

## Getting Started Guide

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright ©Bull SAS 2021

Printed in France

## **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**

**January 2021**

**Bull Cedoc  
357 avenue Patton  
BP 20845  
49008 Angers Cedex 01  
FRANCE**

*The information in this document is subject to change without notice. Bull 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

<b>Preface</b> .....	<b>p-1</b>
Intended Readers .....	p-1
<b>Chapter 1. Accessing the server for the first time</b> .....	<b>1-1</b>
1.1. Connect the server to the power supply .....	1-1
1.2. Connect the server to the LAN .....	1-3
1.3. Place the server in standby mode .....	1-4
1.4. Connect to the Server Hardware Console (SHC) .....	1-5
1.5. Log in to the Server Hardware Console (SHC) .....	1-6
<b>Chapter 2. Installing an Operating System</b> .....	<b>2-1</b>
2.1. Powering on the server from the SHC .....	2-1
2.2. Operating system installation options .....	2-2
2.2.1. Using a bootable USB drive .....	2-2
2.2.2. Using a Pre-boot eXecution Environment (PXE) .....	2-5
<b>Chapter 3. Connecting to the data system</b> .....	<b>3-1</b>
3.1. Connecting the server to the data LAN .....	3-1
3.2. Checking network traffic .....	3-2
<b>Chapter 4. Power operations</b> .....	<b>4-1</b>
4.1. Powering methods .....	4-1
4.2. Power modes .....	4-2
4.3. Powering on with the power button .....	4-3
4.4. Powering on the server from the SHC .....	4-4
4.5. Powering on the server from the MISM console .....	4-5
4.6. Powering off with the power button .....	4-6
4.7. Powering off the server from the SHC .....	4-7
4.8. Powering off the server from the MISM console .....	4-8
<b>Chapter 5. Server Hardware Console (SHC) maintenance operations</b> .....	<b>5-1</b>
5.1. Rebooting the Baseboard Management Controller (BMC) .....	5-1
5.2. Checking event logs .....	5-2
5.3. Checking the hardware status .....	5-3
5.4. Checking the sensors .....	5-4
5.5. Managing firmware versions .....	5-6
5.5.1. Checking firmware versions .....	5-6
5.5.2. Checking the firmware is up-to-date .....	5-8
5.5.3. Updating the BMC firmware .....	5-9
5.5.4. Updating the BIOS and CPLD firmware .....	5-11

<b>Chapter 6. MISM maintenance operation .....</b>	<b>6-1</b>
6.1. Rebooting Baseboard Management Controllers (BMCs) .....	6-1
6.2. Updating firmware .....	6-2
6.2.1. Updating firmware globally .....	6-2
6.2.2. Updating firmware individually .....	6-3
6.3. Enabling syslog forwarding .....	6-4
<b>Appendix A. IPMI Out of Band (OOB) support .....</b>	<b>A-1</b>
A.1. Enabling IPMI OOB support .....	A-1
A.2. Disabling IPMI OOB support .....	A-3
<b>Appendix B. Obtaining an IP address for the BMC .....</b>	<b>B-1</b>
B.1. Obtaining an IP address directly with an auto-discovery tool .....	B-1
B.2. Obtaining an IP address via a laptop DHCP server .....	B-4
B.3. Obtaining an IP address via a network DHCP server .....	B-6
B.4. Connecting to the SHC using the BMC address .....	B-7

---

## Preface

This guide explains how to set up the server.

---

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

---

---

**Important** **ATTENTION: Please read carefully the safety instructions before you perform the procedures described in this manual.**  
***Multilingual Safety Notices Guide***

---

---

## Intended Readers

This guide is intended for use by administrators and operators



---

## Chapter 1. Accessing the server for the first time

---

**Important** The steps in this chapter must be followed in the order indicated.

---

**See** The Installation Guide and the documentation included in the documentation set for more information.

---

### 1.1. Connect the server to the power supply

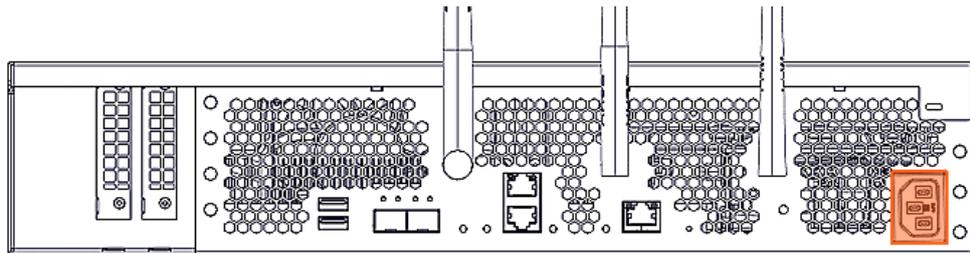
---

**Important** The site power breaker must be OFF when the server is connected to the power supply. The site power supply must remain OFF until the system is ready to be powered on.

---

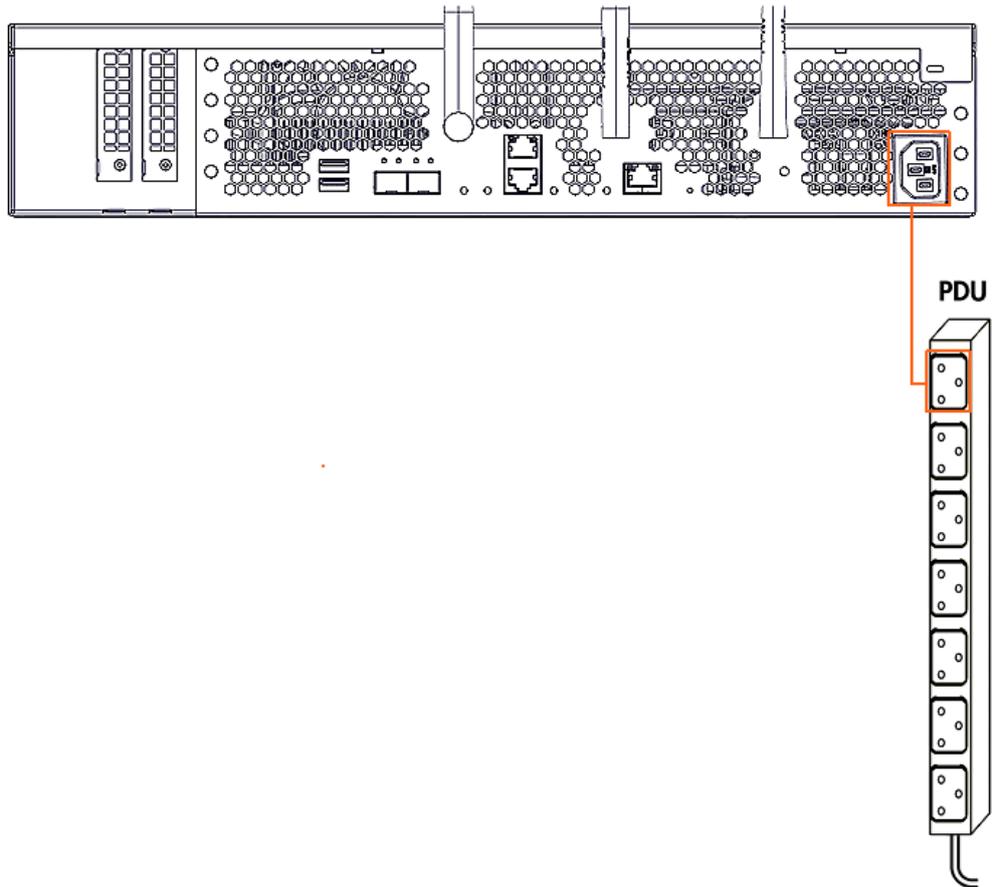
1. Locate the power supply connection.

 **Rear view**



2. Connect the server to the power supply.
  - If the server is installed in a rack cabinet:
    - i. Route the power cable along the cabinet flange to the PDU.
    - ii. Plug the power cable into the required PDU.
  - For any other installation, plug the power cable into the required PDU.

 **Rear view**

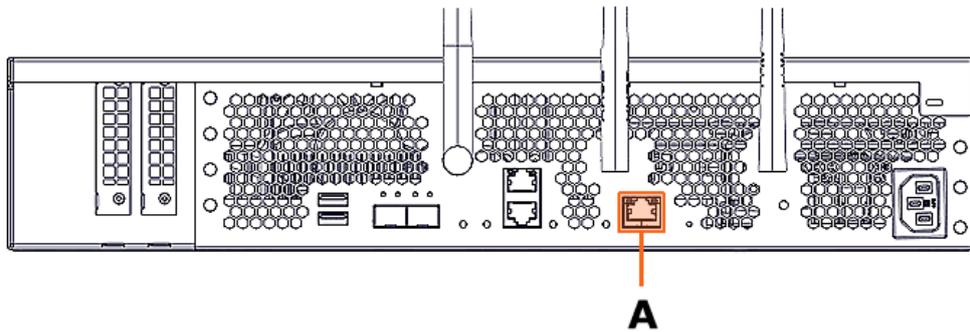


## 1.2. Connect the server to the LAN

### Procedure

Connect a LAN RJ45 Ethernet cable to the BMC port (A).

