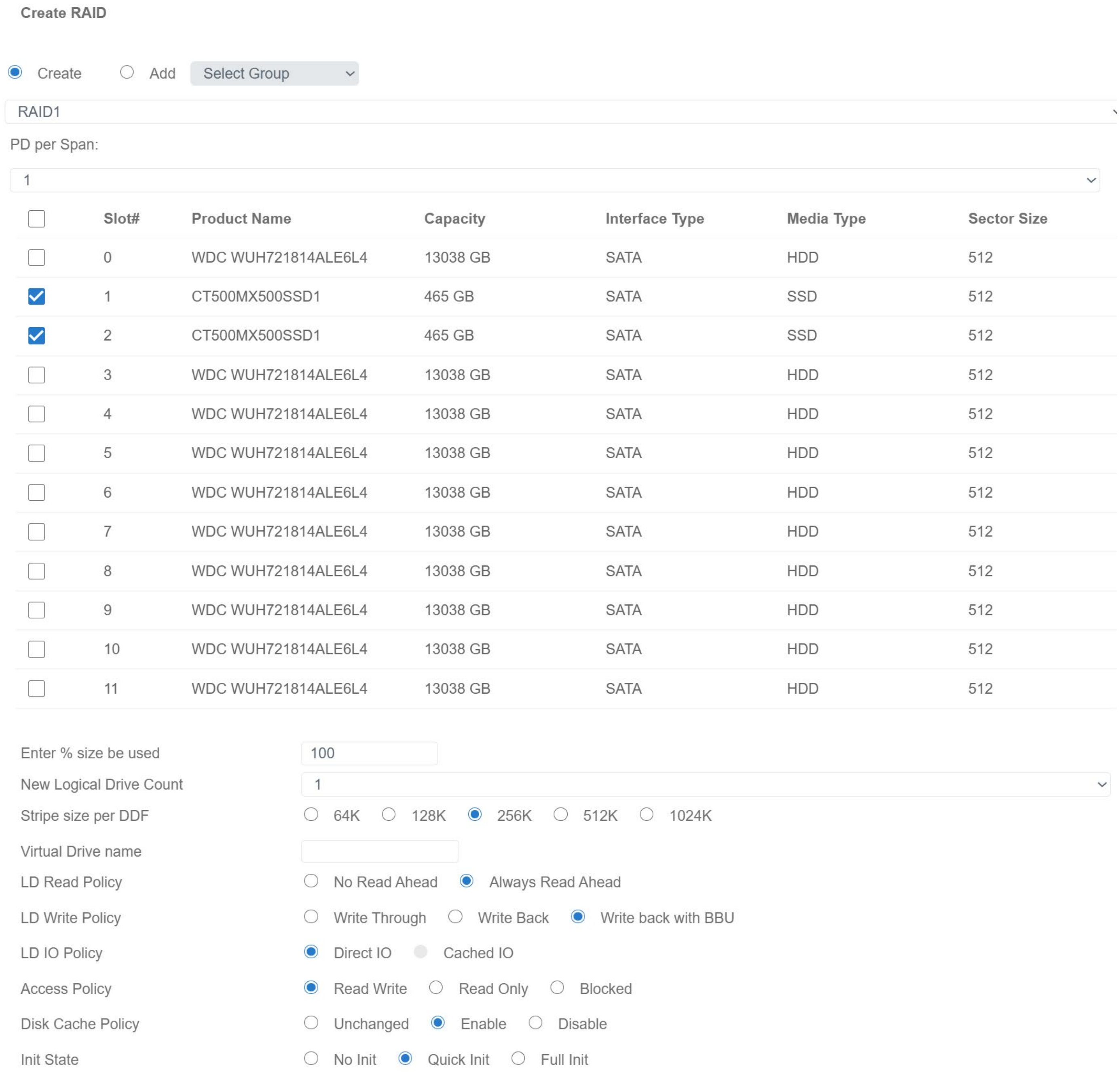
Expand the controller details to access RAID configuration options.

Click "Create RAID".

From the RAID level drop-down menu, select RAID 1 “OS Disk”

Select the two SSDs intended for the OS boot volume.

Submit and proceed to create the RAID 1 set



Create RAID

● Create ○ Add Select Group

RAID1

PD per Span:

1

☐	Slot#	Product Name	Capacity	Interface Type	Media Type	Sector Size
☐	0	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	1	CT500MX500SSD1	465 GB	SATA	SSD	512
☑	2	CT500MX500SSD1	465 GB	SATA	SSD	512
☐	3	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	4	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	5	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	6	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	7	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	8	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	9	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	10	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☐	11	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512

Enter % size be used	100
New Logical Drive Count	1
Stripe size per DDF	○ 64K ○ 128K ● 256K ○ 512K ○ 1024K
Virtual Drive name	
LD Read Policy	○ No Read Ahead ● Always Read Ahead
LD Write Policy	○ Write Through ○ Write Back ● Write back with BBU
LD IO Policy	● Direct IO ○ Cached IO
Access Policy	● Read Write ○ Read Only ○ Blocked
Disk Cache Policy	○ Unchanged ● Enable ○ Disable
Init State	○ No Init ● Quick Init ○ Full Init

Select the "Controller View" in the management interface.

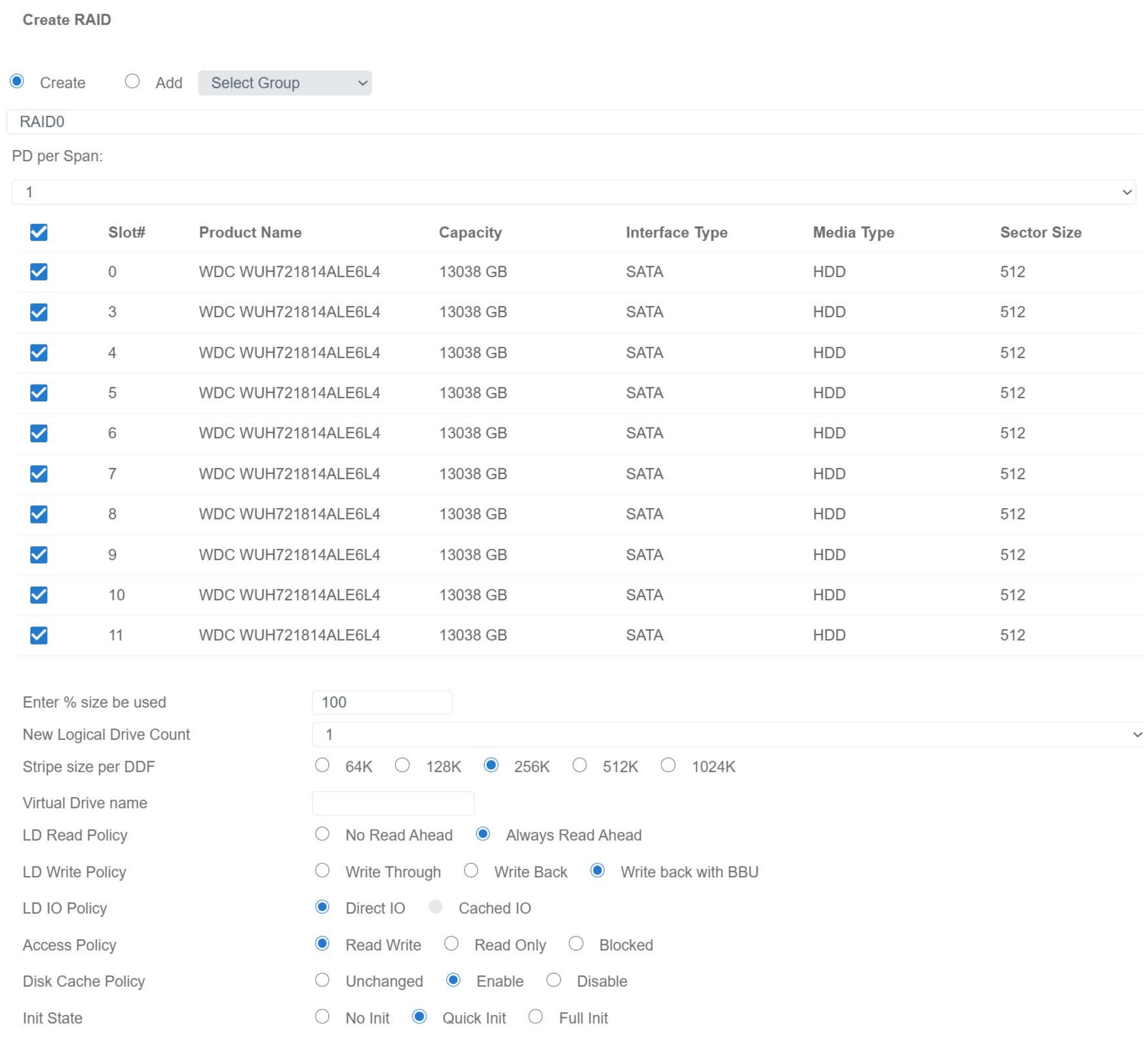
Expand the controller details to access RAID configuration options.

Click "Create RAID".

From the RAID level drop-down menu, select RAID 6 “DATA Disk”

Select the two SSDs intended for the OS boot volume.

