BullSequana Servers

OneBSM Console Reference Guide

86 A1 55FT 01 - October 2024

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark and/or patent misuse.

Hardware

October 2024

Eviden
30 bis rue du Nid de Pie
49000 Angers
FRANCE

The information in this document is subject to change without notice. Eviden will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Table of contents

Preface

This guide explains how to use the OneBSM console to monitor and maintain Eviden systems.

See The Bull support web site for the most up-to-date product information, documentation, firmware updates, software fixes and service offers: https://support.bull.com

Intended Readers

This guide is intended for use by system administrators and operators.

Chapter 1. Getting started

OneBSM console is a graphical management and monitoring system for the following servers:

- BullSequana SH
- BullSequana EXR/EXD
- BullSequana SA

OneBSM will manage and monitor all the BullSequana servers detected on the local network.

BullSequana servers can be viewed within OneBSM individually or grouped together according to server type. The interface is dynamic according to server type.

Note The terms 'device' and 'server' are interchangeable in this guide.

1.1. Installing OneBSM console

1.1.1. Linux systems

To install use the command below:

```
dpkg -i filename.extension
```

To uninstall use the command below:

```
dpkg --purge onebsm
```

1.1.2. Windows systems

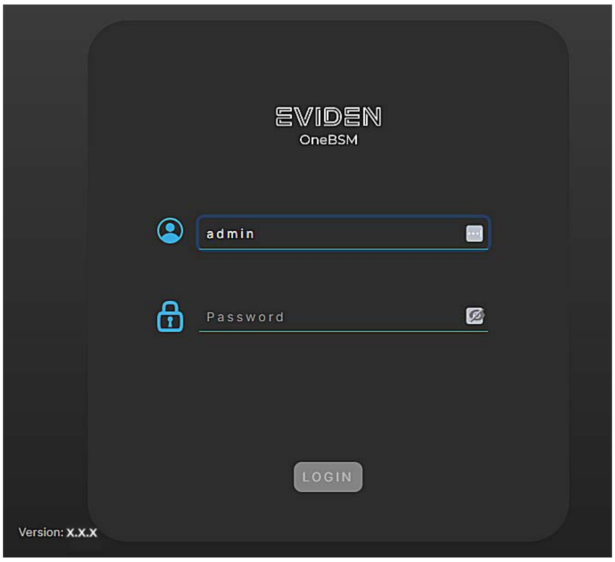
1. Launch the OneBSM installer.
2. Choose the installation folder.
3. Click finish to end the installation process.

Note This will install OneBSM on all Windows versions and launch the related services.

1.2. Connecting to the OneBSM console for the first time

Note On virtual machines the full IP address must be used and not “localhost”.

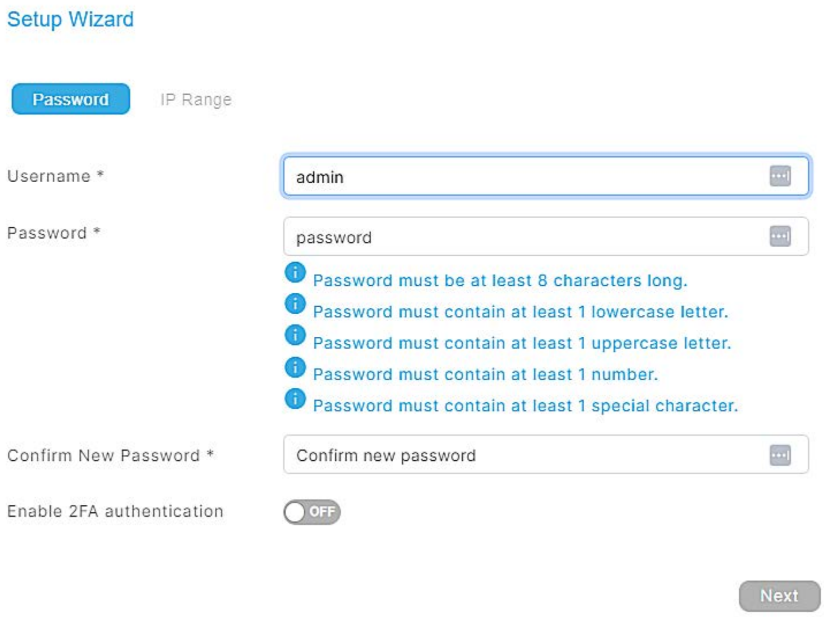
1. Open a web browser on a laptop.
2. Enter the IP address or host name of the server, on the same network, hosting the OneBSM console. The OneBSM console authentication window opens.



3. Enter the first time user name and password.

Note For the first log in the user name = *admin* and the password = *password*.

4. Click the **LOGIN** button. The change password setup wizard opens.



Username * admin

Password * password

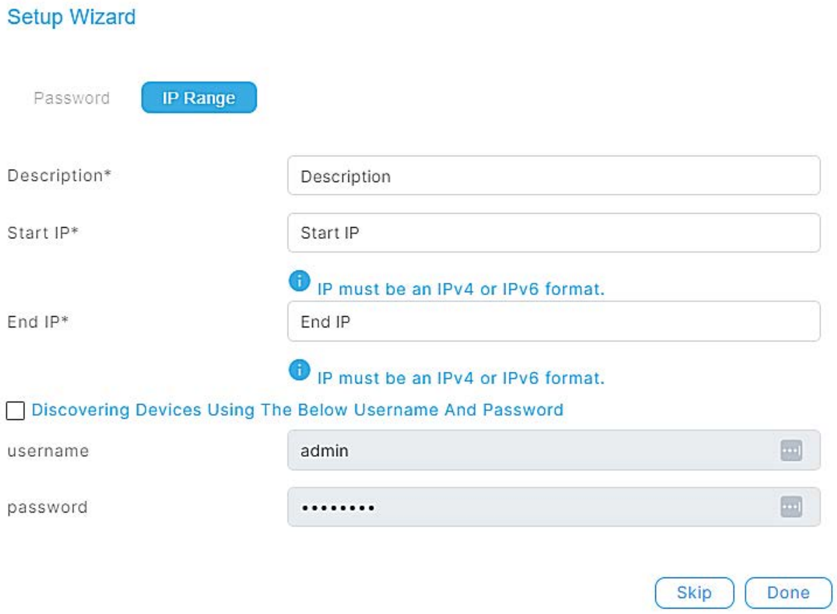
Password must be at least 8 characters long.
Password must contain at least 1 lowercase letter.
Password must contain at least 1 uppercase letter.
Password must contain at least 1 number.
Password must contain at least 1 special character.

Confirm New Password * Confirm new password

Enable 2FA authentication OFF

5. Enter the new user name and password.

6. Click **Next.** The IP Range Setup Wizard opens



Setup Wizard

Description* Description

Start IP* Start IP

IP must be an IPv4 or IPv6 format.

End IP* End IP

IP must be an IPv4 or IPv6 format.

□ Discovering Devices Using The Below Username And Password

username admin

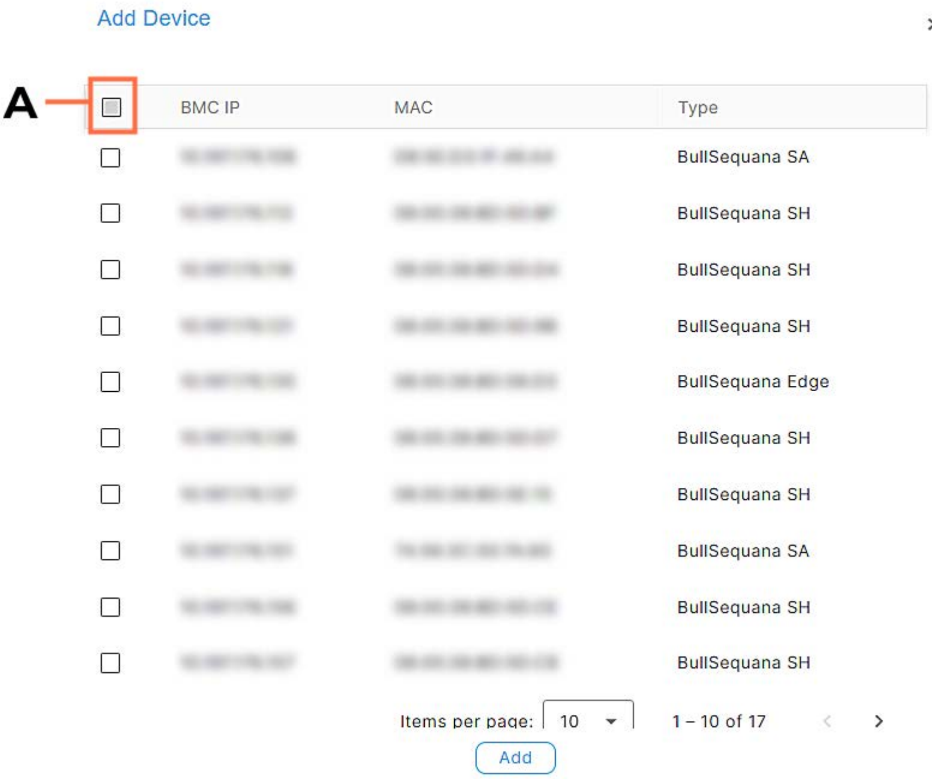
password •••••••••

Note Click **Skip** to postpone the device discovery. See 2.1. Adding devices to the Device List

7. Enter the **Start IP** and the **End IP** for the IP address range for the devices on the network to be included in the OneBSM device list.

Note It is recommended to check **Discovering Devices Using the Below Username and Password** for the BMC user name and password. However, to use this functionality the BMC username and password will need to be known and be the same for all the detected devices on the network. If this box is not checked the devices in the device list will be locked and the BMC username and password will have to entered individually for each device.

8. Click **Done.** The **Add Device** screen opens with the list of detected devices.



Add Device

□	BMC IP	MAC	Type
□	[redacted]	[redacted]	BullSequana SA
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana Edge
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SA
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH

9. The IP range results are displayed. Click the checkbox(A) and click **Add**. This will initiate a discovery action after which all the supported selected devices will be added to the **Device List**.

The OneBSM Device List summary window opens.

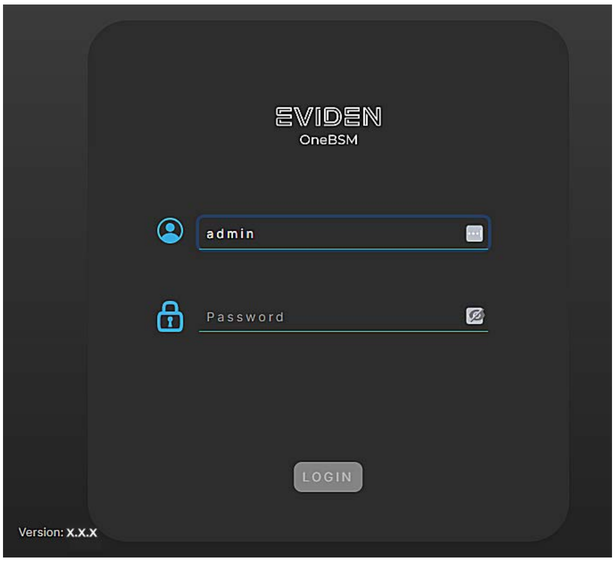
1.3. Logging in to the OneBSM console

Users log in to the system using the account and password created in the user account list.

Procedure

Note On virtual machines the full IP address must be used and not “localhost”.

1. Open a web browser on a laptop.
2. Enter the IP address or host name of the server, on the same network, hosting the OneBSM console. The OneBSM console authentication window opens.



3. Enter the user name and password.
4. Click the **LOGIN** button.
5. If two-factor authentication (2FA) is enabled, click the authenticator icon to get the verification code, which is usually a six-digit number in Chrome.
6. Enter the verification code into the input box and click the **Verify** button.

Note The 2FA code must be validated at the same time on both the OneBSM system and the server. Otherwise, login might fail due to a verification code timing out. For more information, please refer to the time settings section.

See Appendix A. Logging in with the 2FA authentication

The OneBSM Dashboard Device List summary window opens.

1.4. OneBSM console features

The OneBSM console menu tabs provide access to sub-menus to configure and maintain OneBSM and connected devices

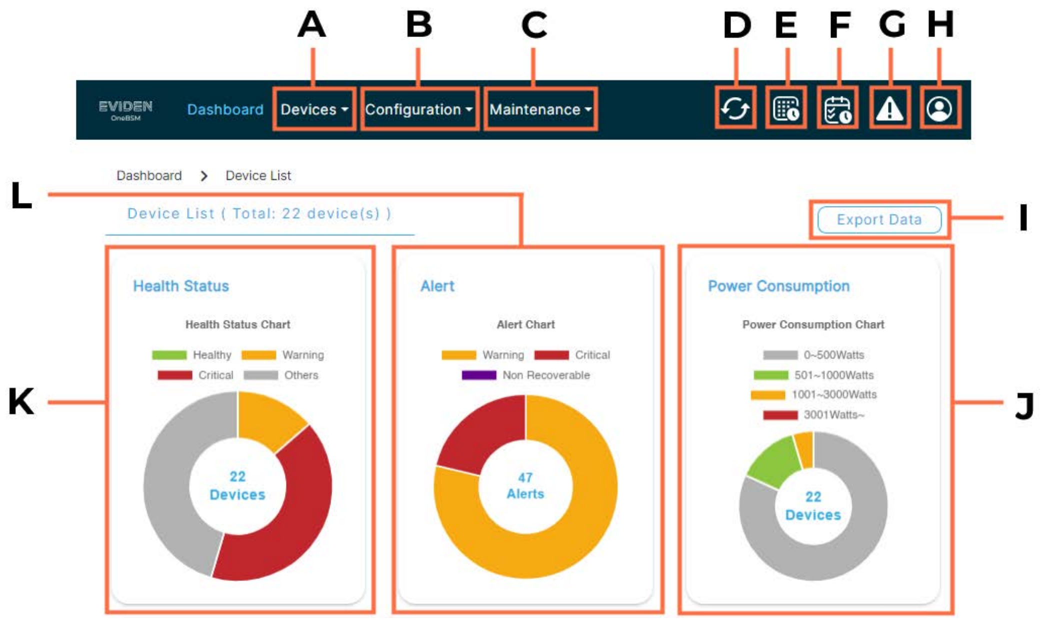
Tab	Item
Devices	Discovery
	Device List
	Groups
Configuration	Account Management
	Notification Settings
	Database
	System Settings
Maintenance	Audit Log
	System Log
	Alert Log
	Update System
	Export Config

1.5. Dashboard overview

The **Dashboard** provides an overview of all connected servers on the network, displaying information such as health status, alert logs, power consumption distribution, total power consumption history, and a list of scheduled tasks with their completion status.

The **Device List** total indicates the number of connected servers whose data is displayed.

Note Some operations, for example, viewing OneBSM alerts, can be performed directly from the buttons on the Dashboard or via the sub-menus.



Mark	Description
A	**Devices** menu
B	**Configuration** menu for OneBSM
C	**Maintenance** menu for OneBSM
D	**Refresh** button
E	**Time** configuration button
F	**Scheduled Tasks** button
G	**Alerts** button
H	**User** button
I	**Export Data** button
J	**Power Consumption** wheel
K	**Health Status** wheel
L	**Alert** wheel

The **Health Status** wheel shows the device breakdown for each state: **Healthy, Critical, Warning**, and **Other.**

The **Alert** wheel shows the number of device breakdown for each state: **Unknown**, **Non-critical,** and **Critical**.

The **Power Consumption** wheel shows the device breakdown for each power range: **0–500 Watts**, **501–1000 Watts**, **1001–3000 Watts**, and above **3001 Watts**.

See Click on the wheel segments to see the devices for each state.

The **Total Power Consumption History** linear chart shows the variations in power consumption for all devices over a 24-hour period.

The **Completed Schedule Tasks List** provides details of the completed tasks. The information displayed can be modified by clicking the three vertical dots at the end of the list of columns.

Chapter 2. Managing devices

The **Devices** tab includes three sub-pages to discover, list and group the manageable devices detected on the network.

2.1. Adding devices to the Device List

There are three ways of detecting and adding manageable devices to the OneBSM console **Device List** :

- Using the **Discovery** page to search for devices within a range of IP addresses.
- Adding a single device to the **Device List** by specifying its IP address.
- Importing devices listed within a .txt file

2.1.1. Discovering devices

Discovery is used to scan machines on the network and to display existing scan segments. It is possible to set a range of IP addresses for a scan, configure scan intervals, and use specific user names and passwords for scanning.

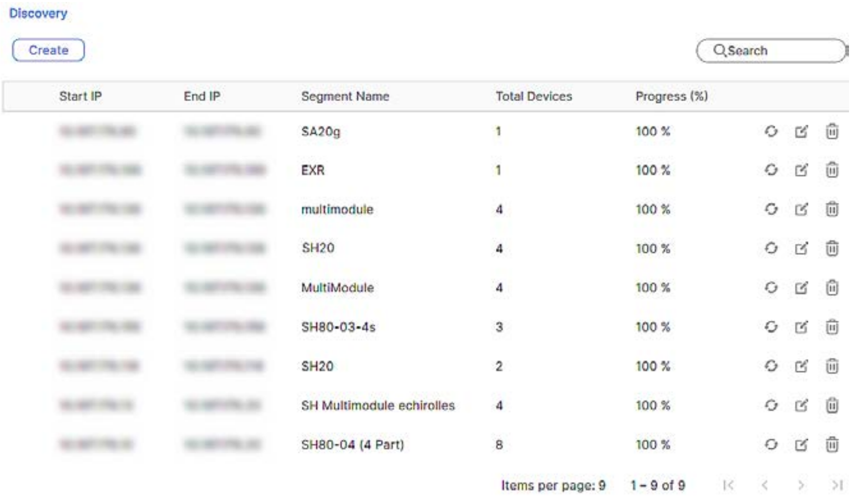
Note Each scan, as set by the scan interval, will also refresh other details periodically, for example BMC hostname, the network configuration and inventory information.

Additionally, it is possible to delete, edit, or re-scan each IP range's data using the action icon buttons.

A keyword search function is available.

Setting a range of IP addresses for a scan

1. From the **Devices** tab, click **Discovery**.



Discovery

Start IP	End IP	Segment Name	Total Devices	Progress (%)
[redacted]	[redacted]	SA20g	1	100 %
[redacted]	[redacted]	EXR	1	100 %
[redacted]	[redacted]	multimodule	4	100 %
[redacted]	[redacted]	SH20	4	100 %
[redacted]	[redacted]	MultiModule	4	100 %
[redacted]	[redacted]	SH80-03-4s	3	100 %
[redacted]	[redacted]	SH20	2	100 %
[redacted]	[redacted]	SH Multimodule echirolles	4	100 %
[redacted]	[redacted]	SH80-04 (4 Part)	8	100 %

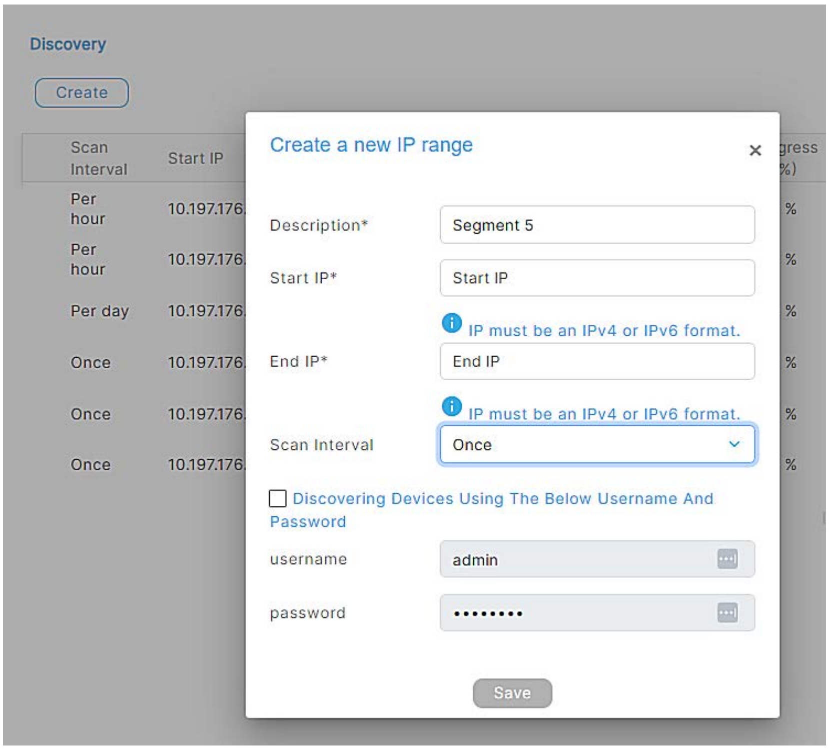
Items per page: 9 1 – 9 of 9

Note All input data should be in a valid format, and the IP address range must not be a duplicate

2. From the **Discovery** page, click the **Create** button

3. Enter the **Start IP** and **End IP** for the IP address range.

4. Set the scan interval for the IP range.



Discovery

Scan Interval	Start IP	gress %)
Per hour	10.197.176.	%
Per hour	10.197.176.	%
Per day	10.197.176.	%
Once	10.197.176.	%
Once	10.197.176.	%
Once	10.197.176.	%

Create a new IP range ×

Description* Segment 5

Start IP* Start IP

IP must be an IPv4 or IPv6 format.

End IP* End IP

IP must be an IPv4 or IPv6 format.