 **Rear view**



---

**Important** BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.

---

### 1.3. Place the server in standby mode

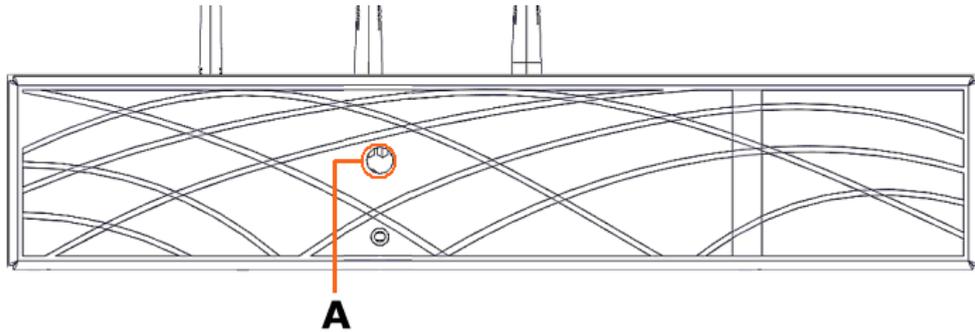
---

**Note** Standby mode means that the power supply for the server is connected but not powered on. The BMC is ON but the Operating System is not launched.

---

1. Turn the site power breakers ON.
2. Check that the power status LED (A) blinks green to indicate that the server is in standby mode.

 **Front view**



## 1.4. Connect to the Server Hardware Console (SHC)

---

**See** The SHC Reference Guide for more information.

---

If there are problems with the host name connection, or if the host name is changed, the connection may be made using the BMC IP address.

---

**See** Appendix B Obtaining an IP address for the BMC for more information.

---

### Prerequisites

- The BullSequana Edge server and the laptop are on the same LAN
- Chrome or Firefox are used to make the connection from the laptop

---

**Note** For browsers with proxy settings, the proxy configuration must allow the proxy to be bypassed for local addresses.

---

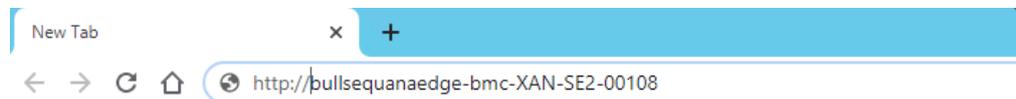
### Procedure

#### 1. Open a web browser

Enter the factory default host name into the address bar.

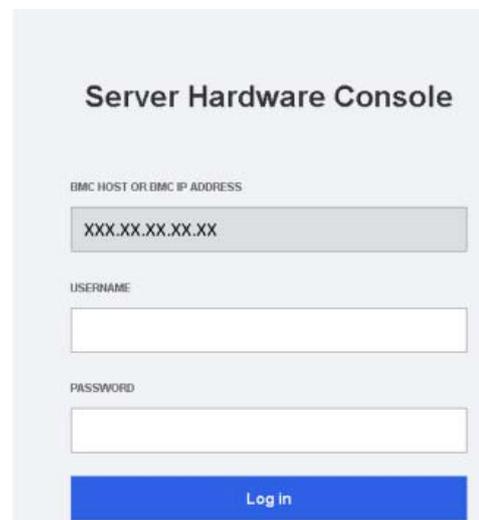
- 
- Notes**
- The factory default host name is in the following format `http://bullsequanaedge-bmc-<Serial_Number>`.
  - The serial number is written on the label on the side.
- 

### Example



#### 2. Ignore any security warning messages displayed

Ignore all security warning messages including advanced messages.  
The Server Hardware Console (SHC) authentication page opens.

A screenshot of the Server Hardware Console (SHC) authentication page. The page has a light blue background. At the top, it says "Server Hardware Console". Below that, there are three input fields: "BMC HOST OR BMC IP ADDRESS" with a placeholder "XXX.XX.XX.XX.XX", "USERNAME", and "PASSWORD". At the bottom, there is a blue "Log in" button.

## 1.5. Log in to the Server Hardware Console (SHC)

### Prerequisites

- The BullSequana Edge server and the laptop are on the same LAN
- Chrome or Firefox are used to make the connection from the laptop

### Procedure

#### 1. Connect to the SHC

A screenshot of the Server Hardware Console login interface. It features a light blue background with the title "Server Hardware Console" at the top. Below the title, there are three input fields: "BMC HOST OR BMC IP ADDRESS" with a placeholder "XXX.XX.XX.XX", "USERNAME", and "PASSWORD". A blue "Log in" button is positioned at the bottom right of the form.

Server Hardware Console (SHC)	
BMC host name or IP address	Automatically completed with the host name or IP address according to the connection method
Username	admin
Password	pass

#### 2. Complete the Username and Password fields and click Log in.

---

**Important** It is strongly recommended to change the default user password once initial setup is completed, taking care to record the new account details for subsequent connections.

---

**See** The SHC Reference Guide for more information.

---

---

## Chapter 2. Installing an Operating System

### 2.1. Powering on the server from the SHC

#### Prerequisites

The server is in standby power mode

#### Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select the power restore policy required.

#### Operations

Power on

#### Server Power Restore Policy

- Always On** (Perform a complete power on process)
- Always Off** (Remain powered off)
- Restore** (Restore power to last requested state recorded before the BMC was reset)

4. Click **Power on**.

## 2.2. Operating system installation options

### 2.2.1. Using a bootable USB drive

#### Prerequisites

- Access to the SHC is in place
- The server is powered on
- A bootable USB drive with the OS to be installed is plugged into the server

---

**Note** It is recommended that the latest version of the **Rufus** tool is used to format and create the bootable USB drive.

---

#### Procedure

##### 1. Access the BIOS interface from the SHC

1. From the **Control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.

### Serial over LAN console

#### Access the Serial over LAN console

---

The Serial over LAN (SoL) console redirects the output of the server's serial port to a browser window on your workstation.



 Open in new tab

2. If required, click the **Open in new tab** link to open the console in a new window.

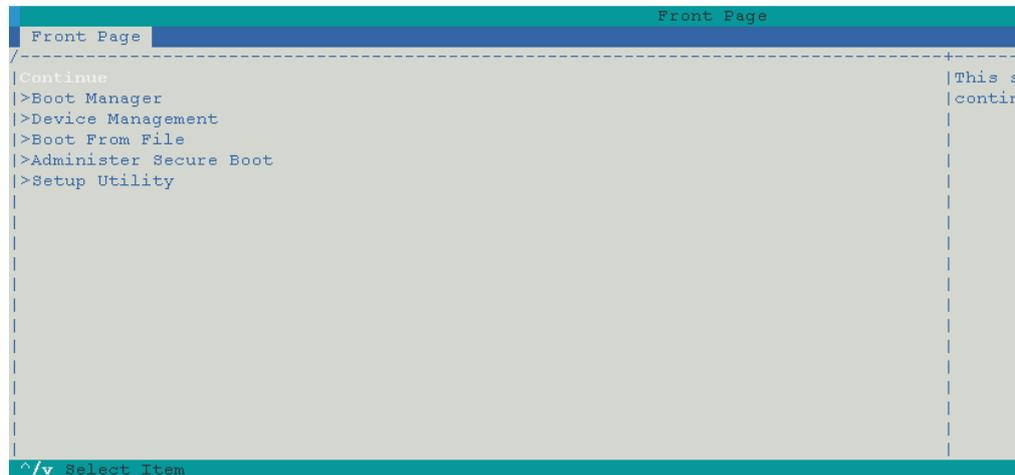
3. Click on the Serial over LAN console screen and quickly press the [Esc] key numerous times to display the BIOS interface.