Submit and proceed to create the RAID 6 set



Create RAID

● Create ○ Add Select Group

RAID0

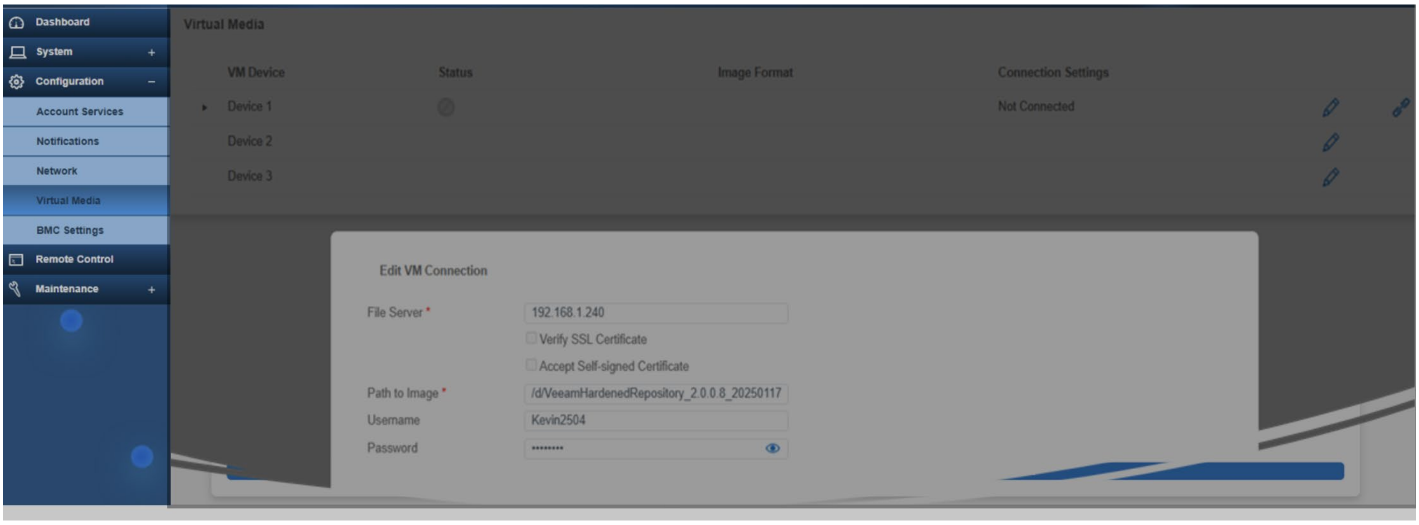
PD per Span:

1

☑	Slot#	Product Name	Capacity	Interface Type	Media Type	Sector Size
☑	0	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	3	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	4	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	5	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	6	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	7	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	8	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	9	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	10	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512
☑	11	WDC WUH721814ALE6L4	13038 GB	SATA	HDD	512

Enter % size be used	100
New Logical Drive Count	1
Stripe size per DDF	○ 64K ○ 128K ● 256K ○ 512K ○ 1024K
Virtual Drive name	
LD Read Policy	○ No Read Ahead ● Always Read Ahead
LD Write Policy	○ Write Through ○ Write Back ● Write back with BBU
LD IO Policy	● Direct IO ○ Cached IO
Access Policy	● Read Write ○ Read Only ○ Blocked
Disk Cache Policy	○ Unchanged ● Enable ○ Disable
Init State	○ No Init ● Quick Init ○ Full Init

In the **Configuration** / **Virtual Media** section, you can attach devices such as storage volumes or ISO files to the server for remote use. By entering the network path to an ISO file stored on shared storage, the server can treat the file as a virtual CD-ROM. As shown in the example below, the ISO becomes available as a bootable device by pressing **F11** during POST. From there, you can install an operating system remotely as if local media were physically connected to the server.



Virtual Media

VM Device	Status	Image Format	Connection Settings
Device 1			Not Connected
Device 2			
Device 3			

Edit VM Connection

File Server * 192.168.1.240

□ Verify SSL Certificate

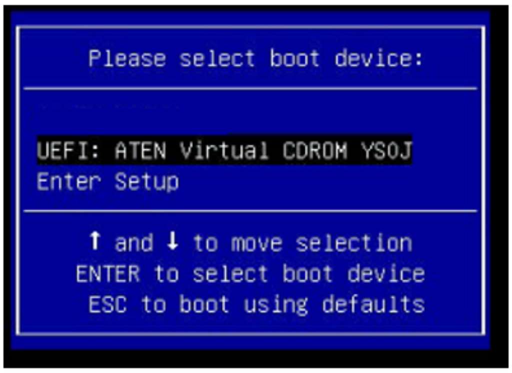
□ Accept Self-signed Certificate

Path to Image * /d/VeeamHardenedRepository_2.0.0.8_20250117

Username Kevin2504

Password ••••••••

Attaching an ISO in Virtual Media



```
      Please select boot device:

UEFI: ATEN Virtual CDROM YSOJ
Enter Setup

      ↑ and ↓ to move selection
     ENTER to select boot device
      ESC to boot using defaults
```

Attached ISO now shows in the boot chain

Install Veeam VHR as directed by Veeam

BMC System Overview

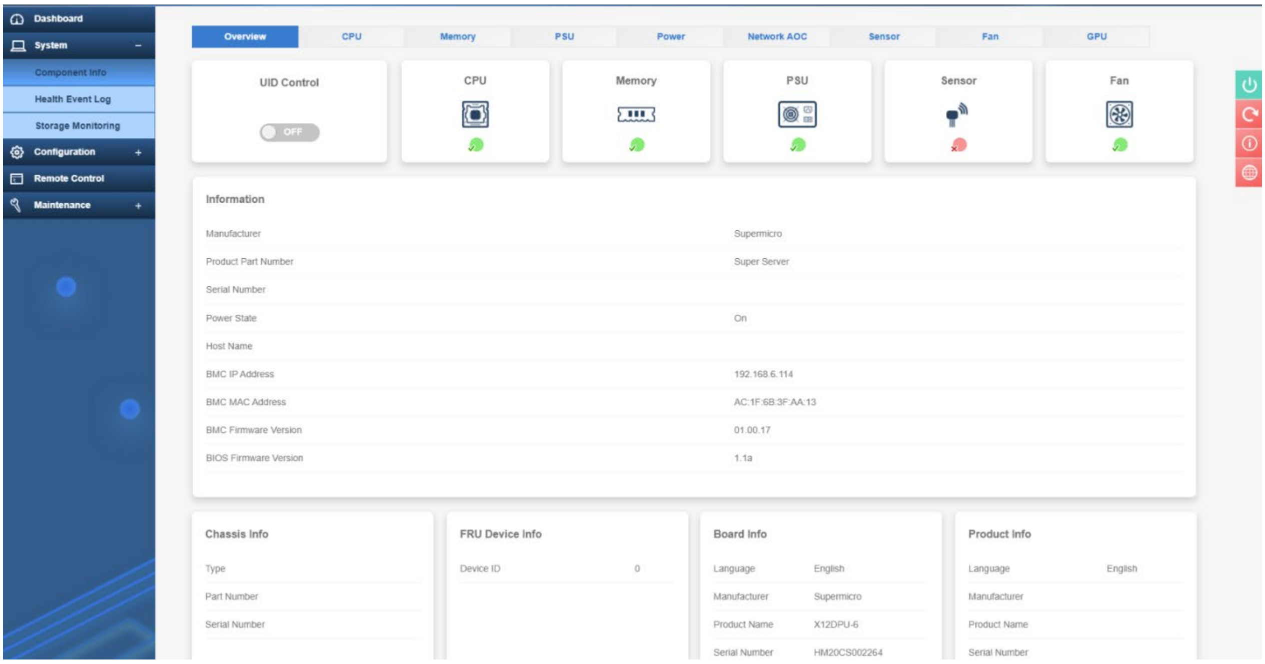
The **Baseboard Management Controller (BMC)** is a specialized microcontroller embedded on the server's motherboard that enables **out-of-band management**. It operates independently of the host system, allowing administrators to monitor and manage the server remotely — even if the OS is unresponsive or powered down.

Key Features:

- Remote power control (on/off/reset)
- System health monitoring (fans, temperatures, voltages)
- Access to logs (SEL – System Event Log)
- Remote KVM (keyboard, video, mouse)
- Virtual media mounting (ISO files, remote storage)

System

In the **System** section, the first subcategory is **Component Info**. This area provides a wealth of useful information about the server. The **Overview** tab includes key inventory details such as product codes, asset tags, serial numbers, and other relevant identifiers that are helpful for asset tracking and system management.



Information

Manufacturer	Supermicro
Product Part Number	Super Server
Serial Number	
Power State	On
Host Name	
BMC IP Address	192.168.6.114
BMC MAC Address	AC:1F:6B:3F:AA:13
BMC Firmware Version	01.00.17
BIOS Firmware Version	1.1a

Chassis Info

Type	
Part Number	
Serial Number	

FRU Device Info

Device ID	0

Board Info

Language	English
Manufacturer	Supermicro
Product Name	X12DPU-6
Serial Number	HM20CS002264

Product Info

Language	English
Manufacturer	
Product Name	
Serial Number	

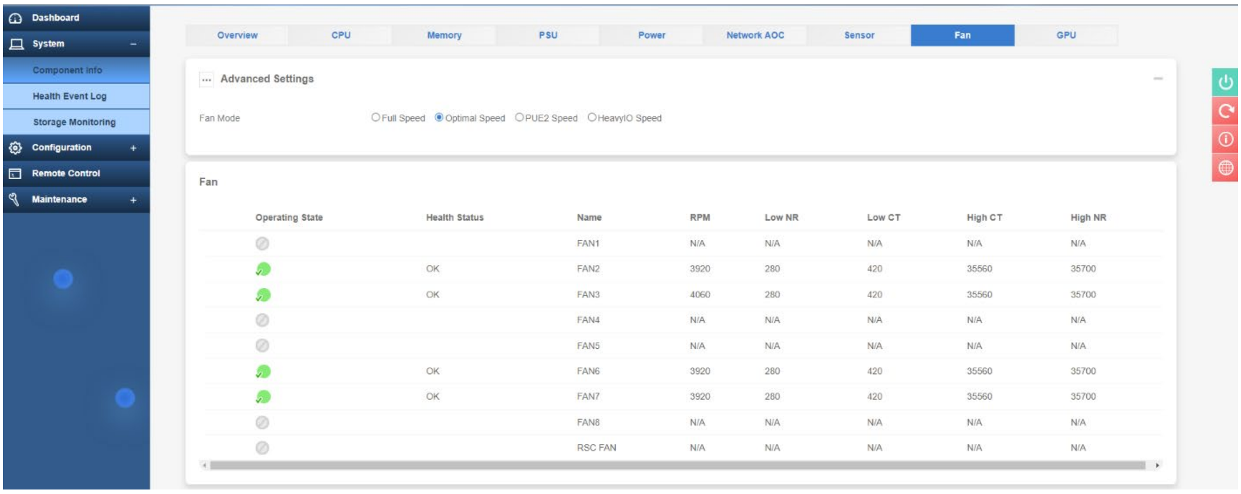
System Overview

Along the top of the **Component Info** section, you'll see various component categories, allowing you to quickly identify if any part of the system is reporting an issue or requires maintenance. Status is indicated by a green or red check mark. For example, if a memory module fails, the **Memory** icon will display a red check, and clicking on it will highlight the specific module that has encountered an issue.