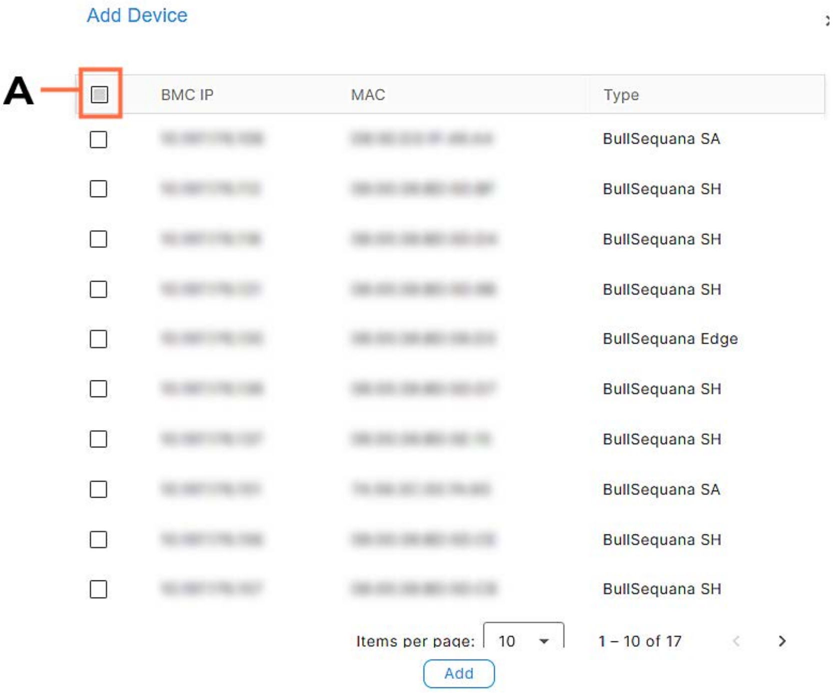
Scan Interval Once

□ Discovering Devices Using The Below Username And Password

username admin

password ••••••••

5. Click **Save.**



	BMC IP	MAC	Type
□	[redacted]	[redacted]	BullSequana SA
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana Edge
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SA
□	[redacted]	[redacted]	BullSequana SH
□	[redacted]	[redacted]	BullSequana SH

6. The IP range results are displayed. Click the checkbox(A) and click **Add**. This will initiate a discovery action after which all the supported selected devices will be added to the **Device List**.

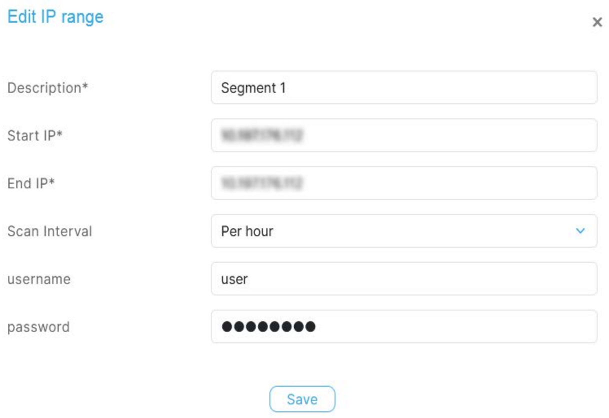
Editing an existing range of IP addresses for a scan

Note All input data should be in a valid format, and the IP range must not be a duplicate.

1. Click the **Edit** button.

2. Modify the input data for the IP range.

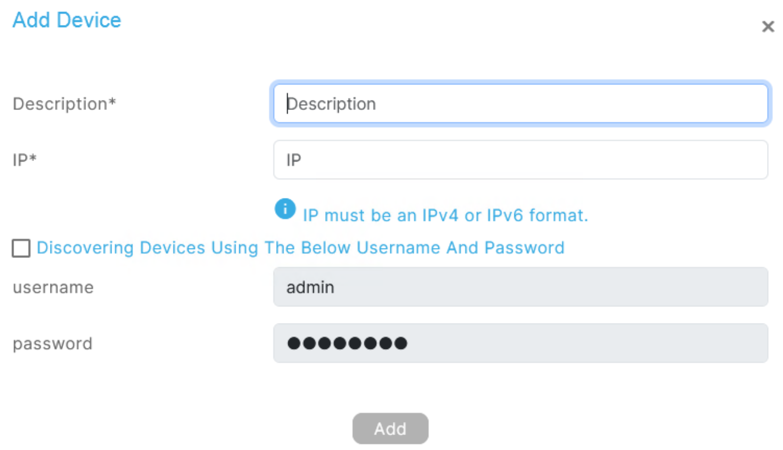
3. Click the **Save** button. The result will be displayed on the screen.



Description*	Segment 1
Start IP*	[redacted]
End IP*	[redacted]
Scan Interval	Per hour
username	user
password	●●●●●●●●

2.1.2. Adding a device to the Device List

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **Add Device.**



Add Device

Description*	Description
IP*	IP

IP must be an IPv4 or IPv6 format.

□ Discovering Devices Using The Below Username And Password

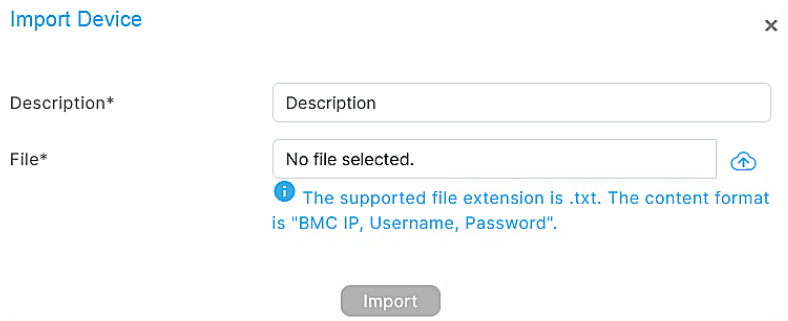
username	admin
password	●●●●●●●●●

3. Enter the IP address and description for the new device.
4. Click **Add**.

2.1.3. Importing devices to the Device List

Note The .txt file must be in the format BMC IP, Username, Password.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **Import Device.**



Import Device

Description*	Description
File*	No file selected.

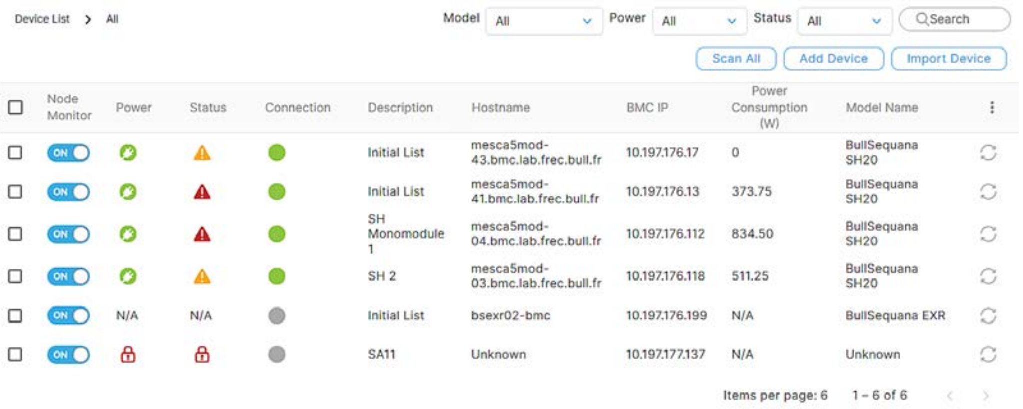
The supported file extension is .txt. The content format is "BMC IP, Username, Password".

3. Add a Description of the device.
4. Fetch the .txt file with the device details.
5. Click **Import**.

2.2. Viewing devices

From the **Devices** tab, click **Device List** to view all the servers on the network managed and monitored by **OneBSM.**

All BullSequana servers are displayed or they can viewed by server type: **BullSequana SA**, **BullSequana EXR/EXD**, **BullSequana SH**.



□	Node Monitor	Power	Status	Connection	Description	Hostname	BMC IP	Power Consumption (W)	Model Name	⋮
□	ON	⏻	⚠	●	Initial List	mesca5mod-43.bmc.lab.frec.bull.fr	10.197.176.17	0	BullSequana SH20	↻
□	ON	⏻	⚠	●	Initial List	mesca5mod-41.bmc.lab.frec.bull.fr	10.197.176.13	373.75	BullSequana SH20	↻
□	ON	⏻	⚠	●	SH Monomodule 1	mesca5mod-04.bmc.lab.frec.bull.fr	10.197.176.112	834.50	BullSequana SH20	↻
□	ON	⏻	⚠	●	SH 2	mesca5mod-03.bmc.lab.frec.bull.fr	10.197.176.118	511.25	BullSequana SH20	↻
□	ON	N/A	N/A	●	Initial List	bsexr02-bmc	10.197.176.199	N/A	BullSequana EXR	↻
□	ON	🔒	🔒	●	SA11	Unknown	10.197.177.137	N/A	Unknown	↻

Items per page: 6   1 – 6 of 6   <   >

Various details are shown for the devices listed, including :

Note The information displayed in the device list can be configured by clicking the three vertical dots at the end of the list of columns.

- Power status
- Node monitor
- Health status
- Connection status
- Segment name for the IP range
- Hostname
- IP address for the BMC
- Power Consumption in watts
- Model name
- Rescan this device button

Note The **Rescan this device** button refreshes device details, for example BMC hostname, the network configuration and inventory information. The **Scan All** button does the same for all listed devices, however this is a time consuming operation.
Using these features does not clear existing sensor history information stored for the device(s).

The Device List page also includes **Add Device** and **Import Device** buttons to add devices to the device list.

Double click on a server row to view more details and to perform management and monitoring operations.

Note It is not possible to redirect to a server's page if the Status indicates **Wrong Password**. In this case the correct BMC user name and password must be entered

A keyword search function will filter data according to the keyword entered.

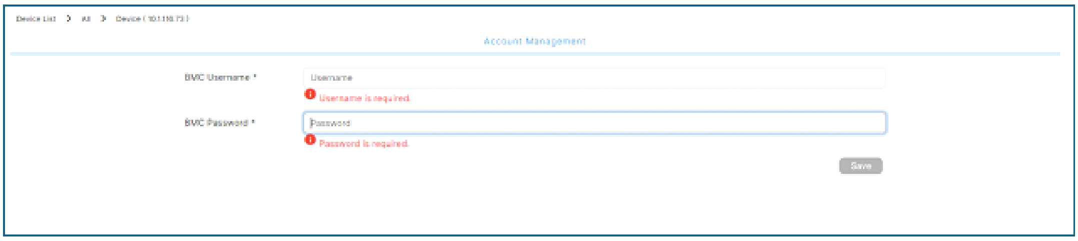
2.3. Accessing a device page

1. From the **Devices** tab, click **Device List**.

2. From the **Device List** page, click **All** or select server type.

3. Click on the server required in the list, the **Information** page opens.

4. If a device with a Wrong Password status is selected, the system will redirect to the **Settings** page and the BMC password and username will have to be reset.



BMC Username * Username

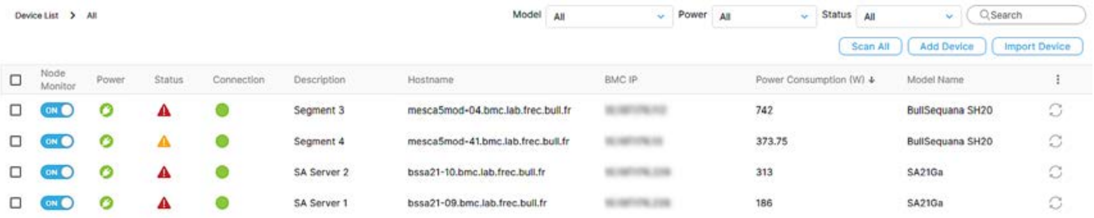
Username is required.

BMC Password * Password

Password is required.

2.4. Filtering devices

From the **Dashboard**, click the health status, alert or power consumption range. A list of devices with the selected status, alert or power consumption range opens.



Device List > All

Model: All | Power: All | Status: All | Search

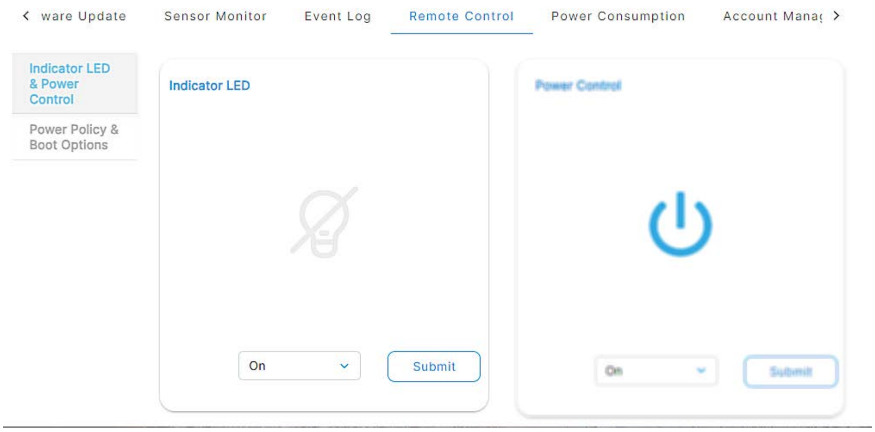
□	Node Monitor	Power	Status	Connection	Description	Hostname	BMC IP	Power Consumption (W) ↓	Model Name	⋮
□	ON	●	⚠	●	Segment 3	mesca5mod-04.bmc.lab.frec.bull.fr	[redacted]	742	BullSequana SH20	↻
□	ON	●	⚠	●	Segment 4	mesca5mod-41.bmc.lab.frec.bull.fr	[redacted]	373.75	BullSequana SH20	↻
□	ON	●	⚠	●	SA Server 2	bssa21-10.bmc.lab.frec.bull.fr	[redacted]	313	SA21Ga	↻
□	ON	●	⚠	●	SA Server 1	bssa21-09.bmc.lab.frec.bull.fr	[redacted]	186	SA21Ga	↻

2.5. Turning on / off the indicator LED for a device

1. From the **Devices** tab, click **Device List**.

2. From the **Device List** page, click **All** or select server type.

3. Click on the server required in the list, the **Information** page opens.



4. From the **Remote Control** tab, click the **Indicator LED & Power Control** button.

5. Choose an option to turn on / off the LED or to make it blink for a specific duration.

Note The default duration for the LED to stay on is 15 seconds.

The result of the LED operation will be displayed on the screen, and the light bulb icon will update to reflect the current LED status.

Chapter 3. Managing groups of devices

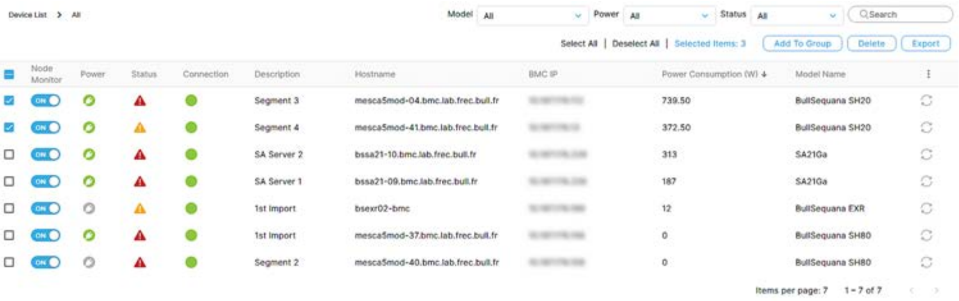
3.1. Grouping devices

Note Different server types cannot be grouped together.

1. From the **Devices** tab, click **Device List.**

2. Select servers for the new group by checking their check boxes (A).

3. Click the **Group** (B) button.



Device List > All

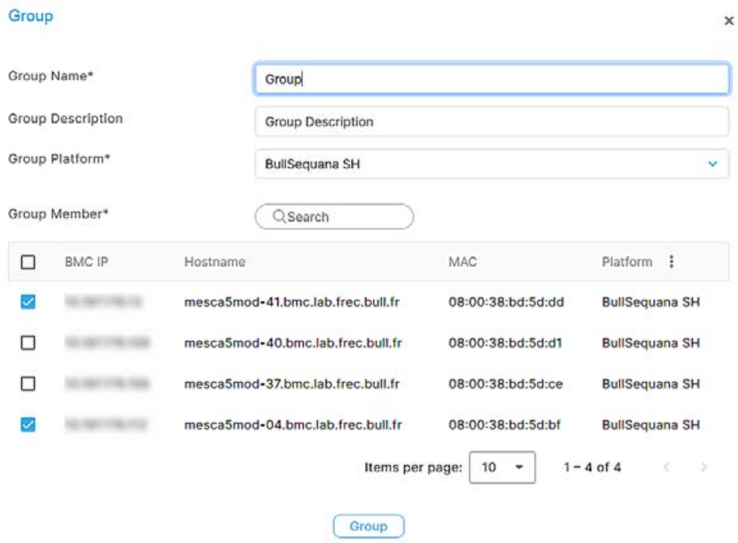
Model: All | Power: All | Status: All | Search

Select All | Deselect All | Selected Items: 3 | Add To Group | Delete | Export

☐	Node Monitor	Power	Status	Connection	Description	Hostname	BMC IP	Power Consumption (W) ↓	Model Name	⋮
☑	ON	○	⚠	●	Segment 3	mesca5mod-04.bmc.lab.frec.bull.fr	[redacted]	739.50	BullSequana SH20	↻
☑	ON	○	⚠	●	Segment 4	mesca5mod-41.bmc.lab.frec.bull.fr	[redacted]	372.50	BullSequana SH20	↻
☐	ON	○	⚠	●	SA Server 2	bssa21-10.bmc.lab.frec.bull.fr	[redacted]	313	SA21Ga	↻
☐	ON	○	⚠	●	SA Server 1	bssa21-09.bmc.lab.frec.bull.fr	[redacted]	187	SA21Ga	↻
☐	ON	○	⚠	●	1st Import	bsexr02-bmc	[redacted]	12	BullSequana EXR	↻
☐	ON	○	⚠	●	1st Import	mesca5mod-37.bmc.lab.frec.bull.fr	[redacted]	0	BullSequana SH80	↻
☐	ON	○	⚠	●	Segment 2	mesca5mod-40.bmc.lab.frec.bull.fr	[redacted]	0	BullSequana SH80	↻

Items per page: 7 1 – 7 of 7

4. Enter the group details and select a platform type for the group.



Group ×

Group Name*: Group

Group Description: Group Description

Group Platform*: BullSequana SH

Group Member*: Search

☐	BMC IP	Hostname	MAC	Platform ⋮
☑	[redacted]	mesca5mod-41.bmc.lab.frec.bull.fr	08:00:38:bd:5d:dd	BullSequana SH
☐	[redacted]	mesca5mod-40.bmc.lab.frec.bull.fr	08:00:38:bd:5d:d1	BullSequana SH
☐	[redacted]	mesca5mod-37.bmc.lab.frec.bull.fr	08:00:38:bd:5d:ce	BullSequana SH
☑	[redacted]	mesca5mod-04.bmc.lab.frec.bull.fr	08:00:38:bd:5d:bf	BullSequana SH

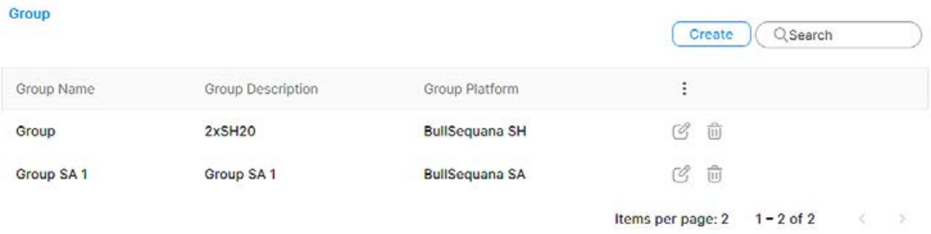
Items per page: 10 1 – 4 of 4

Group

5. Click the **Group** button to submit the data and to see the results on the screen.

3.2. Viewing device groups

1. From the **Devices** tab, click **Group.** All existing groups are displayed, including details of group members.



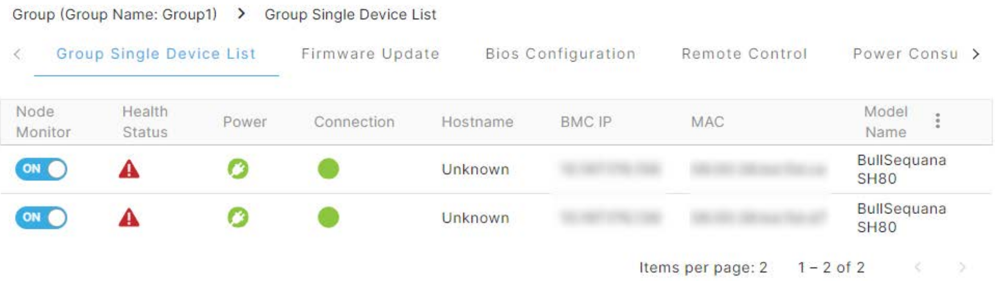
Group

Create | Search

Group Name	Group Description	Group Platform	⋮
Group	2xSH20	BullSequana SH	
Group SA 1	Group SA 1	BullSequana SA	

Items per page: 2 1 – 2 of 2

2. Click on a row in the Group table to see the devices sub-menus, for example, firmware update.



Group (Group Name: Group1) > Group Single Device List

Group Single Device List | Firmware Update | Bios Configuration | Remote Control | Power Consu

Node Monitor	Health Status	Power	Connection	Hostname	BMC IP	MAC	Model Name
ON	⚠	●	●	Unknown	[redacted]	[redacted]	BullSequana SH80
ON	⚠	●	●	Unknown	[redacted]	[redacted]	BullSequana SH80

Items per page: 2 1 – 2 of 2

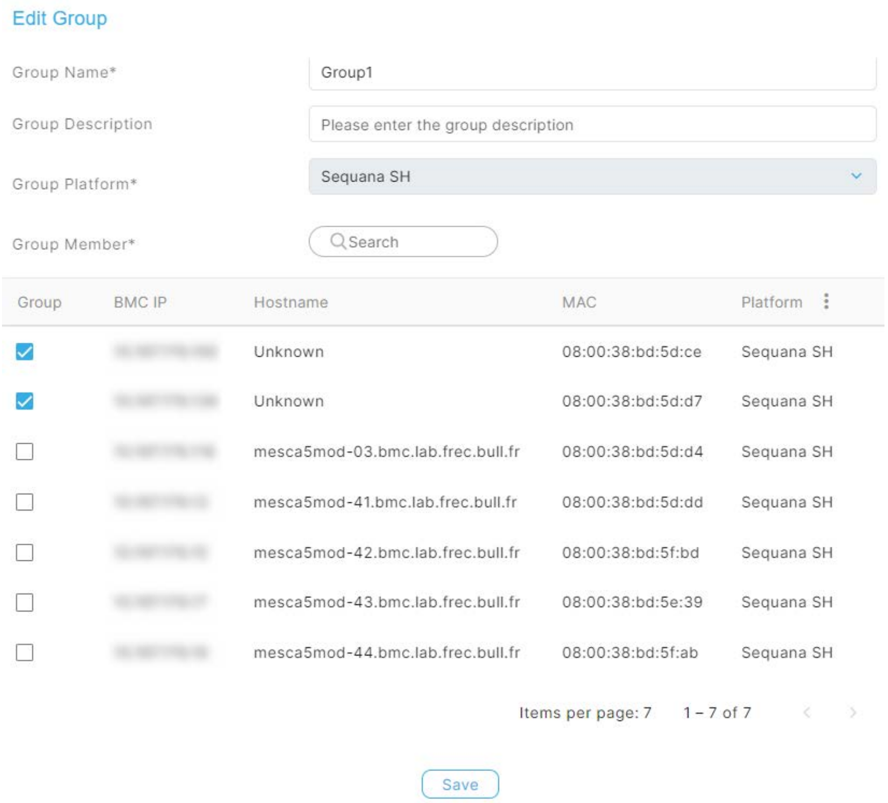
Each group can be deleted or edited using the action icon buttons.