---

**Important** The [Esc] key must be pressed quickly after the Serial over LAN console window opens.

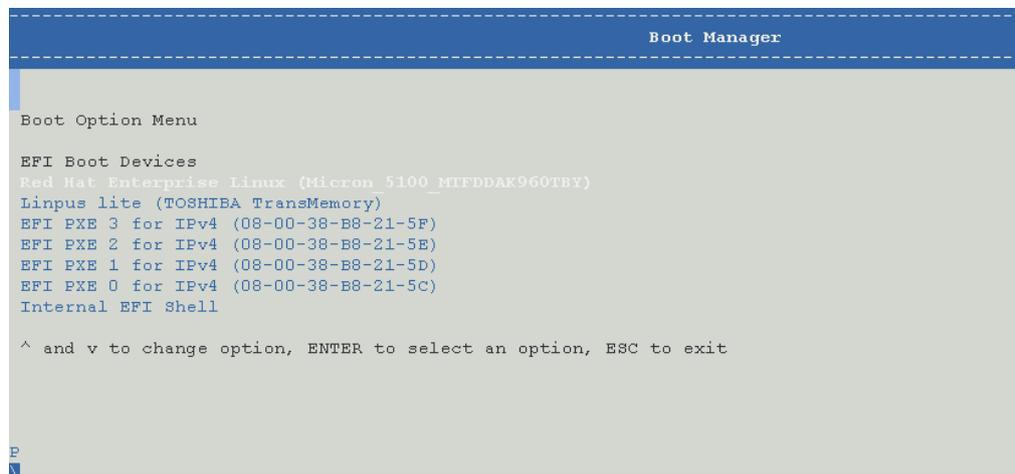
---

The BIOS interface opens.



## 2. Choose the boot device

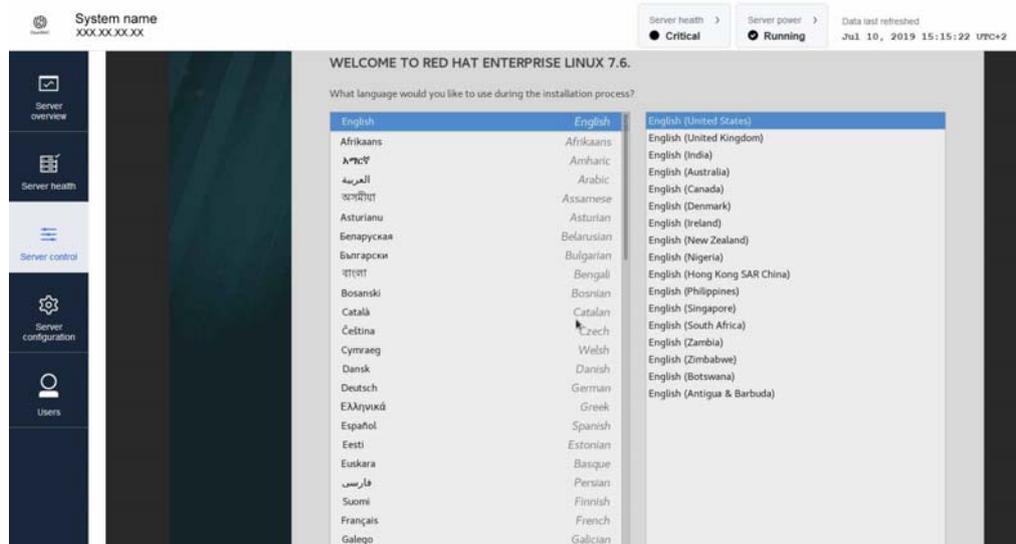
1. Select **Boot Manager** using the navigation arrows and press [Enter].
2. Select the USB drive boot device using the navigation arrows and press [Enter].



3. Follow the instructions displayed to boot from the USB drive.

### 3. Install the OS

1. Click **Server control** > **KVM**. The KVM page opens.



2. Follow the instructions displayed to install the OS.
3. Select the system settings required.

## 2.2.2. Using a Pre-boot eXecution Environment (PXE)

### Prerequisites

- Access to the SHC is in place
- The server is powered on
- A PXE server has been set up and is accessible

### Procedure

#### 1. Access the BIOS interface from the SHC

1. From the **Control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.

### Serial over LAN console

#### Access the Serial over LAN console

---

The Serial over LAN (SoL) console redirects the output of the server's serial port to a browser window on your workstation.



 Open in new tab

2. If required, click the **Open in new tab** link to open the console in a new window.

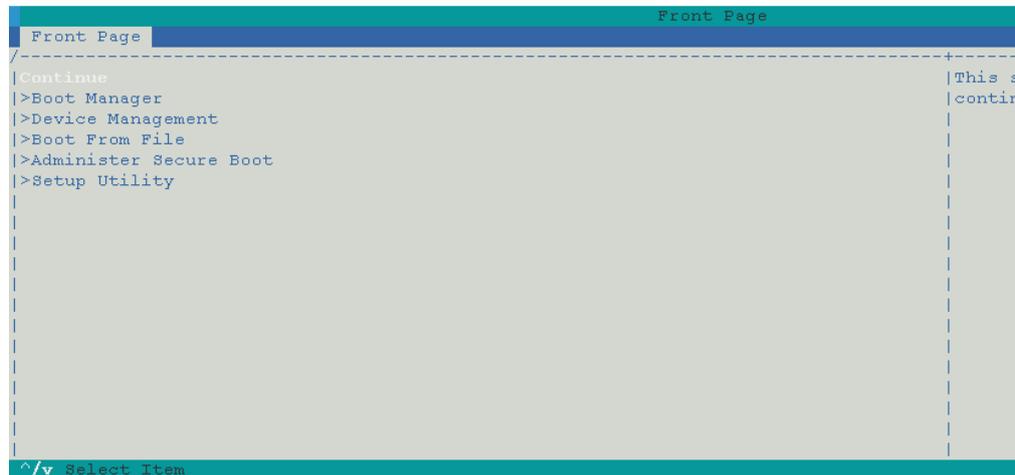
3. Click on the Serial over LAN console screen and quickly press the [Esc] key numerous times to display the BIOS interface.

---

**Important** The [Esc] key must be pressed quickly after the Serial over LAN console window opens.

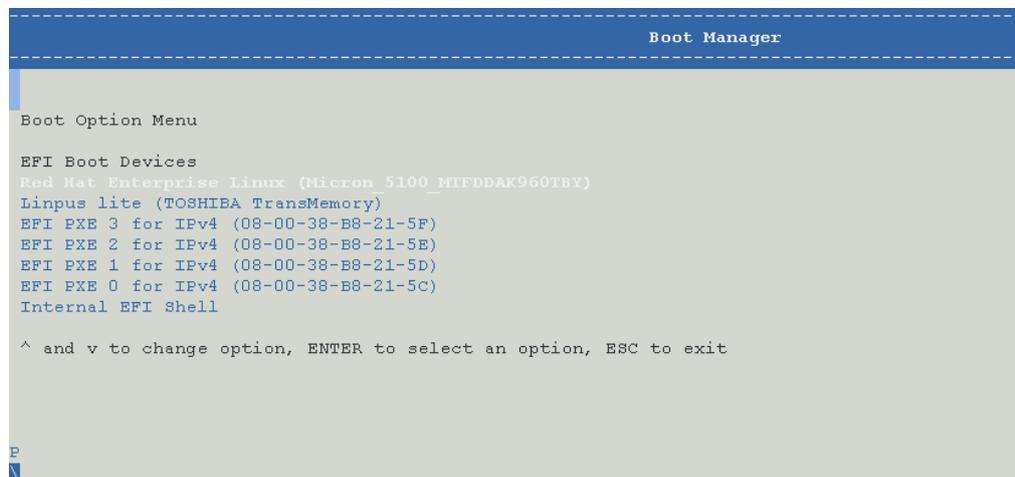
---

The BIOS interface opens.



## 2. Choose the boot device

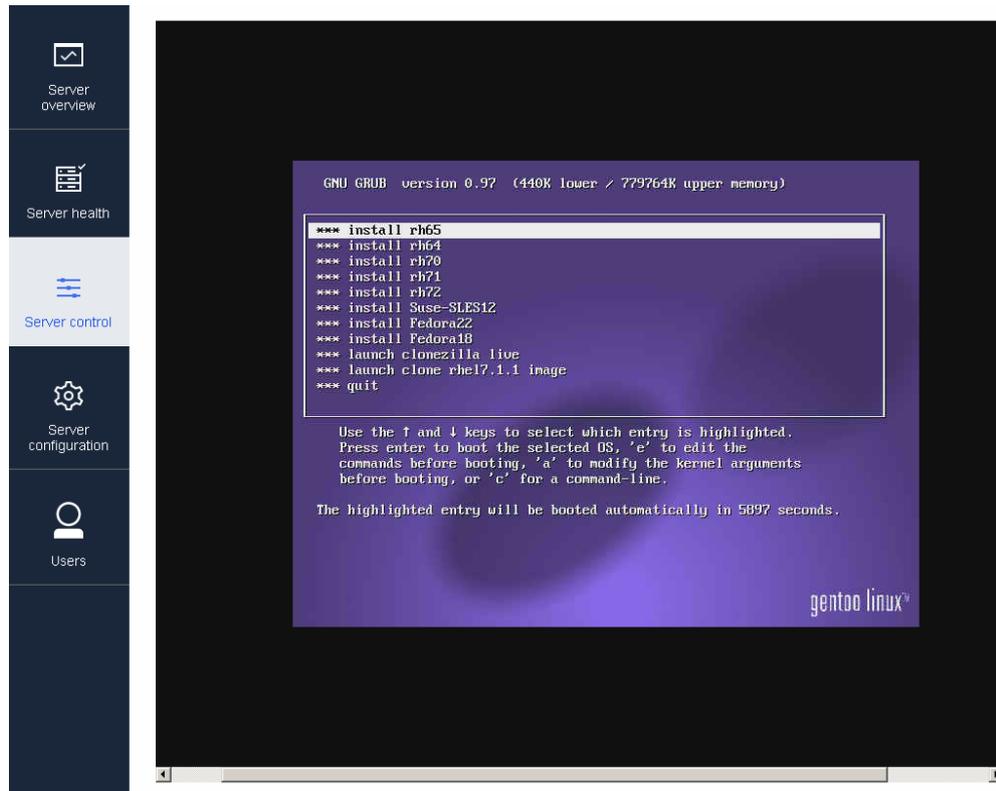
1. Select **Boot Manager** using the navigation arrows and press [Enter].
2. Select the PXE boot device using the navigation arrows and press [Enter].