Each category provides details on the installed components, such as CPUs, power supplies, network cards, and graphics cards. Any hardware issue will be clearly flagged within its respective section.

In the **Fan** section, you can view fan status and speeds, and choose from several fan modes:

- **Standard** – Default fan speed
- **Full Speed** – Maximum cooling
- **Optimal** – Balances fan speed and power usage based on temperature sensors
- **Heavy I/O** – Boosts cooling in areas with high add-on card activity



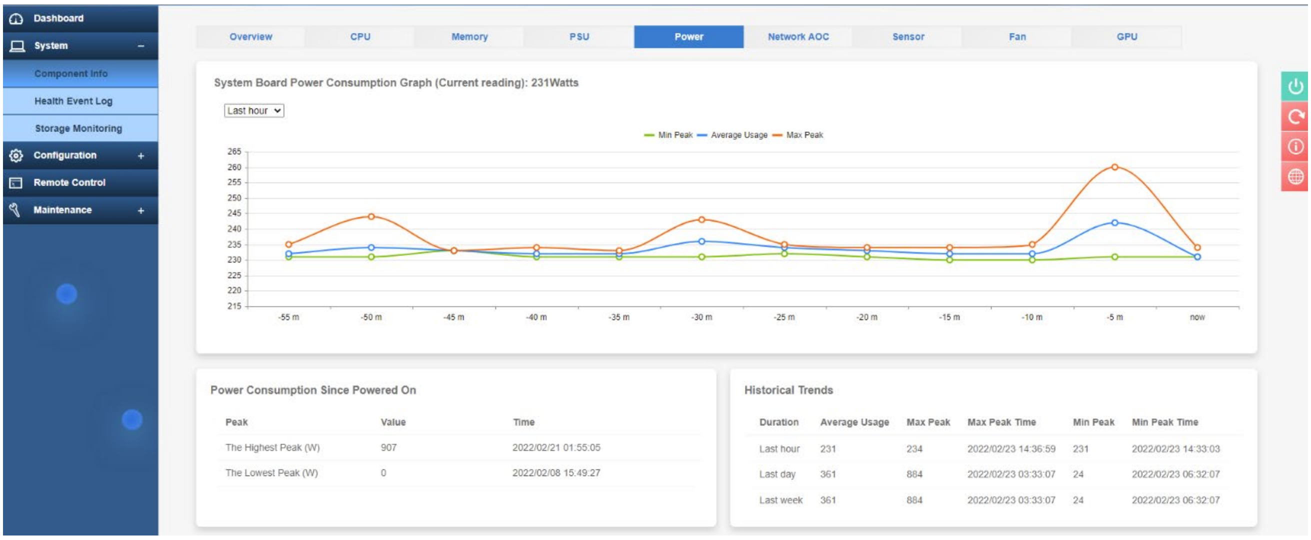
Fan Mode ○ Full Speed ● Optimal Speed ○ PUE2 Speed ○ HeavyIO Speed

Fan

Operating State	Health Status	Name	RPM	Low NR	Low CT	High CT	High NR
⊘		FAN1	N/A	N/A	N/A	N/A	N/A
✓	OK	FAN2	3920	280	420	35560	35700
✓	OK	FAN3	4060	280	420	35560	35700
⊘		FAN4	N/A	N/A	N/A	N/A	N/A
⊘		FAN5	N/A	N/A	N/A	N/A	N/A
✓	OK	FAN6	3920	280	420	35560	35700
✓	OK	FAN7	3920	280	420	35560	35700
⊘		FAN8	N/A	N/A	N/A	N/A	N/A
⊘		RSC FAN	N/A	N/A	N/A	N/A	N/A

Fan control

Other items of note are the power readings. This is useful to see how much power is being drawn as well as historical data.



System Board Power Consumption Graph (Current reading): 231Watts

Power Consumption Since Powered On

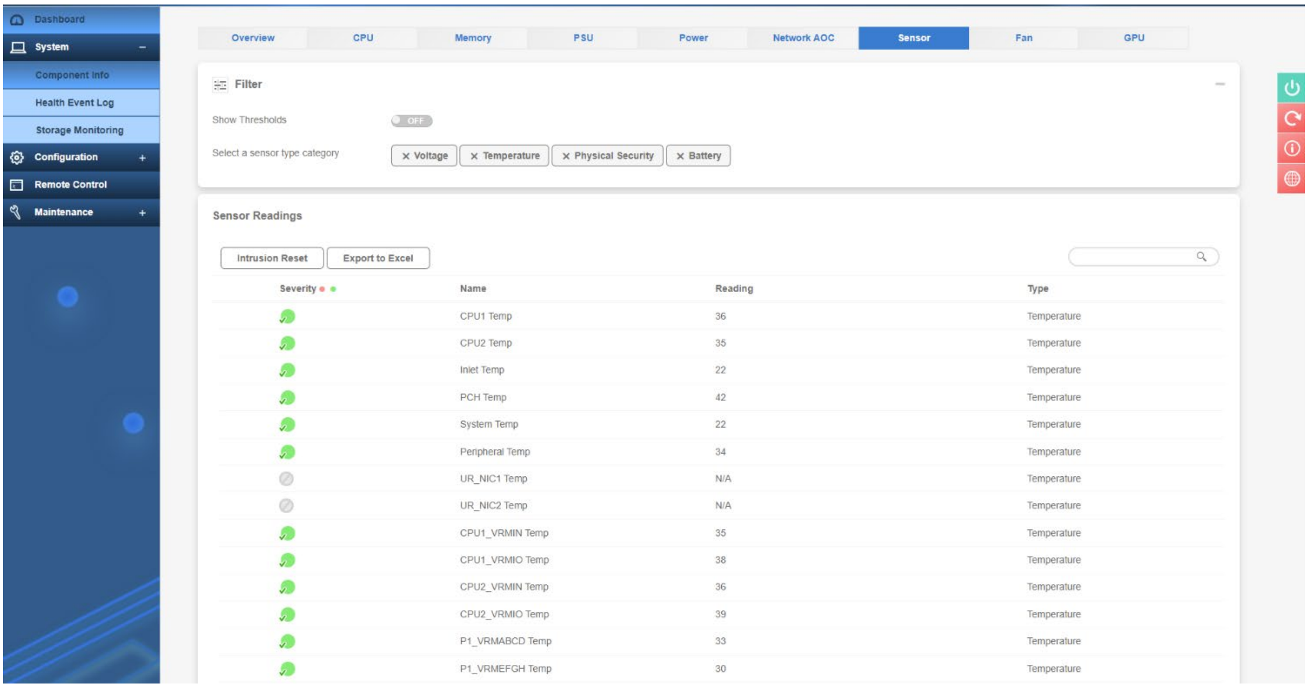
Peak	Value	Time
The Highest Peak (W)	907	2022/02/21 01:55:05
The Lowest Peak (W)	0	2022/02/08 15:49:27

Historical Trends

Duration	Average Usage	Max Peak	Max Peak Time	Min Peak	Min Peak Time
Last hour	231	234	2022/02/23 14:36:59	231	2022/02/23 14:33:03
Last day	361	884	2022/02/23 03:33:07	24	2022/02/23 06:32:07
Last week	361	884	2022/02/23 03:33:07	24	2022/02/23 06:32:07

IPMI power data

The **Sensor** section is a vital part of IPMI for monitoring server health. It provides a wide range of real-time data, including temperatures for components such as CPUs, memory, NICs, and SSDs. It also displays voltage levels and the status of key components like fan speeds and power supplies. This section is an essential tool for gaining a comprehensive overview of the system's operational health and identifying potential hardware issues early.



Show Thresholds OFF

Select a sensor type category × Voltage × Temperature × Physical Security × Battery

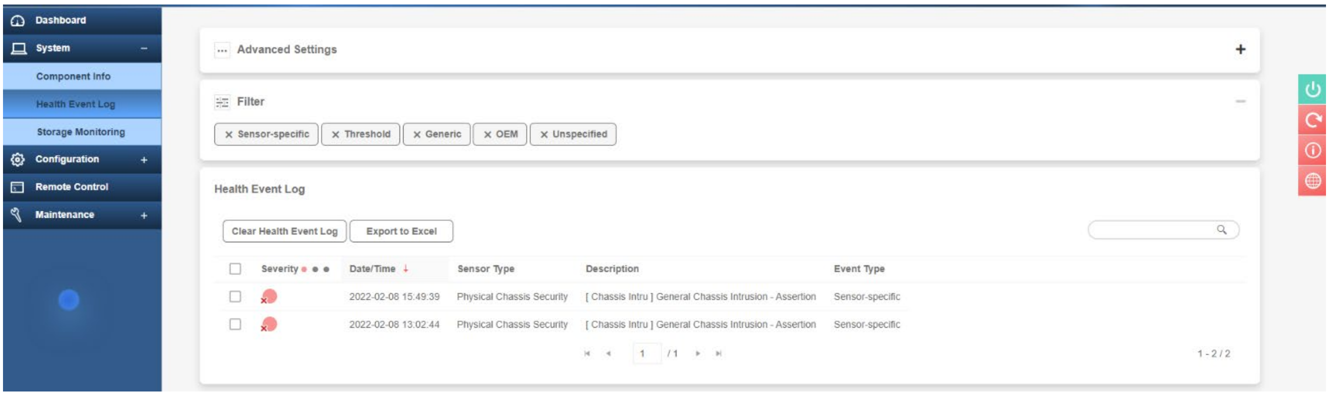
Sensor Readings

Intrusion Reset | Export to Excel

Severity	Name	Reading	Type
●	CPU1 Temp	36	Temperature
●	CPU2 Temp	35	Temperature
●	Inlet Temp	22	Temperature
●	PCH Temp	42	Temperature
●	System Temp	22	Temperature
●	Peripheral Temp	34	Temperature
○	UR_NIC1 Temp	N/A	Temperature
○	UR_NIC2 Temp	N/A	Temperature
●	CPU1_VRMIN Temp	35	Temperature
●	CPU1_VRMIO Temp	38	Temperature
●	CPU2_VRMIN Temp	36	Temperature
●	CPU2_VRMIO Temp	39	Temperature
●	P1_VRMABCD Temp	33	Temperature
●	P1_VRMEFGH Temp	30	Temperature

Sensor readings

The next section is the **Health Event Log**, which records a wide range of system events. These can include routine entries such as the operating system booting, disk drive removal, or chassis intrusion alerts (for security monitoring). More critical and useful entries include component failures, such as fan issues or faulty memory DIMMs. Each event log entry provides detailed information, including the specific component affected — for example, “PS1” would indicate a failure in Power Supply 1 on a dual-PSU system. This level of detail is especially helpful when identifying faulty parts for diagnostics or RMA processing.