A keyword search function will filter data according to the keyword entered.

3.3. Editing a device group

Note Different server types cannot be grouped together.

1. From the **Devices** tab, click **Group.**
2. Click the **Edit** button in the last column of the Group table for the group to be edited.
3. Modify the group's fields, as required.
4. Check the group box to add a device to a group,
5. Click the **Save** button to submit, and the result will be shown on the screen.



Edit Group

Group Name* Group1

Group Description Please enter the group description

Group Platform* Sequana SH

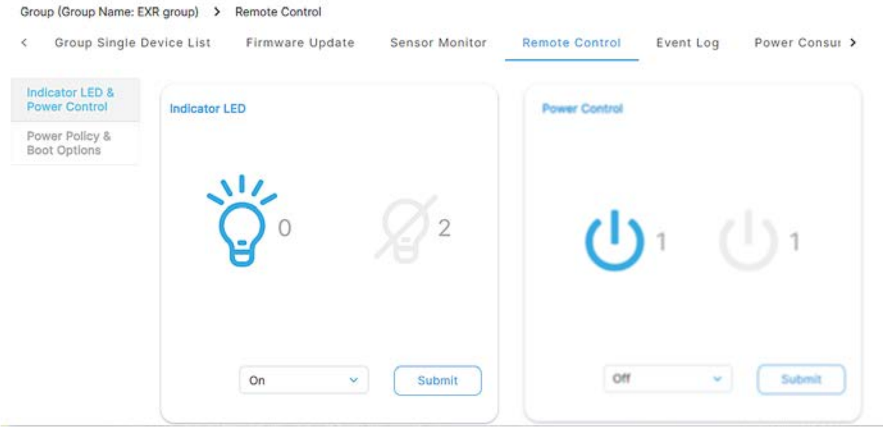
Group Member* Search

Group	BMC IP	Hostname	MAC	Platform
☑	[redacted]	Unknown	08:00:38:bd:5d:ce	Sequana SH
☑	[redacted]	Unknown	08:00:38:bd:5d:d7	Sequana SH
☐	[redacted]	mesca5mod-03.bmc.lab.frec.bull.fr	08:00:38:bd:5d:d4	Sequana SH
☐	[redacted]	mesca5mod-41.bmc.lab.frec.bull.fr	08:00:38:bd:5d:dd	Sequana SH
☐	[redacted]	mesca5mod-42.bmc.lab.frec.bull.fr	08:00:38:bd:5f:bd	Sequana SH
☐	[redacted]	mesca5mod-43.bmc.lab.frec.bull.fr	08:00:38:bd:5e:39	Sequana SH
☐	[redacted]	mesca5mod-44.bmc.lab.frec.bull.fr	08:00:38:bd:5f:ab	Sequana SH

Items per page: 7 1 – 7 of 7

3.4. Turning on / off the indicator LEDs for a group

1. From the **Devices** page, click **Groups**.
2. In the **Group** window, click on the group required.
3. From the **Remote Control** tab, click the **Indicator LED & Power Control** button.



4. Choose an option to turn on / off the ID LED or to make it blink for a specific duration.

Note The default duration for the LED to stay on is 15 seconds.

The result of the LED operation will be displayed on the screen, and the light bulb icon will update to reflect the current LED status.

Chapter 4. Configuring devices

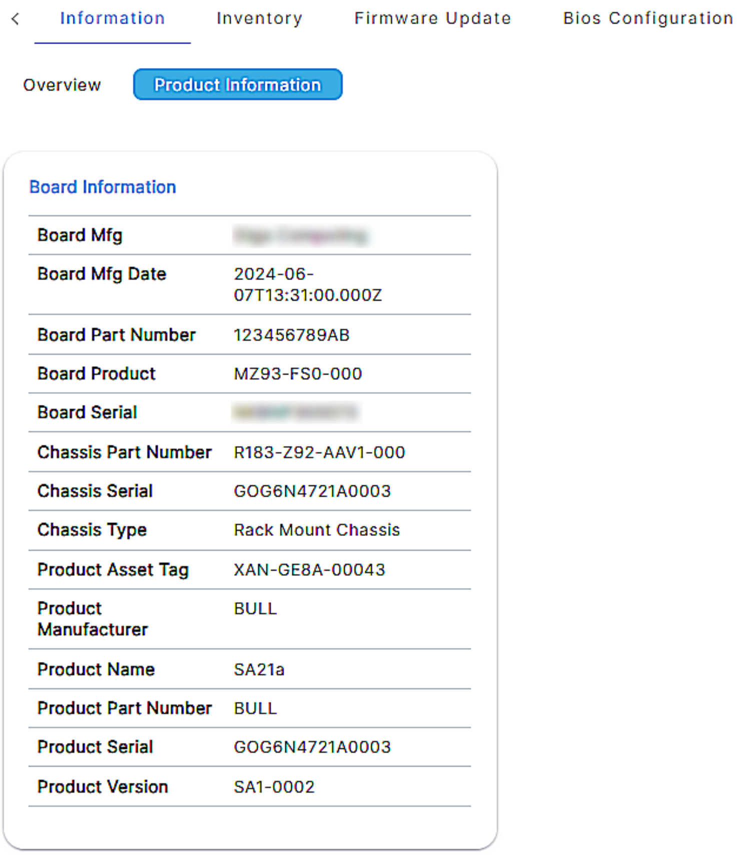
4.1. Obtaining product information

1. From the **Devices** tab, click **Device List**.

2. From the **Device List** page, click **All** or select server type.

3. Click on the server required in the list, the **Information** page opens.

4. Click the **Product information** tab. The **Product Information** sub-page opens with board and product details.



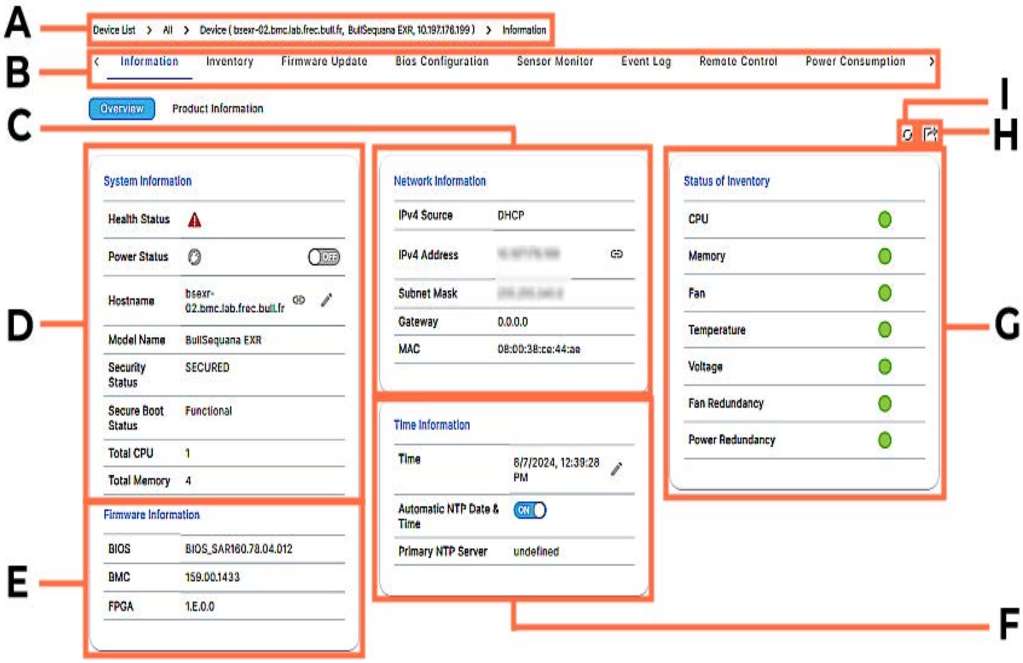
Board Information

Board Mfg	[redacted]
Board Mfg Date	2024-06-07T13:31:00.000Z
Board Part Number	123456789AB
Board Product	MZ93-FS0-000
Board Serial	[redacted]
Chassis Part Number	R183-Z92-AAV1-000
Chassis Serial	GOG6N4721A0003
Chassis Type	Rack Mount Chassis
Product Asset Tag	XAN-GE8A-00043
Product Manufacturer	BULL
Product Name	SA21a
Product Part Number	BULL
Product Serial	GOG6N4721A0003
Product Version	SA1-0002

4.2. Configuring device settings

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Overview** tab. Information is displayed about the system, firmware version, network, time settings and inventory status of the device.

Note For BullSequana SH multi-module servers additional buttons are available at the top of the page to select the individual BullSequana SH modules that make up the multi-module server.



System Information

Health Status

Power Status

Hostname bsexr-02.bmc.lab.frec.bull.fr

Model Name BullSequana EXR

Security Status SECURED

Secure Boot Status Functional

Total CPU 1

Total Memory 4

Firmware Information

BIOS BIOS_SAR160.78.04.012

BMC 159.00.1433

FPGA 1.E.0.0

Network Information

IPv4 Source DHCP

IPv4 Address [redacted]

Subnet Mask [redacted]

Gateway 0.0.0.0

MAC 08:00:38:ce:44:ae

Time Information

Time 8/7/2024, 12:39:28 PM

Automatic NTP Date & Time

Primary NTP Server undefined

Status of Inventory

CPU ●

Memory ●

Fan ●

Temperature ●

Voltage ●

Fan Redundancy ●

Power Redundancy ●

Mark	Description
A	OneBSM path to device overview.
B	Device sub-menus including : Inventory details, Firmware Update, Sensor Monitor, Event Log, Remote Control, Power Consumption.
C	**Network Information** including device IP address , gateway and mac address.
D	**System Information** including device health status, power status and hostname.
E	**Firmware Information** including firmware versions for the server,

Mark	Description
F	**Time information** including NTP settings.
G	**Status of Inventory** indicates the health status of the components included in the inventory.
H	Export BMC Information button
I	Reboot BMC button

Device sub-menus

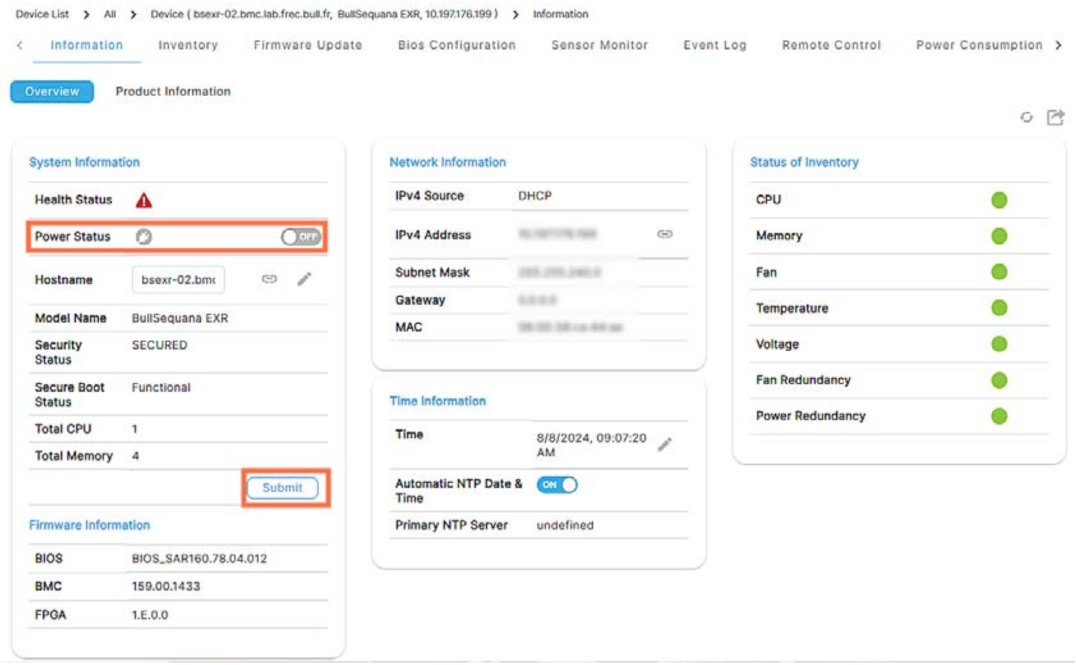
The Device sub-menus displayed at the top of the page for a server vary according to server type.

See Appendix B. Server configuration sub-menus

4.3. Powering on / off a device

4.3.1. Powering on / off from the Overview window

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Overview** tab.
5. Use the slider button to turn the power on or off as required.
6. Click the **Submit** button.



System Information

Health Status	⚠
Power Status	OFF
Hostname	bsexr-02.bm(
Model Name	BullSequana EXR
Security Status	SECURED
Secure Boot Status	Functional
Total CPU	1
Total Memory	4

Firmware Information

BIOS	BIOS_SAR160.78.04.012
BMC	159.00.1433
FPGA	1.E.0.0

Network Information

IPv4 Source	DHCP
IPv4 Address	[redacted]
Subnet Mask	[redacted]
Gateway	[redacted]
MAC	[redacted]

Time Information

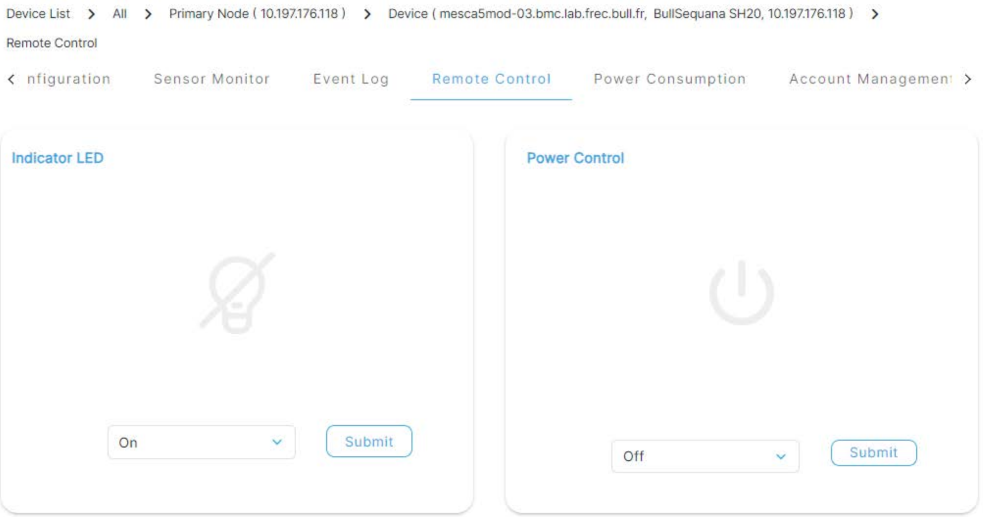
Time	8/8/2024, 09:07:20 AM
Automatic NTP Date & Time	ON
Primary NTP Server	undefined

Status of Inventory

CPU	●
Memory	●
Fan	●
Temperature	●
Voltage	●
Fan Redundancy	●
Power Redundancy	●

4.3.2. Powering on / off a device from the Remote Control window

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. From the **Remote Control** tab, click the **Indicator LED & Power Control** button.



5. Choose an option to perform actions such as **On**, **Off** ,**Hard Reset**, or **Graceful Shutdown**.
6. Click the **Submit** button.
7. Confirm the action in the warning dialogue box.

The result will be displayed and the power icon will update to reflect the new power status.

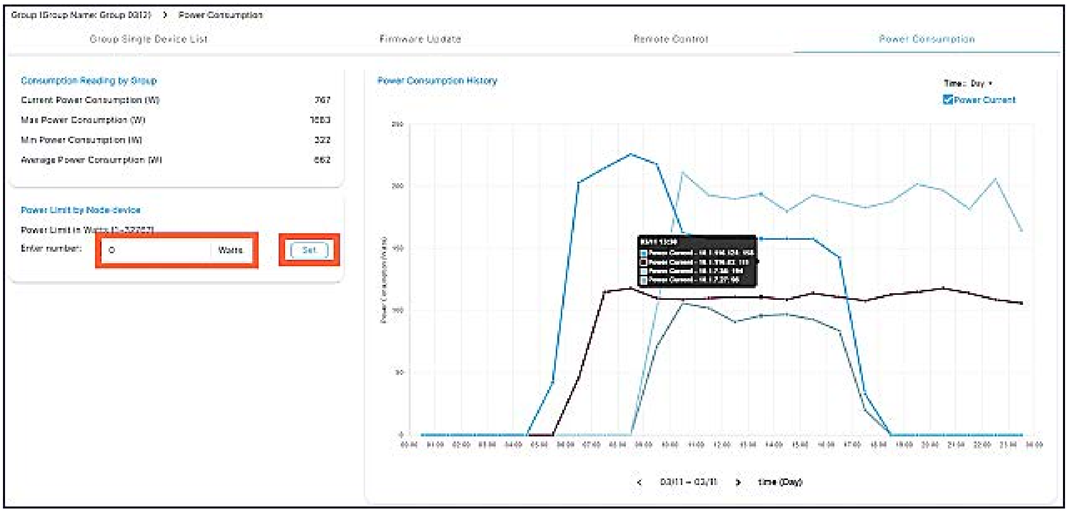
4.4. Configuring power limits for BullSequana SA servers

Note The power limitation option applies to BullSequana SA servers only.

Power Limit settings allow a power limit to be set and activated.

1. Activate the power limit by clicking the slide toggle.

2. Enter the power limit value. The maximum power limit must not exceed 32,768 Watts,



Consumption Reading by Group

Current Power Consumption (W)	767
Max Power Consumption (W)	1083
Min Power Consumption (W)	322
Average Power Consumption (W)	662

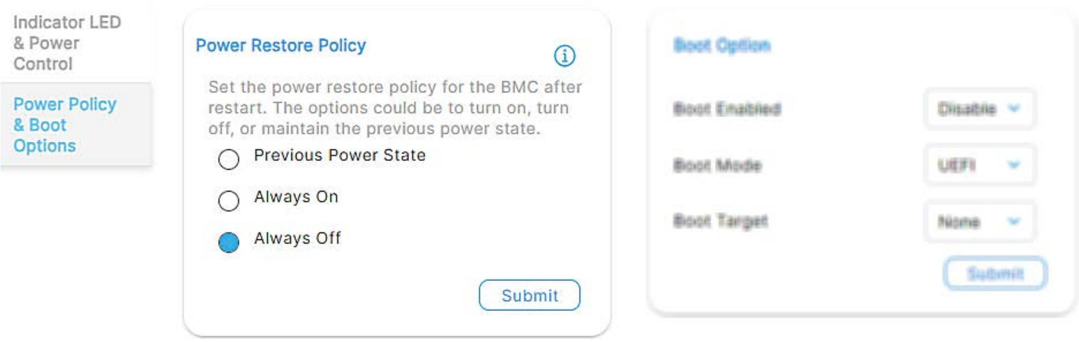
Power Limit by Node device

Power Limit in Watts [1~32767]

Enter number: 0 Watts Set

4.5. Configuring power restore settings

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. From the **Remote Control** tab, click the **Power Policy & Boot Options** button.



Power Restore Policy

Set the power restore policy for the BMC after restart. The options could be to turn on, turn off, or maintain the previous power state.

○ Previous Power State

○ Always On

● Always Off

Boot Option

Boot Enabled: Disable

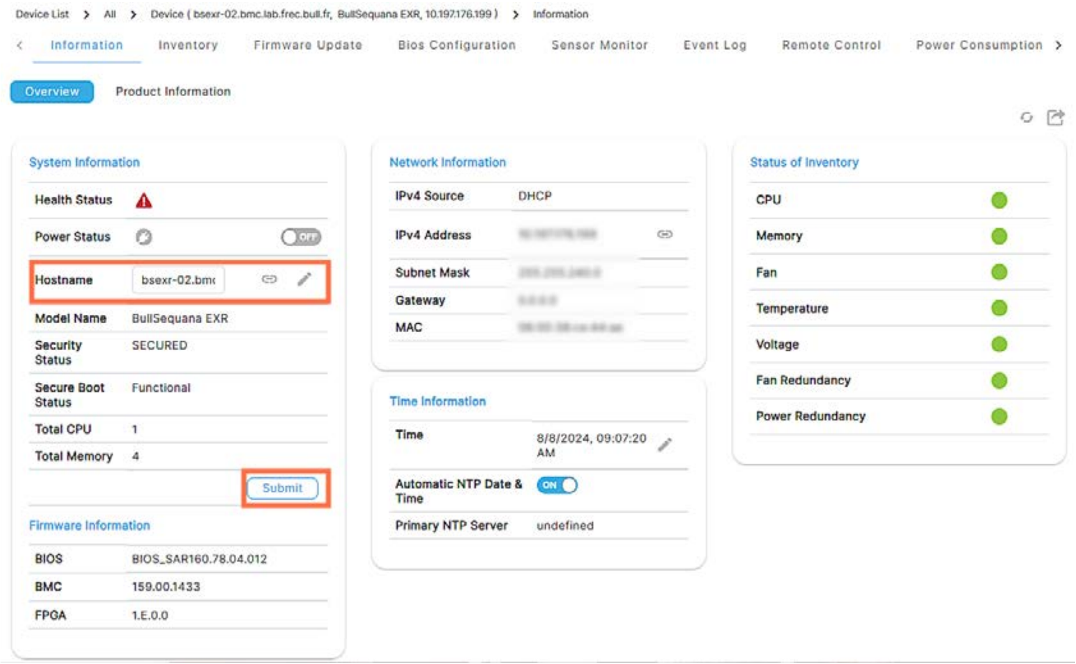
Boot Mode: UEFI

Boot Target: None

5. Select the power restore policy, as required.
6. Click the **Submit** button. The system reloads and displays the new settings.