3. Follow the instructions displayed on the screen to boot the OS from the PXE server.

### 3. Install the OS

1. Click **Server control** > **KVM**. The KVM page opens.



2. Follow the instructions displayed to install the OS.
3. Select the system settings required.



---

## Chapter 3. Connecting to the data system

### 3.1. Connecting the server to the data LAN

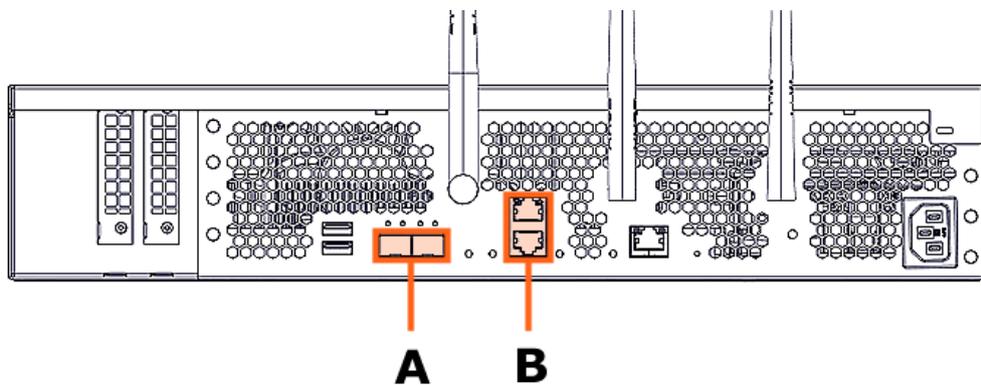
---

**Important** BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.

---

1. Connect an Ethernet cable to an Ethernet port at the rear of the server.

 **Rear view**



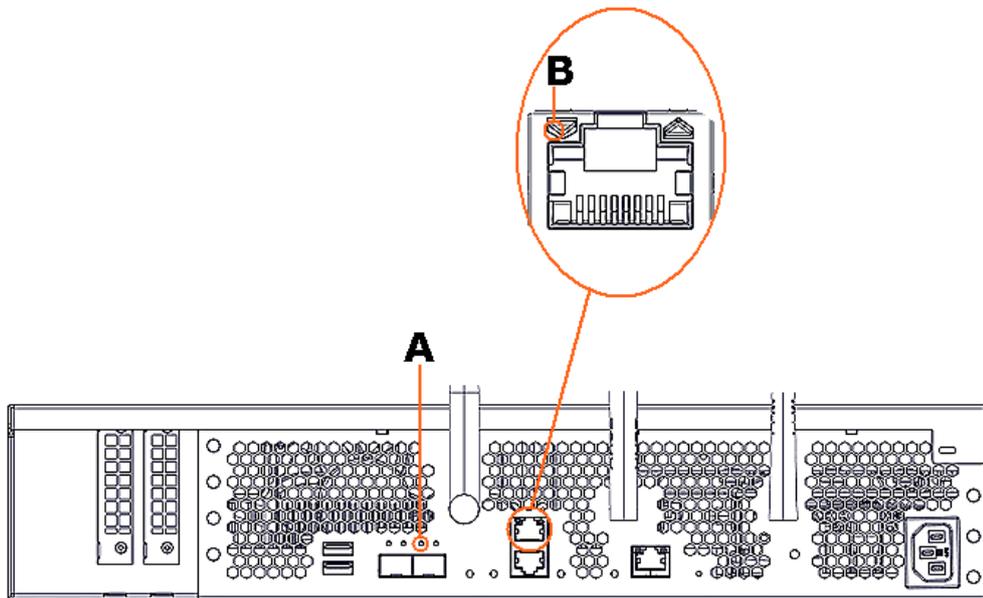
Mark	Port type
A	2 x SFP+ - 10 Gb/s Ethernet
B	2 x RJ45 - 1 Gb/s Ethernet

2. Connect the other end of the cable to the data LAN.

## 3.2. Checking network traffic

Check that the Ethernet LEDs (A or B) are on for the connected cables.

 **Rear view**



---

**See** The Description Guide for more information about the LEDs at the rear of the server.

---

---

## Chapter 4. Power operations

### 4.1. Powering methods

A BullSequana Edge server can be powered on and off using:

- The power button at the front of the server
- The Server Hardware Console (SHC)
- The Machine Intelligence System Management (MISM) console.

The SHC operates via a server Baseboard Management Controller (BMC) and can only intervene on one server at a time. MISM console jobs can operate on groups of servers at a time.

---

**See** The SHC Reference Guide and the Management Console User's Guide for more information.

---

## 4.2. Power modes

Three power modes are possible for a BullSequana Edge server:

- Standby mode means that the power supply for a server is connected but not powered on. The BMC is ON but the Operating System is not launched.
- Powered on mode means that the power supply for a server is connected and powered on. The BMC is ON and the Operating System is launched.

---

**Note** The BMC is ON by default when the power supply is connected to a server.

---

- Powered off mode means that the power supply for a server is disconnected.

---

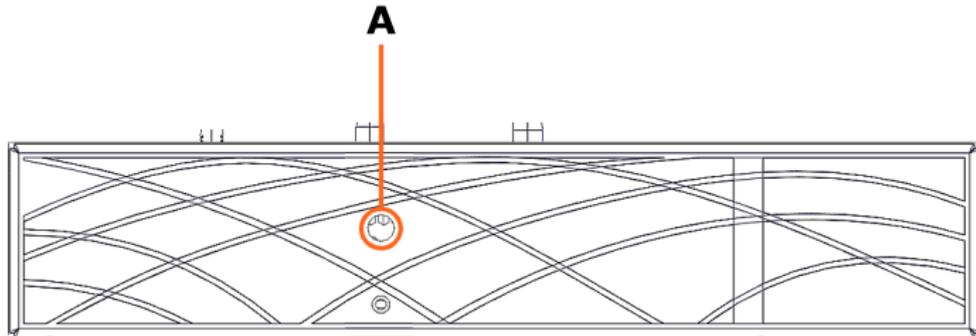
**See** Description Guide for more information about the ports and LEDs.

---

### 4.3. Powering on with the power button

1. Check that the power status LED (A) is blinking green to indicate that the server is in standby mode.
2. Press the power button at the front of the server (A) for approximately one second.

 **Front view**



3. Check that the power button LED is on and solid green to indicate that the server is powered on.

## 4.4. Powering on the server from the SHC

### Prerequisites

The server is in standby power mode

### Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select the power restore policy required.

#### Operations

---

Power on

#### Server Power Restore Policy

---

- Always On** (Perform a complete power on process)
- Always Off** (Remain powered off)
- Restore** (Restore power to last requested state recorded before the BMC was reset)

4. Click **Power on**.

## 4.5. Powering on the server from the MISM console

---

**Important** The https protocol must always be used to connect to the MISM console.

---

### Prerequisites

The server is in standby power mode

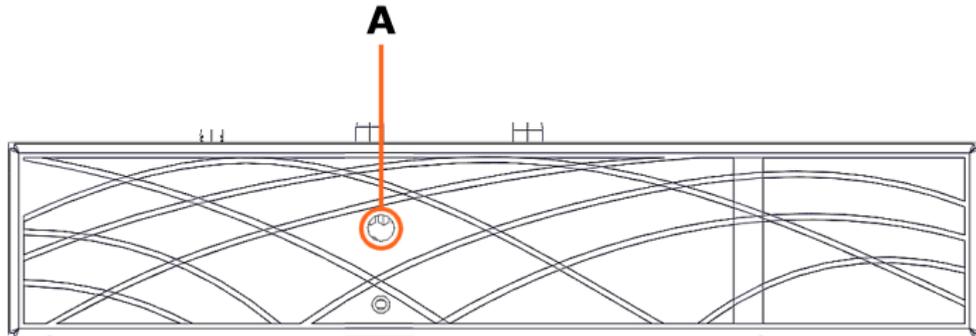
### Procedure

1. Launch the **Power On** job.
2. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check Power On** job.
4. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

## 4.6. Powering off with the power button

1. Check that the power status LED (A) is solid green to indicate that the server is powered on.
2. Press the power button at the front of the server (A) for at least five seconds.