× Sensor-specific × Threshold × Generic × OEM × Unspecified

Health Event Log

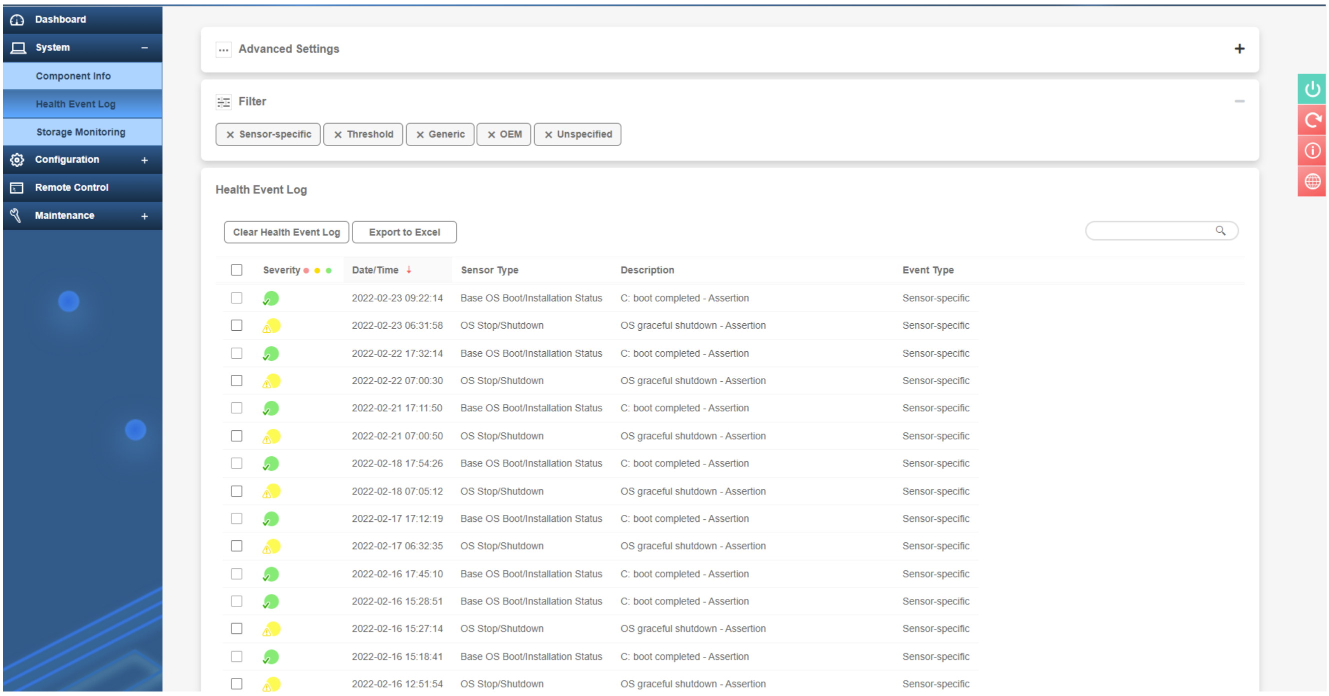
Clear Health Event Log | Export to Excel

□	Severity	Date/Time	Sensor Type	Description	Event Type
□	●	2022-02-08 15:49:39	Physical Chassis Security	[Chassis Intru] General Chassis Intrusion - Assertion	Sensor-specific
□	●	2022-02-08 13:02:44	Physical Chassis Security	[Chassis Intru] General Chassis Intrusion - Assertion	Sensor-specific

1 / 1 1 - 2 / 2

Power supply failure example

The events range in severity from red (critical alert) to green (general info).



□	Severity	Date/Time	Sensor Type	Description	Event Type
□	✓	2022-02-23 09:22:14	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-23 06:31:58	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-22 17:32:14	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-22 07:00:30	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-21 17:11:50	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-21 07:00:50	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-18 17:54:26	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-18 07:05:12	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-17 17:12:19	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-17 06:32:35	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-16 17:45:10	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	✓	2022-02-16 15:28:51	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-16 15:27:14	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific
□	✓	2022-02-16 15:18:41	Base OS Boot/Installation Status	C: boot completed - Assertion	Sensor-specific
□	⚠	2022-02-16 12:51:54	OS Stop/Shutdown	OS graceful shutdown - Assertion	Sensor-specific

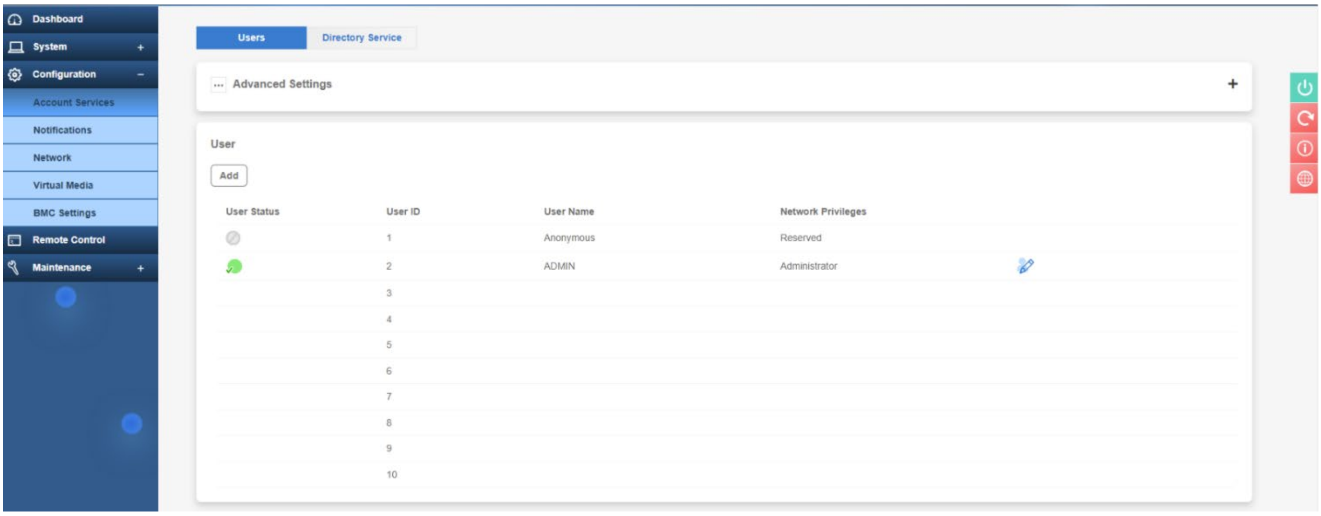
Health Event Log

Finally, the **System** section also includes **Storage Monitoring**, which provides valuable insights into your storage devices, including HDDs, SSDs, and NVMe drives. This section offers both a high-level health overview and detailed physical and logical views of the storage media. The **logical view** becomes active once RAID volumes are configured, showing how drives are grouped and utilized. Additionally, the **Controller View** allows you to manage the dedicated hardware RAID controller — including tasks such as creating RAID volumes and performing firmware management. We'll explore these features in more detail in a future module.

Configuration

The **Configuration** tab is one of the main sections in the IPMI interface, providing access to various system settings.

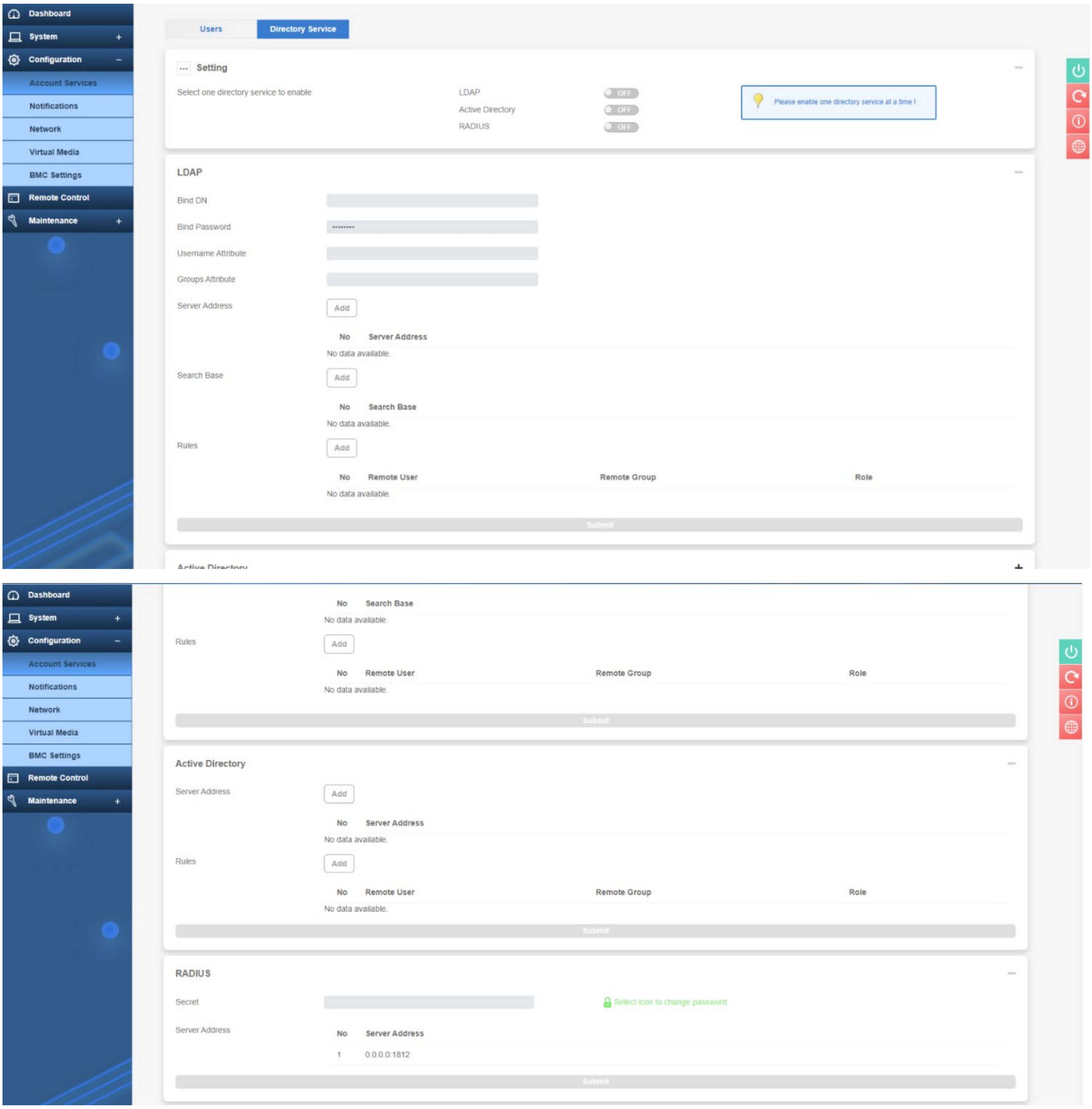
Within **Account Services**



User Status	User ID	User Name	Network Privileges	
⊘	1	Anonymous	Reserved	
✓	2	ADMIN	Administrator	✎
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	10			

IPMI User and Login Control

'Under Directory Service' is where more refined access control exits. Here you can link to an Active Directory service and configure LDAP and RADIUS authentication protocols.