4.6. Changing the host name

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Overview** tab.
5. Double-click the **Hostname** field to enter edit mode.
6. Enter the new host name. To cancel, right-click or double-click again.
7. Click the **Submit** button. The system reloads and displays the new settings.



System Information

Health Status	⚠
Power Status	OFF
Hostname	bsexr-02.bmc
Model Name	BullSequana EXR
Security Status	SECURED
Secure Boot Status	Functional
Total CPU	1
Total Memory	4

Firmware Information

BIOS	BIOS_SAR160.78.04.012
BMC	159.00.1433
FPGA	1.E.0.0

Network Information

IPv4 Source	DHCP
IPv4 Address	[redacted]
Subnet Mask	[redacted]
Gateway	[redacted]
MAC	[redacted]

Time Information

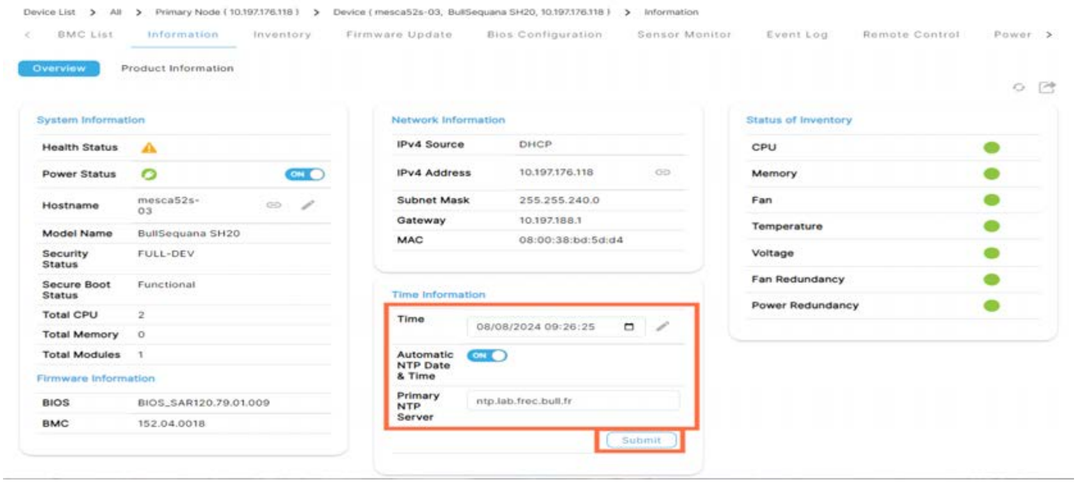
Time	8/8/2024, 09:07:20 AM
Automatic NTP Date & Time	ON
Primary NTP Server	undefined

Status of Inventory

CPU	●
Memory	●
Fan	●
Temperature	●
Voltage	●
Fan Redundancy	●
Power Redundancy	●

4.7. Changing the device time settings

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Overview** tab.
5. Change the time settings, as required.
6. Click the **Submit** button. The system reloads and displays the new settings.



System Information

Health Status	⚠
Power Status	ON
Hostname	mesca52s-03
Model Name	BullSequana SH20
Security Status	FULL-DEV
Secure Boot Status	Functional
Total CPU	2
Total Memory	0
Total Modules	1

Firmware Information

BIOS	BIOS_SAR120.79.01.009
BMC	152.04.0018

Network Information

IPv4 Source	DHCP
IPv4 Address	10.197.176.118
Subnet Mask	255.255.240.0
Gateway	10.197.188.1
MAC	08:00:38:bd:5d:d4

Time Information

Time	08/08/2024 09:26:25
Automatic NTP Date & Time	ON
Primary NTP Server	ntp.lab.frec.bull.fr

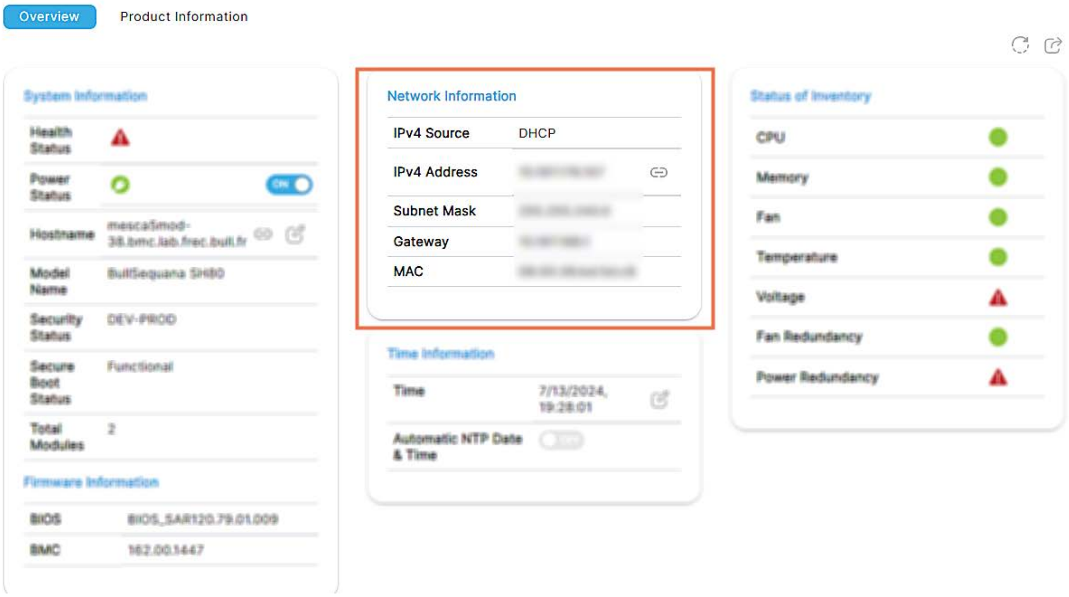
Status of Inventory

CPU	●
Memory	●
Fan	●
Temperature	●
Voltage	●
Fan Redundancy	●
Power Redundancy	●

4.8. Viewing network settings

See The SHC Reference Guide for **BullSequana EX** and **BullSequana SH** servers for more information about network settings.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Overview** tab.



System Information

Health Status	▲
Power Status	● ON
Hostname	mesca5mod-38.bmc.lab.frec.bull.fr
Model Name	BullSequana SH80
Security Status	DEV-PROD
Secure Boot Status	Functional
Total Modules	2

Firmware Information

BIOS	BIOS_SAR120.79.01.009
BMC	162.00.1447

Network Information

IPv4 Source	DHCP
IPv4 Address	[redacted]
Subnet Mask	[redacted]
Gateway	[redacted]
MAC	[redacted]

Time Information

Time	7/13/2024, 19:28:01
Automatic NTP Date & Time	OFF

Status of Inventory

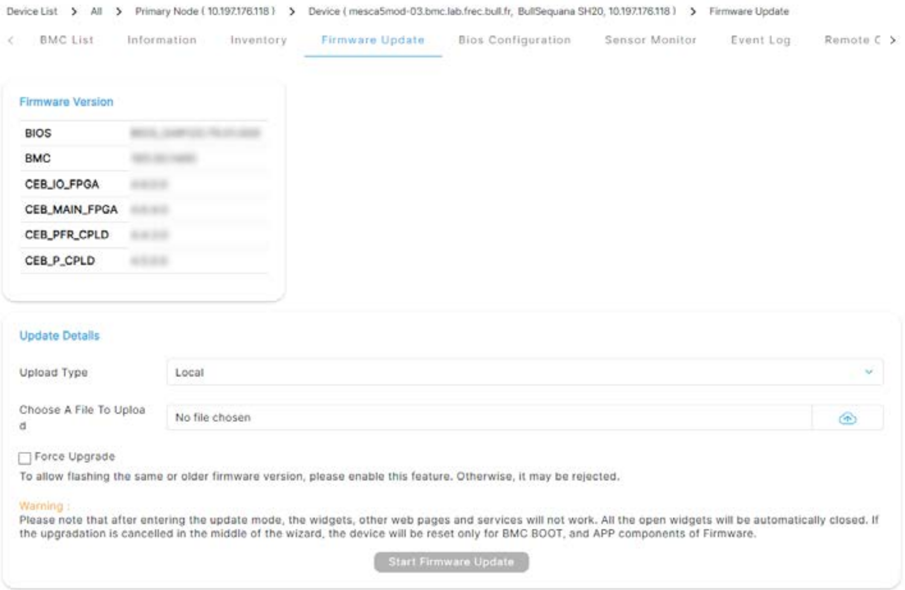
CPU	●
Memory	●
Fan	●
Temperature	●
Voltage	▲
Fan Redundancy	●
Power Redundancy	▲

4.9. Updating device firmware

Note The firmware listed, and that can be updated, varies according to server type.

To update firmware for a single device:

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Select the device and click the **Firmware Update** tab. The firmware update window opens
5. Choose the **Upload Type**, either a local path or a remote path, for the file.


Device List > All > Primary Node (10.197.176.118) > Device (mesca5mod-03.bmc.lab.frec.bull.fr, BullSequana SH20, 10.197.176.118) > Firmware Update
<
BMC List
Information
Inventory
Firmware Update
Bios Configuration
Sensor Monitor
Event Log
Remote C
>

Firmware Version

BIOS	[redacted]
BMC	[redacted]
CEB_IO_FPGA	[redacted]
CEB_MAIN_FPGA	[redacted]
CEB_PFR_CPLD	[redacted]
CEB_P_CPLD	[redacted]

Update Details

Upload Type: Local

Choose A File To Upload: No file chosen

□ Force Upgrade

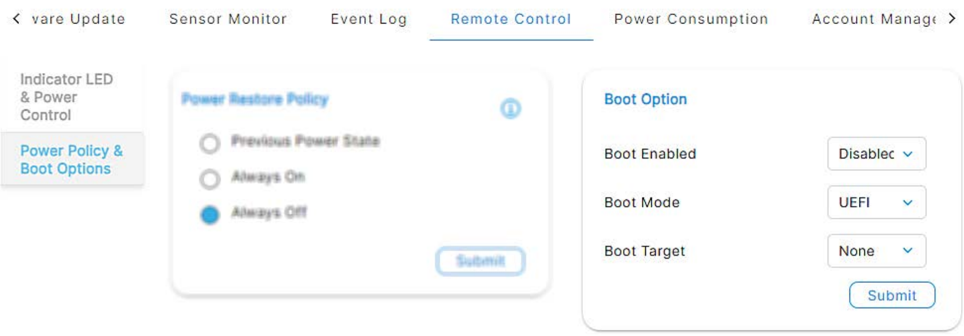
To allow flashing the same or older firmware version, please enable this feature. Otherwise, it may be rejected.

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

6. Select the **Firmware Image Type** to update.
7. If uploading from a local path, select the image to update. Otherwise, click the **Start Firmware Update** button to proceed with remote path setup.
8. If using a remote path, enter the remote path details, such as protocol type, server address, and image name.

4.10. Configuring boot options

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. From the **Remote Control** tab, click the **Power Policy & Boot Options** button.



Power Restore Policy

○ Previous Power State
○ Always On
● Always Off

Boot Option

Boot Enabled: Disablec

Boot Mode: UEFI

Boot Target: None

5. Select the boot options, as required.

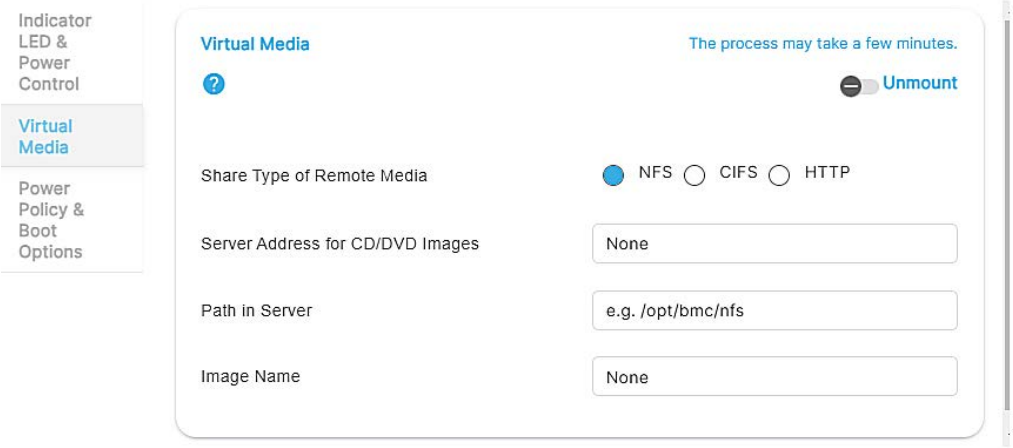
Target	Description
None	
Pxe	Boots from a PXE server
Hdd	Boots from a hard disk
Diags	Boots from a diagnostic partition
BiosSetup	Boots from the BIOS menu
Usb	Boots from a USB key

6. Click the **Submit** button. The system reloads and displays the new settings.

4.11. Mounting virtual media for BullSequana SA servers

Note This procedure applies to BullSequana SA servers only.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Remote Control** tab. The Remote Control window opens.
5. Click the **Virtual Media** button. The Virtual Media window opens



Virtual Media

The process may take a few minutes.

Share Type of Remote Media ● NFS ○ CIFS ○ HTTP

Server Address for CD/DVD Images: None

Path in Server: e.g. /opt/bmc/nfs

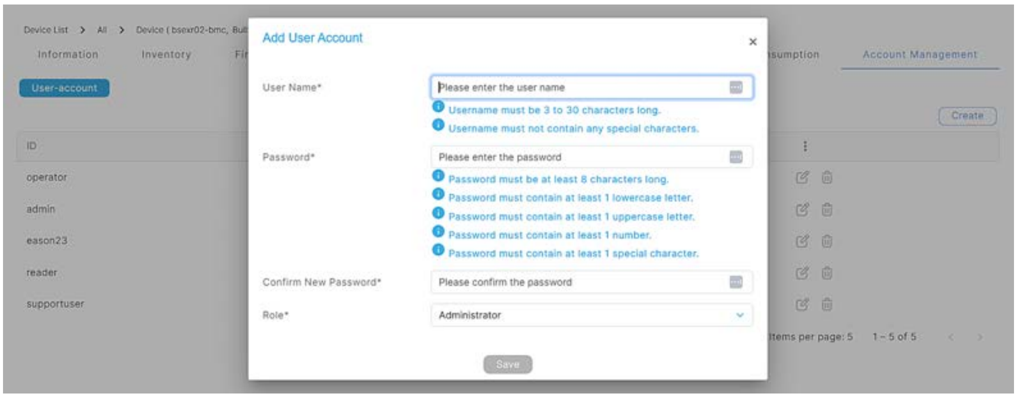
Image Name: None

6. Enter the share type, server address, path on the server, and image name. No input is needed for unmounting.
7. Toggle the switch to perform mount or unmount actions.
8. The result of the virtual media operation will be displayed on the screen.

Note If the image is successfully mounted, it will start and run on the target IP.

4.12. Creating a BMC user account

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. From the **Account Management** sub menu click **Create.**



Add User Account

User Name*: Please enter the user name

Username must be 3 to 30 characters long.

Username must not contain any special characters.

Password*: Please enter the password

Password must be at least 8 characters long.

Password must contain at least 1 lowercase letter.

Password must contain at least 1 uppercase letter.

Password must contain at least 1 number.

Password must contain at least 1 special character.

Confirm New Password*: Please confirm the password

Role*: Administrator

5. Enter the user account details, as required.
6. Click **Save**. The result is displayed on screen.

4.13. Editing a BMC user account

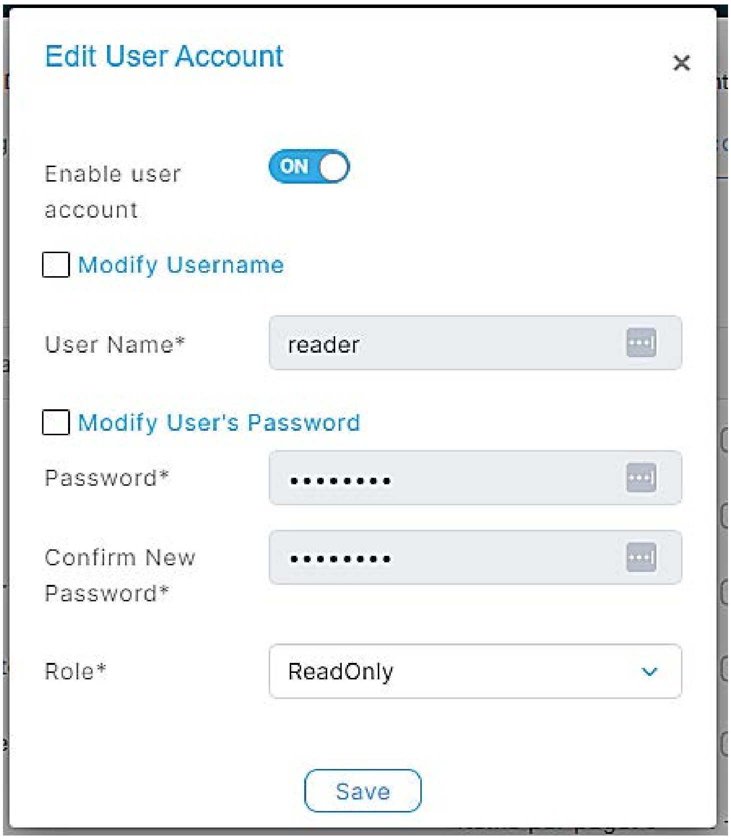
1. From the **Devices** tab, click **Device List**.

2. From the **Device List** page, click **All** or select server type.

3. Click on the server required in the list, the **Information** page opens.

4. From the **Account Management** sub menu, select the user account.

5. Click the **Edit User Account** button on the right.



Edit User Account

Enable user account: ON

□ Modify Username

User Name*: reader

□ Modify User's Password

Password*: •••••••••

Confirm New Password*: •••••••••

Role*: ReadOnly

6. Change the BMC user account details, as required.

7. Click **Save**. The result is displayed on screen.

Chapter 5. Configuring device groups

5.1. Updating group firmware

Note The firmware listed, and that can be updated, varies according to server type.

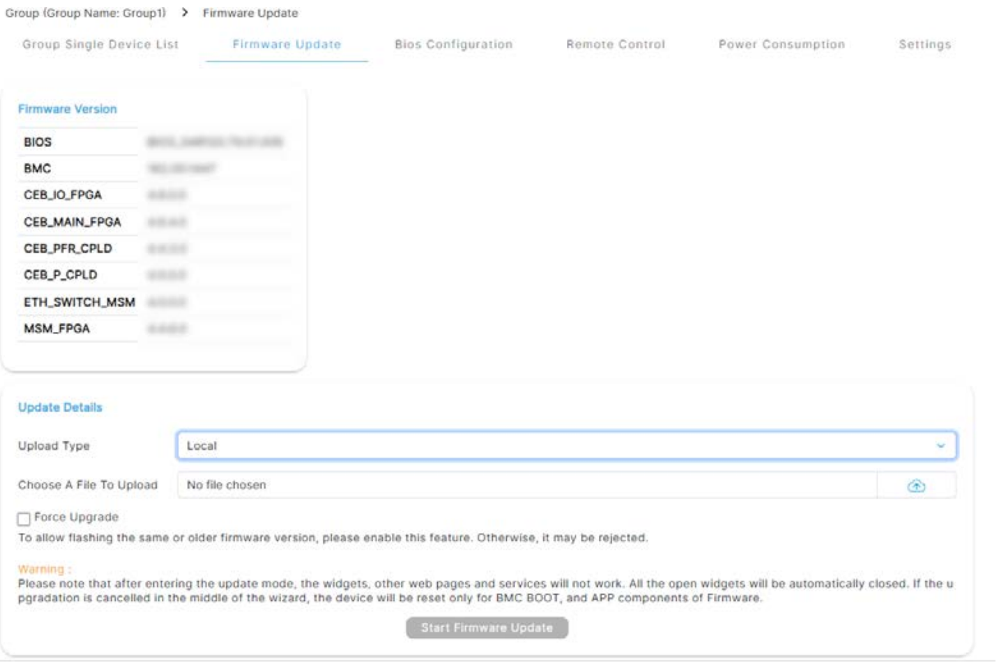
Notes For group firmware updates, only the local path is supported for the **Upload Type**.

1. From the **Devices** page, click **Groups**.

2. In the **Group** window, click on the group required.

3. Click the **Firmware Update** tab. The firmware update window opens

4. Select the **Firmware Image Type** to update.



BIOS	[redacted]
BMC	[redacted]
CEB_IO_FPGA	[redacted]
CEB_MAIN_FPGA	[redacted]
CEB_PFR_CPLD	[redacted]
CEB_P_CPLD	[redacted]
ETH_SWITCH_MSM	[redacted]
MSM_FPGA	[redacted]

Upload Type: Local

Choose A File To Upload: No file chosen

□ Force Upgrade

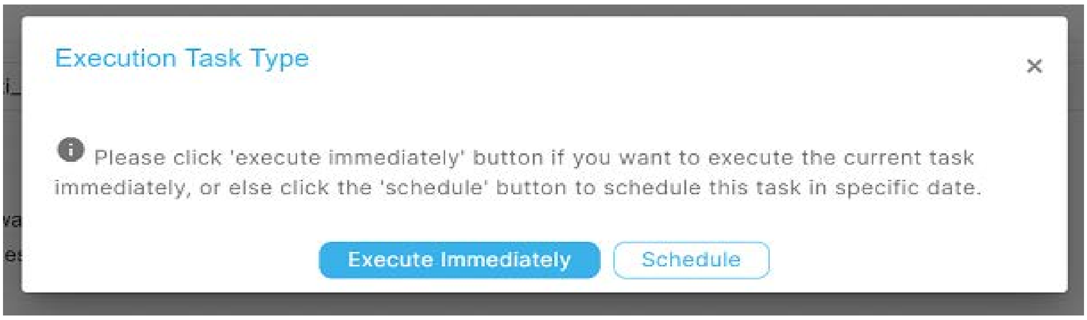
To allow flashing the same or older firmware version, please enable this feature. Otherwise, it may be rejected.