 **Front view**



3. Check that the power button LED is blinking green to indicate that the server is in standby mode.

## 4.7. Powering off the server from the SHC

**W087**  **WARNING**

**W087:**

**The immediate reboot and shutdown buttons should only be used if the Operating System is unable to respond to an orderly reboot or shutdown request.**

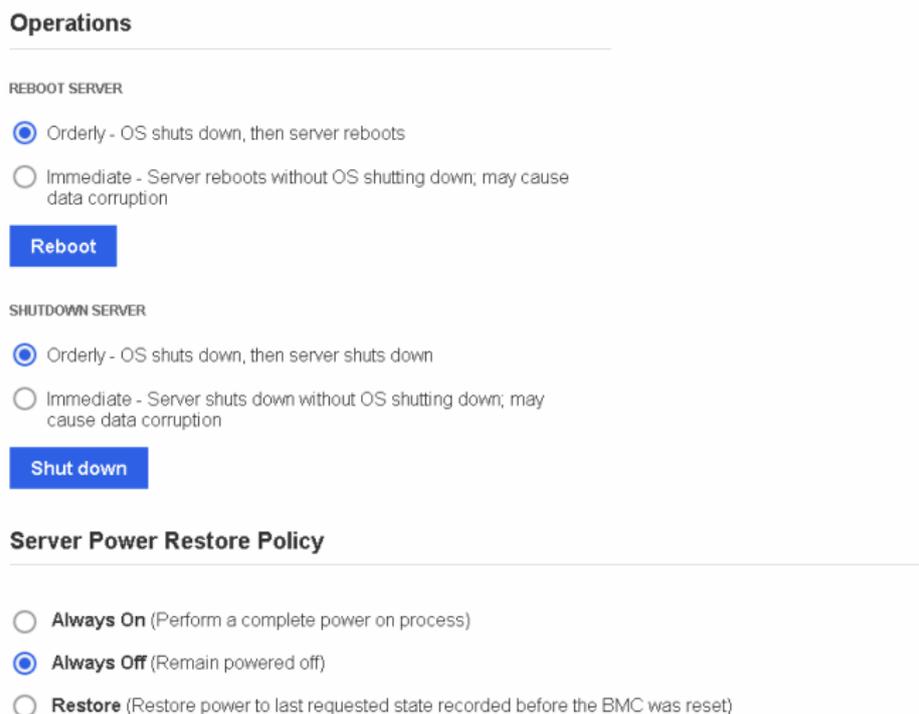
**These sequences may result in data loss and file corruption.**

### Prerequisites

The server is in the powered on state

### Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select either the reboot or shut down option required.



The screenshot shows the 'Operations' section of the SHC interface. It is divided into three main areas: 'REBOOT SERVER', 'SHUTDOWN SERVER', and 'Server Power Restore Policy'. Each area has radio button options for 'Orderly' and 'Immediate' actions, and a corresponding action button.

**Operations**

---

**REBOOT SERVER**

Orderly - OS shuts down, then server reboots

Immediate - Server reboots without OS shutting down; may cause data corruption

**Reboot**

**SHUTDOWN SERVER**

Orderly - OS shuts down, then server shuts down

Immediate - Server shuts down without OS shutting down; may cause data corruption

**Shut down**

**Server Power Restore Policy**

---

**Always On** (Perform a complete power on process)

**Always Off** (Remain powered off)

**Restore** (Restore power to last requested state recorded before the BMC was reset)

4. Select the power restore policy required.
5. Click **Reboot** or **Shut down**.

## 4.8. Powering off the server from the MISM console

**W087**  **WARNING**

**W087:**

**The immediate reboot and shutdown buttons should only be used if the Operating System is unable to respond to an orderly reboot or shutdown request.**

**These sequences may result in data loss and file corruption.**

### Prerequisites

The server is in the powered on state

### Procedure

1. Select the power operation:
  - **Orderly Shutdown**
  - **Immediate Shutdown**
2. Launch the selected job.
3. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Check Power Off** job.
5. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

---

## Chapter 5. Server Hardware Console (SHC) maintenance operations

---

**See** The SHC Reference Guide for more information.

---

### 5.1. Rebooting the Baseboard Management Controller (BMC)

#### Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Reboot BMC**. The **Reboot BMC** page opens.

#### Reboot BMC

**Current BMC boot status**

BMC last reboot at **not available**

When you reboot the BMC, your web browser loses contact with the BMC for several minutes. When the BMC is back online, you must log in again. If the Log In button is not available when the BMC is brought back online, close your web browser. Then, reopen the web browser and enter your BMC IP address.

 A rectangular button with a blue border and a blue circular refresh icon to the left of the text "Reboot BMC".

3. Click the **Reboot BMC** button.

---

**Note** When the BMC is rebooted the browser loses contact with the BMC for several minutes. The log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.

---

## 5.2. Checking event logs

### Prerequisites

The server is in the powered on state

### Procedure

1. Connect to the SHC
2. From the **Health** tab, click **Event log**. The **Event log** page opens.

The screenshot shows the 'Event log' page. At the top right, it says 'REMOTE LOGGING SERVER' and has a '+ Add server' button. Below that, it says 'All events from the BMC' and 'USER TIMEZONE'. There is a search bar labeled 'FILTER EVENTS' with a magnifying glass icon and a 'Filter' button. Below the search bar, there are two filter sections: 'FILTER BY SEVERITY' with buttons for 'All', 'High', 'Medium', and 'Low', and 'FILTER BY DATE RANGE (MM/DD/YYYY)' with two input boxes for dates. Below these is a 'FILTER BY EVENT STATUS' dropdown menu set to 'All events'. At the bottom, there is a table of events. The table has a header row with '3 Events are logged', 'Delete', 'Mark as resolved', and 'Export' buttons. The table contains two rows of event data:

Event ID	Severity	Event Type	Timestamp	Action
#3	LOW	NOTICE	Nov 30, 2020 08:26:03 UTC+1	Dropdown
Host power is ON				
#2	LOW	NOTICE	Nov 30, 2020 08:25:36 UTC+1	Dropdown

3. Set the log name, severity and date range parameters.
4. Click **Filter**. The list of logged events is displayed.

## 5.3. Checking the hardware status

### Prerequisites

The server is in the powered on state

### Procedure

1. Connect to the SHC
2. From the **Health** tab, click **Hardware status**. The **Hardware status** page opens.

## Hardware status

All hardware in the system

[Export](#)

FILTER HARDWARE COMPONENTS

 × Filter

NOTE: System power is off. DIMMs seen below were detected during the last power-on.

Hardware	
System	▼
Motherboard	▼
CPU 0	▼
DIMM 0	▼
DIMM 1	▼
DIMM 2	▼
DIMM 3	▼
Fan 0_PCI	▼
Fan 1_CPU	▼
Fan 2_PSU	▼
HDD_0	▼
HDD_1	▼
PCI_0	▼
PCI_1	▼

3. Enter the hardware component in the search field.
4. Click **Filter**.
5. **Export** the hardware details, as required.

---

**Note** The hardware details are exported as .json data files.

---

## 5.4. Checking the sensors

### Prerequisites

The server is in the powered on state

### Procedure

1. Connect to the SHC
2. From the **Health** tab, click **Sensors**. The **Sensors** page opens.

## Sensors

All sensors present in the system

[Export](#)

FILTER SENSORS

 × Filter

FILTER BY SEVERITY

All Critical Warning Normal

Sensors (19)	Low critical	Low warning	Current	High warning	High critical
Temperature Psu Temp2	0° C	5° C	30.75° C	85° C	100° C
Temperature Psu Temp3	0° C	5° C	33.625° C	85° C	100° C
Temperature Temp Dimm	0° C	5° C	29.437° C	80° C	85° C
Temperature Temp Mpciebmc	0° C	5° C	29.375° C	65° C	70° C

Severity Description	
GREEN	NORMAL Operation correct. No problem has been detected.
ORANGE	WARNING A problem has been detected that may need preventive or corrective action.
RED	CRITICAL A problem has been detected. Immediate preventive or corrective action is required.

3. Enter the sensor name in the search field.
4. Set the severity parameter.
5. Click **Filter**.

6. Click **Export** to export the sensor states, as required.

---

**Note** The sensor states are exported as .json data files.

---

## 5.5. Managing firmware versions

---

**Important** The BMC firmware must be updated before the BIOS and CPLD firmware.

---

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

---

The SHC can be used to change firmware boot priorities and to update BMC, BIOS and CPLD firmware files.