Setting

Select one directory service to enable

LDAP OFF
Active Directory OFF
RADIUS OFF

Please enable one directory service at a time !

LDAP

Bind DN

Bind Password ••••••••

Username Attribute

Groups Attribute

Server Address Add

No	Server Address

No data available.

Search Base Add

No	Search Base

No data available.

Rules Add

No	Remote User	Remote Group	Role

No data available.

Submit

Active Directory

No	Search Base

No data available.

Rules Add

No	Remote User	Remote Group	Role

No data available.

Submit

Active Directory

Server Address Add

No	Server Address

No data available.

Rules Add

No	Remote User	Remote Group	Role

No data available.

Submit

RADIUS

Secret

Select icon to change password

Server Address

No	Server Address
1	0.0.0.0:1812

Submit

LDAP, Active Directory and RADIUS configuration

Other powerful monitoring features within IPMI can be configured in the **Notifications** section. This allows administrators to set up alerts for a variety of events, such as server status changes, component failures, or unauthorized IPMI access attempts. Notifications can be delivered using protocols like **Redfish** or **SNMP traps**, which require a receiving server to capture and process the alerts.

Alerts configuration

The next section under Configuration is Network, where you can configure the IPMI network settings. Assigning a static IP address is highly recommended for IPMI access, and this can be set here or via the BIOS, as shown earlier. You can also define a hostname for each server to help differentiate systems and assign the IPMI interface to a VLAN, if required.

This section also allows you to specify which LAN port the IPMI interface should use. For example, if you prefer not to connect a cable to the dedicated IPMI port, you can choose to share LAN1 for both network and IPMI traffic. Despite using the same physical port, IPMI remains isolated because it has its own MAC address, ensuring there is no interference between IPMI and regular network traffic.

Another available option is Failover mode. In this setup, the system primarily uses the dedicated IPMI port, but if it fails to connect during boot, IPMI will automatically switch to LAN1, maintaining remote management access.

IPMI Network Configuration

The Network section also allows you to change the default ports used by key services such as SSL, iKVM, and SSH. Changing these ports from their defaults can enhance security by reducing exposure to automated attacks that target known ports. Additionally, IP Access Control can be configured to restrict IPMI access to specific IP addresses or subnets.

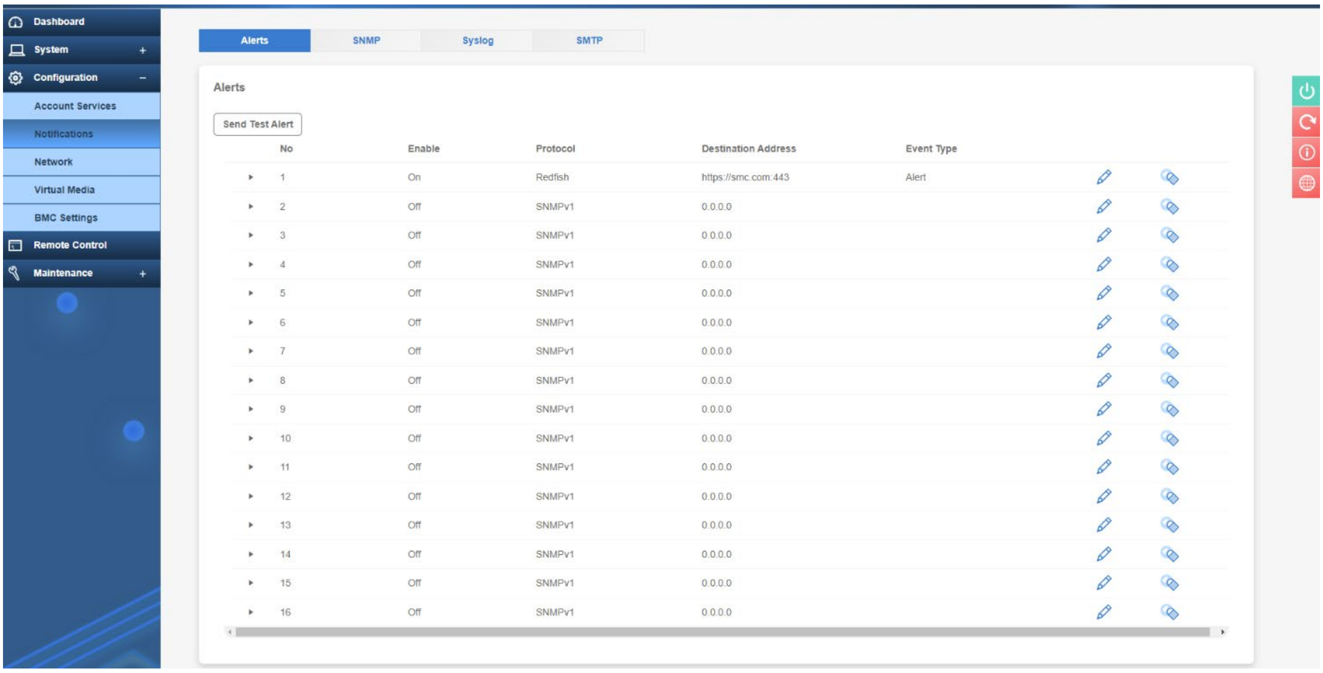
For further security, administrators can upload and configure SSL certificates along with private keys. This ensures encrypted communications and helps prevent unauthorized access. These security features are critical, as unauthorized access to IPMI would present a serious risk to any server infrastructure. Each setting should be reviewed and configured with care to maintain a secure environment.

In the Virtual Media section, you can attach devices such as storage volumes or ISO files to the server for remote use. For example, by entering the network path to an ISO file stored on shared storage, the server can treat the file as a virtual CD-ROM. As shown in the example below, the ISO becomes available as a bootable device by pressing F11 during POST. From there, you can install an operating system remotely as if local media were physically connected to the server.

Attaching an ISO in Virtual Media

Attached ISO now shows in the boot chain

Alternatively, **SMTP** can be configured to send **email alerts**, providing real-time visibility into critical system events.



Alerts

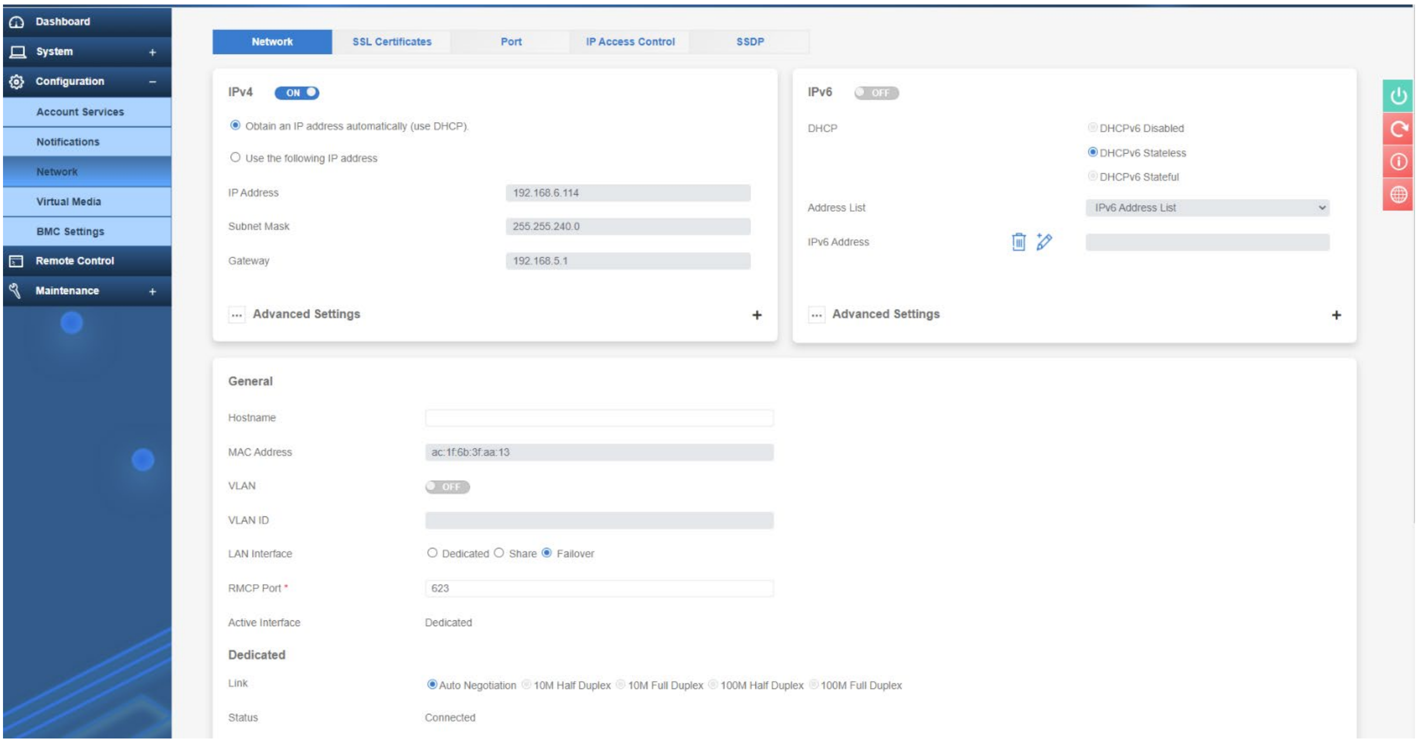
No	Enable	Protocol	Destination Address	Event Type
1	On	Redfish	https://smc.com:443	Alert
2	Off	SNMPv1	0.0.0.0	
3	Off	SNMPv1	0.0.0.0	
4	Off	SNMPv1	0.0.0.0	
5	Off	SNMPv1	0.0.0.0	
6	Off	SNMPv1	0.0.0.0	
7	Off	SNMPv1	0.0.0.0	
8	Off	SNMPv1	0.0.0.0	
9	Off	SNMPv1	0.0.0.0	
10	Off	SNMPv1	0.0.0.0	
11	Off	SNMPv1	0.0.0.0	
12	Off	SNMPv1	0.0.0.0	
13	Off	SNMPv1	0.0.0.0	
14	Off	SNMPv1	0.0.0.0	
15	Off	SNMPv1	0.0.0.0	
16	Off	SNMPv1	0.0.0.0	