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

5. Select the local path for the file to be uploaded.

6. Click **Start Firmware Update**.

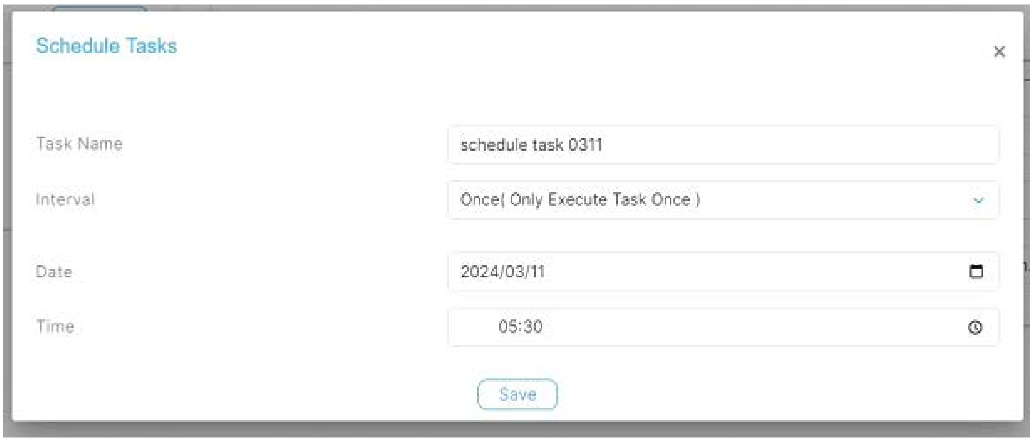
7. Choose the **Execution Task type**, either immediate or scheduled.



Execution Task Type

Please click 'execute immediately' button if you want to execute the current task immediately, or else click the 'schedule' button to schedule this task in specific date.

8. Enter the **Date** and **Time** if scheduled for later.



Schedule Tasks

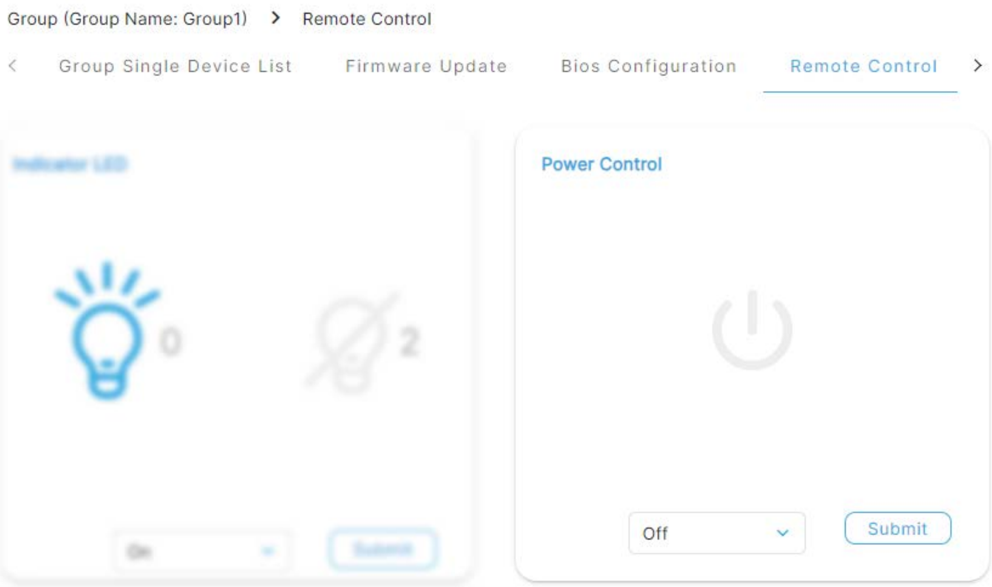
Task Name	schedule task 0311
Interval	Once(Only Execute Task Once)
Date	2024/03/11
Time	05:30

5.2. Powering on / off a device group

1. From the **Devices** page, click **Groups**.

2. In the **Group** window, click on the group required.

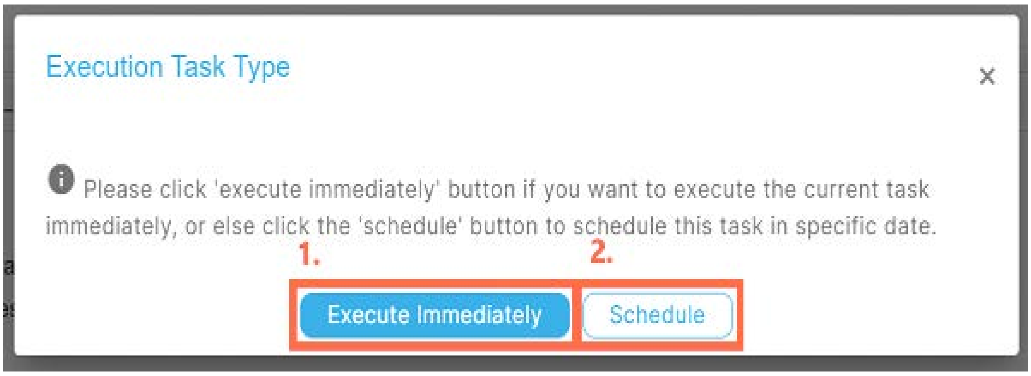
3. From the **Remote Control** tab, click the **Indicator LED & Power Control** button.



4. Choose an option to perform actions such as **On**, **Off**, **Hard Reset**, or **Graceful Shutdown**.

5. Click the **Submit** button.

6. For group power control, decide whether the task should be executed immediately or at a scheduled time.



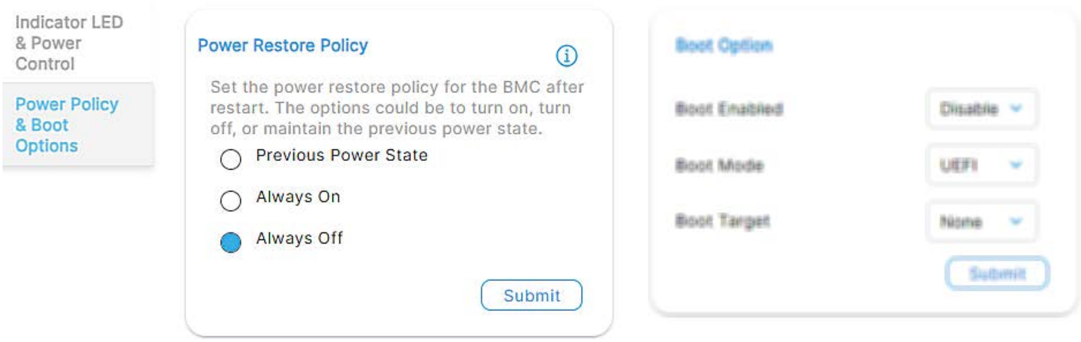
Execution Task Type

Please click 'execute immediately' button if you want to execute the current task immediately, or else click the 'schedule' button to schedule this task in specific date.

7. If scheduled, enter the scheduled time for the task. The result will be displayed after saving. Otherwise, the result will be shown immediately.

5.3. Configuring group power restore settings

1. From the **Devices** page, click **Groups**.
2. In the **Group** window, click on the group required.
3. From the **Remote Control** tab, click the **Power Policy & Boot Options** button.



Power Restore Policy

Set the power restore policy for the BMC after restart. The options could be to turn on, turn off, or maintain the previous power state.

○ Previous Power State

○ Always On

● Always Off

Boot Option

Boot Enabled: Disable

Boot Mode: UEFI

Boot Target: None

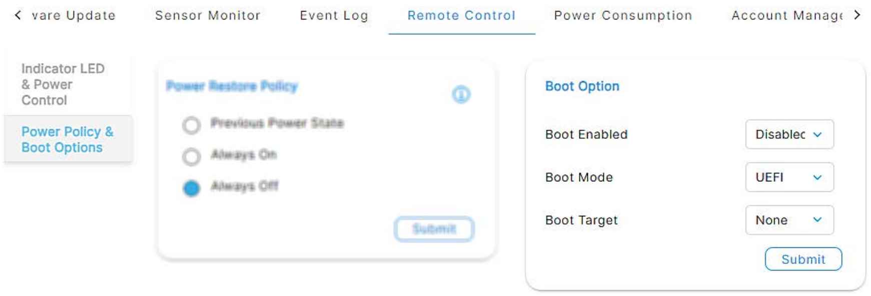
4. Select the power restore policy, as required.
5. Click the **Submit** button. The system reloads and displays the new settings.

5.4. Configuring group boot options

1. From the **Devices** page, click **Groups**.

2. In the **Group** window, click on the group required.

3. From the **Remote Control** tab, click the **Power Policy & Boot Options** button.



○ Previous Power State
○ Always On
● Always Off

Boot Enabled: Disablec
Boot Mode: UEFI
Boot Target: None

4. Select the boot options, as required.

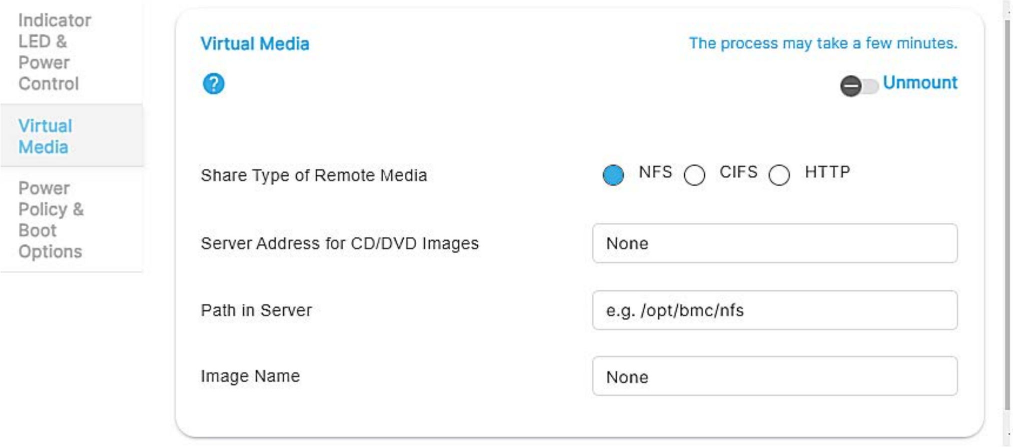
Target	Description
None	
Pxe	Boots from a PXE server
Hdd	Boots from a hard disk
Diags	Boots from a diagnostic partition
BiosSetup	Boots from the BIOS menu
Usb	Boots from a USB key

5. Click the **Submit** button. The system reloads and displays the new settings.

5.5. Mounting virtual media for BullSequana SA server groups

Note This procedure applies to BullSequana SA servers only.

1. From the **Devices** page, click **Groups**.
2. In the **Group** window, click on the group required.
3. Click the **Remote Control** tab. The Remote Control window opens.
4. Click the **Virtual Media** button. The Virtual Media window opens



The process may take a few minutes.

Share Type of Remote Media ● NFS ○ CIFS ○ HTTP

Server Address for CD/DVD Images: None

Path in Server: e.g. /opt/bmc/nfs

Image Name: None

6. Enter the share type, server address, path on the server, and image name. No input is needed for unmounting.
7. Toggle the switch to perform mount or unmount actions.
8. The result of the virtual media operation will be displayed on the screen.

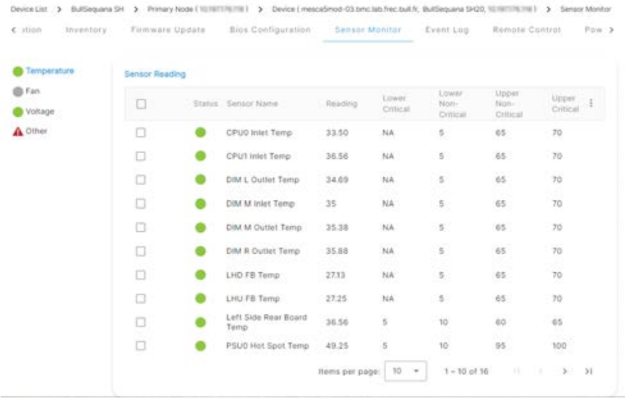
Note If the image is successfully mounted, it will start and run on the target IP.

Chapter 6. Monitoring devices

6.1. Viewing sensor data for a device

The **Sensor Monitor** page displays the status, readings, and thresholds of all sensors for a device. A chart of historical readings for each sensor is also available.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Sensor Monitor** tab. The Sensor Monitor window opens.
5. Select the sensor type : **Temperature, Fan, Voltage,** or **Other**.



Device List > BullSequana SH > Primary Node ([redacted]) > Device (mesca5mod-03.bmc.lab.frec.bull.fr, BullSequana SH20, [redacted]) > Sensor Monitor

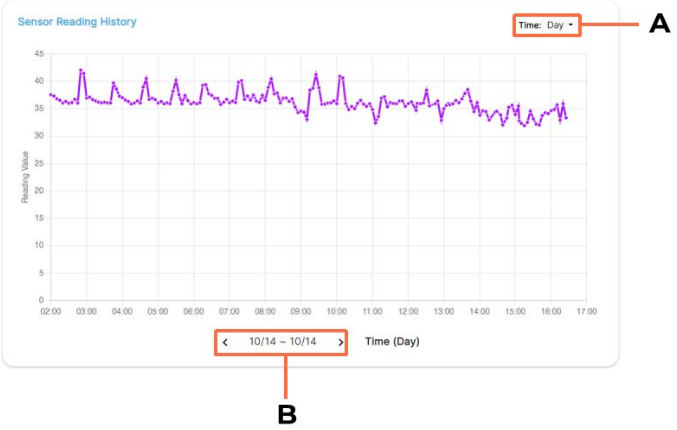
Sensor Reading

□	Status	Sensor Name	Reading	Lower Critical	Lower Non-Critical	Upper Non-Critical	Upper Critical
□	●	CPU0 Inlet Temp	33.50	NA	5	65	70
□	●	CPU1 Inlet Temp	36.56	NA	5	65	70
□	●	DIM L Outlet Temp	34.69	NA	5	65	70
□	●	DIM M Inlet Temp	35	NA	5	65	70
□	●	DIM M Outlet Temp	35.38	NA	5	65	70
□	●	DIM R Outlet Temp	35.88	NA	5	65	70
□	●	LHD FB Temp	27.13	NA	5	65	70
□	●	LHU FB Temp	27.25	NA	5	65	70
□	●	Left Side Rear Board Temp	36.56	5	10	60	65
□	●	PSU0 Hot Spot Temp	49.25	5	10	95	100

Items per page: 10 ▾ 1 – 10 of 16

6. Select an individual sensor.

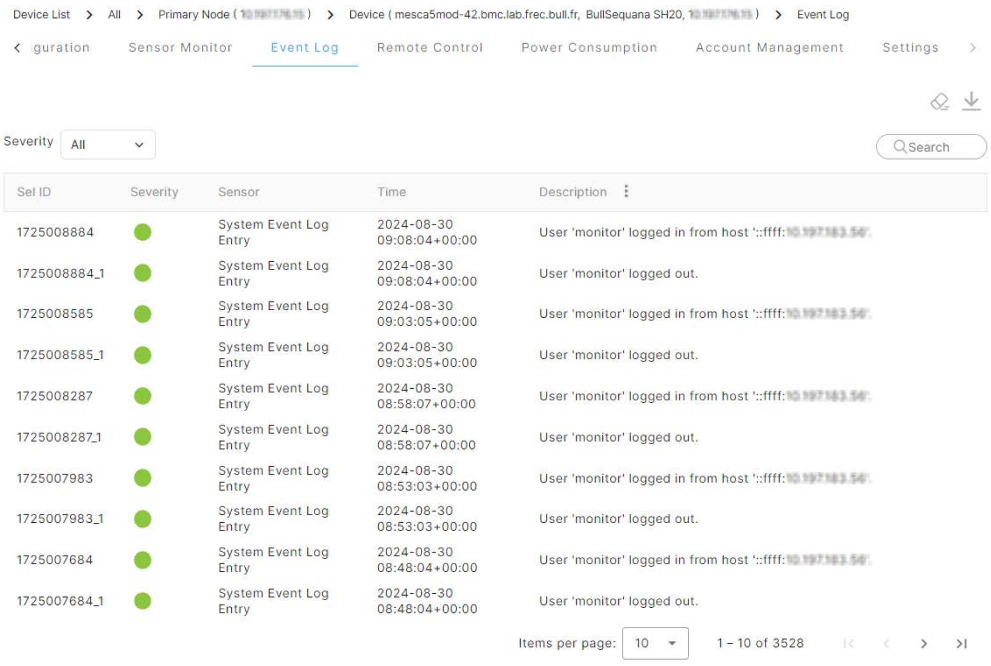
   Scroll down the page to see the Sensor Reading History. The time interval (A) and period (B) can be changed, as required.



6.2. Viewing Event Logs

Each entry in the Event Log table includes the Event ID, Severity (representing the event level), Sensor name, Time stamp, and Event description. The **Severity** attribute has four levels: **Healthy, Critical, Warning**, and Unknown.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Select the device and click the **Event Log** tab. The Event Log window opens.



Device List > All > Primary Node ([redacted]) > Device (mesca5mod-42.bmc.lab.frec.bull.fr, BullSequana SH20, [redacted]) > Event Log

Severity: All

Sel ID	Severity	Sensor	Time	Description
1725008884	●	System Event Log Entry	2024-08-30 09:08:04+00:00	User 'monitor' logged in from host '::ffff:[redacted]'.
1725008884_1	●	System Event Log Entry	2024-08-30 09:08:04+00:00	User 'monitor' logged out.
1725008585	●	System Event Log Entry	2024-08-30 09:03:05+00:00	User 'monitor' logged in from host '::ffff:[redacted]'.
1725008585_1	●	System Event Log Entry	2024-08-30 09:03:05+00:00	User 'monitor' logged out.
1725008287	●	System Event Log Entry	2024-08-30 08:58:07+00:00	User 'monitor' logged in from host '::ffff:[redacted]'.
1725008287_1	●	System Event Log Entry	2024-08-30 08:58:07+00:00	User 'monitor' logged out.
1725007983	●	System Event Log Entry	2024-08-30 08:53:03+00:00	User 'monitor' logged in from host '::ffff:[redacted]'.
1725007983_1	●	System Event Log Entry	2024-08-30 08:53:03+00:00	User 'monitor' logged out.
1725007684	●	System Event Log Entry	2024-08-30 08:48:04+00:00	User 'monitor' logged in from host '::ffff:[redacted]'.
1725007684_1	●	System Event Log Entry	2024-08-30 08:48:04+00:00	User 'monitor' logged out.

Items per page: 10 1 – 10 of 3528

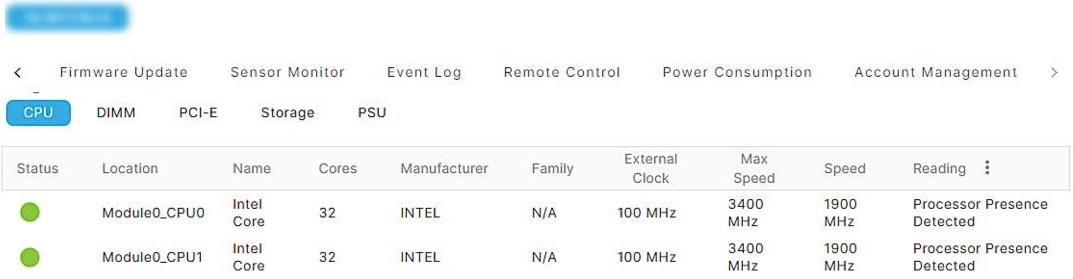
5. Filter the data by **Event Direction**, **Severity** level and **Sensor Type**, as required.
6. Use the options to clear all event log data or to download all event log data, as required

6.3. Obtaining inventory details

Note The components listed on the inventory page vary according to server type.

The CPU, and DIMM sub-pages also show the current status for these components.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Click the **Inventory** tab.
5. Click the tab for the component required.



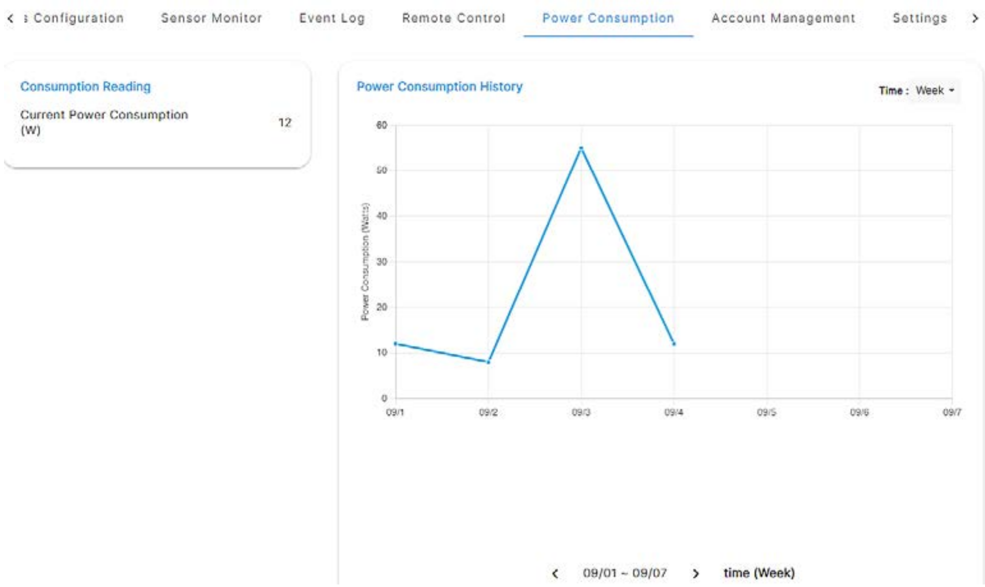
Status	Location	Name	Cores	Manufacturer	Family	External Clock	Max Speed	Speed	Reading
●	Module0_CPU0	Intel Core	32	INTEL	N/A	100 MHz	3400 MHz	1900 MHz	Processor Presence Detected
●	Module0_CPU1	Intel Core	32	INTEL	N/A	100 MHz	3400 MHz	1900 MHz	Processor Presence Detected

6.4. Viewing power consumption for a device

The **Power Consumption History** section displays the changes in power consumption over a specific period using a line chart. It is possible to change the range of the period using the time range drop-down above the chart. Additionally, it is possible to navigate through the current day, week, or month using the previous and next buttons at the bottom of the chart.

The **Consumption Reading** section shows the maximum, minimum, average, and current power consumption values.