### 5.5.1. Checking firmware versions

#### Prerequisites

The server is in the powered on state

#### Procedure

1. Connect to the SHC

- From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.

## Firmware

### [Check and get new firmwares](#)

Note: The server BMC has to be connected to Internet

### Manage BMC, BIOS and CPLD firmware

Use the following tables to manage firmware image files. The image file that is listed at the top, the image with the highest boot priority, is used the next time that the device is booted. To change the boot priority for the image, click the arrow icons.

**Scroll down to upload an image file** to transfer a new firmware image to the BMC. After uploading a new image, Activate it to make it available for use.

#### BMC images

Functional firmware version: 33.00.0420

Boot priority	Image state	Version	Action
 	Functional	33.00.0420	

#### BIOS images

Functional firmware version: BIOS\_SKD080.18.02.002

Boot priority	Image state	Version	Action
 	Functional	BIOS_SKD080.18.02.002	

#### CPLD images

Functional firmware version: 4.2.0.0

Boot priority	Image state	Version	Action
 	Functional	4.2.0.0	

- Check the BMC, BIOS and CPLD functional image versions listed.

## 5.5.2. Checking the firmware is up-to-date

### Prerequisites

- A laptop computer with the Chrome or Firefox browser installed
- Connection to the internet
- The server is in the powered on state

### Procedure

1. Connect to the SHC
2. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
3. Click **Check and get new firmware** to go to the support site.

### Firmware

[Check and get new firmwares](#)

Note: The server BMC has to be connected to Internet

**Manage BMC, BIOS and CPLD firmware**

Use the following tables to manage firmware image files. The image file that is listed at the top, the image with the highest boot priority, is used the next time that the device is booted. To change the boot priority for the image, click the arrow icons.

4. Download the latest versions, if more up-to-date versions are available.

### 5.5.3. Updating the BMC firmware

#### Prerequisites

The server is in the standby power state

#### Procedure

##### 1. Check the server power status

Check that the server is in the standby power state.

##### 2. Connect to the SHC

##### 3. Update the firmware

1. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
2. From the **Specify image file location** section:
  - a. Either click **Choose a file** > **Upload firmware** to upload an image file from a workstation.
  - b. Or click **Download firmware** to download an image file from a TFTP server.

#### Specify image file location

---

Specify an image file located on your workstation or a TFTP server. An image file may contain firmware images for the BIOS, BMC, or other hardware devices. Each image that you upload will be unpacked from the image file and added to the appropriate list above.

##### Upload image file from workstation

Select the image file saved on the workstation storage medium to upload to the server BMC.

Choose a file

No file chosen

Upload firmware

##### Download image file from TFTP server

Specify both the TFTP server IP address and the image file name stored on it to download to the server BMC.

TFTP SERVER IP ADDRESS

FILE NAME

Download firmware

#### 4. Activate the BMC image

1. Select the BMC image using the boot priority arrows.
2. Click **Activate**.

Scroll down to upload an image file to transfer a new firmware image to the BMC. After uploading a new image, Activate it to make it available for use.

BMC images Functional firmware version: 15.00.0179

Boot priority	Image state	Version	Action
 	Functional	15.00.0179	
	Ready	14.00.0162	<a href="#">Activate</a> <a href="#">Delete</a>

3. The Confirm BMC firmware file activation page opens. Click **Activate firmware file and automatically reboot BMC**.

 **Confirm BMC firmware file activation**

When you activate the BMC firmware file, 14.00.0162, the BMC must be rebooted before it will operate with the new firmware code. Note that when you reboot the BMC, the BMC will be unavailable for several minutes and you must log in again.

ACTIVATE FIRMWARE FILE WITHOUT REBOOTING BMC

ACTIVATE FIRMWARE FILE AND AUTOMATICALLY REBOOT BMC

[Cancel](#) [Continue](#)

4. Click **Continue**.

---

**Notes**

- When the BMC is rebooted the browser loses contact with the BMC for several minutes. The normal log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.
- Earlier firmware versions disappear from the BMC image list once a new version has been activated.

---

## 5.5.4. Updating the BIOS and CPLD firmware

---

**Important** Check that the latest BMC firmware version is installed. If not, the BMC firmware must be updated before the BIOS and CPLD firmware.

---

### Prerequisites

The server is in the standby power state

### Procedure

#### 1. Check the server power status

Check that the server is in the standby power state.

#### 2. Connect to the SHC

#### 3. Update the firmware

1. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
2. From the **Specify image file location** section:
  - a. Either click **Choose a file** > **Upload firmware** to upload an image file from a workstation.
  - b. Or click **Download firmware** to download an image file from a TFTP server.

#### Specify image file location

---

Specify an image file located on your workstation or a TFTP server. An image file may contain firmware images for the BIOS, BMC, or other hardware devices. Each image that you upload will be unpacked from the image file and added to the appropriate list above.

##### Upload image file from workstation

Select the image file saved on the workstation storage medium to upload to the server BMC.

<input type="button" value="Choose a file"/>	No file chosen	<input type="button" value="Upload firmware"/>
--	----------------	--

##### Download image file from TFTP server

Specify both the TFTP server IP address and the image file name stored on it to download to the server BMC.

TFTP SERVER IP ADDRESS	FILE NAME	<input type="button" value="Download firmware"/>
<input type="text"/>	<input type="text"/>	

#### 4. Activate the firmware

1. Select the firmware using the boot priority arrows.
2. Click **Activate**.

Boot priority	Image state	Version	Action
	Functional	4.3.0.0	
	Ready	4.1.0.0	<b>Activate</b> Delete

#### 5. Wait two to three minutes and then refresh the page

The firmware is now active.

#### 6. Power on the server

1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.

**Operations**

**Power on**

**Server Power Restore Policy**

- Always On** (Perform a complete power on process)
- Always Off** (Remain powered off)
- Restore** (Restore power to last requested state recorded before the BMC was reset)

2. In the **Operations** section, click **Power on**.

---

## Chapter 6. MISM maintenance operation

Maintenance operations can be performed from the Machine Intelligence System Management (MISM) console.

---

**See** See the Management Console User's Guide for more information.

---

### 6.1. Rebooting Baseboard Management Controllers (BMCs)

#### Prerequisites

- The laptop is connected to the server BMC port
- The server BMC has an IP address allocated
- The server is in standby power mode
- The MISM console is launched

#### Procedure

1. Launch the **Reboot bmc** job.
2. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check BMC alive** job.
4. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

## 6.2. Updating firmware

---

**Important**

- **The BMC must be rebooted after an update of its firmware. If the reboot variable is set as False, it must be done manually for the update to be effective.**
  - **The host must be powered off before updating the BIOS or CPLD firmware. If the forceoff variable is set as False, it must be done manually.**
- 

### 6.2.1. Updating firmware globally

#### Two-step operation

##### 1. Review which firmware will be updated

1. Launch the **Evaluate firmware update from Technical State** job.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

##### 2. Update the firmware

1. Launch the **Update firmware from Technical State** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- technical\_state\_path
  - reboot
  - forceoff
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

#### Three-step operation

##### 1. Review which firmware will be updated

1. Launch the **Evaluate firmware update from Technical State** job to know which firmware will be updated.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 2. Upload the firmware

1. Launch the **Upload firmware images from Technical State** job.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Ready** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 3. Activate the firmware

1. Launch the **Activate firmware updates** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- reboot
  - forceoff
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 6.2.2. Updating firmware individually

1. Launch the **Update firmware from file** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- reboot
  - forceoff
  - file\_to\_update
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 6.3. Enabling syslog forwarding

### Prerequisites

The syslog server is configured for messaging

### Procedure

1. Indicate the syslog server IP address and port as variables in the inventory.

The screenshot shows the 'My first inventory' configuration page. At the top, there are tabs for 'DETAILS', 'PERMISSIONS', 'GROUPS', 'HOSTS', 'SOURCES', and 'COMPLETED JOBS'. Below the tabs, there are input fields for '\* NAME' (containing 'My first inventory'), 'DESCRIPTION', and '\* ORGANIZATION' (containing 'Default'). There are also search fields for 'INSIGHTS CREDENTIAL' and 'INSTANCE GROUPS'. At the bottom, there is a 'VARIABLES' section with tabs for 'YAML' and 'JSON', and an 'EXPAND' button. The 'YAML' tab is active, showing a list of variables: 1 forceoff: true, 2 reboot: true, 3, 4 rsyslog\_server\_ip: <IP address>, 5 rsyslog\_server\_port: <port number>, 6. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

2. Launch the **Set Rsyslog Server IP** job.
3. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Set Rsyslog Server Port** job.
5. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
6. Launch the **Check Rsyslog Server IP and Port** job to check the syslog server parameters.
7. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

---

## Appendix A. IPMI Out of Band (OOB) support

By default, IPMI OOB support is disabled for the BullSequana Edge server BMC.