Alerts configuration

The next section under **Configuration** is **Network**, where you can configure the IPMI network settings. Assigning a **static IP address** is highly recommended for IPMI access, and this can be set here or via the BIOS, as shown earlier. You can also define a **hostname** for each server to help differentiate systems and assign the IPMI interface to a **VLAN**, if required.

This section also allows you to specify which **LAN port** the IPMI interface should use. For example, if you prefer not to connect a cable to the **dedicated IPMI port**, you can choose to share **LAN1** for both network and IPMI traffic. Despite using the same physical port, IPMI remains isolated because it has its **own MAC address**, ensuring there is no interference between IPMI and regular network traffic.

Another available option is **Failover mode**. In this setup, the system primarily uses the **dedicated IPMI port**, but if it fails to connect during boot, IPMI will automatically switch to **LAN1**, maintaining remote management access.



IPv4 ON

● Obtain an IP address automatically (use DHCP).

○ Use the following IP address

IP Address	192.168.6.114
Subnet Mask	255.255.240.0
Gateway	192.168.5.1

... Advanced Settings +

IPv6 OFF

DHCP ○ DHCPv6 Disabled ● DHCPv6 Stateless ○ DHCPv6 Stateful

Address List: IPv6 Address List

IPv6 Address

... Advanced Settings +

General

Hostname	
MAC Address	ac:1f:6b:3f:aa:13
VLAN	OFF
VLAN ID	
LAN Interface	○ Dedicated ○ Share ● Failover
RMCP Port *	623
Active Interface	Dedicated

Dedicated

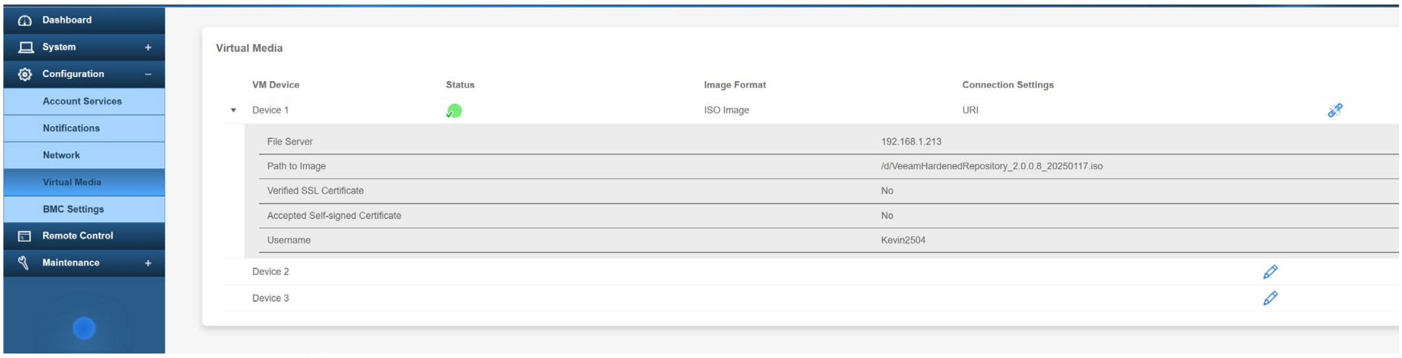
Link	● Auto Negotiation ○ 10M Half Duplex ○ 10M Full Duplex ○ 100M Half Duplex ○ 100M Full Duplex
Status	Connected

IPMI Network Configuration

The **Network** section also allows you to change the default ports used by key services such as **SSL**, **iKVM**, and **SSH**. Changing these ports from their defaults can enhance security by reducing exposure to automated attacks that target known ports. Additionally, **IP Access Control** can be configured to restrict IPMI access to specific IP addresses or subnets.

For further security, administrators can upload and configure **SSL certificates** along with private keys. This ensures encrypted communications and helps prevent unauthorized access. These security features are critical, as unauthorized access to IPMI would present a serious risk to any server infrastructure. Each setting should be reviewed and configured with care to maintain a secure environment.

In the **Virtual Media** section, you can attach devices such as storage volumes or ISO files to the server for remote use. For example, by entering the network path to an ISO file stored on shared storage, the server can treat the file as a virtual CD-ROM. As shown in the example below, the ISO becomes available as a bootable device by pressing **F11** during POST. From there, you can install an operating system remotely as if local media were physically connected to the server.



Virtual Media

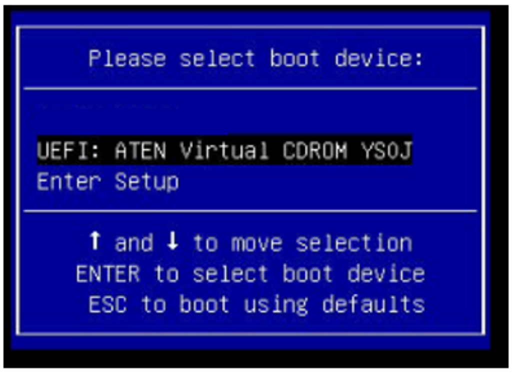
VM Device	Status	Image Format	Connection Settings
▾ Device 1	✓	ISO Image	URI

File Server	192.168.1.213
Path to Image	/d/VeeamHardenedRepository_2.0.0.8_20250117.iso
Verified SSL Certificate	No
Accepted Self-signed Certificate	No
Username	Kevin2504