1. From the **Devices** tab, click **Device List**.
2. From the **Device List** page, click **All** or select server type.
3. Click on the server required in the list, the **Information** page opens.
4. Select the device and click the **Power Consumption** tab. The Power Consumption window opens,



Consumption Reading

Current Power Consumption (W) 12

6.5. Viewing carbon emissions for a device

The **Carbon Emission History** graphs shows changes in carbon emissions over a specific period, using a line chart.

See 8.7.3. Modifying carbon emission viewing settings

1. From the **Devices** tab, click **Device List**.

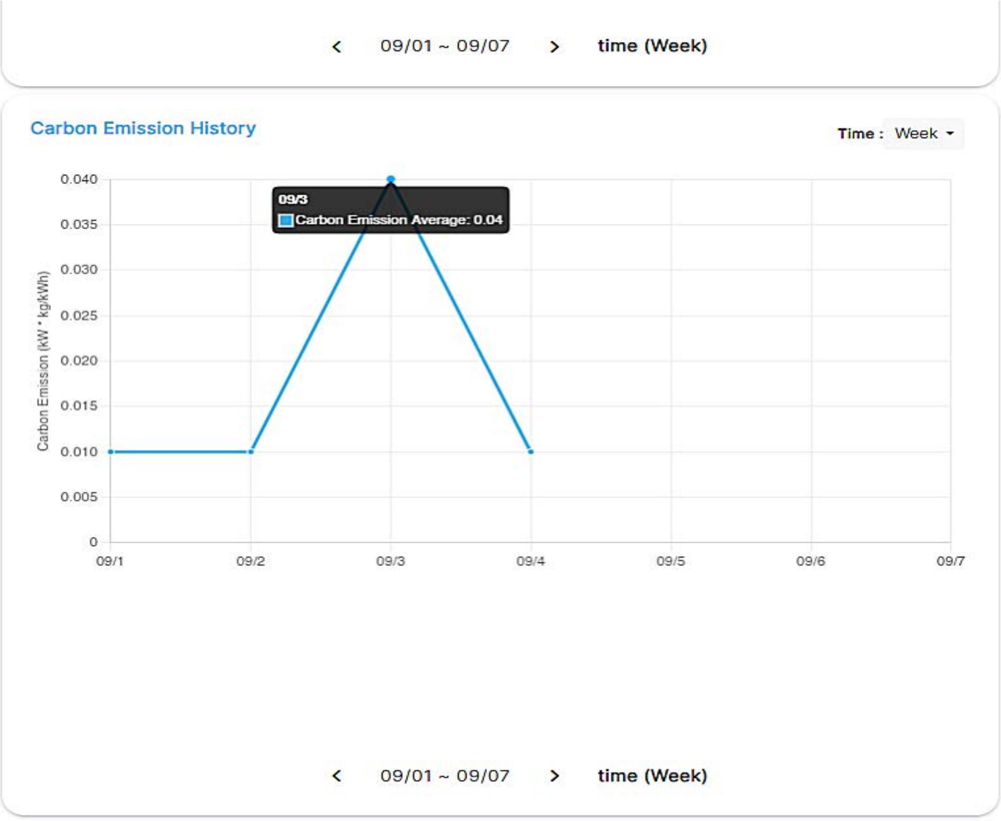
2. From the **Device List** page, click **All** or select server type.

3. Click on the server required in the list, the **Information** page opens.

3. Click the **Power Consumption** tab. The Power Consumption window opens.

4. Scroll down page to see the **Carbon Emission History** graphs.

5. Move the cursor along the graph to see specific measurements.


‹ 09/01 ~ 09/07 › time (Week)
Carbon Emission History
Time : Week
09/3
Carbon Emission Average: 0.04
Carbon Emission (kW * kg/kWh)
0.040
0.035
0.030
0.025
0.020
0.015
0.010
0.005
0
09/1
09/2
09/3
09/4
09/5
09/6
09/7
‹ 09/01 ~ 09/07 › time (Week)

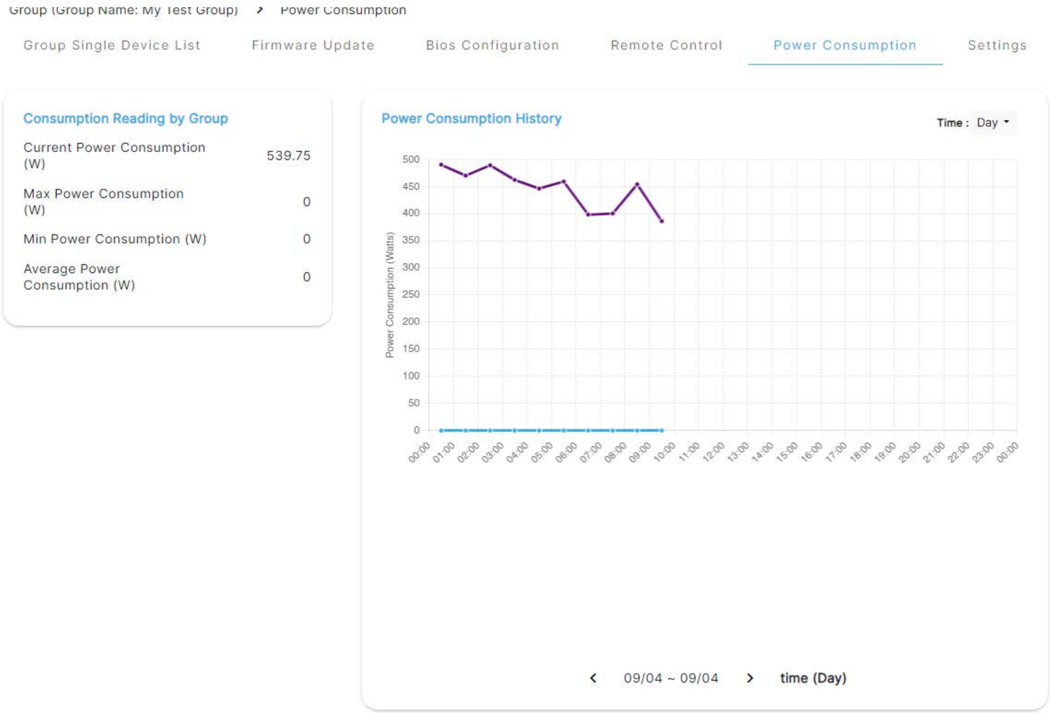
Chapter 7. Monitoring groups

7.1. Viewing power consumption for a group

The **Power Consumption History** section displays the changes in power consumption over a specific period using a line chart. It is possible to change the range of the period using the time range drop-down above the chart. Additionally, it is possible to navigate through the current day, week, or month using the previous and next buttons at the bottom of the chart.

The **Consumption Reading** section shows the maximum, minimum, average, and current power consumption values. For groups of devices, it displays the total power consumption of all group members.

1. From the **Devices** page, click **Groups**.
2. In the **Group** window, click on the group required.
3. Select the group and click the **Power Consumption** tab. The Power Consumption window opens.



Consumption Reading by Group

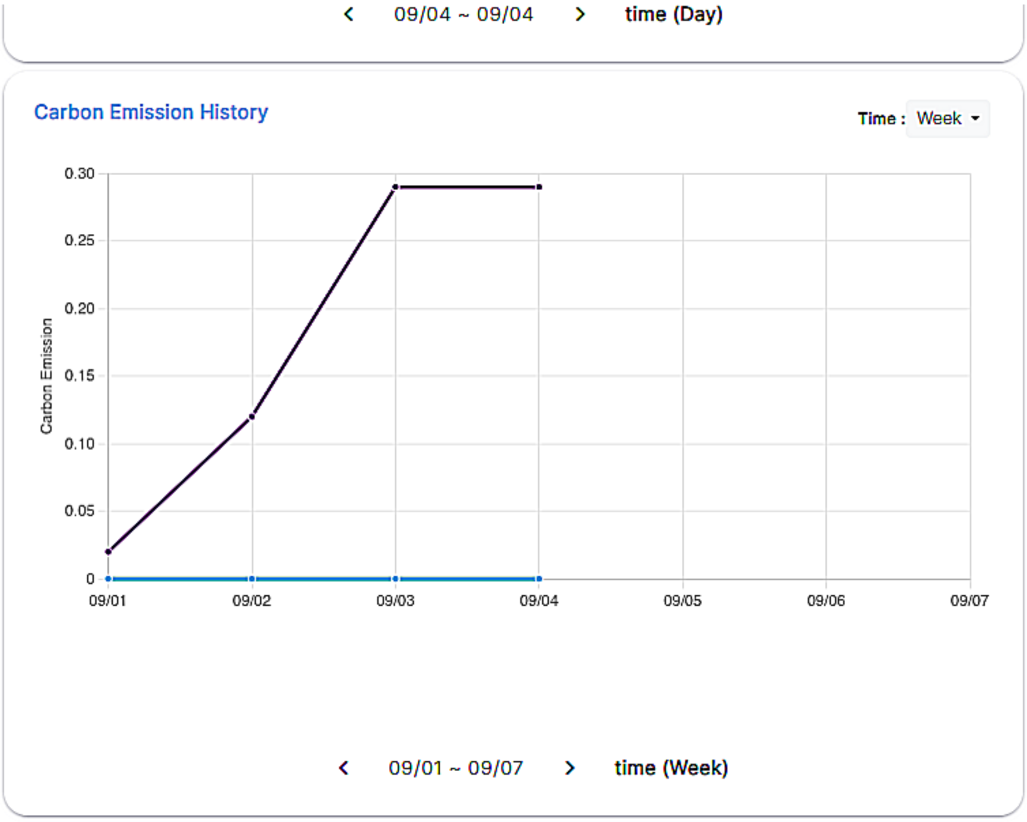
Current Power Consumption (W)	539.75
Max Power Consumption (W)	0
Min Power Consumption (W)	0
Average Power Consumption (W)	0

7.2. Viewing carbon emissions for a group

The **Carbon Emission History** graphs shows changes in carbon emissions over a specific period, using a line chart. For daily periods, each hour has its own factor. For weekly and monthly periods, the average carbon emission factor is calculated for each month and applied to the chart.

See 8.7.3. Modifying carbon emission viewing settings

1. From the **Devices** page, click **Groups**.
2. In the **Group** window, click on the group required.
3. Select the group and click the **Power Consumption** tab. The Power Consumption window opens.
4. Scroll down page to see the **Carbon Emission History** graphs.



Chapter 8. Configuring OneBSM

The **Account Management** page is used for managing user accounts and is divided into two sections: User Account and Role Permissions

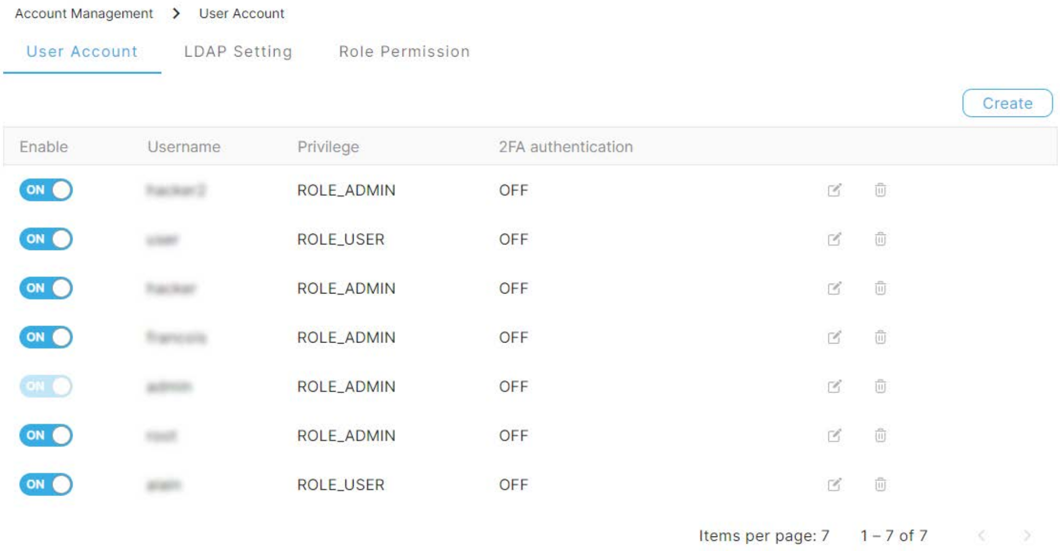
8.1. Viewing user accounts

The **User Account** sub-page displays a table listing all user accounts.

Each row displays the enabled status for the user account, user name, privilege level, and whether 2FA (two-factor authentication) is enabled.

Procedure

1. From the **Configuration** tab, click **Account Management**.
2. From the **Account Management** page, click the **User Account** tab. The list of existing users and their details is displayed.



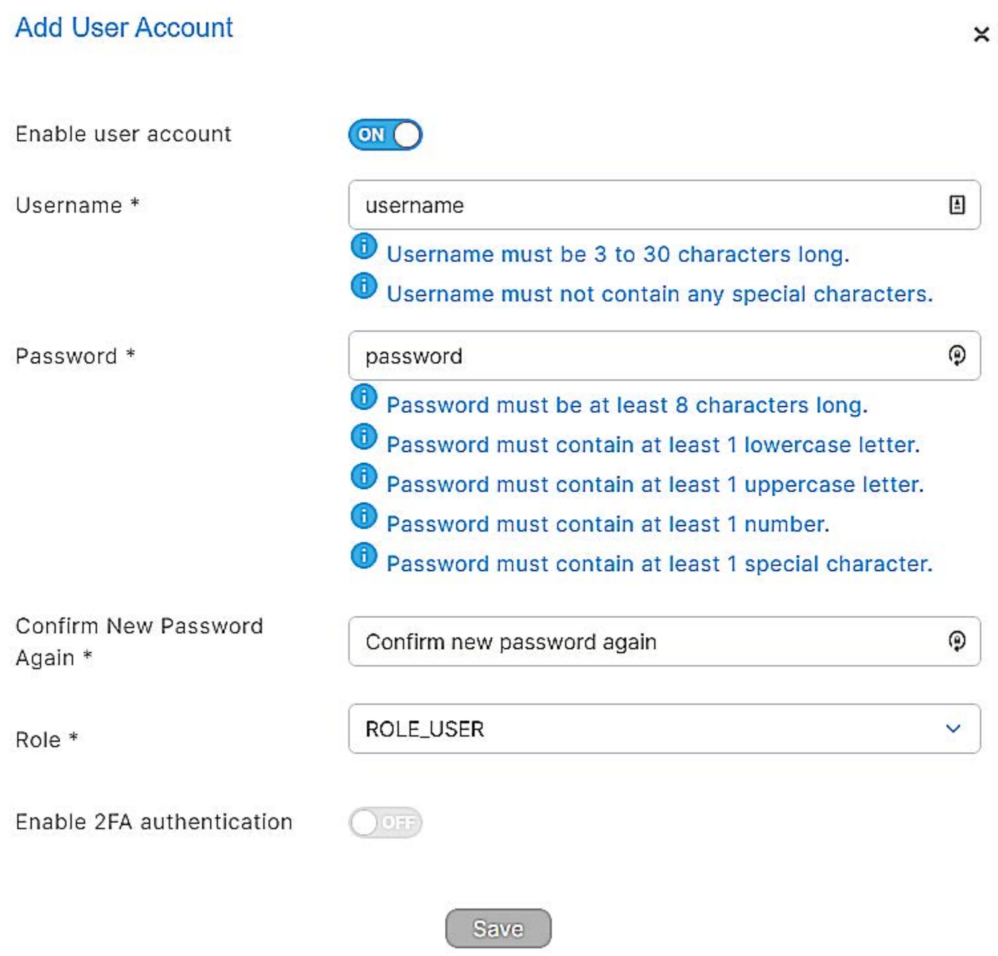
Enable	Username	Privilege	2FA authentication
ON	[redacted]	ROLE_ADMIN	OFF
ON	[redacted]	ROLE_USER	OFF
ON	[redacted]	ROLE_ADMIN	OFF
ON	[redacted]	ROLE_ADMIN	OFF
ON	[redacted]	ROLE_ADMIN	OFF
ON	[redacted]	ROLE_ADMIN	OFF
ON	[redacted]	ROLE_USER	OFF

Items per page: 7 1 – 7 of 7

8.2. Creating a user account

See	Appendix A. Logging in with the 2FA authentication

1. From the **Configuration** tab, click **Account Management**.
2. From the **Account Management** page, click the **User Account** tab.
3. From the **User Account** page, click **Create.**
4. Enter the required user account details.
5. Click **Save**. The result is displayed on screen.

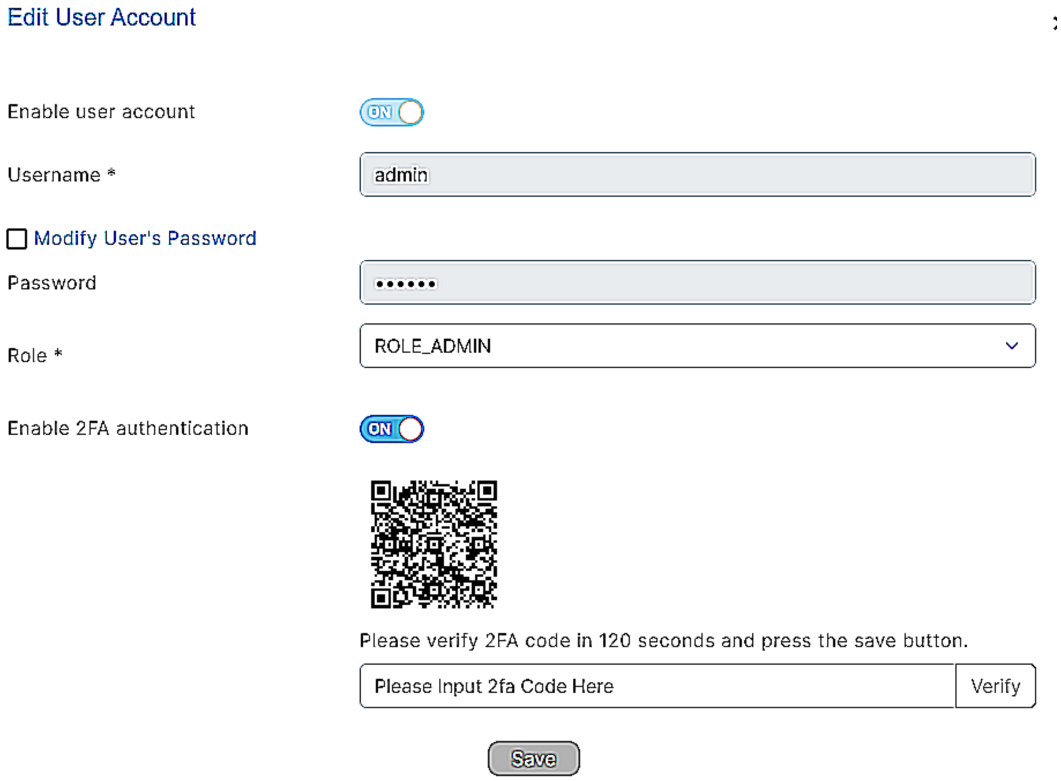


Add User Account

Enable user account	ON
Username *	username ⓘ Username must be 3 to 30 characters long. ⓘ Username must not contain any special characters.
Password *	password ⓘ Password must be at least 8 characters long. ⓘ Password must contain at least 1 lowercase letter. ⓘ Password must contain at least 1 uppercase letter. ⓘ Password must contain at least 1 number. ⓘ Password must contain at least 1 special character.
Confirm New Password Again *	Confirm new password again
Role *	ROLE_USER
Enable 2FA authentication	OFF

8.3. Editing a user account

1. From the **Configuration** tab, click **Account Management**.
2. From the **Account Management** page, click the **User Account** tab.
3. From the **User Account** page, click the **Edit** button next to the user account to be modified.
4. Change the user account details, as required.
5. Click **Save**. The result is displayed on screen.



Edit User Account

Enable user account	ON
Username *	admin
□ Modify User's Password	
Password	••••••
Role *	ROLE_ADMIN
Enable 2FA authentication	ON

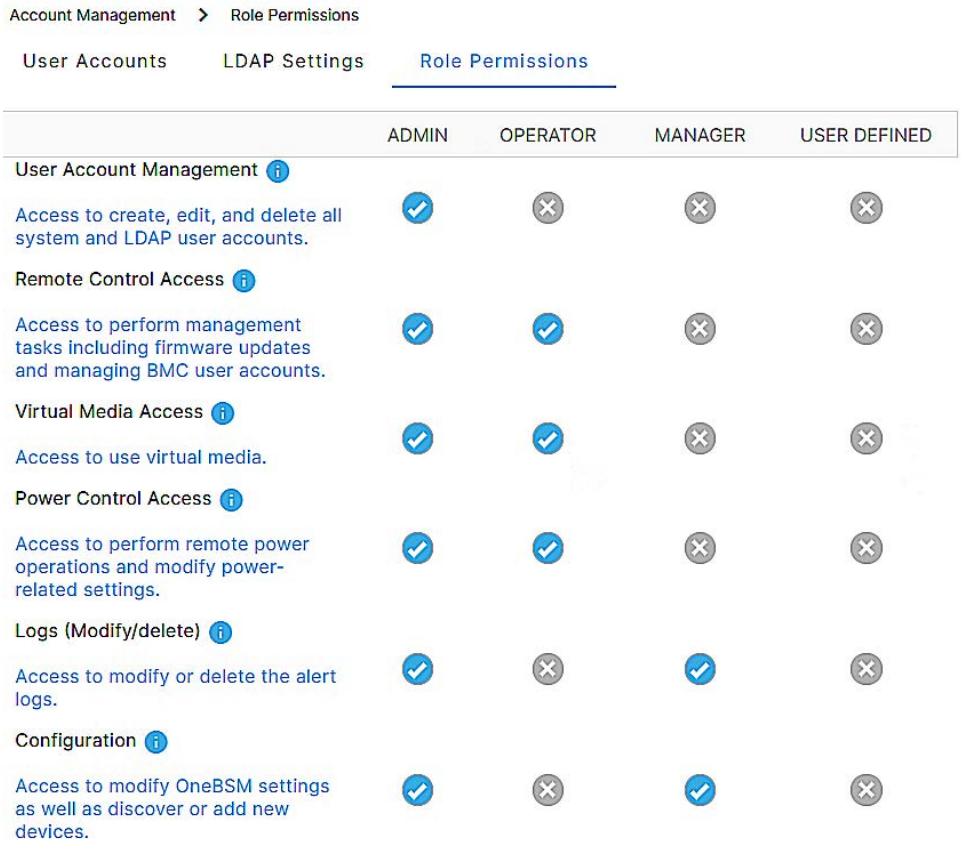
Please verify 2FA code in 120 seconds and press the save button.