### A.1. Enabling IPMI OOB support

#### Prerequisites

- A laptop computer with the Chrome or Firefox browser installed
- The server BMC has an IP address allocated

#### Procedure

1. Connect to the server via **SSH**.
2. Export the BMC credentials:

```
export bmc=<user>:<pwd>@<BMC IP>
```

---

**Note** Any BMC user account with administrator rights may be used.

---

3. Reset the BMC to the default factory settings:

```
curl -b cjar -k -H 'Content-Type: application/json' -X POST -d '{"data":[]}'  
https://${bmc}/xyz/openbmc_project/software/action/Reset
```

---

**Note** After the BMC reset to the factory settings, only the admin default user account with its default password can be used to connect to the BMC.

---

4. Connect to the SHC
5. From the **Control** tab, click **Reboot BMC**. The **Reboot BMC** page opens.

### Reboot BMC

**Current BMC boot status**

BMC last reboot at **not available**

When you reboot the BMC, your web browser loses contact with the BMC for several minutes. When the BMC is back online, you must log in again. If the Log In button is not available when the BMC is brought back online, close your web browser. Then, reopen the web browser and enter your BMC IP address.

 Reboot BMC

6. Click the **Reboot BMC** button.

---

**Note** When the BMC is rebooted the browser loses contact with the BMC for several minutes. The log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.

---

7. Enable IPMI OOB support:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X PUT -d '{"data": "true"}'  
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

8. Check that IPMI OOB support is enabled:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X GET  
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

IPMITOOL commands can now be used to manage the server.

## A.2. Disabling IPMI OOB support

### Prerequisites

The server BMC has an IP address allocated

### Procedure

1. Connect to the server via **SSH**.
2. Export the BMC credentials:

```
export bmc=<user>:<pwd>@<BMC IP>
```

---

**Note** Any BMC user account with administrator rights may be used.

---

3. Disable IPMI OOB support:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X PUT -d '{"data": "false"}'  
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

4. Check that IPMI OOB support is disabled:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X GET  
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

IPMITOOL commands can no longer be used to manage the server.



---

## Appendix B. Obtaining an IP address for the BMC

There are three different methods of obtaining an IP address for the server BMC:

- Directly using an auto-discovery tool
- Via a DHCP server installed on a laptop
- Via a network DHCP server

---

**Note** By default, BullSequana Edge servers are preconfigured for dynamic IP addresses.

---

### B.1. Obtaining an IP address directly with an auto-discovery tool

---

**Important** BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.

---

BullSequana Edge servers support Automatic Private IP Addressing (**APIPA**). An IP address in the 169.254.xxx.xxx range will be allocated automatically, when the BMC is connected to a network without a DHCP server.

#### Prerequisites

- A windows laptop with internet access and administrator rights
- An auto-discovery tool for the IP address
- The server is in standby power mode

#### Procedure

---

**Note** In this section the Bonjour browser is used as an example of an IP address auto-discovery tool.

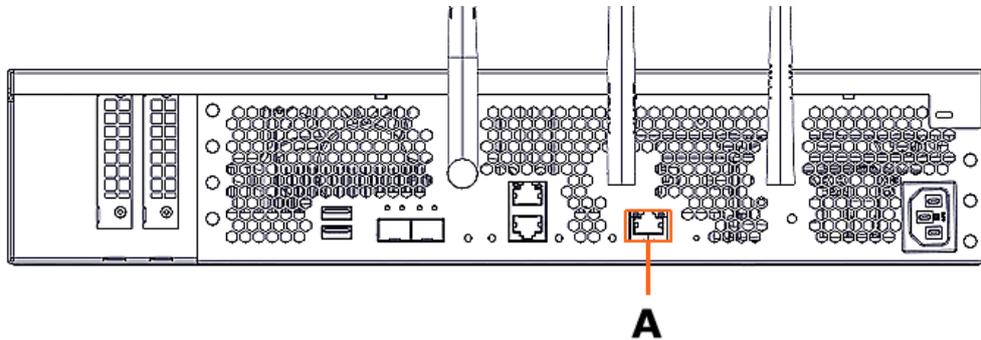
---

#### 1. Install Bonjour on the laptop

1. Download the latest **BonjourBrowserSetup.exe** file.
2. Run **BonjourBrowserSetup.exe** with administrator rights.

## 2. Connect the server directly to the laptop

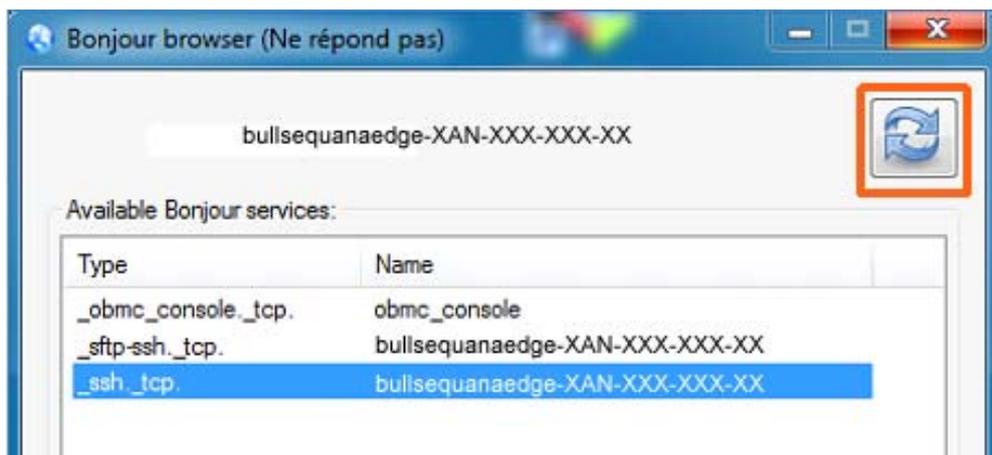
Connect the BMC port (A) of the server to the laptop computer using a RJ45 Ethernet cable.



## 3. Launch the Bonjour browser on the laptop

### 4. Refresh the Bonjour browser

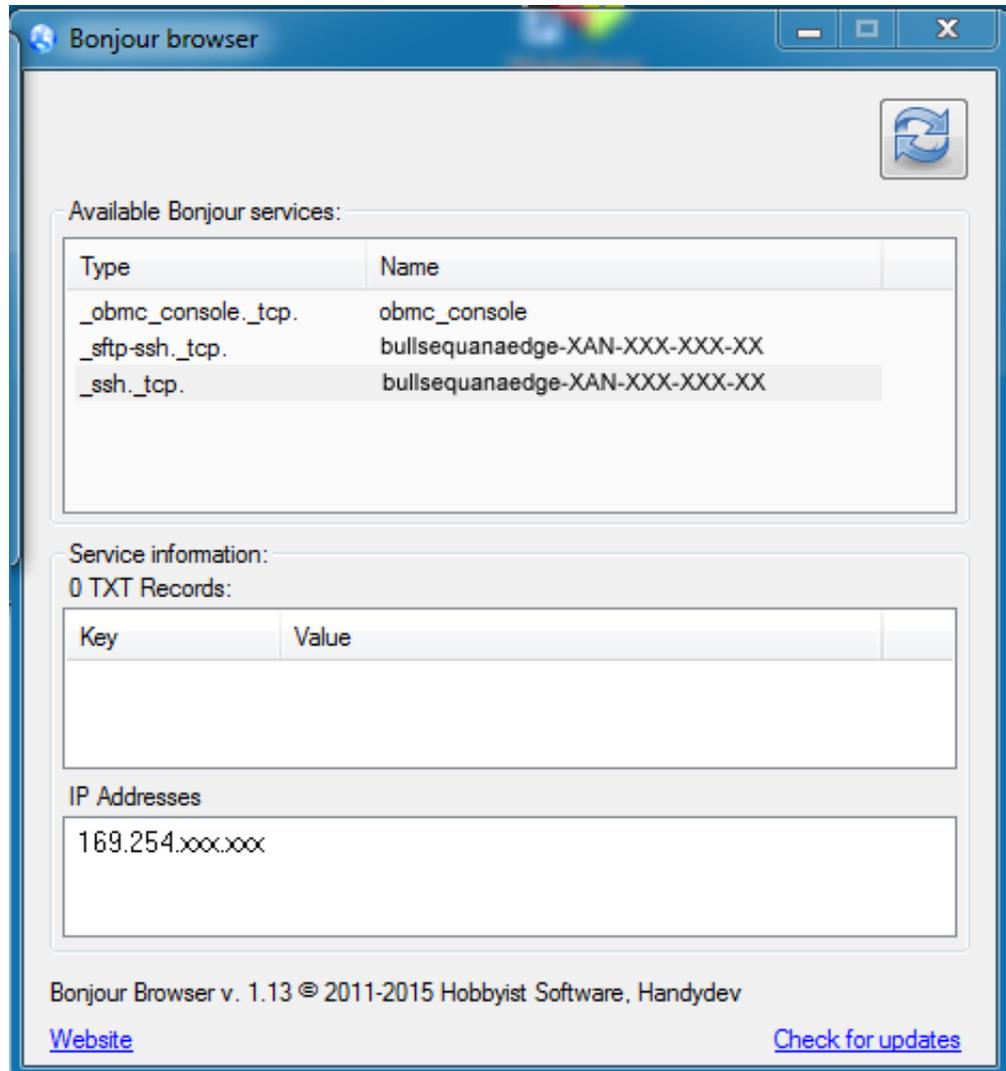
1. Click the Refresh button at the top on right of the browser window.