Device 2

Device 3

Attaching an ISO in Virtual Media

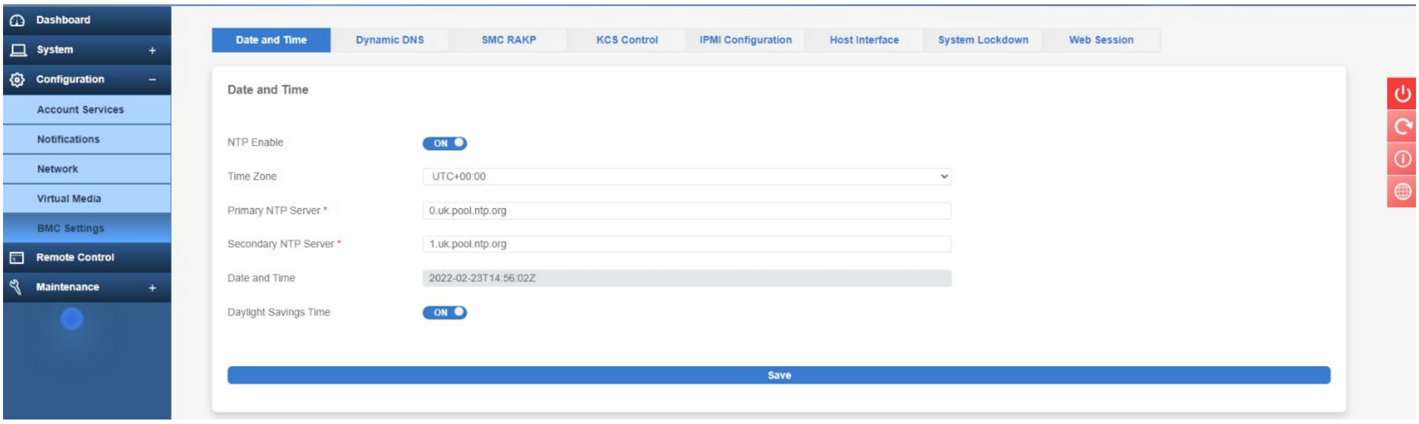


```
Please select boot device:

UEFI: ATEN Virtual CDROM YSOJ
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

The attached ISO now shows in the boot chain

The final section under **Configuration** is **BMC Settings**, which relates to the **Baseboard Management Controller (BMC)** — the hardware component that powers IPMI functionality. One important item here is the **Date and Time** configuration. This allows you to manually set the time or, preferably, configure an **NTP (Network Time Protocol) server** to ensure the system clock stays accurate and synchronized with your network's time source.

.



Date and Time

NTP Enable: ON

Time Zone: UTC+00:00

Primary NTP Server *: 0.uk.pool.ntp.org

Secondary NTP Server *: 1.uk.pool.ntp.org

Date and Time: 2022-02-23T14:56:02Z

Daylight Savings Time: ON

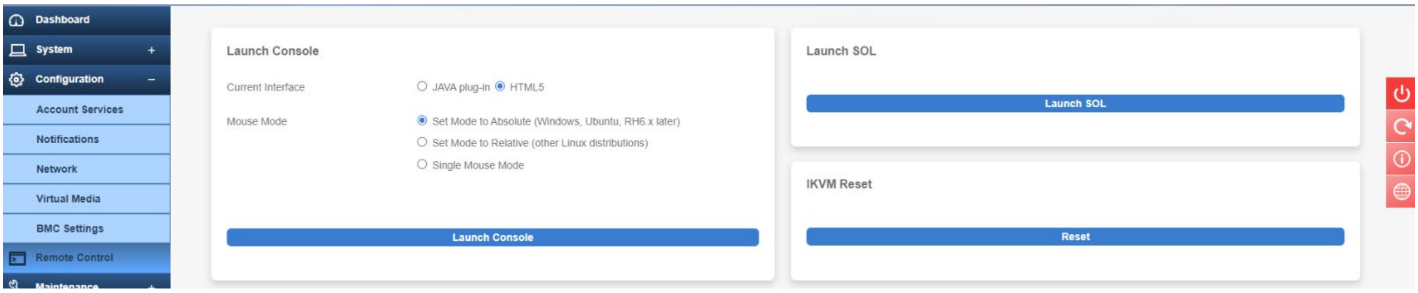
Using an NTP server for Date and Time

You can also **save the current IPMI configuration to a file** for backup purposes — a useful feature if you ever need to reset the BMC or replace the motherboard. Restoring this configuration can save time and ensure consistency across hardware changes.

In the **Web Session** settings, you can define the **inactivity timeout** for IPMI logins. This is a good security practice to help prevent unauthorized access in unattended sessions. By default, the timeout is set to **30 minutes**, but it can be adjusted to suit your organization's security policies.

Remote Control

A great feature of IPMI is the ability to fully control the server as if you were sitting right in front of it. A powerful admin tool indeed.



Launch Console

Current Interface: ○ JAVA plug-in ● HTML5

Mouse Mode:
● Set Mode to Absolute (Windows, Ubuntu, RH6.x later)
○ Set Mode to Relative (other Linux distributions)
○ Single Mouse Mode

Launch SOL

IKVM Reset

IPMI Remote Control Options

You can launch the remote console using either **Java** or the newer **HTML5** interface. For a smoother and more reliable experience, the **HTML5 console** is recommended, as it's less prone to compatibility issues and doesn't require Java to be installed on your local machine — something that may be restricted in security-conscious environments.

However, it's important to note that the **HTML5 console does not support virtual media attachment by default**. This functionality requires a **Supermicro license upgrade**, which we'll cover in more detail in a future article.

To launch the console, simply click the **Launch Console** button for the selected interface. If using the Java console, a small **JNLP (Java Network Launch Protocol)** file will be downloaded and executed.

Once inside the console, you'll find features similar to those in the web interface. For example, under **Virtual Media**, you can attach a local ISO file to perform an OS installation as if it were physically connected to the server. The **Macro** section offers useful shortcuts like *Ctrl+Alt+Del*, which can be essential during setup or troubleshooting.

In the **Preferences** tab, you can adjust display, input, and language options — though in most cases, the defaults are sufficient. Lastly, the **Power Control** section allows you to safely shut down the server (via *Software Shutdown*), force a power-off, or perform a hard reboot

Configure BMC Network Settings with Security on This Server

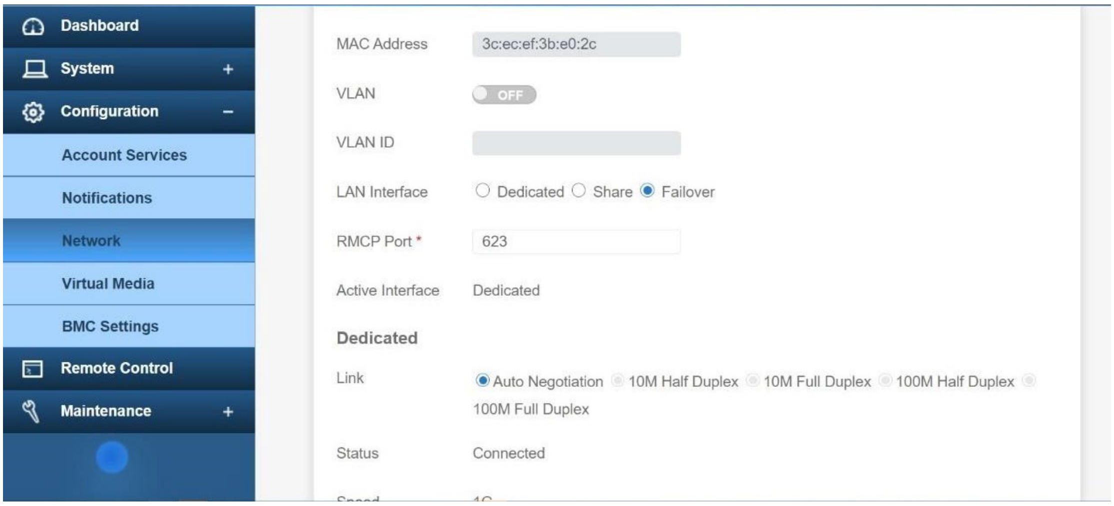
While this feature increases convenience and productivity, server administrators must understand that BMCs are embedded controllers with an operating system and network stack that can be vulnerable to attacks if not configured correctly. This feature guide provides several practical use cases to help users understand how proper BMC configurations can mitigate vulnerability attacks.

IP Address Assignment

DHCP is the default protocol for receiving IP addresses. However, administrators are encouraged to set static IP addresses or restrict the assignment of DHCP addresses to a secure set of IP addresses or subnet.

LAN Access

The BMC can be accessed through either a dedicated Ethernet LAN interface (if available) or through a shared LAN (System LAN) Interface. The default setting is 'failover,' which means the BMC will first check for the presence of an active, dedicated LAN interface; otherwise, it will respond through a shared LAN interface. The failover setting helps IT administrators receive default connectivity to the BMC, irrespective of their network topology, and provision systems remotely. It is recommended that administrators configure BMCs LAN access through a dedicated LAN interface instead of a System LAN. The BMC is not exposed to the internet or unauthorized user access outside of a firewall.
While the IPMI standard protocol defines UDP port 623 for RMCP communications, BMCs also provide additional remote services to efficiently provision and debug servers. Some of these services include VNC for debugging an OS, access to http/https ports for BMC settings and reading server health, and Virtual media for remotely accessing files and images.



MAC Address 3c:ec:ef:3b:e0:2c

VLAN OFF

VLAN ID

LAN Interface ○ Dedicated ○ Share ● Failover

RMCP Port * 623

Active Interface Dedicated

Dedicated

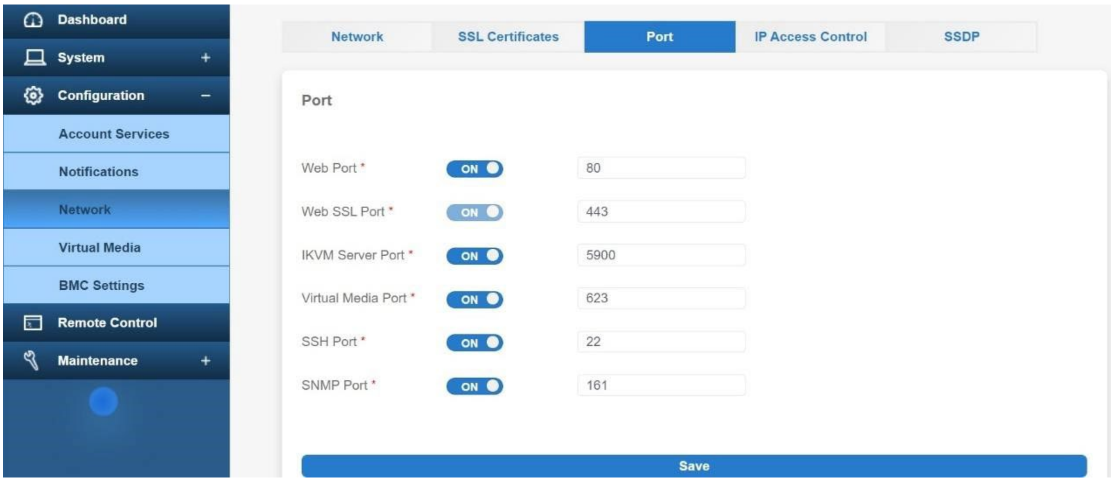
Link ● Auto Negotiation ○ 10M Half Duplex ○ 10M Full Duplex ○ 100M Half Duplex ○ 100M Full Duplex

Status Connected

Note: Unhooking an Ethernet cable from a dedicated LAN interface does not stop accessing BMCs from a shared LAN interface.

Service Ports

All these services run on TCP/UDP ports (please see the security feature guide for the latest information), and it is important to restrict these ports to secure the server management network. Alternatively, the administrator can reconfigure the port numbers or disable unused services to avoid unnecessary security exposure on BMCs. For example, http can be configured to listen on port 76680 such that attackers cannot find the servers through common port scanning tools.



Port

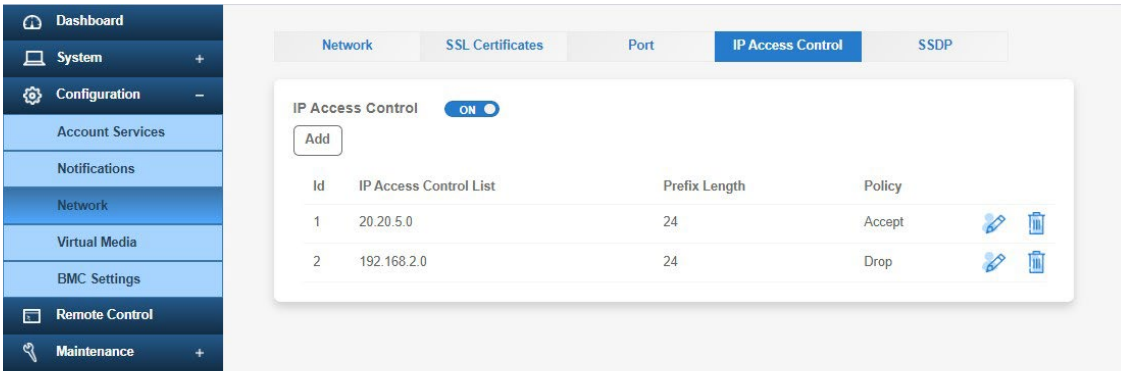
Web Port *	ON	80
Web SSL Port *	ON	443
IKVM Server Port *	ON	5900
Virtual Media Port *	ON	623
SSH Port *	ON	22
SNMP Port *	ON	161

RAKP

IPMI standard dictates using the RAKP protocol to authenticate RMCP sessions between IPMI clients and BMC servers. The current RAKP hash is typically weak, meaning that one can use brute methods to retrieve passwords. The Supermicro BMC provides a stronger hash option for RAKP authentication. Since this is an OEM implementation and may not be suitable in every environment, administrators still recommend blocking UDP port 623 on unsecured networks.

IP Access Controls

BMC access should be restricted to include only known machine IP Addresses. This eliminates unwarranted access to corporate servers from inside the network accidentally or deliberately.



IP Access Control ON

Id	IP Access Control List	Prefix Length	Policy
1	20.20.5.0	24	Accept
2	192.168.2.0	24	Drop

VLAN Configurations

Configure traffic from BMCs to IPMI clients on a unique VLAN so that management traffic can be segregated from the rest of the server data.

Configuring the BMC Network

Though BMCs provide security features to defend against unwarranted attacks, it is strongly recommended that administrators follow the best practice of configuring BMCs on the networks where they are locally accessible and restrict traffic on sensitive ports between networks. Traffic on default ports for BMCs such as TCP/5900 and UDP/ 623 should be restricted to secure and known networks using firewall rules in routers.

BMC management account security

Supermicro BMC provides the following two secure functions to enhance BMC user accounts security and protect from excessive failed login attempts:

1. Authentication failure lockout controls

When user authentication fails, the Supermicro BMC solution can notify the user about the logging fault threshold and deny the user further login authentication, even with the correct password. In addition, the frequency of event logs, the number of failed attempts, and the time for the lockout to expire can be adjusted via the BMC web user interface.