Please Input 2fa Code Here

8.4. Configuring role permissions for users

Note The different accesses for each role permission is as shown in the image below.

1. From the **Configuration** tab, click **Account Management**.
2. From the **Account Management** page, click the **Role Permissions** tab.
3. From the **Role Permissions** page, enable / disable the privileges for each user role, as required.



	ADMIN	OPERATOR	MANAGER	USER DEFINED
User Account Management ⓘ				
Access to create, edit, and delete all system and LDAP user accounts.	✓	✗	✗	✗
Remote Control Access ⓘ				
Access to perform management tasks including firmware updates and managing BMC user accounts.	✓	✓	✗	✗
Virtual Media Access ⓘ				
Access to use virtual media.	✓	✓	✗	✗
Power Control Access ⓘ				
Access to perform remote power operations and modify power-related settings.	✓	✓	✗	✗
Logs (Modify/delete) ⓘ				
Access to modify or delete the alert logs.	✓	✗	✓	✗
Configuration ⓘ				
Access to modify OneBSM settings as well as discover or add new devices.	✓	✗	✓	✗

Note It not possible to modify the privileges for the Admin role.

8.5. Configuring and backing up the OneBSM database

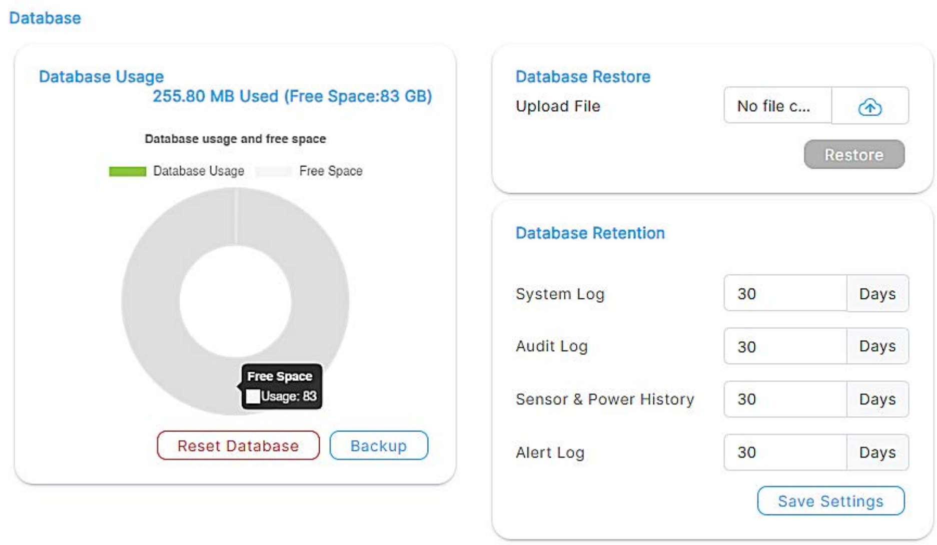
The **Database Usage** page displays details about the OneBSM database, including database usage statistics, maintenance options, and data retention intervals.

When backing up the database, the system generates a zip file containing all the data. The download process typically takes three to five minutes.

Clicking the **Reset Database** button will clear all data from the database.

Procedure

1. From the **Configuration** tab, click **Database**.
2. From the **Database Usage** page, modify the maintenance and log settings, as required.
3. Click **Save Settings.**



Database

Database Usage

255.80 MB Used (Free Space:83 GB)

Database Restore

Upload File: No file c...

Database Retention

System Log: 30 Days

Audit Log: 30 Days

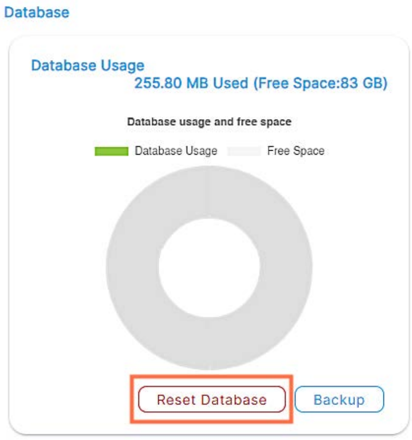
Sensor & Power History: 30 Days

Alert Log: 30 Days

8.6. Resetting the OneBSM database

Important	**Resetting the OneBSM database will clear everything from the database.**

1. From the **Configuration** tab, click **Database**.
2. From the **Database Usage** page, click **Reset Database.**



Database

Database Usage

255.80 MB Used (Free Space:83 GB)

3. Click **Yes** on the warning screen.

The OneBSM console returns to the first login screen.

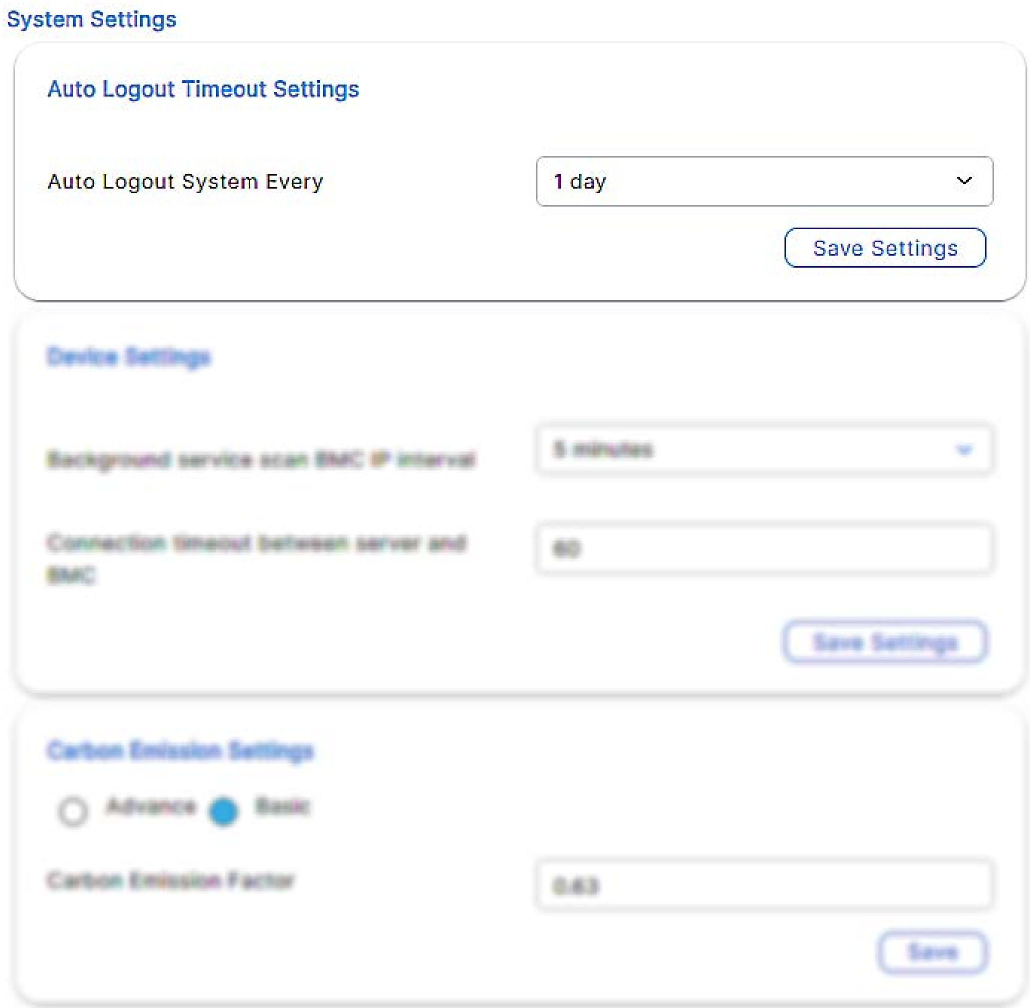
See	1.2. Connecting to the OneBSM console for the first time

8.7. Configuring OneBSM system settings

8.7.1. Modifying the automatic log-out setting

The automatic log-out interval determines how long the system can remain idle before automatically logging out.

1. From the **Configuration** tab, click **System Settings.**
2. From the **System Settings** page, change the Auto Logout Timeout, as required.



System Settings

Auto Logout Timeout Settings

Auto Logout System Every: 1 day

Device Settings

Background service scan BMC IP interval: 5 minutes

Connection timeout between server and BMC: 60

Carbon Emission Settings

○ Advance ● Basic

Carbon Emission Factor: 0.63

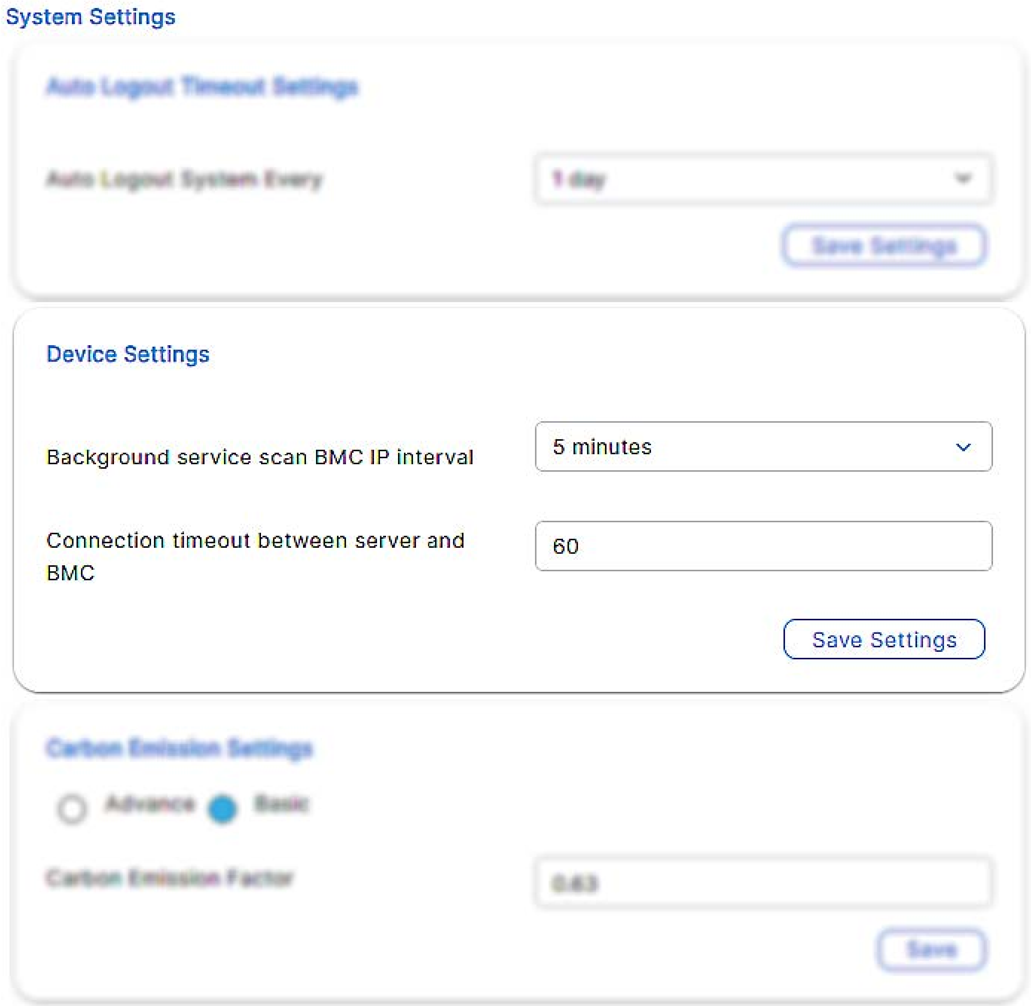
3. Click **Save Settings**.

8.7.2. Modifying BMC scan settings

The background service scan for the BMC impacts metrics for sensors, health status, and power consumption. It does not clear existing sensor history information stored for the device. The scanning interval for the sensor values from the device BMC can also be changed.

Procedure

1. From the **Configuration** tab, click **System Settings.**
2. From the **System Settings** page, change the device scan settings as required.



Auto Logout System Every: 1 day

Background service scan BMC IP interval: 5 minutes

Connection timeout between server and BMC: 60

Carbon Emission Factor: 0.63

3. Click **Save Settings**.

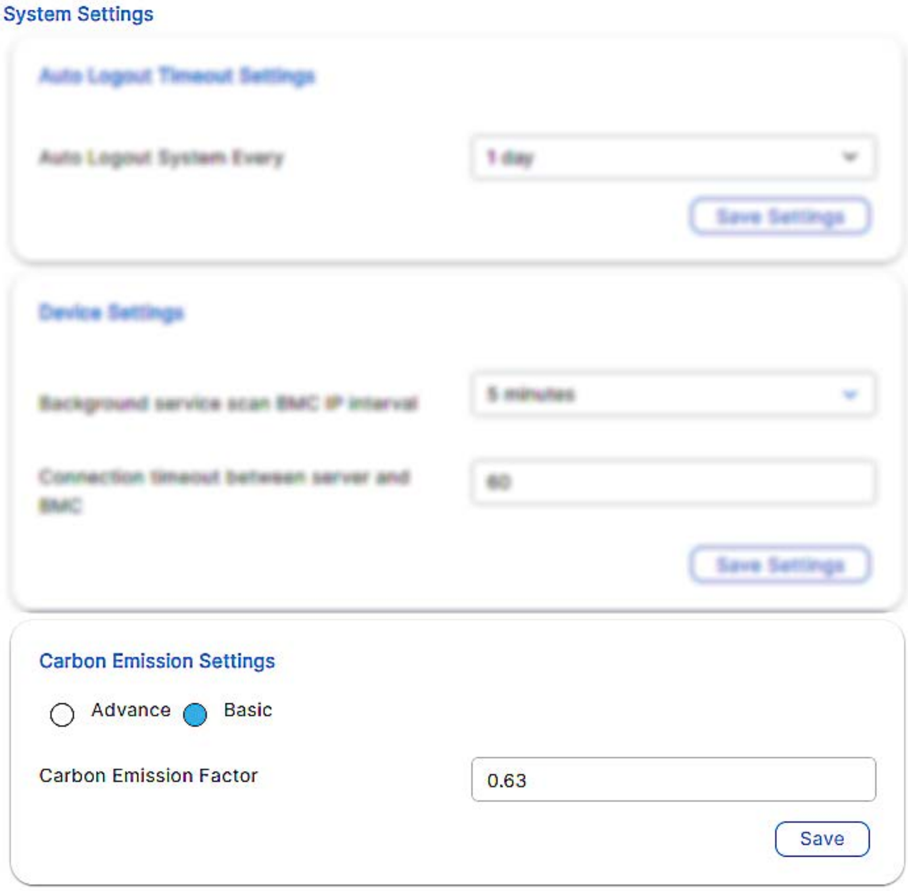
8.7.3. Modifying carbon emission viewing settings

Two modes are available for viewing and editing carbon emissions.

- **Basic mode** : only a single factor value can be entered, which will be applied to all timestamps in the carbon emission factor table.
- **Advance mode** : it is possible to view and edit the carbon emission factor table with hourly and monthly data.

Procedure

1. From the **Configuration** tab, click **System Settings.**



System Settings

Auto Logout Timeout Settings

Auto Logout System Every: 1 day

Save Settings

Device Settings

Background service scan BMC IP interval: 5 minutes

Connection timeout between server and BMC: 60

Save Settings

Carbon Emission Settings

○ Advance ● Basic

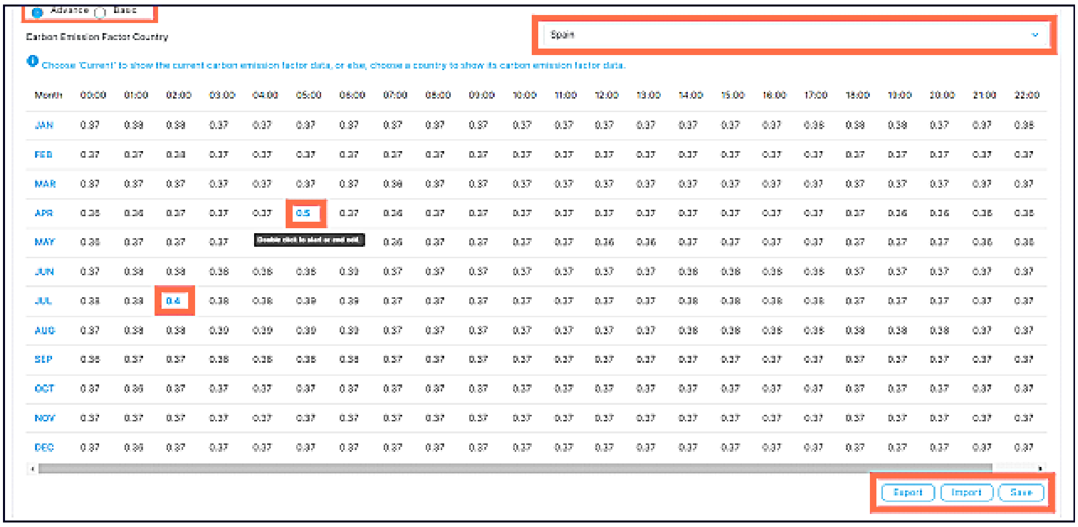
Carbon Emission Factor: 0.63

Save

2. From the Carbon Emission Settings pane select **Advance** or **Basic.**

   a. In **Basic** mode enter the factor value directly into the field.

   b. In **Advance** mode:



● Advance ○ Basic

Carbon Emission Factor Country: Spain

Choose 'Current' to show the current carbon emission factor data, or else, choose a country to show its carbon emission factor data.

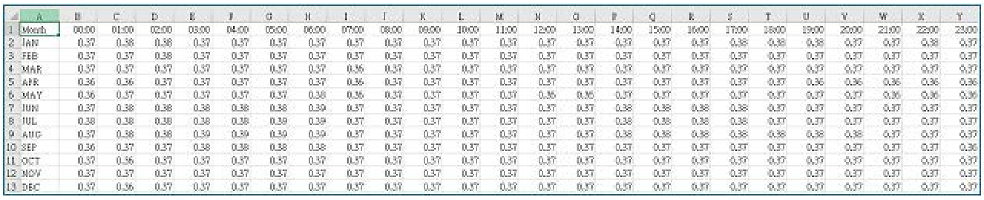
Month	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00
JAN	0.37	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.37	0.37	0.38
FEB	0.37	0.37	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
MAR	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
APR	0.36	0.36	0.37	0.37	0.37	0.5	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.36	0.36	0.36
MAY	0.36	0.37	0.37	0.37				0.36	0.37	0.37	0.37	0.37	0.36	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.36
JUN	0.37	0.38	0.38	0.38	0.38	0.38	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37
JUL	0.38	0.38	0.4	0.38	0.38	0.39	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37
AUG	0.37	0.38	0.38	0.39	0.39	0.39	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.38	0.38	0.38	0.37	0.37
SEP	0.36	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
OCT	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
NOV	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
DEC	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37

i. Update the table with factor data

ii. Select a country from the drop-down to apply its factor data.

iii. Double-click a value in the table to edit it manually.

iv. Import factor data by uploading a file in the **.csv** format, as shown.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	Month	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
2	JAN	0.37	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.37	0.37	0.38	0.37
3	FEB	0.37	0.37	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
4	MAR	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
5	APR	0.36	0.36	0.37	0.37	0.37	0.37	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.36	0.36	0.36	0.36
6	MAY	0.36	0.37	0.37	0.37	0.37	0.37	0.38	0.36	0.37	0.37	0.37	0.37	0.36	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36	0.36	0.36
7	JUN	0.37	0.38	0.38	0.38	0.38	0.38	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37
8	JUL	0.38	0.38	0.38	0.38	0.38	0.39	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37
9	AUG	0.37	0.38	0.38	0.39	0.39	0.39	0.39	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.38	0.38	0.38	0.38	0.38	0.38	0.38	0.37	0.37	0.37
10	SEP	0.36	0.37	0.37	0.38	0.38	0.38	0.38	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.36
11	OCT	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
12	NOV	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37
13	DEC	0.37	0.36	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37	0.37

v. Select the **Current** option in the country drop-down to apply the current carbon emission factor data.

vi. Any modified values in the table will be marked.

3. Click **Save** to view the results.

4. If required, click **Export** to export the carbon emission factor data in the **.csv** format.

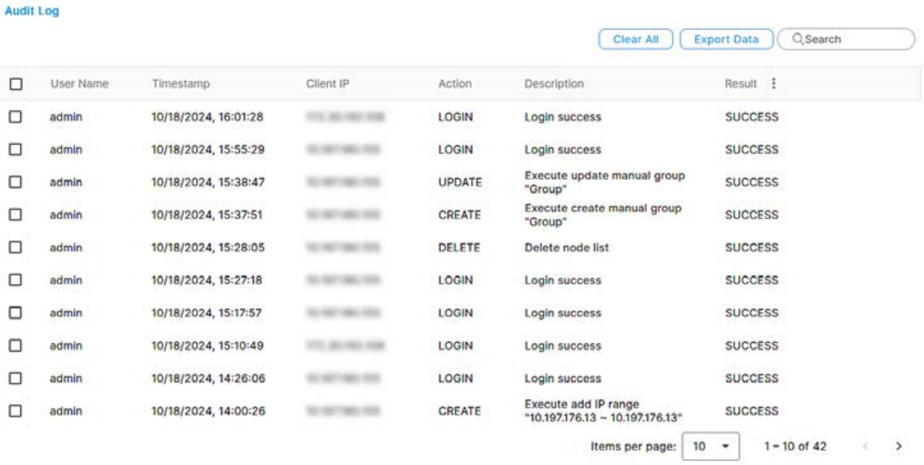
Chapter 9. Managing OneBSM

9.1. Viewing OneBSM audit logs

Audit logs shows the specific history on OneBSM activity including, including log ins, account creation, deletion, and action results.

Records are displayed in a paginated table, with a maximum of 50 rows per page.

1. From the **Maintenance** tab, click **Audit Log**.
2. From the **Audit Log** window, click **Search** to filter logs, as required.
3. Click **Clear All** to clear all the logs.
4. Click **Export Data** to download audit log data.