2. The available services are displayed.

## 5. Note the server IP address

1. Select the **\_ssh.\_tcp** Bonjour service for the server BMC.
2. The Bonjour IP BullSequana Edge server IP address is displayed in the **IP Addresses** field.



3. Note the IP address indicated.

## B.2. Obtaining an IP address via a laptop DHCP server

---

**Important** BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.

---

### Prerequisites

- A windows laptop computer with internet access and administrator rights
- A DHCP server is installed on the laptop
- The server is powered off and disconnected from the power supply

---

**Note** In this section Tftpd64 is used as an example of DHCP server installed locally on a laptop.

---

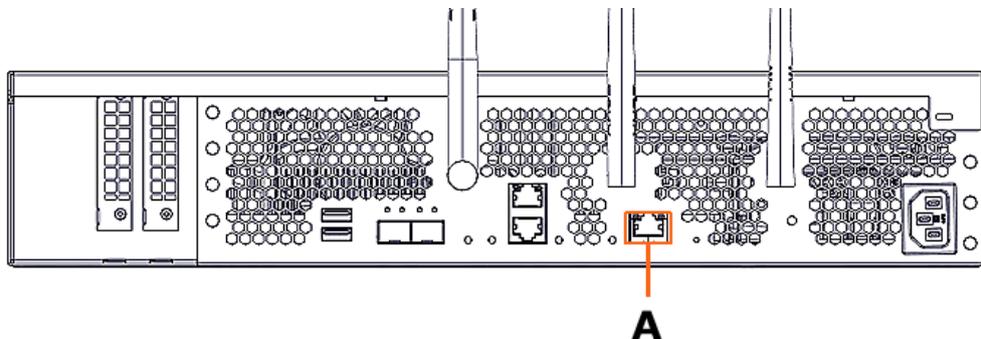
### Procedure

#### 1. Install Tftpd64 on the laptop

1. Download the latest **Tftd64.exe** file.
2. Run **Tftd64.exe** with administrator rights.

#### 2. Connect the server to the laptop

Connect the BMC port (A) of the server to the laptop using a RJ45 Ethernet cable.



#### 3. Connect the server power cable to the power socket

#### 4. Wait for the BMC to boot

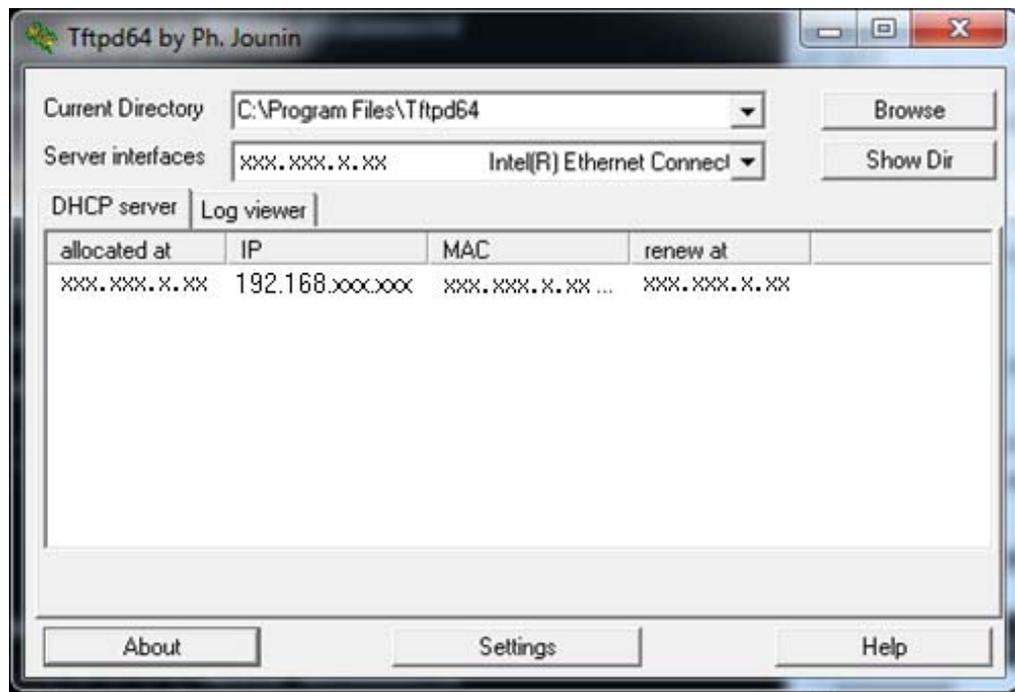
---

**Note** The BMC boot will take several minutes.

---

**5. Launch the DHCP server on the laptop**

**Note** The TFTP64 DHCP server interface below is shown as an example.



**6. Note the BMC IP address indicated**

## B.3. Obtaining an IP address via a network DHCP server

---

**Important** BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.

---

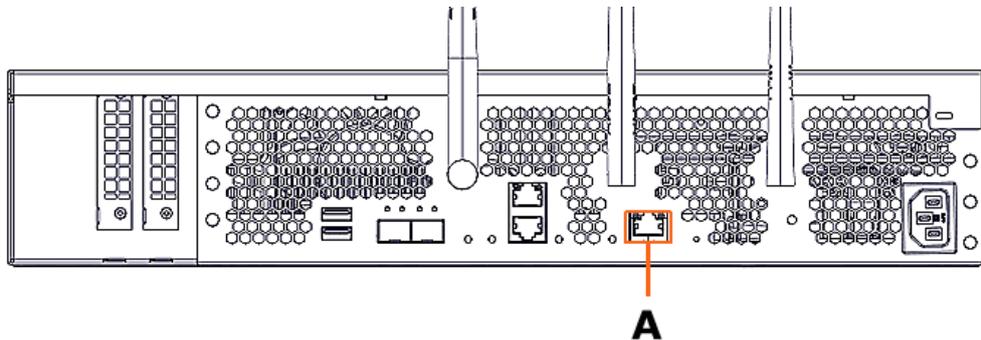
### Prerequisites

- A laptop computer with administrator rights
- The server is in standby power mode
- The LAN includes a DHCP server
- The details of the DHCP server are known and the server is accessible

### Procedure

#### 1. Connect the server to a switch

Connect the BMC port (A) of the server to a 1 Gb/s Ethernet switch using a RJ45 Ethernet cable.



#### 2. Connect the switch to the laptop

Connect an Ethernet port of the laptop to the 1 Gb/s Ethernet switch using a RJ45 Ethernet cable.

#### 3. Connect the switch to the LAN

Connect the 1 Gb/s Ethernet switch using a RJ45 Ethernet cable to the LAN either via a router or directly.

#### 4. Access the DHCP server that is part of the LAN

Retrieve the IP address from the DHCP server table.

#### 5. Note the IP address allocated to the server BMC

## B.4. Connecting to the SHC using the BMC address

### Prerequisites

- The BullSequana Edge server and the laptop are on the same LAN
- Chrome or Firefox are used to make the connection from the laptop
- The server BMC has an IP address allocated

### Procedure

**1. Open a web browser**

Enter the BMC IP address into the address bar.

**2. Ignore any security warning messages displayed**

Ignore all security warning messages including advanced messages.

The Server Hardware Console (SHC) authentication page opens.

A screenshot of the Server Hardware Console (SHC) authentication page. The page has a light blue background. At the top, it says "Server Hardware Console". Below that, there are three input fields: "BMC HOST OR BMC IP ADDRESS" with a placeholder "XXX.XX.XX.XX", "USERNAME", and "PASSWORD". At the bottom, there is a blue "Log in" button.

---

**See** [The SHC Reference Guide for more information.](#)

---





**Bull Cedoc**  
**357 avenue Patton**  
**BP 20845**  
**49008 Angers Cedex 01**  
**FRANCE**