2. Password complexity and value rules

Supermicro BMC solution secures each user account with password complexity, preventing hackers from easily or systematically cracking the user account password. As a result, either IT administrators or ordinary users can enjoy a secured remote management environment provided by the Supermicro BMC solution.

Password Security

Supermicro BMC solution equips every Supermicro product with a preprogrammed BMC management password, which is unique. It requires a user to generate a new means of authentication before access is granted to the device for the first time. This security mechanism can secure customers to have a more secure management environment afterward. More importantly, it can comply with SB-327 law (California Law). Otherwise, Special characters like #,$ are not allowed into the password field, as these characters can enable shell injection from intruders. Instead, use strong passwords that are at least eight characters long and include a mix of numbers, capital, and lower-case letters.

System Lockdown

Supermicro BMC solution can support the System Lockdown feature, and it offers IT administrators a secure way to prevent unintentional system configuration changes. All system configuration changes, including firmware updates, are restricted when system lockdown is enabled. As a result, the ordinary user only receives notifications when the IT administrator makes a system configuration change. System lockdown can be configured by following Supermicro interfaces:

- Web GUI
- IPMI command
- Redfish
- BIOS GUI
- SUM (Supermicro Update Manager)

HTTPS for Web access

Supermicro BMC web server provides HTTPs connection by default to provide both IT administrators and ordinary users a more secure method to access runtime remote management data via the Supermicro BMC solution HTTPS uses the SSL/TLS protocol to encrypt communications to avoid attackers stealing data. In addition, the Supermicro BMC solution contains SSL/TLS design, preventing impersonations and stopping multiple kinds of cyber attacks.

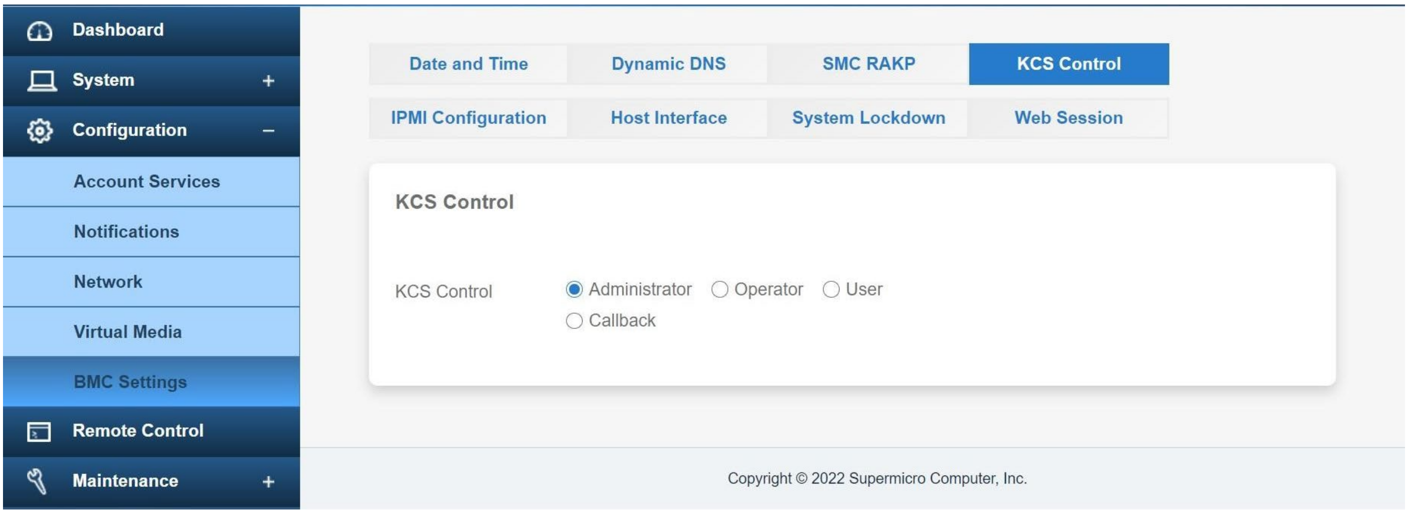
SNMPv3

Supermicro BMC solution also provides a more secure Simple Network Management Protocol Ver. 3(SNMPv3). The biggest security concern in SNMPv1 and SNMPv2 is that community strings are sent as clear-text strings and not encrypted, which means data transmission over SNMPv1 and SNMPv2 is not secure. This security concern has been fixed by SNMPv3 and ensures community strings are always encrypted. IT Administrators can use SNMPv3 on the Supermicro BMC solution directly to make your data center's network environment secure.

KCS Privilege Control

Supermicro BMC solution also enhances the security of legacy IPMI in-band interface – KCS (Keyboard Controller Style). IPMI spec defines the privilege for IPMI Messaging Interface, but it is not applied to the KCS interface since it is a session-less interface. That causes the security issue. To secure the KCS interface, the Supermicro BMC solution offers enhanced features to secure your system inside.

IT Administrators can configure KCS privileges by BMC Web and redfish API.



KCS Control

KCS Control ● Administrator ○ Operator ○ User ○ Callback

Disallow In-band firmware updates over the KCS interface

This restriction is implemented in the latest Supermicro X12 platforms or later. Disable in-band firmware updates over the KCS
interface and only support in-band firmware updates through LAN/USB interface, which is much faster and more secure. ● Detailed conventions:

- Only Update Manager can update BIOS and BMC firmware through the BMC in-band interface
- 3rd party tools (which are NOT validated by Supermicro) will not be allowed to work from Supermicro X12 platforms

Secure Redfish APIs

Supermicro BMC solution also can support DMTF Redfish®. A standard API delivers simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). This modern interface builds on widely used tools to accelerate development. Today's customers demand a well-defined API that uses the protocols, structures, and security models standard in Internet and web services environments.

Secure In-band authentication through the Host interface

Furthermore, the Supermicro BMC solution can support Redfish Host Interface Specification (DSP0270), providing BMC a secure communication channel to the host OS or UEFI.

Main security features include:

- Support authentication, confidentiality, and integrity:
    - Support environments where users do not want to rely on Host/OS access control mechanisms solely Provide a mechanism to optionally (if configured) pass credentials to an OS Kernel for sensor monitoring (with configurable privilege)
    - Support security requirements with authentication and confidentiality

BIOS-BMC secure features

The server BMC solution can configure BIOS secure features, Secure Boot, and Secure Drive Erase via Redfish's secure interface. As a result, IT administrators can leverage these two security features when provisioning or maintaining a system.

- Secure Boot
    - Secure boot is part of the UEFI firmware standard (since 2.3.1c). A machine refuses to load any UEFI driver or app with secure boot enabled unless the operating system bootloader is cryptographically signed.

- Secure Drive Erase
    - IT administrators can apply an action to erase the disk connected with the Broadcom MegaRAID controller, and it allows IT administrators to render data on attached drives instantly and securely.

Summary of Nexsan VHR-Series

What Nexsan Will Deliver with Veeam-Certified VHR-Series

Upon Veeam's validation and certification of the Nexsan VHR-Series, we will bring to market a fully integrated, enterprise-class Hardened Repository appliance purpose-built for Veeam environments. The VHR-Series will be preloaded with the Veeam Hardened Repository ISO, designed to meet stringent requirements for immutability, security, and performance in ransomware-resilient backup.

With a usable capacity range from 64TB to 3.3PB, and seamless scalability through integration with Nexsan's proven E-Series expansion shelves, the VHR-Series will offer a flexible solution for organizations of all sizes—from mid-market to petabyte-scale enterprises.

From Planning to Operation — We'll Deliver Full Lifecycle Support

Once certified, Nexsan will provide end-to-end support—from architecture planning through production rollout. Our technical team will work directly with customers and integration partners to define optimal configurations based on data growth, workload needs, and retention policies. Every system will be factory-configured and QA-tested to ensure readiness, reliability, and speed of deployment.

Post-deployment, Nexsan's global support team will be available to assist with firmware updates, tuning, and expansion—ensuring the Nexsan VHR-Series remains secure, high-performing, and aligned with evolving business needs.

SOBR-Ready for Distributed Backup Environments

The VHR-Series will be fully compatible with **Veeam Scale-Out Backup Repository (SOBR)**, enabling organizations to scale incrementally and intelligently manage backup workloads across multiple nodes. This means flexible expansion, efficient tiering, and centralized policy control, all while preserving data immutability.

Whether starting with 64TB or scaling to multi-petabyte environments, the VHR-Series will deliver the backbone for secure, compliant, and resilient Veeam infrastructure at a cost-effective price.

Summary: What Nexsan Will Deliver with Veeam Certification

- Certified appliance preloaded with Veeam Hardened Repository ISO
- Immutable storage with full DISA STIG compliance
- Scalable from 64TB to 3.3PB usable
- Factory-configured and QA-validated for rapid, low-risk deployment
- Veeam SOBR-compatible for distributed environments
- Enterprise-class performance and reliability
- 5-year global hardware support standard
- Built by Nexsan—25+ years of trusted enterprise storage expertise