Audit Log

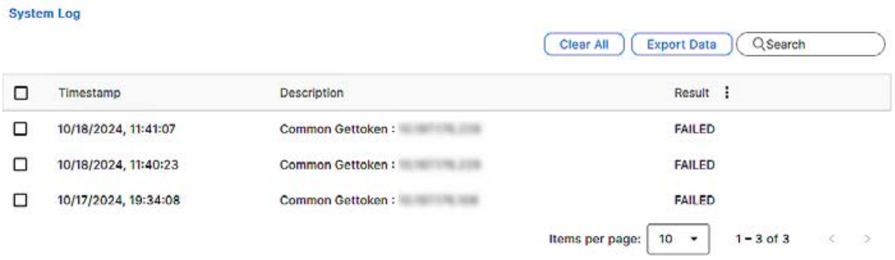
□	User Name	Timestamp	Client IP	Action	Description	Result
□	admin	10/18/2024, 16:01:28	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 15:55:29	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 15:38:47	[redacted]	UPDATE	Execute update manual group "Group"	SUCCESS
□	admin	10/18/2024, 15:37:51	[redacted]	CREATE	Execute create manual group "Group"	SUCCESS
□	admin	10/18/2024, 15:28:05	[redacted]	DELETE	Delete node list	SUCCESS
□	admin	10/18/2024, 15:27:18	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 15:17:57	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 15:10:49	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 14:26:06	[redacted]	LOGIN	Login success	SUCCESS
□	admin	10/18/2024, 14:00:26	[redacted]	CREATE	Execute add IP range "10.197.176.13 ~ 10.197.176.13"	SUCCESS

9.2. Viewing OneBSM system logs

System logs show abnormal state sensor records for target IP addresses.

Records are displayed in a paginated table, with a maximum of 50 rows per page.

1. From the **Maintenance** tab, click **System Log**.
2. From the **System Log** window, click **Search** to filter logs, as required.
3. Click **Export Data** to download system log data.



□	Timestamp	Description	Result ⋮
□	10/18/2024, 11:41:07	Common Gettoken : [redacted]	FAILED
□	10/18/2024, 11:40:23	Common Gettoken : [redacted]	FAILED
□	10/17/2024, 19:34:08	Common Gettoken : [redacted]	FAILED

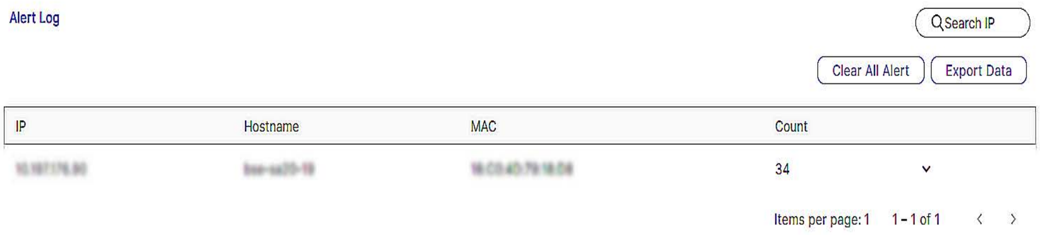
9.3. Viewing OneBSM alert logs

Alert logs show records related to sensor health, such as sensor readings. Click on the warning icon for an alert log to get more details.

The number displayed above the icon indicates the number of alert events that have occurred. If the total number of alerts exceeds 99, it will be shown as 99+.

Each data row in the alert log can be expanded by clicking on it. The expanded section will display all alert details for the target IP address .

1. From the **Maintenance** tab, click **Alert Log**.
2. From the **Alert Log** window, click **Search IP** to filter logs for a particular IP address, as required.
3. Click **Clear All Alerts** to clear the alerts listed.
4. Click **Export Data** to download audit log data.



IP	Hostname	MAC	Count
[redacted]	[redacted]	[redacted]	34 ⌄

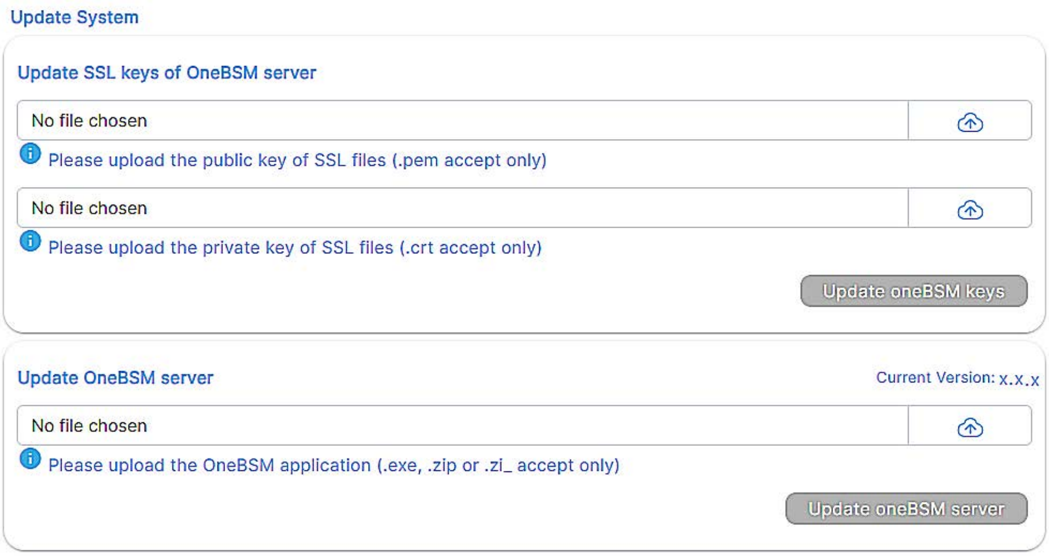
Items per page: 1 1 – 1 of 1 ‹ ›

9.4. Updating the OneBSM system

1. From the **Maintenance** tab, click **Update System.**.

2. From the **Update System** window, update the private and public SSL files, as required.

3. Click **Update OneBSM server** to update the version of OneBSM installed.



Update System

Update SSL keys of OneBSM server

No file chosen

Please upload the public key of SSL files (.pem accept only)

No file chosen

Please upload the private key of SSL files (.crt accept only)

Update OneBSM server

Current Version: x.x.x

No file chosen

Please upload the OneBSM application (.exe, .zip or .zi_ accept only)

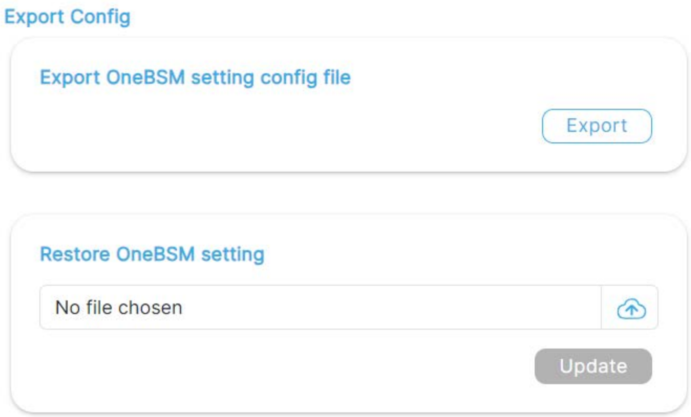
9.5. Exporting the OneBSM configuration settings

Notes

A full backup of OneBSM, including the database, can only be performed from the **Configuration > Database** tab.

OneBSM system settings are stored in a.**JSON** file.

1. From the **Maintenance** tab, click **Export Config**.
2. From the **Export Config** window, click **Export** to export the OneBSM setting config file.
3. Wait 3 to 5 seconds for the settings file to export.



No file chosen

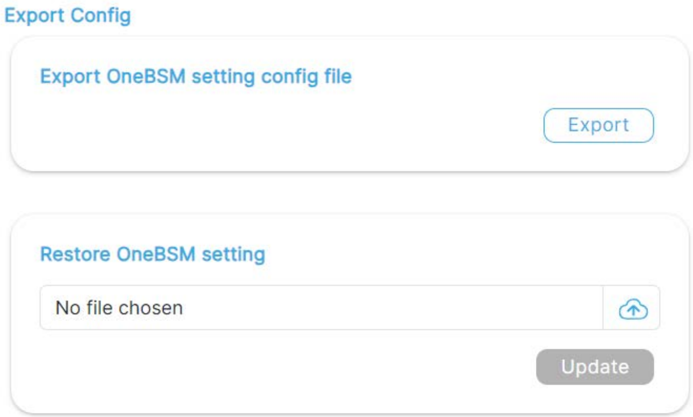
9.6. Restoring OneBSM configuration settings

Notes

A full backup of OneBSM, including the database, can only be performed from the **Configuration > Database** tab.

OneBSM system settings are stored in a.**JSON** file.

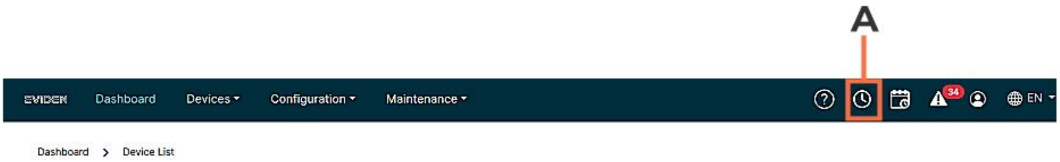
1. From the **Maintenance** tab, click **Export Config**.
2. From the **Export Config** window, select the restore .JSON file.
3. Click **Update** to restore the OneBSM setting config file.
4. Wait 3 to 5 seconds for the settings file to update.



9.7. Setting the system time and timezone for OneBSM

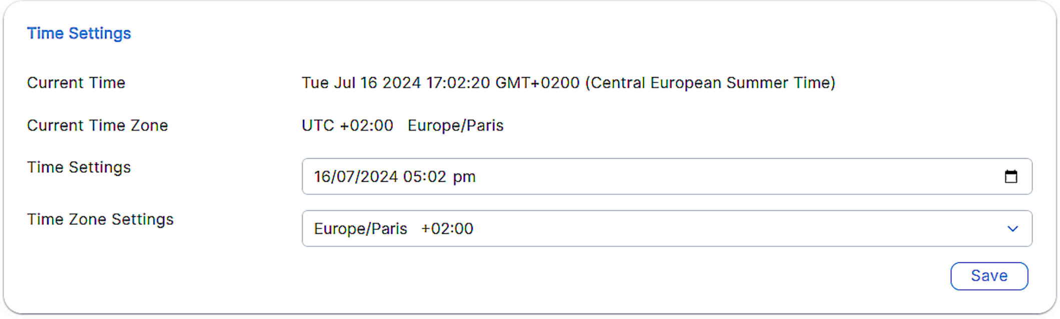
Note The date and time shown on this page reflects the time of the Operating System where OneBSM is installed. Modifying the settings will also modify the settings of the OS.

1. From the Dashboard task bar, click the **Time** button (A).



2. From the **Time** window, change the time and timezone, as required,

3. Click **Save.**



Time Settings

Current Time Tue Jul 16 2024 17:02:20 GMT+0200 (Central European Summer Time)

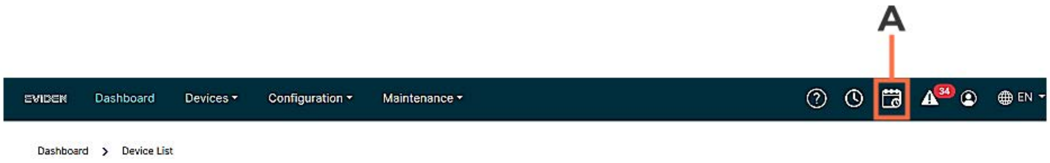
Current Time Zone UTC +02:00 Europe/Paris

Time Settings 16/07/2024 05:02 pm

Time Zone Settings Europe/Paris +02:00

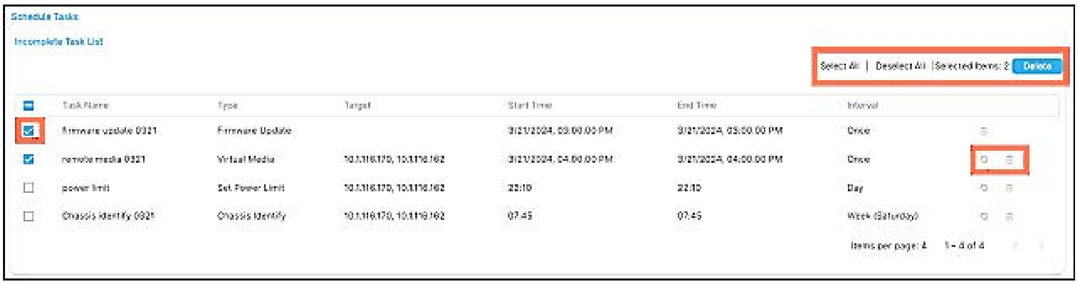
9.8. Viewing scheduled tasks

Click the **Schedule Tasks** button in the menu bar.



The Scheduled Tasks windows displays tasks according to one of three statuses:

- The **Incomplete Schedule Tasks List** table includes information such as task name, task type, target, starting time, ending time, and interval. The interval for each task can be **once**, which means the task runs once at the scheduled date and time. Other options are **daily** or **weekly**, indicating the task will execute every day at the scheduled time or every week on the scheduled weekday and time includes the same details as the Completed Task List table. Tasks in the incomplete table can be run immediately or deleted using the action buttons.



Schedule Tasks

Incomplete Task List

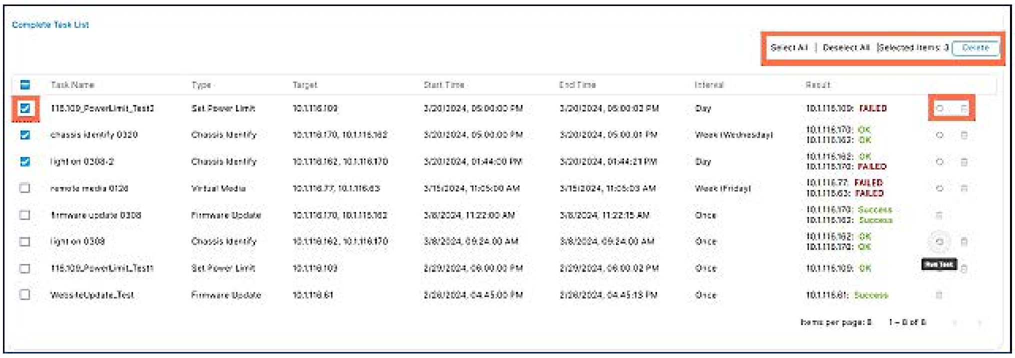
Select All | Deselect All |Selected Items: 2 Delete

	Task Name	Type	Target	Start Time	End Time	Interval
☑	firmware update 0321	Firmware Update		3/21/2024, 03:00:00 PM	3/21/2024, 03:00:00 PM	Once
☑	remote media 0321	Virtual Media	10.1.116.170, 10.1.116.162	3/21/2024, 04:00:00 PM	3/21/2024, 04:00:00 PM	Once
□	power limit	Set Power Limit	10.1.116.170, 10.1.116.162	22:10	22:10	Day
□	Chassis Identify 0321	Chassis Identify	10.1.116.170, 10.1.116.162	07:45	07:45	Week (Saturday)

Items per page: 4 1 – 4 of 4

- The **Ongoing Schedule Tasks List** table shows the task status in the last column as a progress bar. Only tasks involving firmware updates appear in the ongoing task table because they require some time to complete.

- The **Completed Schedule Tasks List** table includes the same details as the In Complete Task List table. The completed task table also shows the execution result of each task. Tasks can be re-run or deleted using the action buttons.



Complete Task List

Select All | Deselect All |Selected Items: 3 Delete

	Task Name	Type	Target	Start Time	End Time	Interval	Result
☑	115.109_PowerLimit_Test2	Set Power Limit	10.1.116.109	3/20/2024, 06:00:00 PM	3/20/2024, 06:00:02 PM	Day	10.1.116.109: FAILED
☑	chassis identify 0320	Chassis Identify	10.1.116.170, 10.1.116.162	3/20/2024, 05:00:00 PM	3/20/2024, 05:00:01 PM	Week (Wednesday)	10.1.116.170: OK 10.1.116.162: OK
☑	light on 0308-2	Chassis Identify	10.1.116.162, 10.1.116.170	3/20/2024, 01:44:00 PM	3/20/2024, 01:44:21 PM	Day	10.1.116.162: OK 10.1.116.170: FAILED
□	remote media 0126	Virtual Media	10.1.116.77, 10.1.116.63	3/15/2024, 11:05:00 AM	3/15/2024, 11:05:03 AM	Week (Friday)	10.1.116.77: FAILED 10.1.116.63: FAILED
□	firmware update 0308	Firmware Update	10.1.116.170, 10.1.116.162	3/8/2024, 11:22:00 AM	3/8/2024, 11:22:15 AM	Once	10.1.116.170: Success 10.1.116.162: Success
□	light on 0308	Chassis Identify	10.1.116.162, 10.1.116.170	3/8/2024, 09:24:00 AM	3/8/2024, 09:24:00 AM	Once	10.1.116.162: OK 10.1.116.170: OK
□	115.109_PowerLimit_Test1	Set Power Limit	10.1.116.109	2/29/2024, 06:00:00 PM	2/29/2024, 06:00:02 PM	Once	10.1.116.109: OK
□	WebsiteUpdate_Test	Firmware Update	10.1.116.61	2/28/2024, 04:45:00 PM	2/28/2024, 04:45:13 PM	Once	10.1.116.61: Success

Items per page: 8 1 – 8 of 8

Note Tasks involving firmware updates cannot be run again once they are completed.

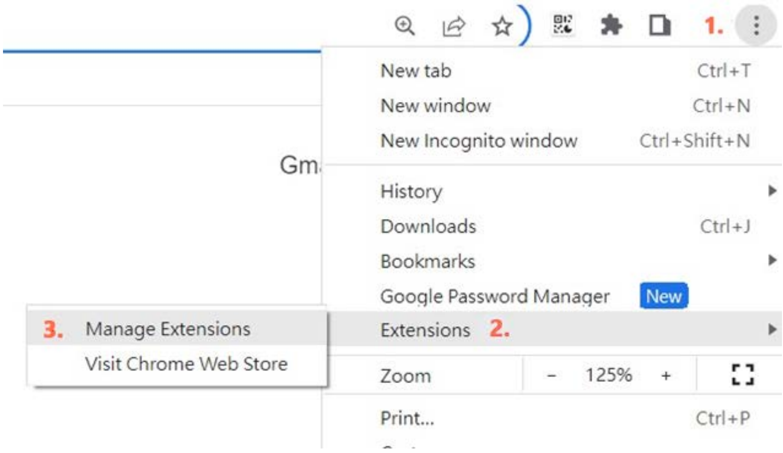
Appendix A. Logging in with the 2FA authentication

For web browser 2FA authentication, an authenticator app is required.

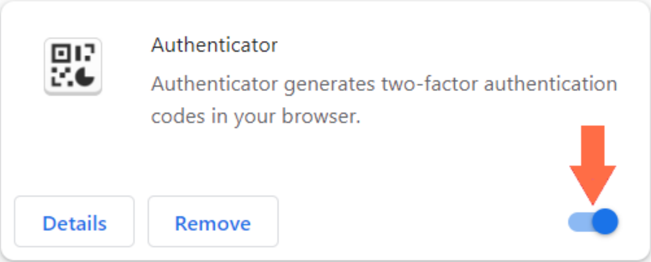
A.1. Installing the authenticator app

Example for Chrome

1. Download the Authenticator app from the Chrome web store.
2. Install the Authenticator app.
3. Enable the Authenticator app in the extension settings page.



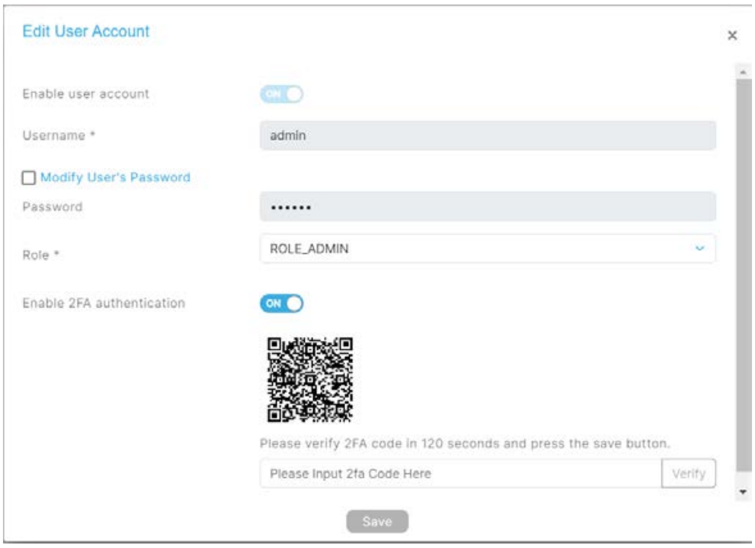
4. Enable the authenticator app. The app will be pinned on the toolbar after enabling.


Authenticator
Authenticator generates two-factor authentication codes in your browser.
Details
Remove

A.2. Enabling 2FA authentication for OneBSM users

Note For 2FA code to be accepted the date and time of the OneBSM should be synchronized with the time of the authenticator app.

1. From the **Configuration** tab, click **Account Management**.
2. From the **Account Management** page, click the **User Account** tab.
3. From the **User Account** page, click the **Edit** button next to the user account to be modified.
4. Enable 2FA authentication for the user.



Edit User Account

Enable user account: ON

Username *: admin

□ Modify User's Password

Password: ••••••

Role *: ROLE_ADMIN

Enable 2FA authentication: ON

Please verify 2FA code in 120 seconds and press the save button.

Please Input 2fa Code Here

5. Scan the QR code with a smart phone and enter the 2FA code.
6. Click **Save**.

Appendix B. Server configuration sub-menus

The Device sub-menus displayed at the top of the page for a server vary according to server type.

	Info	Inventory	Firmware Update	Sensor Monitor	Event Log	Remote Control	Power Consumption	Account Management
BullSequana SA	√	√	√	√	√	√	√	√
BullSequana SH 20 (monomodule)	√	√	√	√	√	√	√	√
BullSequana EXR/EXD	√	√	√	√	√	√	√	√
BullSequana SH multimodule (Primary module)	√	√	√	√	√	√	√	√
BullSequana SH multimodule (Secondary module)	√	√	N/A	√	√	N/A	N/A	N/A
BullSequana SH multimodule (Group)	N/A	N/A	√	N/A	N/A	√	√	N/A

eviden.com